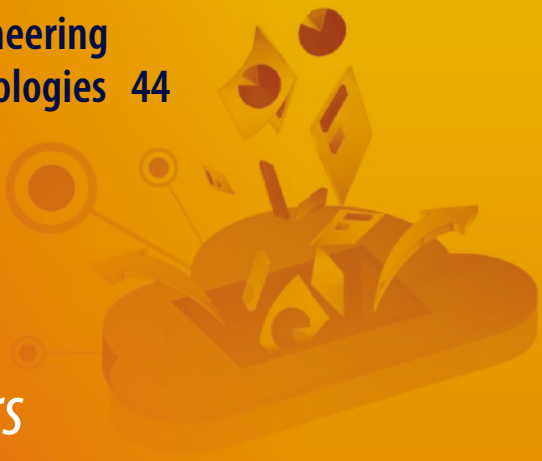
Lecture Notes on Data Engineering and Communications Technologies 44



S. Smys
Tomonobu Senjyu
Pavel Lafata *Editors*

Second International Conference on Computer Networks and Communication Technologies

ICCNCT 2019

Springer

Lecture Notes on Data Engineering and Communications Technologies

Volume 44

Series Editor

Fatos Xhafa, Technical University of Catalonia, Barcelona, Spain

The aim of the book series is to present cutting edge engineering approaches to data technologies and communications. It will publish latest advances on the engineering task of building and deploying distributed, scalable and reliable data infrastructures and communication systems.

The series will have a prominent applied focus on data technologies and communications with aim to promote the bridging from fundamental research on data science and networking to data engineering and communications that lead to industry products, business knowledge and standardisation.

**** Indexing: The books of this series are submitted to SCOPUS, ISI Proceedings, MetaPress, Springerlink and DBLP ****

More information about this series at http://www.springer.com/series/15362

S. Smys · Tomonobu Senjyu · Pavel Lafata
Editors

Second International Conference on Computer Networks and Communication Technologies

ICCNCT 2019

Springer

Editors
S. Smys
Department of Computer
Science Engineering
RVS Technical Campus
Coimbatore, Tamil Nadu, India

Pavel Lafata
Department of Telecommunication
Engineering
Faculty of Electrical Engineering
Czech Technical University in Prague
Prague, Czech Republic

Tomonobu Senjyu
University of the Ryukyus
Okinawa, Japan

ISSN 2367-4512 ISSN 2367-4520 (electronic)
Lecture Notes on Data Engineering and Communications Technologies
ISBN 978-3-030-37050-3 ISBN 978-3-030-37051-0 (eBook)
https://doi.org/10.1007/978-3-030-37051-0

© Springer Nature Switzerland AG 2020, corrected publication 2020, 2024
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

We are honored to dedicate the proceedings of ICCNCT 2019 to all the participants and editors of ICCNCT 2019.

Foreword

It is with deep satisfaction that I write this Foreword to the Proceedings of the ICCNCT 2019 held in Coimbatore, Tamil Nadu on May 23 and 24, 2019.

This conference was bringing together researchers, academics, and professionals from all over the world, experts in Computer Communications and Networks.

This conference particularly encouraged the interaction of research students and developing academics with the more established academic community in an informal setting to present and to discuss new and current work. The papers contributed the most recent scientific knowledge known in the field of Computer Networks, Ad hoc and Sensor Networks, Internet and Web Applications, and Ubiquitous Networks. Their contributions helped to make the Conference as outstanding as it has been. The Local Organizing Committee members and their helpers put much effort into ensuring the success of the day-to-day operation of the meeting.

We hope that this program will further stimulate research in wireless ad hoc and sensor networks, information-centric networking, embedded networks, and opportunistic networking and provide practitioners with better techniques, algorithms, and tools for deployment. We feel honored and privileged to serve the best recent developments to you through this exciting program.

We thank all authors and participants for their contributions.

Coimbatore, India
May 2019

S. Smys
Conference Chair, ICCNCT 2019

The original version of the book was revised: Following chapters 44, 82, 89, 101 are retracted. The retraction note to the book is available at https://doi.org/10.1007/978-981-99-5394-3_109

Preface

This Conference Proceedings volume contains the written versions of most of the contributions presented during the conference of ICCNCT 2019. The conference provided a setting for discussing recent developments in a wide variety of topics including Network Operations and Management, QOS and Resource Management, Wireless Communications, and Delay-tolerant networks. The conference has been a good opportunity for participants coming from various destinations to present and discuss topics in their respective research areas.

ICCNCT 2019 Conference tends to collect the latest research results and applications on Computer Networks and Inventive Communication Technologies. It includes a selection of 107 papers from 337 papers submitted to the conference from universities and industries all over the world. All of accepted papers were subjected to strict peer reviewing by 2–4 expert referees. The papers have been selected for this volume because of quality and the relevance to the conference.

ICCNCT 2019 would like to express our sincere appreciation to all authors for their contributions to this book. We would like to extend our thanks to all the referees for their constructive comments on all papers, especially, we would like to thank organizing committee for their hard working. Finally, we would like to thank the Springer publications for producing this volume.

Coimbatore, India
May 2019

S. Smys
Conference Chair, ICCNCT 2019

Acknowledgements

ICCNCT 2019 would like to acknowledge the excellent work of our conference organizing the committee, keynote speakers for their presentation on May 23 and 24, 2019. The organizers also wish to acknowledge publicly the valuable services provided by the reviewers.

On behalf of the editors, organizers, authors, and readers of this Conference, we wish to thank the keynote speakers and the reviewers for their time, hard work, and dedication to this Conference. The organizers wish to acknowledge Dr. Smys for the discussion, suggestion, and cooperation to organize the keynote speakers of this Conference. The organizers also wish to acknowledge for speakers and participants who attend this conference. Many thanks are given for all persons who help and support this conference. ICCNCT would like to acknowledge the contribution made to the organization by its many volunteers. Members contribute their time, energy, and knowledge at a local, regional, and international level.

We also thank all the Chair Persons and Conference Committee Members for their support.

Contents

Monitoring Air Pollutants Using Wireless Sensor Networks

Shweta A. Patil(✉) and Pradeep Deshpande

BLDEA'S V.P. Dr. P.G. Halakatti College of Engineering and Technology, Vijayapur, Karnataka, India
shweta_agp@yahoo.co.in

Abstract. IOT is an emerging area of network which acts as a future technology trend of sensing, computing, and communication. Internet of things integrates several techniques as wireless sensor network, Radio frequency identification and embedded devices with existing internet. IOT extends the concept of internet from network of homogeneous devices to network of heterogeneous devices. Air pollution is a major issue for providing healthy environment to the mankind. Healthy environment keeps mankind healthy. Hazardous gases detection becomes important. Hence a system for measuring and monitoring of air pollutants is to be provided. Wireless sensor network is found to be an efficient method of measuring and monitoring air pollutants.

Keywords: IoT · WSN · Zigbee · Sensor · Microcontroller

1 Introduction

IoT is an emerging area of network that integrates several techniques as wireless sensor network, Radio frequency identification and embedded devices with existing internet. IOT extends the concept of internet from network of homogeneous devices to network of heterogeneous devices [12]. Internet of things means inter-connecting the different devices which can sense the required data, transmit the data, and process it by using wireless sensor network. Wireless sensor network is one of the most powerful tools for measuring, remote controlling and monitoring. WSN is a network of small sensing devices called as sensor nodes which are distributed over the area to gather the data. Wireless sensor network establishes a channel to process and communicate data with each other and to communicate with centralized control. They have wide range of application in variety of fields such as health care, home automation, agriculture, industry, environment monitoring, structural monitoring, disaster management, emergency response etc. Sensor nodes have various energy and computational constraints because of their in-expensive nature and ad-hoc method of deployment [11].

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 1–8, 2020.
https://doi.org/10.1007/978-3-030-37051-0_1

Population of mankind in city is increasing drastically day by day which has resulted to various problems as traffic congestion, environmental degradation, lack of resources, job stress etc. In order to overcome these problems different innovative operations under urban and management mode are to be taken. Clear, systematic and scientific planning along with intelligent building and efficient management helps to overcome the problems. Hence smart city construction becomes essential. Smart city is nothing but the combination of digital city and internet of things. In the application of smart city environmental protection has caught more attention. The environment is badly affected due to the continuous and rapid growth of industries and wide spread use of vehicles because of which 2.4 million people die every year world-wide, hence leading to Air pollution which in turn leads to global warming and acid rains. Air pollution affects the human-health, environment and quality of life. Thus air pollution monitoring becomes important and becomes necessary to balance the nature [8].

Wireless sensor network is an efficient method for the measurement and monitoring of air pollutants. Many advantages like low cost, multifunctional etc. can be achieved by WSN. WSN can be implemented with different wireless protocols for data transmission as Bluetooth, UWB, and Zigbee, WI-FI etc. Air pollution monitoring system measures different air pollutants such as Carbon dioxide (CO_2), Sulphur dioxide (SO_2), Nitrogen dioxide (NO_2), Carbon Monoxide (CO), Hydrocarbon (HC), Ammonia (NH_4). The information is collected from the sensors and then stored in central server using the means of internet periodically. Then the message is sent from server to the users [2, 8].

2 Existing System

Air pollution lead to extreme distraction and harms the human being and environment very badly. Thus it is life threatening. Hence it's important to monitor air pollution [2].

Conventional monitoring system uses laboratory analysis which used large equipments, complex technology. Thus this system was complex, huge and costly.

To overcome all these disadvantages different experts started using internet of things concept in their systems. Some developed the system using sensors for measuring different compositions of air and used machine learning algorithms for air quality indexing [4]. Some system used AVR A Tmega-32 microcontroller [14]. In some systems results of air quality was displayed on city map. In some systems Carbon nano tube is used as a Metal Oxide (MOX) gas sensor which needs to be heated up for a longer periods. These nano tubes are sensitive and costly. Some methods use sensors which consume more energy. Hence they are not efficient. In some methods pollutant quality information transmission is done within small distances. Thus many systems were developed to measure the pollutants of air. Different approaches emerged to measure the air contamination and monitor it.

3 System Architecture

The block diagram shown below represents the architecture of environmental monitoring system.

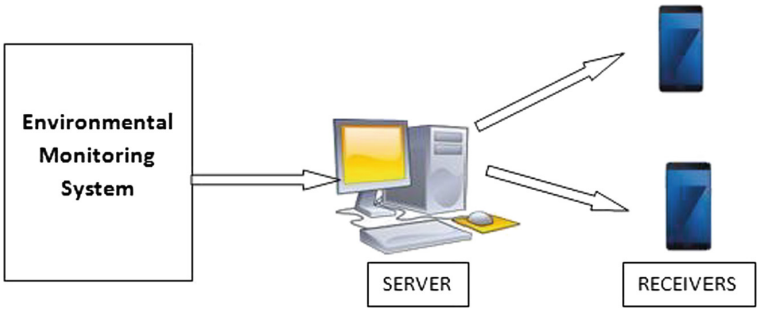


Fig. 1. Architecture of environment monitoring system

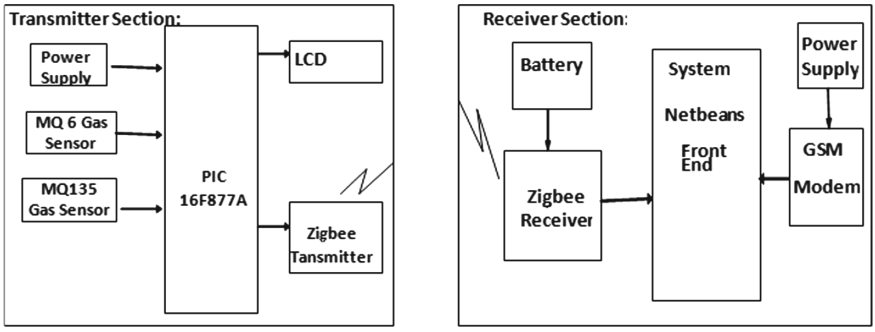


Fig. 2. Transmitter and receiver sections

Figure 1 shows the architecture of air pollutant monitoring system. It consists of a transmitter and a receiver section (shown in Fig. 2). The aim of the system is to monitor the environment. The contents of the air such as CO_2, O_2, SO_2, and NO_2 are to be monitored; we need to gather this information using different sensors. These sensors are placed as terminals at different locations in the city. The sensed data is to be transmitted to central server. Hence the sensed data passing through the microcontroller (PIC16F877A) get collected at the central server through Zigbee transmitter. The central server is nothing but a personal computer. At the server, the Zigbee receiver collects the sensed data of air from each location which is further stored in server through microcontroller at that unit. Location wise the sensed content of constituents of gas are compared with the normal values, if the content of pollutant gas exceeds the normal range then a message will be sent to the people over that location through the server to their mobiles about the percentage of pollutant present and message as "Air is Polluted" is displayed. Thus the system finds whether the air is polluted or not. If polluted, it finds the percentage of pollutant and transmits this information wirelessly to the mankind. This helps the people to know about the air quality.

Many different technologies are available for wireless sensor technologies. Some of them are Wi-Fi, Bluetooth, cloud computing based transmission, Zig-bee etc. In this paper Zig-bee technology is used as a mode of transmission method to transfer the data from different nodes to central server. Zig-bee has more advantages over others. Some of advantages are low cost and high performance.

Zigbee is one of the best means of communication built for sensor networks on IEEE 802.15.4 standard for wireless personal area networks (WPANs). It is the product from Zigbee alliance. This enables physical and Media Access Control (MAC) layers to handle many devices at very low-data rates. These Zigbee's WPANs operate at different frequencies as 868 MHz, 902–928 MHz and 2.4 GHz frequencies. The two way transmission of data between sensors and controllers can be done at 250 kbps data rate. Zigbee is low-cost network. Its power consumption is very low hence it is widely used for controlling and monitoring applications. The distance of communication ranges from 10 to 100 m. The distance of communication in network can be increased by using routers and thus communication can be achieved in wider area network. Zigbee communication is less expensive and simpler than any other shortrange wireless sensor networks such as Bluetooth and Wi-Fi. Zigbee supports different network configurations for master to master or master to slave communications. Zigbee facilitates two modes of operations for which the battery power is conserved [13].

This system has following advantages

- System
  - It is very Simple to use.
  - It is compact so portable.
  - Very easy to handle.
  - System is Real time.
- Sensors
  - Life time of sensors is very high.
  - Low cost sensors are used.
- Operating voltage: System uses very low voltage of 5 V, −20 °C to +50 °C.
- System can be used to check quality of air indoor as well as outdoor.
- Continuous update of change in percentage of quality can be got.
- Very much helpful for patients especially for asthma patients.

4 Results and Discussions

4.1 Hardware Implementation of Transmitter Section

Each nodes act as transmitters which are placed at different areas where environment needs to be monitored. Figure 3 shows transmitter section. It consists of sensors, microcontroller unit and Zig-bee.

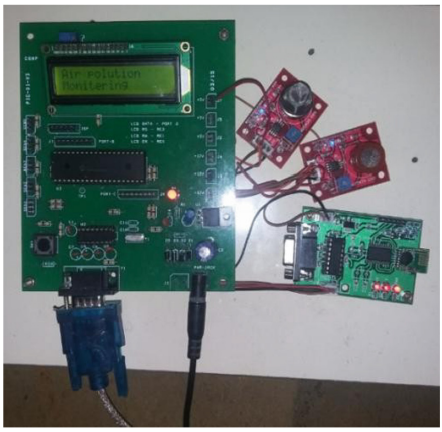


Fig. 3. Hardware implementation of of Transmitter

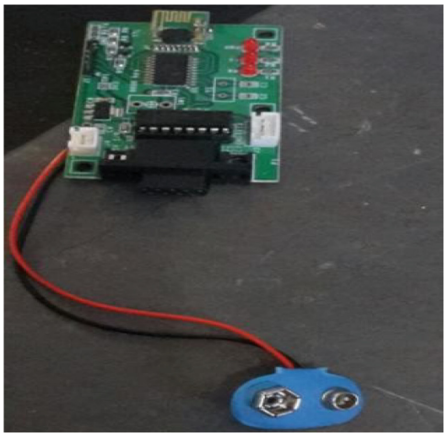


Fig. 4. Hardware implementation Receiver

Figure 4 shows the receiver section which contains Zig-bee module which has to be connected to central server.

4.2 GSM Section

Figure 5 shows the GSM module used at the receiver side at the central server to send message to the mankind about polluted air and its percentage of contamination.

Fig. 5. GSM module

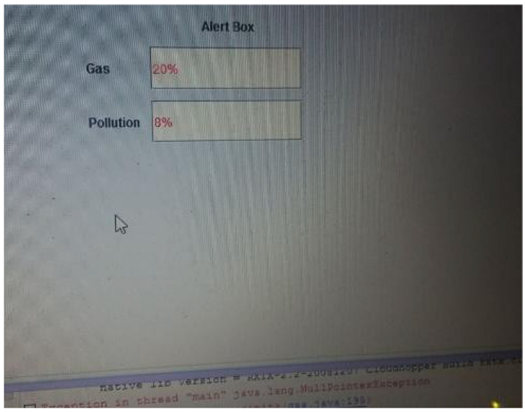


Fig. 6. Output display at server section

Figure 6 shows the display at the central server. The sensed gas is transmitted to the central server through the Zigbee transmitter. Here the percentage of pollutant is compared with the standard amount of that content in the air. If that content is more than the set value then air is polluted. So the percentage of Gas sensed and the percentage of pollution present is displayed as shown in figure.

5 Applications

Below are few applications of air quality monitoring using IoT.

- In agriculture: Many gases like SO_2, NO_2, fly ash etc. affect the growth of plants and can cause different diseases in plants. By monitoring of such gases we can give appropriate treatment and pesticides to the plants and we can avoid the occurrence of diseases in plants thus can be applied in agriculture to improve plant growth.
- In gas leakage detection: It can be used in Gas leakage applications where gas sensors detect the presence of LPG leakage which helps to get information of gas leakage inside and outside home. This will help to prevent causalities and fatalities.
- In indoor/outdoor air quality monitoring: It can be used to measure the percentage of different components present in the air. If the percentage of any hazardous gaseous substance is more it sends the information to the surrounding people.
- In public transport vehicles: All vehicles are fixed with sensors that measure the emission of fuel. If the smoke emission is more than the system intimates the same to the driver by which fuel emission of transport vehicles can be monitored.
- In health monitoring: The system can be applied in health monitoring of patients by sending them information of air quality in their surroundings.

6 Conclusion

The air quality monitoring is an emerging issue in the area of Internet of Things. We address the possibility of air pollution by using different gas sensors. The proposed model uses Zigbee transmitter and receiver to transmit the sensed data to the server, where the amount of pollutants is calculated, and if the pollutant value is more than threshold value then, the proposed model sends the message about the percentage of pollutant to the registered mobile numbers wirelessly. This is the efficient method of transmitting the data over certain distance of 1 km. The repeaters are used to extend the distance. Thus this monitoring system is useful for asthma patients to find the quality of air. Thus intimates the person about air pollution in the different areas which helps to monitor effect of air pollutants on health. This system can also be applied to find gas leakages, fuel emission in vehicles etc. This air monitoring helps to avoid global warming and removes the threat of acid rain. Further this model can be enhanced for different applications food quality monitoring, agriculture, etc. by using different sensors.

References

1. Aram, S., Troiano, A., Pasero, E.: Environment sensing using smartphone. In: 2012 IEEE Sensors Applications Symposium Proceedings, pp. 1–4 (Feb 2012)
2. Bhattacharya, S., S. Sridevi, S., Pitchiah, R.: Indoor air quality monitoring using wireless sensor network. In: 2012 Sixth International Conference on Sensing Technology (ICST), pp. 422–427 (2012)
3. Chan, H.T., Rahman, T.A., Arsad, A.: Performance study of virtual fence unit using wireless sensor network in IoT environment. In: 2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS), pp. 873–875. IEEE (2014)
4. Elvitigala, C.S., Sudantha, B.H.: Machine learning capable, IoT air pollution monitoring system with upgradable sensor array. In: Conference: ISIS 2017 At: Daegu, South Korea (Oct 2017)
5. Folea, S., Bordencea, D., Hotea, C., Valean, H.: Smart home automation system using Wi-Fi low power devices. In: Proceedings of 2012 IEEE International Conference on Automation, Quality and Testing, Robotics, pp. 569–574. IEEE (May 2012)
6. Postolache, O., Pereira, J.M., Girao, P.: Distributed air quality monitoring based on Bluetooth sensing nodes and virtual TEDS. In: 2007 8th International Conference on Electronic Measurement and Instruments, pp. 4–1. IEEE (2007)
7. Shi, S., Jie, S.: Design an indoor air quality controller based on LPC2478. Sens. Transducers, 18–19 (2014)
8. Hongyang, Z., et al.: Environmental effect removal based structural health monitoring in the internet of things. In: 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 512–517. IEEE (2013)
9. Wen, S., Li, Q., Tham, C.-K.: Wireless deployed and participatory sensing system for environmental monitoring. In: 2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 158–160. IEEE (2014)

10. Walczak, D., Wrzos, M., Radziuk, A., Lewandowski, B., Mazurek, C.: Machine-to-machine communication and data processing approach in future internet applications. In: 2012 8th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), pp. 1–5. IEEE (July 2012)
11. Le, Z.: An IOT system for environmental monitoring and protecting with heterogeneous communication networks. In: 2011 6th International ICST Conference on Communications and Networking in China (CHINACOM), pp. 1026–1031. IEEE (2011)
12. Mainetti, L., Patrono, L., Vilei, A.: Evolution of wireless sensor networks towards the internet of things: a survey. In: SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks. IEEE (2011)
13. Somani, N.A., Patel, Y.: Zigbee: a low power wireless technology for industrial applications. Int. J. Control. Theory Comput. Model. (IJCTCM) **2**(3) (2012)
14. Patil, P.S., Sawant, S.R., Mudholkar, R.R.: AVR micro-controller based embedded weather monitoring system. Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET) **4**(VII) (2016). ISSN: 2321-9653

Framework for Data Hiding Operation Using Motion Vectors for Effective Imperceptibility Performance

K. Manjunath Kamath[1(✉)] and R. Sanjeev Kunte[2]

[1] Yenepoya Institute of Technology, Moodbidri, India
kamathsjce@gmail.com
[2] JNN College of Engineering, Shivamogga, Karnataka, India
sanjeevkunte@gmail.com

Abstract. Data Hiding is one of the frequently used security approaches for safeguarding the sensitive information of the available data as well as to transmit secret information among different ends in a vulnerable network. However, majority of data hiding scheme evolved till date is focused on its embedding capacity or else focused on introducing the distinct parameters of encryption. However, all these approaches will not only make the embedded file bulky but also, they will lose its imperceptibility characteristics. Therefore, the proposed paper introduces a simple and robust reversible data hiding process where a secret image is embedded within a video as a cover image. Motion prediction and histogram shifting approach is also utilized for obtaining highly secured bit-streams. The outcome of the study shows that the proposed system offers a better signal quality and retains maximum imperceptibility irrespective of the size of the secret image.

Keywords: Reversible data hiding · Image imperceptibility · Video encoding Secret image · Compression

1 Introduction

With the recent progressive growth of multimedia technologies, almost all the commercial applications have started using it in a commercial way. In this regard, the usage of various multimedia file system are mainly shared and exchanged by the user from a practical viewpoint. Various studies have already been carried out to prove that the multimedia security still remains as a big challenge to overcome [1–6]. Hence, security approaches have been evolving in order to counter-attack the threats [6–10]. One of the most frequently used counter-mechanisms is data hiding scheme where a secret data is embedded for security purpose. The embedding of information, in most cases, causes the carrier to lose a part of the data, so the carrier cannot be completely recovered after it gets extracted. In some special applications, such as in the fields of medicine, military, and law, false positives would be caused even by slight distortion of a digital image. Therefore, any irreversible loss of carrier data is not allowed. Basically, Reversible Data Hiding scheme is capable of extracting the actual set of information from the given source ensuring the highest quality of information i.e. zero loss of data.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 9–20, 2020.
https://doi.org/10.1007/978-3-030-37051-0_2

Therefore, this topic is currently a center of attention for various researchers. Therefore, the proposed system introduces a very simple and novel reversible data hiding process by considering video as a cover file, which mainly targets on accomplishing the imperceptibility of the embedded secret image. The organization of the paper is as follows – Sect. 2 briefs of existing studies while research problem is briefed in Sect. 3. Adopted methodology and system design is discussed in Sect. 4 and Sect. 5 respectively. Result analysis is discussed in Sect. 6 while conclusion is briefed in Sect. 7.

2 Related Work

This section discusses about recent research work towards reversible data hiding. The most recent work is carried out by Puteaux and Puech [11] where a predictive scheme of *most significant bit* is used emphasizing on improving the high capacity. Qian et al. [12] have used a dual embedding scheme towards generating an encrypted bitstream. Qian et al. [13] have also used an iterative process of data hiding where first the encryption of image is carried out followed by embedding on extra information for obtained ciphered image into the server. A unique three-dimensional data hiding process using mesh framework was introduced by Jiang et al. [14]. According to the scheme, the vertex coordinates are used for mapping the integers from the decimals followed by usage of the least significant bits. Usage of homomorphic encryption is carried out by Xiang and Luo [15] along with the usage of Paillier encryption approach. The work of Yi and Zhou [16] has used a labeling scheme based on binary tree structure over the image pixels in order to facilitate encryption over image. Chen et al. [17] have used sorting of pixel approach as well as extension of the errors caused due to prediction for data encryption mechanism using directional property of the predictor. The work of Wu et al. [18] has adopted a color partitioning process for developing a unique data hiding scheme. Usage of motion vector over video encoded by H264 is carried out by Niu et al. [19]. The study discussed by Hou et al. [20] have considered the distortion problem and used reversible steganography for data hiding. Xiong et al. [21] have used homomorphic encryption while Wang et al. [22] have used histogram shifting approach for data hiding. The work of Zhang [23] used have optimal value of host data where pixel and auxiliary information is used for estimating errors. Many researchers have proposed theories for video steganography as well as compressed domain reversible video steganography using various conventional approaches of compression. Steganography system proposed by Hu et al. [24] is based on non-uniform rectangular partition uses an uncompressed domain. It uses secret video to hide inside a cover video, and the size of cover video and secret video are of same size. Similarly, various others authors e.g. Ni et al. [25], Hong et al. [26], Zhang et al. [27, 30], Ma et al. [28], and Shanableh et al. [29] have also carried out work towards addressing the problem of data hiding scheme where different conventional methodologies are applied for data hiding operation. The next section outlines the research problem.

3 Problem Description

From the review of the existing system, it can be seen that there are various forms of solutions towards strengthening the process of reversible data hiding procedure. Almost all schemes that are recently evolved are very unique and distinct from each other where the performance is found to offer a better data hiding scheme. However, a thorough investigation of its performance shows that existing system is not claimed to offer a good balance between the image quality and embedding policies. Not all work has actually emphasized on imperceptibility concept that is mandatory in data hiding scheme. Apart from this, the studies towards data hiding scheme over video is quite a less to found. The few work carried out towards video encoding scheme and data hiding actually doesn't consider imperceptibility factor associated with reversible data hiding.

4 Proposed Methodology

The main idea of the proposed system is to offer a cost effective data hiding scheme where a multimedia file system is considered as a cover file. The proposed system implements an analytical research methodology where a unique operation flow is constructed in order to obtain a secured bit-stream of data (Fig. 1). Another interesting part of the proposed methodology is that it uses the process of video encoding mechanism, which is a part of signal compression approach where a balance between compression and data security is achieved.

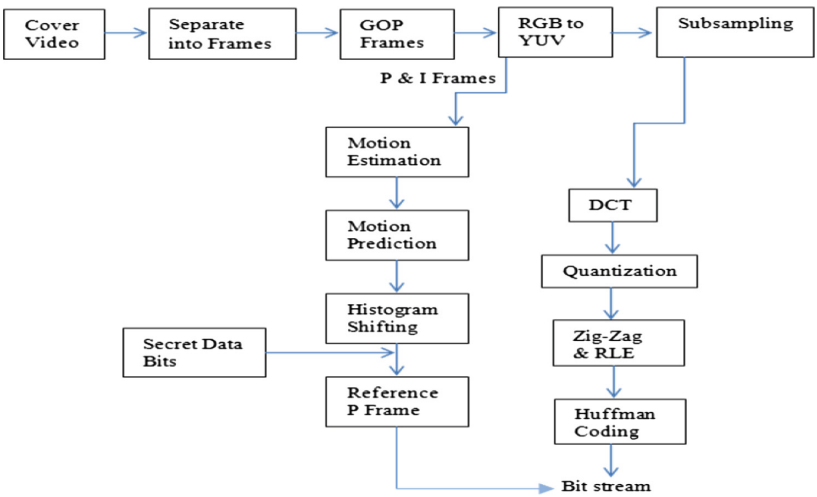


Fig. 1. Operational flow of proposed system

A closer look into Fig. 1 shows that proposed system uses the concept of motion estimation followed by prediction operation where histogram shifting operation is carried out in order to obtain reference P frame. It also applies discrete cosine transform for better compression performing after sub-sampling is carried out. The complete operation leads to generation of an encoded video where data is hidden. An illustrative discussion of this method is carried out in next section.

5 System Implementation

The proposed approach deals with embedding and extraction of the secret image pixels into a MPEG2 compressed video using Histogram shifting method in motion vectors. The cover video considered in this work is an MPEG2 compressed video file. This system presents an efficient way of transfer of information from sender to the receiver as data is hidden in the motion vectors of the selected frames. An uncompressed video is selected as cover video to hide secret image. Initially the frames are extracted and Group of Pictures (GOP) is formed from the extracted frames [11]. These frames are subjected to YCbCr color conversion. The proposed system uses luminance value obtained from the red component while other color components i.e. U and V are obtained from green and blue components respectively. In the next stage reduction of the resolution is done using Chroma subsampling. The proposed system then applies the concept of motion compensation for the purpose of minimizing the redundancy factor with respect to the temporal data in it while this operation is followed by applying standard discrete cosine transform scheme for obtaining better compression outcome. Finally, quantization operation is applied on the top of this process for effective compression as well as for better control of redundancy factor with respect to spatial data. At the end, the proposed system applies a lossless compression scheme of run length encoding for achieving better encoding performance and further Huffman encoding scheme is also continued on it. At the receiver side the process has to be reversed that is called as decoding. In decoding stage the de quantization of the data is to be carried out. The proposed system uses motion vectors where the chunks of the ciphered data is basically hidden in the form of P frame and this operation is carried out only after histogram shifting is done. During the compression, the secret image bits are extracted from the corresponding motion vectors and histogram is shifted back. This achieves reversibility characteristics. This section discusses about the algorithm implemented for this purpose.

5.1 Algorithm for Reversible Data Hiding

The steps of the proposed system are as follows: The proposed algorithm takes the input of cover video (I), which is then used for framing up group of pictures G_{op} (Line-1). After digitizing the secret image (which is required to be hidden), the next step is to distinguish all the obtained frames into different macroblock size (Line-2). The proposed system then performs following operation on all the macro-blocks (Line-3): a standard discrete cosine transform (DCT) is applied on the macro-blocks from the spatial to frequency domain (Line-4) which is followed by applying standard quantization

technique over the obtained matrix of DCT (Line-5). This process leads to generation of a dedicate motion vector obtained for all the values of P-frames (Line-7). The next process is to apply Histogram Shifting (HS) method for the generated motion vector for each P-frame (Line-8). A conditional statement is constructed (Line-9) which checks of the bits to be embedded is equivalent to 1. In case of positive scenario, the value of the pixel is maximized to 1 (Line-10) otherwise it is retained as it is (Line-12). This operation is iterated until a stopping criteria is met which is to check if the bits of complete secret image is actually populated in the destined motion vector corresponding to all the P-frame. The proposed system than apply Entropy encoding so that data is read in zig-zag order (Line-13) followed applying Huffman encoding to reduce size. Finally, the system stores the bit stream in a file.

Algorithm for Reversible Data Hiding
Input: I (cover video), I_{sec} (secret image)
Output: I_{p1} (Stego Video)
Start
1. init I, G_{op}→I, I_{sec}
2. I_1→M_{Block}(8x8)
3. **For Each** M_{block}=1: n
4. I_p→DCT(I_{sec}(I_1))$^{s\to f}$
5. I_p→quan(I_p)
6. **End**
7. *Generate* M_{vec}→P_{frame}(I_p)
8. I_{p1}→HS(M_{vec})
9. **If** e_{bit}=1
10. I_{p1}=I_{p1}+1;
11.**Else**
12. I_{p1}= I_{p1}
13. I_{p1}→Huff(e_{bit}(I_{p1}))

The proposed system uses MPEG2 standard that supports motion vectors of different block sizes compared to AVI files. Each macroblock can be divided into different modes. Owing to availability of enriched and varied number of motion vectors in MPEG2, it is seen that videos which have rich texture contain more blocks and more motion vectors. The process for extracting the hidden image from the encoded video is just reverse of the algorithmic steps of encoding (Fig. 2). In order to initiate decoding, the proposed system. The decoding process starts with the output of the encoding that is bit stream is taken. For the embedded video bit steam the reverse Huffman and Reverse of HS process is applied. During this process secret data bits are extracted from each frame. All the obtained motion vector is restored in its legacy form followed by applying inverse operation of quantization. Finally original video is converted from YUV to RGB sequence and original bits are restored. Therefore, a very simplified process of image hiding approach over a cover video file is discussed in the present paper. The implementation idea is not only simple but also robust as it offers better and cost effective form of reversible data hiding scheme. A closer look into the algorithm

implementation will also highlight that proposed system there is a significant contribution of histogram-shifting process over the presented video decoding system. The data hiding capacity is enhanced by incorporating motion vector for embedding data in the video stream of MPEG2. The decoding process is quite simple as it offers better form of reconstructed data in the lossless format. The embedded video can be decoded, and it can be reconstructed in lossless format by shifting histogram to its normal position after extraction of the secret information. Therefore, the proposed algorithm offers a cost effective mechanism to perform an effective data hiding process over video stream without using any complex encoding scheme. Figure 2 highlights the operational steps involved in decoding process.

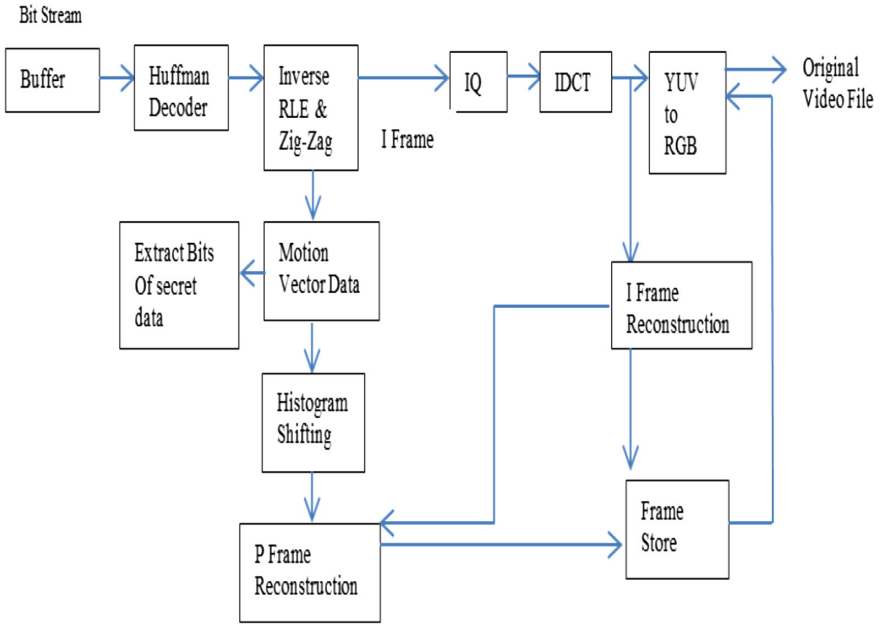


Fig. 2. Block diagram for the process of video decoding

6 Result Analysis

Before starting the discussion about the result obtained by the proposed system, it is essential to understand that proposed system implements MPEG2 compression approach. The MPEG2 compressed bit stream has more motion vectors than uncompressed video standards, so it is suitable to use motion vectors as embedding cover of reversible data hiding process. The proposed system presents an RDH scheme for HS to perform a wide range of applications. A large number of RDH schemes based on HS are proposed. It offers the capability of extensibility between the different domain as well as between different carriers that results in better performance enhancement of

encoding operation. As for the compressed video, embedded information gained by modifying the motion vector allows for a great distortion of the contents, so most of algorithms are developed on the basis of the alteration carried out by the coefficient of DCT over histogram. In this paper, we have implemented histogram shifting process in generated motion vectors of MPEG2 video. Prior to starting actual analysis, the proposed system performs analysis of the histogram operation over a sample standard video which is subjected to standard MPEG2 encoding system. The main purpose of this process is to assess the trends of results obtained from the histogram shifting process. In the below histogram, peak value occurs for motion vector MV = 10 and zero point in the motion vector histogram occurs at motion vector MV = 6. Figure 3 shows the vector histogram of one frame of *bus* video clip encoded by MPEG2.

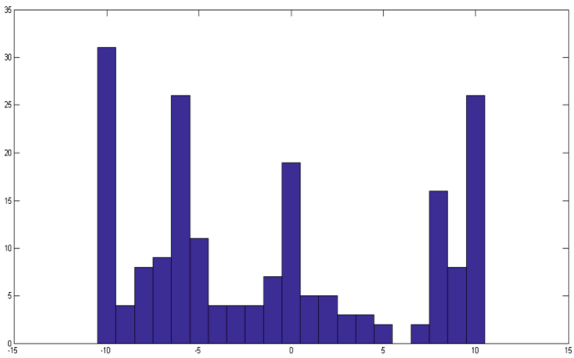


Fig. 3. Sample histogram obtained from MPEG2 encoding

In the proposed work, there are two modules in the system called as Encoding Procedure and Extraction Procedure. In the Encoding procedure secret information bits (Image) are hidden into the Histogram Shifted portion of the motion vectors. Finally corresponding output bit stream is transmitted over the network. The embedded bits of information are obtained in the process of decoding steps with the aid of histograms respective to the motion vector, and histogram is shifted back to its original position and corresponding motion vectors are restored. So that after extraction of secret information, original cover video is restored back. This achieves reversibility. The proposed system uses standard images as the secret image which is showcased in Fig. 4. The analysis of the proposed system is also carried out over other standard video sequences e.g. *city, news, carphone, mobile, foreman, container, salesman,* and *coastguard* [31]. For each video sequence we take 170 frames. The GOP format used is (IPPPPPI). The proposed analysis selects one frame considered as a cover file where the secret image is embedded (Fig. 5). Multiple forms of other images are also considered while carrying out the analysis. The segment of histogram is used for embedding the secret data of motion vector.

Fig. 4. (a) Lena image (b) Baboon image

Fig. 5. (a) One frame of cover video (b) Extracted secret image

The analysis of the outcome of the embedding process is carried out with respect to Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The first analysis is carried out for both MSE and PSNR on secret image that is embedded within the cover video file. The analysis shows following trend – MSE increases with increase in dimensions of same secret image (Fig. 6). Nearly similar trend is also observed for PSNR (Fig. 7), where PSNR drops with increase of secret image size. Although, there is a drop of PSNR, but a closer look will show that this drop is very much negligible. Similar analysis is also carried out on other images too and nearly similar performance of MSE and PSNR is noticed with a fluctuation less than 5% in both PSNR and MSE of secret image.

The next part of the assessment is associated with the MSE and PSNR trends on cover video file. This analysis is carried out considering different sample video where same secret image is embedded. All the three sample video considers are of different size and hence it is required to assess how the size of the secret image affects the PSNR (Fig. 9) and MSE (Fig. 8).

The outcome shows that MSE is slightly degraded with different video samples, however, the fluctuation is highly less (Fig. 8). On the other hand, There is no significant degradation in PSNR value even in different video samples to prove that size of secret image doesn't have any potential degradation. Similar assessment is carried out on different combination of sizes of secret images on same as well as on different video to find that PSNR stays in the range of 30–40 dB. Hence, the proposed study can be said to offer a better form of data hiding performance.

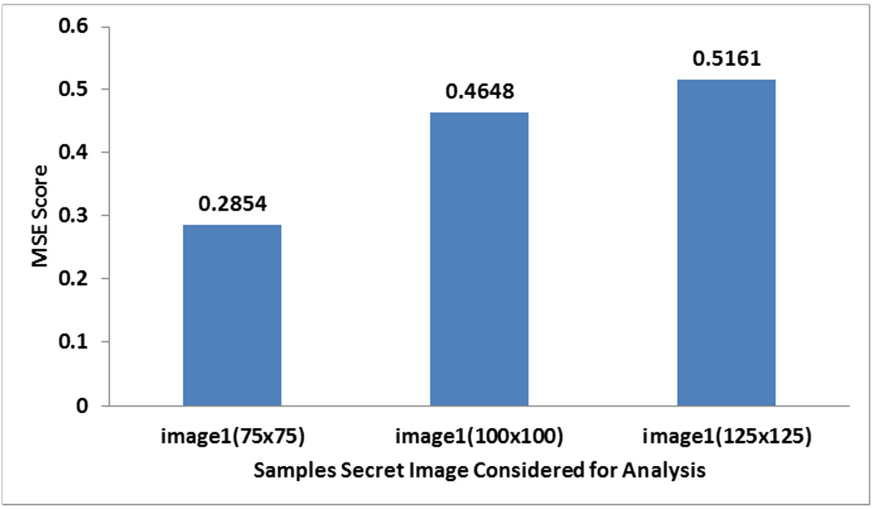


Fig. 6. Analysis of MSE of secret image

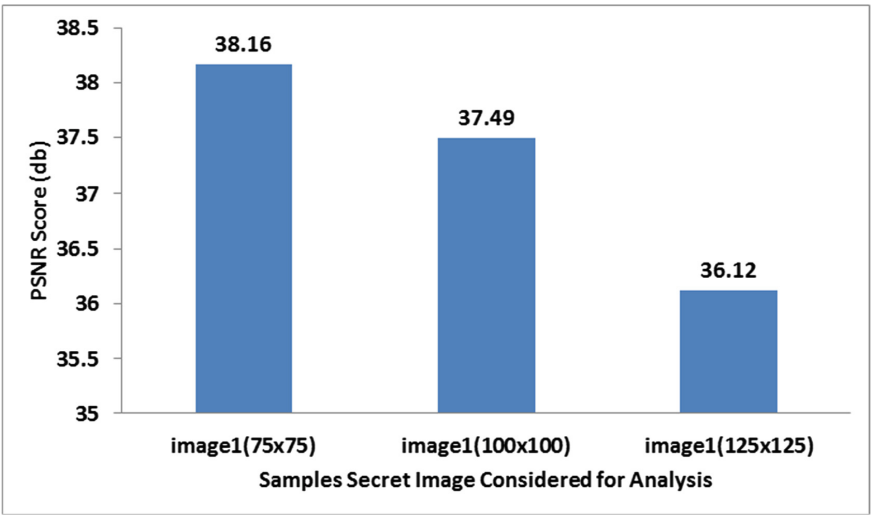


Fig. 7. Analysis of PSNR of secret image

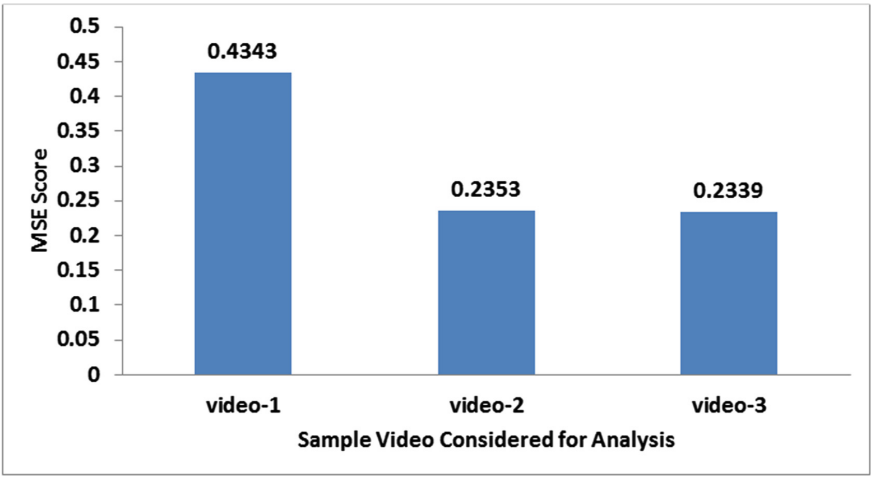


Fig. 8. Analysis of MSE of cover video image

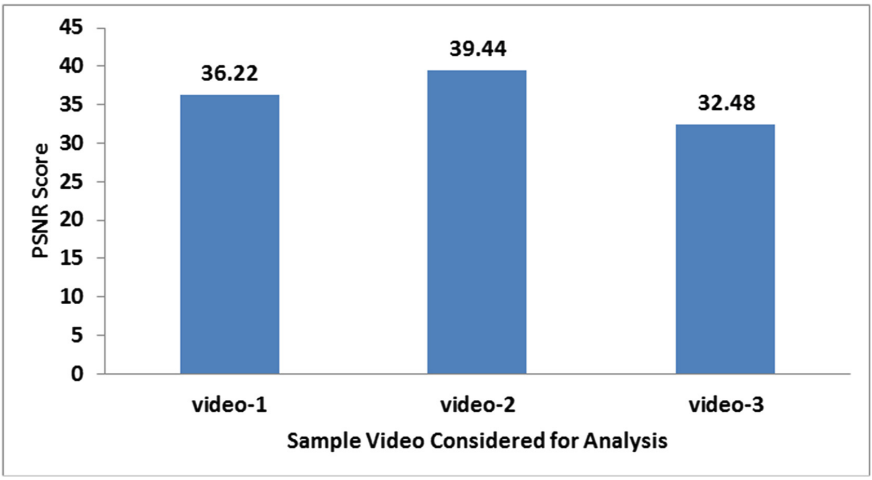


Fig. 9. Analysis of PSNR of cover video image

7 Conclusion

This research paper has presented a unique data hiding scheme which remains reversible in nature. The process lets the secret image to be efficiently hidden within a multimedia file like video in the form of motion vector. To achieve the reversibility of cover video, Histogram Shifting of motion vectors has been done before the data embedding process. The proposed technique is less computationally complex and can be adjusted according to the varying needs. The analysis has been proved that the proposed system offers good and stabilized MSE and PSNR performance. The

inference of the outcome shows that the proposed system offers a good imperceptibility towards the embedded multimedia file where PSNR performance is found good. At present, the method is only applicable to the MPEG2 video sequences. In future, the work can be deployed to other video formats in the compressed video domains.

References

1. Mallikarjunan, K.N., Muthupriya, K., Shalinie, S.M.: A survey of distributed denial of service attack. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, pp. 1–6 (2016)
2. Basha, S.H., Jaison, B.: Survey on patended and unpatented video watermarking techniques. In: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, pp. 1–8 (2017)
3. Minemura, K., Wong, K., Phan, R.C., Tanaka, K.: A novel sketch attack for H.264/AVC format-compliant encrypted video. In: IEEE Transactions on Circuits and Systems for Video Technology, vol. 27, no. 11, pp. 2309–2321 (Nov 2017)
4. Panchal, U.H., Srivastava, R.: A comprehensive survey on digital image watermarking techniques. In: 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, pp. 591–595 (2015)
5. Venugopala, P.S., Jain, S., Sarojadevi, H., Chiplunkar, N.N.: Study of possible attacks on image and video watermark. In: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, pp. 3505–3510 (2016)
6. Le, T.H.N., Nguyen, K.H., Le, H.B.: Literature survey on image watermarking tools, watermark attacks and benchmarking tools. In: 2010 Second International Conferences on Advances in Multimedia, Athens, pp. 67–73 (2010)
7. Singh, S., Singh, A.K., Ghrera, S.P.: A recent survey on data hiding techniques. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, pp. 882–886 (2017)
8. Mancy, L., Maria Celestin Vigila, S.: A survey on protection of medical images. In: 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, pp. 503–506 (2015)
9. Igorevich, R.R., Yong, H., Min, D., Choi, E.: A study on multimedia security systems in video encryption. In: INC2010: 6th International Conference on Networked Computing, Gyeongju, pp. 1–5 (2010)
10. Moravčík, M., Segeč, P., Hrabovský, J., Papán, J., Uramová, J.: Survey of real-time multimedia security mechanisms. In: 2016 International Conference on Emerging eLearning Technologies and Applications (ICETA), Vysoke Tatry, pp. 233–238 (2016)
11. Puteaux, P., Puech, W.: An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images. IEEE Trans. Inf. Forensics Secur. **13**(7), 1670–1681 (2018)
12. Qian, Z., Xu, H., Luo, X., Zhang, X.: New framework of reversible data hiding in encrypted JPEG bitstreams. IEEE Trans. Circuits Syst. Video Technol. **29**(2), 351–362 (2019)
13. Qian, Z., Zhou, H., Zhang, X., Zhang, W.: Separable reversible data hiding in encrypted jpeg bitstreams. In: IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 6, pp. 1055–1067 (1 Nov–Dec 2018)
14. Jiang, R., Zhou, H., Zhang, W., Yu, N.: Reversible data hiding in encrypted three-dimensional mesh models. IEEE Trans. Multimedia **20**(1), 55–67 (2018)

15. Xiang, S., Luo, X.: Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group. IEEE Trans. Circuits Syst. Video Technol. **28**(11), 3099–3110 (2018)
16. Yi, S., Zhou, Y.: Separable and reversible data hiding in encrypted images using parametric binary tree labeling. IEEE Trans. Multimedia **21**(1), 51–64 (2019)
17. Chen, H., Ni, J., Hong, W., Chen, T.: High-fidelity reversible data hiding using directionally enclosed prediction. IEEE Signal Process. Lett. **24**(5), 574–578 (2017)
18. Wu, H., Shi, Y., Wang, H., Zhou, L.: Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification. IEEE Trans. Circuits Syst. Video Technol. **27**(8), 1620–1631 (2017)
19. Niu, K., Yang, X., Zhang, Y.: A novel video reversible data hiding algorithm using motion vector for H.264/AVC. Tsinghua Sci. Technol. **22**(5), 489–498 (2017)
20. Hou, D., Zhang, W., Yang, Y., Yu, N.: Reversible data hiding under inconsistent distortion metrics. IEEE Trans. Image Process. **27**(10), 5087–5099 (2018)
21. Xiong, L., Dong, D., Xia, Z., Chen, X.: High-capacity reversible data hiding for encrypted multimedia data with somewhat homomorphic encryption. IEEE Access **6**, 60635–60644 (2018)
22. Wang, J., Ni, J., Zhang, X., Shi, Y.: Rate and distortion optimization for reversible data hiding using multiple histogram shifting. IEEE Trans. Cybern. **47**(2), 315–326 (2017)
23. Zhang, X.: Reversible Data hiding with optimal value transfer. IEEE Trans. on Multi. **15**(2), 316–325 (2013)
24. Hu, S.D., KinTak, U.: Faculty of information technology: a novel video steganography based on non-uniform rectangular partition. In: IEEE International Conference on Computational Science and Engineering CSE/I-SPAN/IUC, pp. 57–61 (2011)
25. Ni, Z., Shi, Y., Ansari, N., Wei, S.: Reversible data hiding. IEEE Trans. Circuits Syst. Video Technol. **16**(3), 354–362 (2006)
26. Hong, W., Chen, T.S., Wu, H.Y.: An improved reversible data hiding in encrypted images using side match. IEEE Signal Pro. Lett. **19**(4), 199–202 (2012)
27. Zhang, X.: Separable Reversible data hiding in encrypted image. IEEE Trans. Inf. Forensics Security **7**(2), 826–832 (2012)
28. Ma, K.D., Zhang, W.M., Zhao, X.F., Yu, N., Li, F.: Reversible data hiding in encrypted images by reserving room before encryption. IEEE Trans. Inf. Forensics Security **8**(3), 553–562 (2013)
29. Shanableh, T.: Data Hiding in MPEG video files using multivariate regression and flexible macro block ordering. IEEE Trans. Inf. Forensics Security **7**(2), 455–464 (2012)
30. Zhang, X.P.: Reversible data hiding in encrypted image. IEEE Signal Process. Lett. **18**(4), 255–258 (2011)
31. https://media.xiph.org/video/derf/

Privacy Protection and Con Dentiality in Medical IoT

Anjana George(✉), Anu S. Alunkal, Gopika G. Nair, Poornasree R. Mohan, and Fasila K. A

Muthoot Institute of Technology & Science, Varikoli P.O., Puthencruz, Ernakulam, Kerala, India
anjanamg97@gmail.com
http://www.mgmits.com

Abstract. The central issue of any IoT device is its security in sharing the sensitive data. Different methods have been proposed for sharing of data from any IoT device. The ranges of security in these methods are different in various IoT architectures. This paper is a comparative study of these security schemes to determine which scheme allows the fastest and most accurate output. Our findings indicate that the attribute matching functions decreases the usage of keys and leads to an efficient key management technique. It helps in the easy addition and searching of the attributes and solves the trouble of complete re-initialization of attributes during updation. Attribute matching functions also reduces the need of large number of keys and is based on hashing of attributes towards a specified position that enhances the security. The authenticated people whose attributes matches with the specified condition can upload and retrieve medical files whereas non-matching attribute holders may be able to request and they cannot download the medical files nor have access to its contents. Since medical world is booming and the associated technology is advancing formerly and protection of the data from tampering and its sharing to various terminals need security enhancing methods and procedures which adds on the relevance of this work.

Keywords: IoT · Attribute · Bloom · Filter · Con dentiality · Privacy attributes

1 Introduction

The security of medical IoT is a project undertaken for enhancing the privacy preserving efficiency of a smart medical terminal that stores vital information. Traditionally used encryption methods (e.g.: AES) does not provide a fine grained access. The public key approach does not have one to many relations, so a large number of keys are required for security as the number of user increases and key management becomes difficult. Traditionally we use attribute matching functions to retrieve and protect data which does not exhibit more efficiency. In many cases all attributes have to be collected and fed into the terminal and complete re-initialization have to be done. There is a chance that the data may get decrypted as it passes to the terminals, if cipher text is not produced soon.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 21–27, 2020.
https://doi.org/10.1007/978-3-030-37051-0_3

table.jpg

Criteria	Homomorphic Encryption	ABE	KP-ABE	CP-ABE	ABE w. non monotonic	HABE	AES	HIBE
Data Confidentiality	✓	✗	✓	✓	✓	✓	✓	✓
Fine grained access	✓	✓	✓	✓	✓	✓	✗.	✗
Scalability	✓	✗	✗	✗	✗	✓	✗	✓
User revocation	✓	✗	✓	✓	✓	✓	✗..	✓
User Rejoin	✓	✗	✓	✓	✓	✓	✗..	✓
Collusion Resistance	✓	✓	✓	✓	✓	✓	✗..	✗
User Accountability	✗	✗	✗	✓	✗	✓	✗.	✗
Ciphertext Size	Same as Plaintext	Larger ***	Larger ***	Larger ***	Larger ***	Larger ***	Same as Plaintext	Gets larger as l increases
Time Complexity	$O(t^{3.5})$ bit operations	$\|A_{CT}\|G_1+G_2$	$\|A_{CT}\|G_1+G_2$	$(2\|A_{CT}+1\|)G_1+G_2$	$(2\|A_{CT}+1\|)G_1+G_2$	$\|A_{CT}\|G_1+G_2$	$O(n)$	$O(l+\log T)$

Fig. 1. Comparison table of CP-ABE with other encryption methods

This proposed work focuses upon the solutions to these problems. Here we use the modern attribute based encryption to increase the efficiency and privacy of data sharing, where the cipher text is accompanied by a grained access control data structure. Here we use a set of attributes instead of keys. Users take a partially decrypted data from terminals and the set of their matching attributes in the cipher helps to completely decrypt data which provides additional security. Bloom filters are used based on hashing that helps easy retrieval and security of data. Due to bloom filters; initially you need not add every single attribute. Instead you can add it at any stage without complete re-initialization unlike the old attribute matching function.

Medical data is increasing at an alarming rate and has really sensitive contents which needs secure mechanisms for transmission and processing. The work was initially implemented using AES but reached to a conclusion that CP-ABE algorithm is much suited for the work and since there is involvement of storage and processing in cloud platform, Java was found to be suitable. The main focus was cast upon the usage of attributes instead of keys that created confusions and problem of management. Matching of attributes was considered for granting and rejecting access.

Section 1 gives a general introduction to the area of research and the various motivations that led to the proposal. Sections 2 and 3 discusses the brief literature survey done and the comparison of the existing methodologies. Section 4 deals with the proposed methodology. Section 5 illustrates the workflow of different modules. Section 6 discusses the design diagrams. Section 7 shows the expected result from the proposed idea. Sections 8 and 9 deals with the conclusion and idea of enhancement for the proposed solution.

2 Literature Survey

2.1 Security in the Internet of Things

Internet of Things (IoT) [1], is a smart network, where devices are connected over a network. The devices may include wireless sensors, Radio frequency identification (RFID), in order to achieve a reliable and smart wireless network and technologies. When everything is connected to everything, there are more ways to access the information. This can make an attractive target for people who want to make a protocol to the network data. Since valuable data are transmitted between terminals the confidentiality, integrity and privacy are needed to consider more.

2.2 Security Model for IoT

There [2] are many models of securities in IoT applications. Here, this paper introduces a cube structure, which provides trust, privacy, integrated and interrelated security. The cube structure depicts security, confidence and privacy convergence. Privacy is meant to develop secrecy of data and unauthorized access prevention. The cube model clearly explains the importance of each security parameters.

2.3 IoT Device Security Based on Proxy Re-encryption

In [3] this paper, a gateway based on a proxy server is introduced. In the existing networks, many nodes are connected and information are shared between them, but the number of encryption required may be same as that of number of nodes. So the computation amount will remain high. In the proposed proxy server based approach, each node creates n encryption keys and sends it to the proxy server. This proxy cipher converts the plaintext to cipher text and each node in the network can decrypt the cipher text. Here the encryption calculation amount is decreased and also the communication track becomes smooth and overall secrecy and security is also improved. User access control strategy can be used for securing the data in cloud. Additional computations ae required for this polynomial equation but not for attribute based encryption methods.

2.4 A Lightweight and Flexible Encryption Scheme to Protect Sensitive Data in Smart Building Scenarios

This [4] paper introduces a smart building scenario. Fire meters, sensors, smart meters all are connected via a gateway, where data encryption and decryption process are based on attributes. This entire process involves four phases, (Encrypted data event publication, Symmetric key encryption and storage, Encrypted data event publication, (Encrypted data event retrieval, Here SymCpabe provides an efficient approach. Cp-Abe, cipher text policy and attribute based encryption, provides a scalable working in IoT scenarios. This can be used for group sharing network. Because each nodes in the network is assigned with attributes, other nodes which satisfy these attribute matching can take the data. This provides data secrecy, confidentiality etc.

2.5 A Survey on Authentication Techniques for Internet of Things

Identification [5] of a specific object in such a huge network of interconnected smart objects poses a fundamental task that influences all other system functions such as its governance, privacy features, access control, and overall architecture. Traditional authentication methods like certificate based are discussed. Most of the traditional ones require complete change in protocols and cause key generation overheads. Gateway, controller and central data store authentication architecture requires new hardware implementations. ID based one was listed as the strongest one against various attacks. Overhead problems are solved using access structure.

2.6 Identity-Based Authentication Scheme for the Internet of Things

For [6] addressing the heterogeneity in IoT devices and to integrate the wide ranging protocols of the network, a common identity and authentication mechanism is necessary. Private and public keys of devices are not stored by Key Distribution Centre (KDC) and instead all the attributes/identities are stored. When user log in and give their attributes it is checked with the stored attributes and only valid identification will be permitted. Public key of a recipient is not needed in an identity based encryption but it can simply use identity for the purpose. Even the recipient will not hold the corresponding private key at the time when cipher text is generated. Servers can be used for direct generation of the private key. The only thing required is a secure channel and an IBE server for a private key transmission.

2.7 Authentication and Access Control in E-Health Systems in the Cloud

The [7] Internet of Things (IoT) has the potential to transform the healthcare sector. From the pacemakers to blood pressure cuffs, IoT healthcare can help doctors to have a better analysis of diseases, monitor patients, and improve the treatment outcomes but healthcare data security still remains as a substantial risk, which needs to be significantly addressed. Processing, storing, hosting and archiving become more important. In our project access control structure is added with encrypted data into the cloud, which provides access only to the authorized data owners and users, which provide a fine grained access.

2.8 E-Health Care and Le Hierarchical Encryption

The [8] e-healthcare system plays a major role in society. It provides a smart way of health monitoring and helps to provide adequate medical treatment. This system's objective is to collect and store patient details and share health-related information. In this system, in terms of text and image, they send the PHI to the cloud, as well as other personal questions about their medical history. In cloud computing, PHI collected should match with the doctors' experiences and observations. Unfortunately A series of security measures may take by providing delegating storage and computing untrusted authority. There may be chances of de-duplication. In this paper the author explains a technique for eliminating duplicate copies of data in cloud storage and reduces storage space.

2.9 Attribute Based Encryption for Secure Sharing of E-Health Data

Cloud [9] computing is a revolutionary computer paradigm that makes it possible to use computer resources flexibly, on demand and at low cost. The reasons for security and protection problems arise because the health information of patients. The active customers are stored on some cloud servers instead of under their own control. In this paper, there are cloud computing systems based on multiple parties to make medical data safer. Where medical data is encrypted using key policy and attributes. And the member with a specific attribute and key policy alone can decipher health data after verification by the "key distribution Center" and the "secure data distributor." In the medical field, this technique can be used to securely store patient details and restrict access to an outsider. In order to secure the scalable data, the health data must be encrypted before outsourcing.

There are lots of methods for the data preserving in medical IoT. From the survey we analyzed that, for a group sharing the best choice is CP-ABE. Processing, storing, hosting and archiving data. To decrease heavy computational and communication overhead on data owners, most of the process of authentication and access control is given to an AAM (authentication and access management).

3 Comparison of Existing Techniques

Confidentiality and privacy is important in the scenario of medical IOT. For a group sharing it is better to use Ciphertext based attribute based encryption. It should ensure that only authorized people will get access data. Initially algorithms like AES was implemented and checked, but is considered to be an old method that uses extra keys but with CP-ABE uses less number of keys.

4 Proposed Work

The main idea behind the work is to ensure a more secure and practical method for transmission and storage of medical data. Instead of using private and public keys preference was given to the usage of attributes. Single attributes are taken which involves designation of the person logging in. All registered members can log in and add confidential medical less in their respective accounts.

Person who wishes to retrieve these les can place a request for it from their respective account. Acceptance and rejection is done and if by chance or accidentally request is permitted for an unauthenticated person, then it will be disabled for download. The security algorithm chosen is CP-ABE, after checking upon AES method. CP-ABE is more suitable for works involving cloud platforms.

The medical data is proposed to be collected on a real time basis from temperature and pulse sensors. ECG variations are also taken into account using potentiometer.

Data collected from these hardwares are taken in as a CP-ABE and then encryption is performed on it. On the occurrence of tampering inside the cloud contents an alert notification is placed to inform the same.

5 Methodology

The main focus of the project is to reduce the number of keys used as in other methods. Instead we use attributes to check the granting of access and to enhance the security. Attributes used here is the designation of people or it can be any other factors assigned or selected, can be multiple in numbers which replaces the use of extra security keys for granting access.

The medical data sharing model involves entities like cloud server, attribute authority, data owner and data user. The cloud server is third party, which is used to store ciphertext and attribute bloom filter. The attributes are provided by attribute authority.

The scheme model involves these steps.

Initialization: Authority attribute executes this algorithm. It takes as input a security parameter and generates the output PK and MSK where PK is public key and MSK is the Master Secret Key.

Key generation: Key generation is done using PK, MSK and user-attribute set S that produces SK (secret key) as output for each user.

Online encryption: Takes as inputs the user's public key and library generated private key parameters and outputs an intermediate ciphertext. Online Encryption: Sensors or smartphones are based on the public PK parameters, an intermediate ciphertext IT and the information m to be encrypted, as well as an access structure (M,). Then output is a ciphertext CT.

ABF Build: The data owner takes an access structure (M), and generates the attribute of the bloom filter.

Decryption: ABFQuery and Dec have two subalgorithms.

ABFQuery: Inputs set S, ABF and PK attribution. The algorithm ABF-Query produces a reconstructed mapping attribute 0 = (rownum, att) S. The mapping shows the cascading of the corresponding row number of matrix M and all att level S attributes.

Dec: Inputs the SK, ciphertext CT and reconstructed mapping attribute 0,

then returns message m if the access policy attributes can be fueled, otherwise the algorithm will be omitted.

In overall, the key is generated using the key gen values. The private key and the public key will be automatically generated for each user's and is tied with the set of attributes which represents user's permission. For encryption, both keys and attributes are provided so that security is enhanced.

6 Conclusion

Instead of using the public key approach which uses a large number of key pairs attributes were collected for each user which reduced the confusion and problems created by large number of keys. Extra level of security was ensured by applying online-online encryption before installing the data to cloud. Access control structures were used to provide authentication. ABF Build was used to create attribute bloom filters which provided a particular position for storing the data by hashing and storing method. Hashing of attributes to a particular position enhanced the security of storage. With attribute bloom filters addition of new attribute at any stage of execution become easier and it does not require complete re-initialization of all the existing attributes when new ones are added.

7 Future Scope

The work has got a great relevance in the protection of vital medical information. Various encryption methods have been used at different stages for protecting the data. A modification can also be added, along with the medical images that were generated a video was tried to be compressed and encrypted.

References

1. Suoa, H., Wan, J., Zoua, C., Liua, J.: Security in the Internet of Things International Conference on Computer Science and Electronics Enginerring (2012)
2. Babar, S., Mahalle, P., Stango, A., Prasad, N., Prasad, R.: Proposed security model and threat taxonomy for the internet of things (IoT) (2012)
3. IoT device security based on proxy re-encryption. IEEE Trans. Cybern.
4. A lightweight and flexible encryption scheme to protect sensitive data in smart building scenarios. https://www.researchgate.net/publication/322906864. Department of Information and Communication Engineering, University of Murcia, Murcia, Spain 2 FINCONS SpA, Bari, Italy Corresponding author: Salvador Prez (e-mail: salvador.p.f@um.es)
5. A survey on authentication techniques for the internet of things. https://www.researchgate.net/publication/320028921. A survey on authentication techniques for the internet of things/download. https://www.researchgate.net/publication/320028921 (July 2017)
6. Identity-based authentication scheme for the internet of things. https://www.researchgate.net/publication/306301807, 9–10 April 2016 Paper June 2016
7. Authentication and access control in e-health systems in the cloud. https://ieeexplore.ieee.org/document/7502258 Paper 9–10 April 2016
8. E-health care and le hierarchical encryption. In: International Conference on Information, Communication Embedded Systems (ICICES 2017)
9. Attribute based encryption for secure sharing of E-health data https://www.overleaf.com/project/5b90a960903c3733c4aef07f. IOP Conference Series: Materials Science and Engineering, vol. 263, p. 042030 (2017). https://doi.org/10.1088/1757-899x/263/4/042030

Review on Evacuation Systems for Indoor Fire Situation

Pallavi S. Ghorpade(✉) and Shilpa K. Rudrawar

School of Electrical Engineering, MIT Academy of Engineering, Pune, India
psghorpade@mitaoe.ac.in, skrudrawar@etx.maepune.ac.in

Abstract. Casualties and huge losses could result from fire disasters in buildings. On the event of fires, evacuation from an isolated place of course becomes difficult and complicated due to factors such as fire spread, panic in evacuee movement and consequent congestion, failure in communication due to errors and delays, etc. This paper aims to compare competitive algorithms used for the calculation of shortest paths or the safest paths to mitigate the problem of evacuation. It also reviews corresponding evacuation models implemented in the past. By comparison with all existing methods, challenging issues are discussed, which should be met to enable basic requirements of an evacuation routing system. We conclude by underlining future directions towards enhancing the abilities for fire evacuation.

Keywords: Evacuation · Emergency · Routing algorithms · Safest path · Congestion

1 Introduction

Fires cause destruction and devastation, costing the lives and livelihoods of people. With increased housing density, it has never been more important to protect against fires and to detect fire risks [1]. Building structures are progressively becoming complex. Innumerable individuals travel through them constantly. Fitting to this intricacy is fundamental to secure lives and comply to safety standards. In the event of fire emergency, individuals' lives are put at risk, and this causes a quick movement of individuals needing to escape from the hazardous area. This brings in the need of emergency navigation systems, as a way of managing safety exit of evacuees when indoor fires occur. It is a corporate practice to make individuals go through pre-planned evacuation drills to make sure that they know how to escape through the infrastructure they are into. Work site readiness is essential, not only to reduce emergency mortality rates, related to emergency events, but also for creating a culture and climate of emergency preparedness. These is also a growing body of evidence that this type of culture can support worker resiliency and help reduce long-term mental health consequences of disaster survivor-ship. Furthermore, a culture and climate of preparedness may empower personal responsibility for employees actions. By understanding their role in supporting the safety of the entire population of occupants, employees may be more likely to ensure that they are personally as well prepared as feasibly possible [2].

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 28–37, 2020.
https://doi.org/10.1007/978-3-030-37051-0_4

However, this does not realistically picturize the real emergency and dynamics of the fire situation.

Guaranteeing that alarm and evacuation systems frameworks are reliable and productive is the need of the hour. Major trends in the market of fire alarm systems focus on detection systems, put in place for protection of the building population in case of fire and gas leakage. These systems monitor building areas for harmful gases and fire, and provide warning in advance so that appropriate mitigation actions can be taken in a reasonable time. According to Inderpreet Shoker, in the survey report of Fire Alarm Systems Global Market Research for the span 2017–2022 report, growing consciousness about fire protection systems and the perceived benefits of advanced technology for fire prevention are accelerating growth in the fire alarm market. Moreover, investments tend to be associated with retrofits or replacement projects or modernization in developed nations, while developing countries like China, India, etc. are undergoing massive growth propelling investment in grassroots projects. The market of Intelligent Evacuation Systems mainly focuses on software and hardware solution integration developed to promote the individual safety measures in emergencies [3]. Such systems provide a format of alert and notification supporting smooth and trouble - free evacuation during fire situation. Trends are mainly into visual and acoustic alarming for people with impaired hearing, multilingual voice alarming. The market for smart evacuation systems is impacted by increased demand for technologically sophisticated products, increased need for rapid response management for emergency, and supportive regulatory structure.

Egress models, are computer simulation models for fire evacuation which anticipate the time for inhabitants of a building structure to evacuate. Many egress models are like zone models, which determine the time to the beginning of illogical conditions in a building. Egress models are frequently utilized in performance-based design analyses for code compliance of alternative design and for figuring out during egress, where the blockage zones would probably develop. EESCAPE, Simulex, building EXODUS, EGRESS, ELVAC, EVACNET4, EVACS, EXIT89, EXITT, PATHFINDER, are some of the egress models developed for fire evacuation in the past. The next section discusses the different approaches proposed as a solution to fire emergency evacuation.

2 Literature Review

2.1 Building Information Modelling (BIM)

In 2014, Wang et al., highlighted how to employ BIM as a detailed building information supplier, to work with virtual reality, together building an adaptable immersive serious game environment to provide real - time guidance on fire evacuation. This idea utilized an adjustable A* algorithm and layered grid graph for responding towards a scenario of building emergency using a database of Apache, My SQL and PHP [4]. Ma, J., Jia, W., Zhang, J., proposed a BIM for guidance about three-dimensional building within the considered evacuation path. Through complete integration of virtual reality technology with BIM, the proposed system aimed at forming a management platform,

through which evacuation drills become more convenient and management personnel can direct the rescue operation more accurately [5].

2.2 Agent-Based Modelling

The evacuation model proposed in [6] simulated a more realistic pedestrian/evacuee movement within a cell-based environment. By taking care that agents don't only move to an adjacent cell having lowest distance cost or the nearest node to final target for more than one node with the equal lowest cost, agents being forced to move to the same grid location is avoided by their modified algorithm, (by using priority queue flood fill and A* algorithm) enabling the pedestrian movement to be determined by step numbers and directions instead of the calculated costs.

Bakar et al., in [7] focused on the unpredictability that comes in human movement during fire emergency, due to panic behaviours, and therefore proposed a simulation model based on Agent-Based Simulation (ABS) and Social Force Simulation (SFS) Model to improve on fire evacuation modelling in a restricted space such as a building.

Richardson et al., suggested a model of micro as well as macro - pedestrian dynamics composed of a space-continuous agent based representation (micro - level) and a compressible continuum flow model (macro - level) in [8]. He also established, that there is a strong impact on evacuation time when actual number of people with surroundings knowledge falls below a certain threshold. Their simulations indicate that even in some cases, having environmental knowledge raises the risk of smoke and fire exposure, possibly because, alternatives other than the fastest exit route are not seriously considered.

2.3 Network-Optimization Based Algorithms for Fire Evacuation

Barnes et al., in [9] proposed graph based solution for fire evacuation, capable of incorporating 3D cases naturally, nodes are sensors of the network, but specialized nodes for isolated floors/exits are not used. $F_{u,v}$ is time taken for a hazard to spread from the sensor locations u to v; $R_{u,v}$ is time for a human to navigate from the sensor location of u to v. (these are Hazard weight and Navigation weight resp.)

Suppose at a moment, if a number of fire hazard locations are detected by the WSN, then a hazard time H_u for each graph's node, calculated by graph traversal, will be, as stated in Eq. (1), with u_0 hazardous,

$$H_u = \min\left\{ \sum_{i=1}^{n-1} F_{u_i,u_{i+1}} : (u_0, ..u) \right\} \tag{1}$$

Calculation for a paths' safety can recursively be as, Eq. (2),

$$S((v_{exit})) = H_{V_{exit}} \ldots (\text{hazard time to reach exit}) \quad (2)$$

Also, if safety path $p = (v_1, v_2, \ldots v_{exit})$ is known, below path 'p' in Eq. (3), has the safety value as stated in Eq. (4).

$$p = (v_0, v_1, v_2, \ldots v_{exit}) \quad (3)$$

$$S(p_1) = \min\{ S(p) - R_{V_0,V_1}, H_{V_0} \} \quad (4)$$

By assuming that a building has a fire hazards sensing network is efficiently deployed, to detect fire in early stages, the model by Tabirca et al., in 2009 uses a dynamic navigation graph to monitor the fireside dynamics along with progress of evacuation, to make sure that evacuees keep safely sooner than the hazard. Instead of distributed approaches in [9], it creates a dynamic graph by centralized computation, where the arc weights change after some time contingent upon the fire hazard presence, the arc weight represents the anticipated time to travel alongside the arc and this fluctuates depending upon the time at which the arc is traversed with respect to the incoming danger. This study lays the proposition that the dynamic cost function in shortest dynamic path problem satisfies the FIFO rule, also calculates and ensure that safe transitions, that are, maximum amount of times one can safely delay at the start node, are finite. Additionally, that these safety values are decreasing over time is also established by this paper [10]. The dynamic model generates information estimated on the dynamics of the fire hazard; and then generates a set of dynamic weights of navigation $c^t(u,v)$ portraying the time required to actually walk between two neighboring locations u and v. Also, the model continues to generate a series of dynamic centrality indices that provide useful data on each node's importance entire process of evacuation order.

2.4 Behavior Based Modelling of Crowd in Fire Emergency

From values based on experimental research, the variability factor, of physical abilities of standard occupants and people having permanent or temporary locomotion impairment, in a music festival area was accounted by their approximate unrestricted distribution of walking speed. This evacuation model, by Ronchi et al., in [11], incorporates these distributions in order to reproduce human behaviour during evacuation, for e.g. delay time distributions, etc. Individuals movement was replicated within Pathfinder by investigating the embedded multi-agent based continuous evacuation models to deliver estimates of the time curves for people-evacuation in connection to various evacuation scenarios. With quick responders' evacuation overlapping, in the overall evacuation, route choice is simulated using the model's default algorithm, which has a locally quickest path planning approach, i.e., courses/routes are positioned hierarchically utilizing nearby data about individuals' location and exits' queuing times.

Radianti et al., proposed a dynamic Bayesian network (DBN) based model which underpins crowd behaviour of distinct kinds during evacuation, and is predicated on studies of physical fire models, crowd psychology models, and corresponding flow

models. Their proposed Crowd Evacuation Model is implemented with SMILE engine and simulated by GeNIe Modeler and is such that it keeps track of people's location, people's flow until their escape, and hazard development status at these locations, at consequent time steps [12]. In [13], Lu et al., captured anxiety's impacts on route opted for and ability to interact with psycho-logical features such as guidance and herding responses. This is achieved by using an optimization framework where the number of planning steps and values of psychological parameters are affected by anxiety. To validate their approach, anxiety levels have been manipulated by hazardous conditions and the lengths of planning horizon are assessed by comparing extracted route options with data in Virtual Reality experiments. Aiming to optimize the distribution and composition of the occupants, estimate strategies for evacuation, and consequentially increase the efficiency of evacuation, Hu et al., in 2018 studied influence by human and fire factors and by their interaction on an evacuation process, which was based on typical assumed exit choice strategies [14]. In a systematic view, they set fire to 50000-kJ/kg combustion value, and correspondingly the temperature, height, and CO and CO_2 concentrations of smoke layer for ignition room, corridor staircase were all assumed. To reflect the exit balance situation and efficiency of whole evacuation, they took the weighted value δ as the experiment index, expression of which is as stated in Eq. (5),

$$\delta = 0.8 * \frac{\text{required safety evac.time}}{\text{total evacuee number}} + 0.2 \times \text{occupant pass situation} \tag{5}$$

2.5 Multi-objective Optimization Based Approaches for Fire Evacuation

Shikhalev, D., Khabibulin, R., Wagoum, A., in 2014, in [15] formulated the optimization problem, constraint being, to minimize the following assumed criteria: 'information regarding usage of the current section', 'criterion of timeliness that leads away from routes where fire hazards could be reachable', and the 'relative physical length of the current section'. The problem was hence, to calculate the safest escape route for person N_1, N_2…, N_i from the starting positions m_1, m_2,…, m_i to the safety areas s_1, s_2,…, s_i. They used a safest path criterion φ as optimization, stated in Eq. (6),

$$\varphi = \sqrt{(\alpha.a_i)^2 + (\beta.b_i)^2 + (\gamma.l_i)^2} \tag{6}$$

Here weight coefficients α, β, γ at a_i, b_i, $l_i \rightarrow$ min, where i = 1,..,n. are added for importance regulation of the individual criterion. On calculating φ, determination of an optimal escape route is achieved using the Floyd Warschall algorithm, means of which are expressed below, stated in Eq. (7). Here, d_{ij}^{m} denotes shortest distance between vertices 'i' and 'j'; 'm' is the intermediate vertices between of the path.

$$d_{ij}^{m} = \min\left\{d_{im}^{m-1} + d_{mj}^{m-1}, d_{ij}^{m-1}\right\} \tag{7}$$

Cisek and Kapalka, in [16], considered a queuing system concept, in an evacuation process simulation. Upon starting a simulation, current data from a movement sensing system will initiate an amount of people in it in individual nodes. In the process of moving of evacuees from a given room to a door, time at which each person in i^{th} room arrives at j^{th} room's door is calculated based on Eq. (8),

$$T_{ij}^{n} = T_i + \frac{L_{ij}}{v_i * P_i(0)} * n \tag{8}$$

Here 'n' denotes person's number, v denotes mean speed of movement within a room, P denotes number of individuals present there, 'L' defines travel distance. For entities migrating between rooms 'i', 'j', the time to attain then the next doors, is determined by the fraction $(L_{i\ j\ k})/(v_j)$.

Another type of queuing system additionally considers possibility to include density - dependent changes in the pace of movement. Basically, the time F_{ij} between rooms to cross the doors is determined product of 'F' and 'W_{ij}', 'F' giving the assumed maximal flow of individuals, and 'W' denoting door width between rooms. To analyse the efficiency of their model, a series of simulation experiments was conducted for a selected building, which was assumed to be occupied by 450 people. They summarized the results to indicate that the evacuation time is cut shorter when the system of evacuation routing is put to use in situation where hazard is not taken into account. The evacuation time with guidance is longer in cases where a hazard is present; however, the forecasted death toll is smaller, particularly for people's uneven distribution in the endangered area [16].

2.6 Some Interdisciplinary Frameworks

Using artificial systems for testing prearranged emergency plans, parallel execution and computational experiments, Hu et al., [17] in 2014 proposed an approach based on cyber physical - social systems (CPSS), in which it is possible to fully connect with building structures, fire scenarios, safety managers and evacuees. According to this study, construction of data-driven parallel mechanisms implemented between artificial and physical evacuation systems, can potentially help to achieve real time guidance for evacuation.

Liu et al., assumed deployed sensors for determination of state whether a considered building area is blocked or transitable. A communication network carries the sensor information and the central server aggregates it. Here, using a collection of those transitable areas, calculation of evacuation paths, is done on the A* algorithm basis. The central server computes in real-time, the evacuation route, and again through the communication network, sends the recommendation information to the evacuee/occupant. For validation at model level, their fire model assumed fire with constant spreading direction and speed. Their simulation results showed that routing using a safety margin

distance has the potential to increase the success ratio for evacuation during spreading fire scenario [18].

3 Challenging Issues in Existing Systems

3.1 Complexity of Decision-Making

Modelling of fire emergency management can be done as a problem of optimization (can be of a nonlinear combinatorial nature) in order to allocate resources to tasks thereby minimizing overall costs also. Because classical optimization algorithms can be easily get stuck in local minima and exact solutions, and can be computationally expensive as well as time-consuming, therefore, meta-heuristics algorithms inspired by natural and artificial intelligence have motivated considerable research.

Although heuristic algorithms cannot guarantee that the optimal solution will be discovered, they can in polynomial time find a suboptimal solution. Li et al., in [19] during 2018 researched on evacuation for fire in a library of a University, concluding that dense population and evacuation channels which are relatively narrow, lead to congestion, due to which velocity of safe evacuation is greatly reduced. For their case, exit was the first to attain the dangerous state. Moreover, it was observed that hazardous area's direction was paradoxically the direction of safe evacuation. Also, people quickly flocked on the exit causing congestion. Therefore, route indicator, emergency exit and lighting, along with fire alarm system required improvement.

3.2 Route Searching

Available static evacuation plans in most buildings possess drawbacks when environment/conditions for evacuation, change during severe fires. Moreover, evacuees or end-users with a disability, due to limitations in their movement, may need the safest evacuation route instead of the shortest. Therefore, it is necessary to further investigate more onto the choice of precise and reliable path finding algorithms for their type of situation.

3.3 Communication Delays and Network Security

Majumder et al., showed that their entire system which was an IOT based model currently takes 25 to 40 s from sensing the fire to correctly updating the website. Using a dedicated server for hub processing could significantly improve speed [20]. Hence, a need to incorporate the support of a robust network coupled with adequate data transmission is felt in most of the approaches reviewed. Wireless sensor networks are usable, but their deployment is particularly prone to denial of service and denial of sleep attacks due to dependency on computing power, memory, bandwidth and battery power. Also for approaches which consider centralized mechanisms for route calculation, need higher speed data transmission for overall shrinking of recommendation updation to the concerned evacuee.

4 Conclusion

In this paper, we discuss different approaches developed for fire emergency management and the challenging issues that need to be addressed to enable the requirements for these approaches. Decision - making complexity, optimization of algorithms, route search, network security, and energy - efficient management are key research issues for any emergency management evacuation. In addition, multidisciplinary collaborative research is highly needed to design future fire evacuation management systems due to requirement of including technologically different elements in system design, followed by interface. Finally, we conclude by highlighting below, a few directions for future research in this area.

4.1 Updation of Dynamic Signs with Enhanced Frequency

While the objective of formulated algorithms for evacuation would ultimately be of their integration into an evacuation system using dynamic indicators to provide recommendations/instructions of safe directions during evacuation but theoretically different considerations come into picture. More frequently upgrading the dynamic signs provide sharper command over the evacuees, allowing the system to approach an optimal solution more closely. However, potentially allowing the recommendations to update directions too often lowers the evacuee compliance, because evacuees observe the switching directions/signs as they reach them, it may confuse them regarding which specific instructions to obey. Therefore, the update rate should be a balance that delivers adequate and decent performance while maintaining the evacuee's compliance. Also, the lack of information about the evacuees who actually respond to dynamic and predicted signs would deter the research from reaching a final conclusion.

4.2 Performance Gauged During Low-Occupancy Scenarios

For scenarios of high - evacuee headcount, several systems tend to perform better. Evacuating crowded buildings takes longer, and this allows the signs to perform more updates or time steps, thus better distributing the evacuees across different paths. On the one hand, desirable feature can be improved performance in crowded buildings as fire scenarios inherently carry a higher risk. On the other hand, the system developer's initial objective can be to design a system that minimizes the evacuation time regardless of the building's distribution and number of evacuees. However, as the number of evacuees decreases, congestion is increasingly becomes a predominant factor. This inherently makes it far less relevant to a dynamic congestion management system. For systems which aim at Congestion - Optimization, will have a low operating when limit headcount evacuee is considered.

4.3 Performance of Simulation Models

In short, simulation of personal actions in evacuation being complex, till now, there is no single model that can fully resolve the different aspects of evacuation behavior. However, it can be anticipated that more details will be contained in the future

evacuation model, moving towards prediction of individual behavior, simulation of large populations and complex characteristics along with managing the complex inter-dependencies between the infrastructure, environment and human behavior. A proper, relevant criterion for validation of decision making and calculated route also needs to be investigated.

5 Future Research Plan

For widespread infrastructures, since it would be difficult for its facility users or visitors to navigate from one location to the other, and this issue could aggravate in the times of emergency; also, GPS-based navigation does not work indoors, hence there arises a need to have any application in place to guide users with the shortest route within the facility, based on floor maps, to their destination; thereby enabling the users to exit on time, safely. Also for emergency of fire, management should be empowered with high speed ethernet solutions. So, the future aim is to study on embedded aspect, that is, hardware solution, that can be provided to this problem. The above different approaches given by various researchers in the past, can't just be compared for their superiority, but their collective working on multicore processor architechture, is aimed to be developed for more dependable outcomes.

Acknowledgements. Firstly, I extend my sincere gratitude to my guide, Shilpa K. Rudrawar, for her useful advice and suggestions, helping me to learn how this topic could be studied indepth. Special thanks to my parents, for their support.

References

1. ISO and Construction, ISBN 978-92-67-10779-0 (2017)
2. Gershon, R.R.M., Magda, L.A., Riley, H.E.M., Sherman, M.F.: The World Trade Center evacuation study: factors associated with initiation and length of time for evacuation. Fire Mater. **36**, 481–500 (2012)
3. Fire Alarm Systems Market Driven by Rapid Growth in Developing Nations. ARC AdvisoryGroup. https://www.arcweb.com/press/fire-alarm-systems-market-driven-rapid-growth-developing-nations
4. Wang, B., Li, H., Rezgui, Y., Bradley, A., Ong, H.N.: BIM based virtual environment for fire emergency evacuation. Sci. World J. **2014**, 1–22 (2014)
5. Ma, J., Jia, W., Zhang, J.: Research of building evacuation path to guide based on BIM. In: 29th Chinese Control and Decision Conference (CCDC), pp. 1814–1818. IEEE Press, Chongqing (2017)
6. Roan, T.-R., Haklay, M., Ellul, C.: Modified navigation algorithms in agent-based modelling for fire evacuation simulation. In: The 11th International Conference on Geo Computation, pp. 43–49. London (2011)
7. Bakar, N.A.A., Adam, K., Majid, M.A., Allegra, M.: A simulation model for crowd evacuation of fire emergency scenario. In: 2017 8th International Conference on Information Technology (ICIT), pp. 361–368. IEEE, Amman, Jordan (2017)

8. Richardson, O., Jalba, A., Muntean, A.: Effects of environment knowledge in evacuation scenarios involving fire and smoke: a multiscale modelling and simulation approach. Fire Technol. **55**(2), 415–436 (2018)
9. Barnes, M., Leather, H., Arvind, D.K.: Emergency evacuation using wireless sensor networks. In: 32nd IEEE Conference on Local Computer Networks (LCN 2007), pp. 851–857. IEEE, Dublin, Ireland (2007)
10. Tabirca, T., Brown, K.N., Sreenan, C.J.: A Dynamic model for fire emergency evacuation based on wireless sensor networks. In: 2009 Eighth International Symposium on Parallel and Distributed Computing, pp. 29–36. IEEE, Lisbon, Portugal (2009)
11. Ronchi, E., Uriz, F.N., Criel, X., Reilly, P.: Modelling large-scale evacuation of music festivals. In: Case Studies in Fire Safety, vol. 5, pp. 11–19. Elsevier (2016)
12. Radianti, J., Granmo, O.-C., Sarshar, P., Goodwin, M., Dugdale, J., Gonzalez, J.J.: A spatio-temporal probabilistic model of hazard-and crowd dynamics for evacuation planning in disasters. Appl. Intell. **42**, 3–23 (2015)
13. Lu, X., Luh, P.B., Tucker, A., Gifford, T., Astur, R.S., Olderman, N.: Impacts of anxiety in building fire and smoke evacuation: modeling and validation. IEEE Robot. Autom. Lett. **2**, 255–260 (2017). https://doi.org/10.1109/LRA.2016.2579744
14. Hu, Y., Wang, F.-Y., Liu, X.: A quantitative study of factors influence on evacuation in building fire emergencies. IEEE Trans. Comput. Soc. Syst. **5**(2), 544–552 (2018)
15. Shikhalev, D., Khabibulin, R., Wagoum, A.: Development of a safest routing algorithm for evacuation simulation in case of fire. In: Proceedings of the 6th International Conference on Agents and Artificial Intelligence, pp. 685–690. SCITEPRESS—Science and Technology Publications, ESEO, Angers, Loire Valley, France (2014)
16. Cisek, M., Kapalka, M.: Evacuation route assessment model for optimization of evacuation in buildings with active dynamic signage system. Transp. Res. Procedia. **2**, 541–549 (2014)
17. Hu, Y., Wang, F.-Y., Liu, X.: A CPSS approach for emergency evacuation in building fires. IEEE Intell. Syst. **29**, 48–52 (2014)
18. Liu, J., Rojas-Cessa, R., Dong, Z.: Sensing, calculating, and disseminating evacuating routes during an indoor fire using a sensor and diffusion network. In: 2016 IEEE 13th International Conference on Networking, Sensing, and Control (ICNSC), pp. 1–6. IEEE, Mexico (2016)
19. Li, M., Zhu, S., Wang, J., Zhou, Z.: Research on fire safety evacuation in a university library in Nanjing. Procedia Eng. **211**, 372–378 (2018)
20. Majumder, S., O'Neil, S., Kennedy, R.: Smart apparatus for fire evacuation—an IoT based fire emergency monitoring and evacuation system. In: 2017 IEEE MIT Undergraduate Research Technology Conference (URTC), pp. 1–4. IEEE, Cambridge, MA (2017)

A Healthcare Application Model for Smarthome Using Frequent Pattern Based KNN Algorithm

Amrutha Raveendran(✉) and U. Barakkath Nisha

Department of CSE, ICET, KTU University, Kerala, India
amruthanairicet@gmail.com, ubnisha@gmail.com

Abstract. Nowadays most of the people are moving from rural to urban areas and they would rather prefer the advanced healthcare applications in their daily life. So in this century, the studies behind this idea are growing fast. In urban areas most of the homes are being equipped with smart devices and therefore the scope of the healthcare applications in this area can be done without any awkwardness. In this paper, the data collected from the smart devices can be used as the source data for this purpose. The human activities are monitored by the proposed system. From this huge data the patterns are being recognized by the use of Frequent Pattern mining and the appliance to appliance and appliance to time associations are built using incremental k-means clustering algorithm. The activity prediction will be done by frequent pattern based KNN algorithm. This system can predict the human activity pattern along with greater accuracy for the purpose of healthcare applications.

Keywords: Frequent pattern mining · Incremental K-means clustering · Frequent pattern based KNN algorithm

1 Introduction

You will find here In this century most of the people are migrating to urban areas, and most of them are staying alone. So in this situation, the role of healthcare applications in smart homes are relevant. Many discoveries are carried out in this area. The senior citizen people are taking advantage of this thought. Monitoring everyday routines is the key role for developing such a tremendous work. Anomalous activity of people can be recognized by the everyday routines. The idea behind the paper will be useful not only for the old age people who stays alone at home but also for individuals who are busy with their work.

This arise the need for new concepts in cities to invest in digital transformation. Currently, in urban areas most of the homes are being equipped with smart devices which help to monitor their activities and thereby more concern to their health. The data collected from the smart devices are the main source of inspecting a person's habit. The usage of appliances may be related with creating patterns and locating their regular activities. By monitoring these patterns, a hasty change can be noted.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 38–48, 2020.
https://doi.org/10.1007/978-3-030-37051-0_5

For the evaluation of the proposed mechanism this research uses the UK Domestic Appliance Level Electricity Data Set (UK Dale). The readings collected from the smart meters help us to find the behavioural changes of the individuals and thereby providing a solid data for the healthcare applications. The measures are related to the day to day activities of the human beings. For example if the music system is in "ON" state this can be associated with the human activity of "Leisure time". Another example is, if the Microwave oven and the Music System is in "ON" state, we can associate "Food Preparation" and "Listening to Music together. In this way we can predict what type of operations are done together by multiple appliance usage with respect to time. The appliance-appliance usage and appliance-time associations are detected by this observation and we propose different mining schemes that continuously mine the data for sorting out the associations.

Here we take advantage of K-nearest neighbors algorithm (KNN). We are not using the algorithm directly to this model, but we are using an advanced version by the help of frequent patterns. So here we can say this as frequent pattern based KNN algorithm. We have derived this algorithm from the basic KNN algorithm. The main contributions are: We present a human activity pattern based on appliance usage of individuals in smart homes. For the pattern recognition we make use of Frequent Pattern mining algorithm and for identifying associations between appliance and time k-means clustering algorithm is utilized. Based on the individual and multiple appliance usage activity predictions can be done and for this purpose we apply our new frequent pattern based KNN algorithm.

The leftovers of the paper are organized as follows: Sect. 2 is explained some related literature reviews of our proposed algorithm. Section 3 presents the proposed approach and methodology. Section 4 interns experimental evaluation based on real data set. Section 5 explains the comparison results. Finally the Sect. 6 explains the future work for concluding the paper.

2 Related Work

To understand the behavioural pattern of person who is staying alone, is the main goal to achieve. In this section we scrutinize the existing work to analyse the occupant's behaviour.

Mining human activity patterns from smart home for healthcare applications by using Bayesian network is carried out in paper [1]. Here make use of incremental frequent pattern mining algorithm for pattern recognition and appliance–appliance associations. K-means clustering algorithm is used for appliance-time associations. To build the activity prediction model, the integration of these results are given to the Bayesian network which is a directed acyclic graph. It not only gives the activity prediction but also the appliance to time associations to learn about the use of multiple appliances. The work in [2] proposes data mining techniques for detecting house hold characteristics based on smart meter data. Here the raw data is collected from the smart home by using a smart meter. After the data preparation, some algorithmic approaches are used for detecting the patterns. The paper conveys hierarchical clustering, C-Means Clustering and Multidimensional scaling algorithms. The collected patterns can be used

either for the health care applications or to help the consumers understand their energy usage.

Mining Human Activity Patterns From Smart Home using Map Reduce algorithm [3] illustrates how Big Data algorithm provide accurate results whether a person suffers with any kind of health problem by mining the person's frequent activity patterns generated by the smart appliances. The MR-growth algorithm uses Map Reduce to mine frequent patterns from huge amounts of uncertain data.

The Bayesian Network which is an acyclic graph where nodes represent random variables and edges represent probabilistic dependencies, is used for the activity prediction model. After extracting the frequent patterns of human activities, a clustering analysis mechanism is used to discover appliance usage periodically. A Health Care Service Model Using Human Activity Patterns [4] encapsulates how the health care application works by make use of the data from smart meters. The mapping is done by frequent pattern association mining and clustering. The paper has adopted the SVM Classifier technique for predicting the individual's behaviour.

3 Proposed System

Our proposed model for healthcare application begins with the collection of data. We have collected the data from five houses from United Kingdom. The proposed work starts by cleaning and preparing the data and then applying the frequent pattern mining algorithm. The result of this mining gives us the frequent patterns of appliances which are used by the person. i.e. the appliance-to-appliance association.

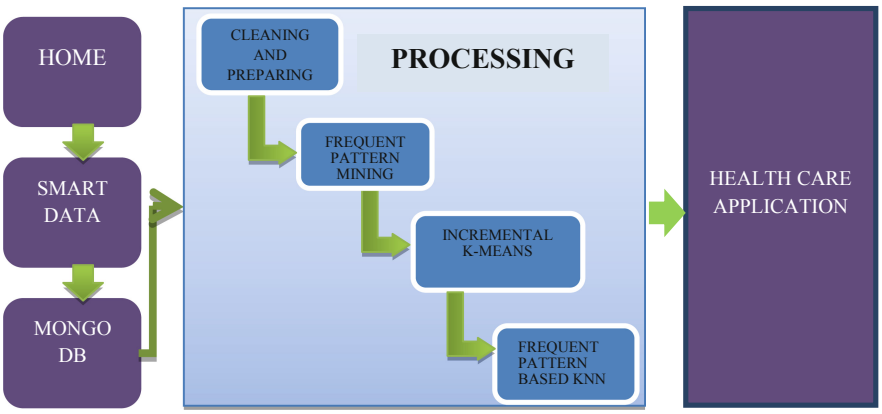


Fig. 1. Proposed model for frequent pattern mining and activity prediction

After that we are using the k-means clustering algorithm to determine the appliance-to-time associations. With these two processes, the system is able to extract the pattern of appliance usage which is then used as input to the new frequent pattern based KNN algorithm for activities prediction. The output of our model can be used by

the healthcare applications. They can monitor the daily activities of people who lives alone at home or people who are busy with their work. They can use the benefits of this output for better assistance.

Figure 1 instantiates the new model which helps us to create our system for the activity prediction. The model explains us, how to mould our proposed system. The data is collected from the houses through the smart meter data. The data can be kept in the database. The collected data may go through three important steps which are frequent pattern mining, incremental K-means, and the frequent pattern based KNN. After going through these unique steps we will get the result which tells the activity prediction. This can be useful to the healthcare applications.

3.1 Preparation of Data

In this paper we have used a collection of data from smart meters in United Kingdom. The data set contains millions of raw data. The data contains noises which have to be removed. In the first step of processing the cleaning procedure is done to remove the noises from the data and ready for mining. After the cleaning procedure the dataset will be reduced.

The Table 1 shows the examples of ready to mine source data which contains the appliances which are active in one hour. Here in between 07:00 and 08:00 Four appliances are active, laptop speaker and washing machine. Table 2 illustrates clustering source database. Here 'time of the day' and 'hour of the day' have been mentioned. These examples have taken four appliances from one house with the start time and end time of each appliance usage. The time of the day measures morning, afternoon, evening sessions in a day. Table 1 shows the appliances which are active in diffrent hours of the same day.

Table 1. Ready-to-mine data

Date	ST	ET	Active appliances
2013-10-20	07:00	08:00	Laptop, Speaker, Washing Machine
2013-10-20	08:00	09:00	Laptop, Speaker, Dish washer
2013-10-20	09:00	10:00	Laptop, Speaker
2013-10-20	10:00	11:00	Speaker
ST-Start Time	ET-End Time		

3.2 Selection of Frequent Patterns of Human Activities

By the use of these, we have to discover the human activity patterns from smart home data. By discovering the human activity patterns, we can find the associations between the appliances and thereby finding the appliances which are working together [7]. By the use of these frequent patterns, the healthcare applications can monitor the individuals and if some irregular patterns are found, they can send the alert to the hospital or to the emergency sector.

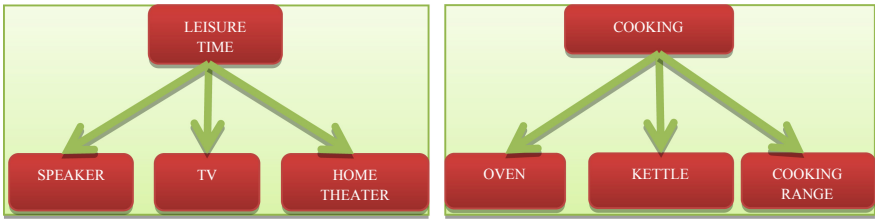


Fig. 2. Feasible relationships between usage and daily activities

Some regular activities such as "Watching TV, preparing food, listening music, using laptop"are the examples which can be used for monitoring the personal routines. The aim is to detect the patterns of these activities and from which the application can recognize the frequent patterns which help to check the irregular activities of patient's behaviour. All the appliances that are active in one-hour time interval are included in the source database. This is used for the frequent pattern mining. Here incremental frequent pattern mining algorithm [15] is used for extracting the patterns from the daily behaviour. Our first aim is to discover the patterns of daily activities of people.

For finding the patterns we can consider the individual appliance usage and the appliance to appliance usage. Incremental frequent pattern mining algorithm is used for this task. The task for the frequent item set mining algorithm is then to find all common sets of items, defined as those item sets that have at least a minimum support. Once a set of frequent item set has been found, association rules can be generated. By the use of this we can identify the patterns that are frequently performed.

Let S be the set of all item sets S = {s1, s2, s3…sn}. Here the item sets are the appliances which are active. For the frequent pattern mining, we measure the support and confidence of the item sets. Minimum support is some threshold value which is predefined.

Table 2. Clustering source data

Appliances	Time of the day	Hour of the day
Laptop	07:00–08:00	M
Speaker	08:00–09:00	E
Washing machine	10:00–11:00	A
M-Morning	E-Evening	A-Afternoon

Figure 2 illustrates the feasible relationships between usage and daily activities. For example in leisure time, the TV, speaker and home theatre might be worked together. Similarly in cooking time the appliances such as oven, kettle, and cooking range can be worked together. So this possible relationships show us the possible frequent patterns.

Table 3. Example for appliances active in 24 h

Hours	Appliances active		
12:00–12:59	Laptop	Monitor	Speaker
13:00–13:59	Laptop	Monitor	Router
01:00–01:59	Laptop	Router	
06:00–06:59	Washing machine	Oven	Kettle

Algorithm 1 describes incremental frequent pattern mining [10] procedure and the algorithm calculates the appliance-appliance association. The output of this algorithm tells which appliances are being used frequently and which are combined together. The result in Table 3 shows the active appliances in 24 h. For example in an hour between 12:00–12:59, laptop, monitor, speaker are active. Similarly in between 01:00–01:59, the appliances such as laptop and router are active. Figure 3 shows the example of active appliance (laptop) that indicate two different activities at home. The energy trace of appliances indicate the human activities such as leisure time, cooking time etc. This example shows the possible relationship between appliance usage and activities.

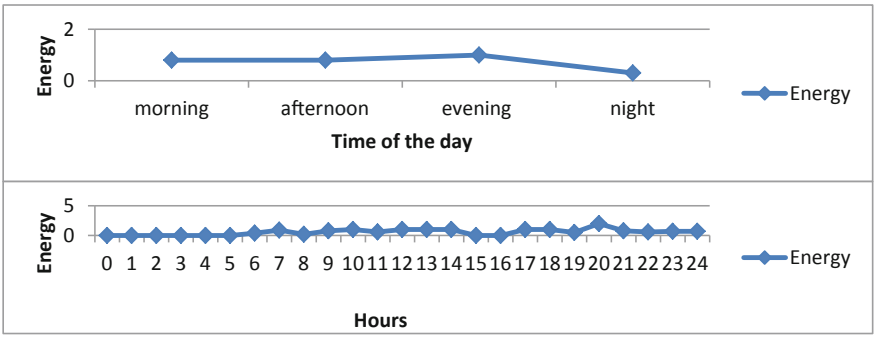


Fig. 3. Example of hour and time of the day for active appliance laptop

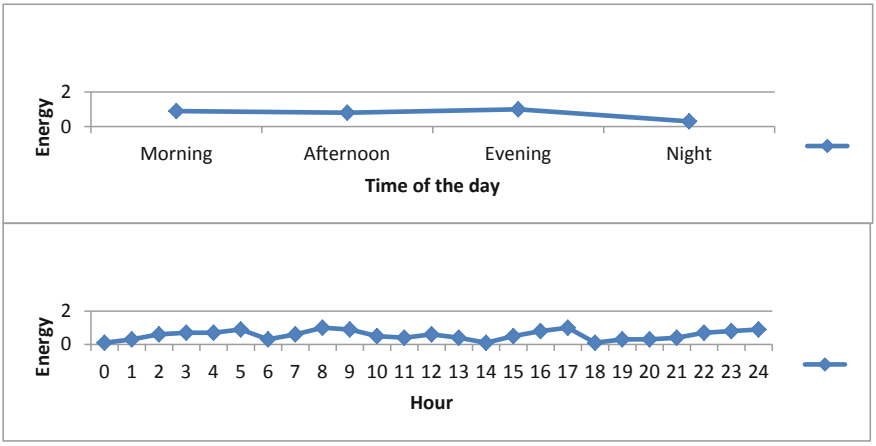


Fig. 4. Example of hour and time of the day for active appliance monitor

Figure 4 shows the active appliance (monitor) as an example. These two figures explain about the active appliances in hourly basis and also in 'time of the day' basis.

The FP-Growth Algorithm [14] is an efficient and scalable method for mining the complete set of frequent patterns by pattern fragment growth. The FP-Growth Algorithm is an effective way to find frequent item sets without using candidate generations, thus improving performance. We have to find the support and confidence of the item sets for frequent pattern mining. Support value will be the number of transactions. A threshold value is defined for minimum support. Confidence is the measure of number of transactions. The support and confidence measures are important for generating the frequent patterns and thereby framing the association rules.

The Table 4 shows the frequent patterns discovered. The output determines the probability of appliances being active concurrently. As an example in an hour between 01:00–01:59 the count of laptop is 8 and the count of router is 6. Like that in an hour between 12:00–12:59 the count of laptop is 3, monitor is 4 and the speaker is 5.

Table 4. Frequent patterns: Frequent patterns discovered

Hours	Frequent patterns		
12:00–12:59	Laptop = 3	Monitor = 4	Speaker = 5
13:00–13:59	Laptop = 8	Monitor = 6	Router = 8
01:00–01:59	Laptop = 8	Router = 6	
06:00–06:59	Washing machine = 3	Oven = 5	Kettle = 5

3.3 Data Clustering by Incremental K-Means

As the dataset is dynamic, to collect all the data objects before clustering is not possible. If we are using non-incremental k-means the re-clustering is needed when new data comes which decreases efficiency and wasting computational resource. To overcome this situation we can replace it with incremental k-means clustering [12]. It updates new cluster to previous clustering results. The K-means clustering algorithm is used to handle incremental data in existing database very effectively [13]. The drawbacks of basic k-means algorithm can be overcome by using this incremental k-means clustering algorithm. The basic k-means algorithm is computationally very expensive [6]. After doing the incremental k-means algorithm we are getting the cluster centroids in hourly basis i.e. 24 h period. We are assigning the value of 'K' as 24 for getting 24 cluster centroids. i.e. finding clusters for every hour.

3.4 Frequent Pattern Based K-Nearest Neighbours Algorithm for Activity Prediction

We make use of this algorithm for developing the new algorithm in our model. We have created a new unique algorithm for our purpose. We can call it as 'frequent pattern based k-nearest neighbors algorithm' [18] which uses frequent pattern, weight of appliances (importance of appliances), and cluster centroid as parameters. This new technique can be used for the classification purpose. The value of 'k' can be taken

randomly for better result. We could use frequent pattern mining in KNN [19]. For example, if we have a database about some users, where each user is a transaction, you could find patterns common to these users, and these patterns could guide the KNN search or be used to generate clusters. Our algorithm predicts based on frequent pattern mining [8].

We are considering frequent pattern, activity matrix, and activity frequency as input to the frequent pattern based KNN algorithm. By using these parameters we can predict the normal and abnormal activities. In this algorithm we consider the frequent patterns of appliances which are used more than five times and the distance between activity matrix of test date and the cluster centroid which is collected from the incremental k-means. Another parameter we have collected is the total score of frequent pattern. By make use of these parameters we can calculate the final score of this algorithm which is used for the activity prediction.

$$\frac{(\textit{Total score of frequent pattern}) + \textit{distance}}{2} = \textit{final score}$$

We introduce a threshold value for the prediction. If the threshold value is greater than the final score, then the activity is normal else it is abnormal.

4 Result Analysis and Discussion

For the evaluation of the proposed model, we performed our experiments using the UK-Dale dataset which contains millions of data collected from UK Energy Research Centre. This is one of the largest dataset having millions of data which can be used for our model. The dataset includes power consumption collected between 2012 and 2015. The dataset contains time series data for five houses with a total of 100+ appliances. The proposed system is developed in JAVA. The main objective of our model is to predict the short and long term activities inside the house along with the appliance usage as an indication of human activity patterns. Our data can lead a key role in healthcare applications for the active monitoring, alert generation etc. along with high accuracy in prediction by the help of frequent pattern based KNN algorithm. Figure 5 shows the detected appliances with probability distribution over 24 h period. Here we have chosen five appliances for explaining the results. They are the appliances such as laptop, washing machine, dishwasher, speaker and treadmill. We have mentioned percentage of working in 24 h period. In Fig. 5 we can see that in between 13:00 PM and 14:00 PM the usage of speaker is high and there is no working of washing machine. Similarly in between 12:00 and 13:00 the usage of laptop and speaker is prominent than other appliances. This information helps us to predict the activity distinctly whether it is normal activity or abnormal activity.

The activity prediction in our proposed model depends upon the total score, we have collected from the frequent pattern based KNN algorithm. The total score and the threshold value tell us the human activity is normal or abnormal. If the final score is greater than the threshold value, then we can predict that the activity is abnormal else it is normal. Figure 6 exhibits the probability distribution of detected appliances for the

day of the week. For example in weekends the working of laptop is low and the working of washing machine is high. By the use of these data, we can calculate daily activities and routines. Similarly in working days the use of laptop is high. This graph shows the percentage of working of appliances in 'day of the week'.

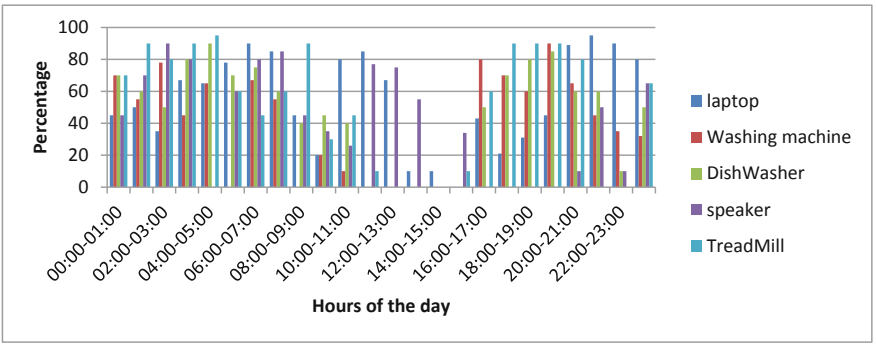


Fig. 5. Probability distribution of detected appliances in 24 h period.

The total score value is calculated form the score which is collected from the frequent pattern mining. The frequent pattern based KNN algorithm calculates the total score which can be derived from the frequent pattern mining.

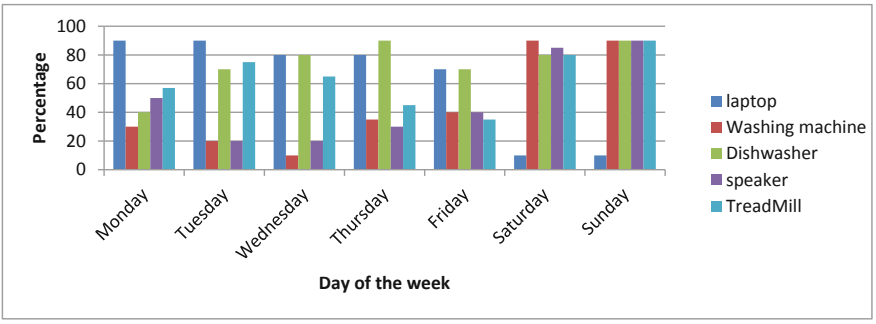


Fig. 6. Probability distribution of detected appliances for the day of the week.

When we get the source data, it goes through the pre-processing stage, where we convert data in hourly basis through the repeated process. Our dataset contains timestamp and the voltage and it should be converted into our time series. For the pre-processing stage we are considering only one month and we are calculating the total usage in hourly basis. After that a matrix is generated which contains the total voltage consumption in every hour. Here a matrix is created for each data. Then activity of appliances is calculated, that is in 24 h which appliances are active. Here we get activity frequency and activity matrix as output. After this process the system is moving to the frequent pattern mining. Here we get the frequent patterns of the

appliances as output. Then incremental k-means processing happens. Here we get the cluster centroids in hourly manner. The KNN algorithm is modified and we are using the modified frequent pattern based KNN algorithm for activity prediction. This algorithm not only calculates the distance between the activity matrix of test date (selected date for prediction) and the cluster centroids but also the final score which depends upon the frequent patterns. This final score and the random threshold value which we are giving tell us whether the activity is normal or abnormal.

5 Conclusion and Future Work

In this paper we have introduced a model for analysing human activity patterns from the smart meter data. Occupant's routines and behaviour follow a pattern that could be used in healthcare applications to track the individuals who lives alone or having self-limiting conditions. The behavioural activities can be recognized from appliance-to-appliance and appliance-to-time associations. For collecting these data, we have presented frequent pattern mining and k-means clustering. For the activity prediction we have introduced a new algorithm known as frequent pattern based KNN algorithm for better accuracy.

For future work we are planning to refine the model in a real time manner. This will help the healthcare applications to send alert to the patients or care providers. This will give a tremendous change in people who lives alone or with limited conditions.

Acknowledgemnet. All Author states that there is no conflcit of interest. We used UK dale dataset (https://jack-kelly.com/data/) in this study.

References

1. Yassin, A., Singh, S., Alamri, A.: Mining human activity pattern from smart home bigdata for health care applications. IEEE Access **5**, 13131–13141 (2007). ISSN: 2169-3536
2. Gajowniczek, K., Ząbkowski, T.: Data mining techniques for detecting household characteristics based on smart meter data. Energies **8**, 7407–7427 (2015)
3. Karpagam, V., Pooja, M.U., Swathi, M.: Mining human activity patterns from smarthome big data by using MapReduce algorithm. Glob. Res. Dev. J. Eng. (2018). ISSN: 2455-5703
4. Nandhini, R., Viswanadhan, B.: A health care service model using human activity patterns. In: International Conference on Applied Soft Computing Techniques (2018). ISSN: 2455-1341
5. Liao, J., Stankovic, L., Stankovic, V.: Detecting household activity patterns from smart meter data. In: International Conference on Intelligent Environments, Department of Electronic and Electrical Engineering University of Strathclyde, Glasgow, UK (2014). ISBN: 978-1-4799-2947-4
6. Yadav, A., Singh, G.: Incremental k-means Clustering Algorithms: A Review. Int. J. Latest Trends Eng. Technol. **5**
7. Zhang, M., He, C.: Survey on association rules mining algorithms. In: Advancing Computing, Communication, Control and Management, pp. 111–118. LNEE 56 (2010)

8. Alghamdi, A.S.A.: Efficient implementation of FP growth algorithm-data mining on medical data. Int. J. Comput. Sci. Netw. Secur. **11**(12) (2011)
9. Ahalya, G., Pandey, H.M.: Data clustering approaches survey and analysis. In: 1st International Conference on Futuristic trend in Computational Analysis and Knowledge Management (2015)
10. Jadhav, J., Ragha, L., Katkar, V.: Incremental frequent pattern mining. Int. J. Eng. Adv. Technol. (IJEAT) **1**(6) (2012). ISSN: 2249 – 8958
11. Gu, J., Zhou, J., Chen, X: An enhancement of k-means clustering algorithm. In: International Conference on Business Intelligence and Financial Engineering, Aug 2009
12. Shah, N.S.: A modified approach for incremental k-means clustering algorithm. IJEDR **3**, 1081–1084 (2015). ISSN: 2321-9939
13. Kanungo, T., Mount, D.M., Netanyahu, N.S., Piatko, C.D., Silverman, R., Wu, A.Y.: An efficient k-means clustering algorithm: analysis and implementation. IEEE Trans. Pattern Anal. Mach. Intell. **24**(7) (2002)
14. Wang, L., Fan, X.J., Liu, X.L., Zhao, H.: Mining data association based on a revised fp-growth algorithm. In: International conference on machine learning and cybernetics, Nov 2012
15. Song, Y., Wei, R.: Research on application of data mining based on fp-growth algorithm for digital library. IEEE (2011)
16. Qi, J., Yu, Y., Wang, L., Liu, J.: K*-Means: an effective and efficient k-means clustering algorithm. In: IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom), Oct 2016
17. Taneja, S., Gupta, C., Goyal, K., Gureja, D.: An enhanced k-nearest neighbor algorithm using information gain and clustering. In: Fourth International Conference on Advanced Computing & Communication Technologies, Apr 2014. ISBN: 978-1-4799-4910-6
18. Sun, S., Huang, R.: An adaptive k-nearest neighbor algorithm. In: Seventh International Conference on Fuzzy Systems and Knowledge Discovery, Sept 2010
19. Jivani, A.G.: The novel k nearest neighbor algorithm. In: International Conference on Computer Communication and Informatics, February 2013
20. Gajowniczek, K., Za_bkowski, T.: Data mining techniques for detecting household characteristics based on smart meter data. Energies **8**, 7407 (2015)
21. Zhou, Cheng, Cule, Boris, Goethals, Bart: Pattern based sequence classification. IEEE Trans. Knowl. Data Eng. **28**, 1285–1298 (2015)
22. Hassanat, A.B., Abbadi, M.A.: Solving the problem of the k parameter in the KNN classifier using an ensemble learning approach. Int. J. Comput. Sci. Inf. Secur. **12**(8) (2014)
23. Peddi, S.V.B., Kuhad, P., Yassine, A., Pouladzadeh, P., Shirmohammadi, S., Shirehjini, A. A.N.: An intelligent cloud-based data processing broker for mobile e-health multimedia applications. Future Generat. Comput. Syst. J. **66**, 71–86 (2017)
24. Hossain, M.S.: A patient's state recognition system for health care using speech and facial expression. J. Med. Syst. **40**(12), 272:1–272:8 (2016)
25. Ul Alam, M., Roy, N., Petruska, M., Zemp, A.: Smart-energy group anomaly based behavioral abnormality detection. In: Proceedings of the IEEE Wireless Health, Oct 2016, pp. 1–8 (2016)

Application of Big Data in Health Care with Patient Monitoring and Future Health Prediction

K. M. Thasni(✉) and Rosna P. Haroon

Department of CSE, KTU University, Thiruvananthapuram, India
thasnikmicet@gmail.com, rosna.haroon@gmail.com

Abstract. Healthcare analytics is a rapidly growing industry. Healthcare analytics have the potential to reduce cost of treatment, avoid preventable disease and improve the quality of life. This paper is an application of big data analytics in healthcare. A co-relation analysis on clinical big data from clinical reports and doctor's notes are performed. Doctors consider similarity between health parameters to take better decisions. The co-relation analysis of health parameter is being used to cluster the patients based on similarity. Finally random model is designed to predict future health condition of most co-related patients based on the current health status. The future health prediction helps the monitoring of patients in diagnosis process. The system used modified future health prediction algorithm which is capable of predicting one or more diseases, which increase the possibilities of algorithm in health care. The performance evaluation gives about 97% of accuracy.

Keywords: Big data · Health care · Prediction

1 Introduction

Advanced healthcare systems patient data are collected through wearable devices equipped with different sensors. Recently mobile technology also takes a vital role on data collection. Smart phones with multi sensor devises are used as data collecting devices. Electrocardiogram (ECG), Electromyography (EMG), Electroencephalography (EEG), motion sensors, in-plant pacemakers etc, is the examples of devices used in healthcare environment. The data collected by the devices are different health parameters such as, blood pressure; pulse rate body temperature health related images are used to take medical decisions and patient monitoring. Indeed, huge amount of medical data collected for years are costly and time consuming. There is a huge need of Big data in healthcare due to the rising cost of healthcare in the countries like United states. McKinsey's last report states "After more than 20 years of steady increase, healthcare expense now 17.6 percent of GDP- nearly $600 billion more than expected benchmark of united state's size and wealth". So the physician's treatment is more and more evidence based. The new attitude of treatment is a greater demand in big data analytics in health care facilitate than ever before. Now-a-days many data intensive applications are emerged. Many stochastic models are developed by many authors. Even, existing

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 49–59, 2020.
https://doi.org/10.1007/978-3-030-37051-0_6

model do not support both analysis and processing of structured and unstructured data. Here using Map Reduce framework for the analysis of data. Map Reduce have the capability of processing large volume of data in parallel.

The rest of the paper is organized as follows: Existing works on big data in health care environment are discussed in Sect. 2. The system architecture of our proposed system are explained in Sect. 3 and the subsection gives detailed discussion of various sub sections of system. Modified future health prediction is the core part of system is explained in Sect. 4. The performance evaluation process for result analysis is included in Sect. 5. Conclusion and future work remarks in Sect. 6.

2 Related Works

A system designed for analyzing big data in health care with prediction for future health condition [1]. The system use correlation algorithms within cluster and between clusters. Future health prediction is implemented with prediction of flu disease. An attempt with modified future health prediction algorithm is performed in proposed work which capable of predicting one or more disease instead of one. A system designed for BSN (Body Sensor Networks) which consist of number of nodes deployed on a human body [2]. The patients have to practice certain fixed pattern excises. The node placed on the body captures the body motion during practice. Correlations among different patients have not used in this. Only clinical data are considered, histories of disease symptoms are ignored. A clinical decision support system based on machine learning approach is introduced [3]. This is capable of analyzing large number of variables that are already available from Electronic Health Records. System used to predict patient's outcomes from the analyzed reports. This is a big data driven machine leaning approach compared to traditional analytic methods.

Map Reduce is a simple programming model to develop distributed data applications. A full-fledged framework on Map Reduce platform to process streaming data in healthcare applications [4]. Framework is a work load prediction method base on data arrival rate. The Map Reduce split is based on the data arrival rate. So this extends the traditional Map Reduce framework. Advanced Wireless Technology provides many opportunities in healthcare platform. A study about Body area Sensor Networks [5], including application challenges and perspectives. A set of challenges such as scalability, energy efficiency, Quos, Co-existence, security and privacy are taken to account. Big data in healthcare enormous not only because of its volume but also diversity of data types and speed of data management [6]. By digitizing or complaining big data lead to many advantages. Detecting diseases at early stages they can be treated early and more effectively. The proposed work actually is a Big Data analytic in healthcare. The advantages are widespread and that end several challenges must considered.

3 Proposed System

The proposed system consist of a data collection phase in which the clinical data of patient from hospitals is collected. Data may be any format which should be converted in to a common format to make implementation easy. Before choosing a collected data as our data set should ensure all the relevant parameters are included. After fixing the data sets being used for the system pre-processing is done. Hospital data may have unfilled fields of data and irrelevant data. Make sure all unwanted data is eliminated. Data analysis is the main processing steps of our system. The correlation algorithms are executed here. The result of these two algorithms gives a group of high risk patients. The future health condition of that high risk group of patients is predicted in the future health prediction phase

3.1 Data Collection

Collecting data is a crucial fact in system performance. So we collect the patient data who visited more number of times the hospital in a particular window. Window can be a week, month, or three month etc. In the healthcare big data environment physiological data, 3D imaging, EHR, radiology images, geological sequencing, clinical and billing data is all sources of Big data which describes the volume of data. Real time and emergency patient monitoring such as health beat monitoring and Intensive Care Unit (ICU) monitoring are the source of streaming data. ECG, EMG and clinical reports are unstructured data whereas personal data, patient visits, etc are structured data which

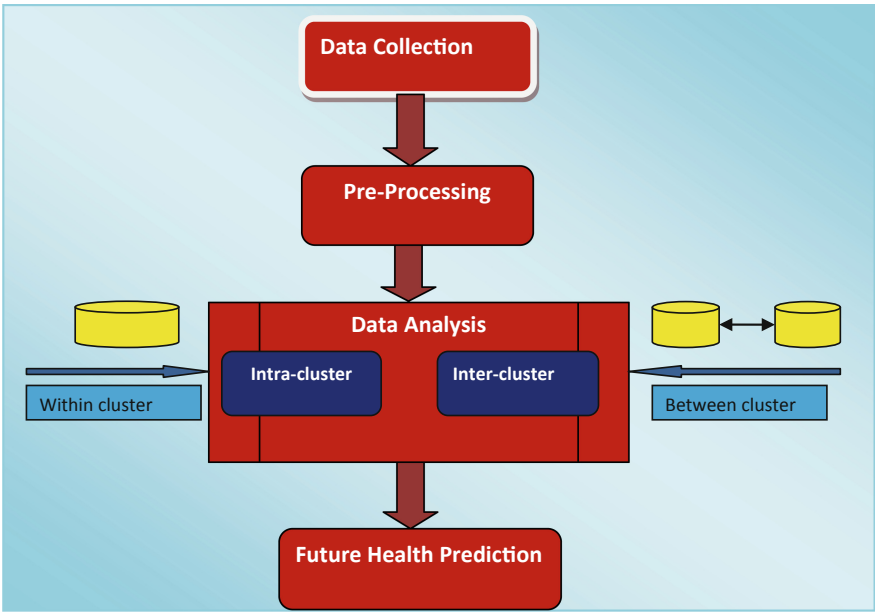


Fig. 1. System architecture

determines verity of data [9]. If we consider f is the frequency of visit, w is the window size, l be the minimum limit, then f > l in w that patient data is valid and it should be collected (Fig. 1).

3.2 Data Analysis

The processing of data collected is in the analysis phase. A successful system having an accurate analysis phase. The total amount of data (Dtot) collected in data collection phase is used for analysis. The size of data determines the complexity of processing. Here we use the data partition mechanism to reduce complexity of data. This huge amount of data is divided in to small partitions for parallel processing that reduce the complexity to process the bulky data. The size of the data chunks can be any size depends on the ease of processing. If x is the size Dp is the number of datas in one partition and Dtot is the total collected data in the data set, then Dp = Dtot/x. The number of partition must be take carefully becouse the size of data must be appropriate for processing. Then each data partition is taken for processing. The processing is done in MapReduce framework.

3.2.1 Analysis in Map Reduce Framework

The analysis of data chunks is in the Map Reduce framework. There is a number of Map functions, a number of reducers and shuffle or sort functions. Number of Map functions Map () execute in parallel. In the system implementation mapper is used for preprocessing. Correlation analysis is done in another mapper. The shuffle and sort function forward this correlation values which is received by the reducers. The mean, variance and correlation values are calculated in reducers. The number of mappers and reducers should be proper. The intermediate results from Map function are sorted and forward to Reducers reduce () for the data locality and better performance. The number of Reducers(N(R)) should be less than or equal to number of Map functions(N(M)) i.e., N (M) <= N (R). The output from Reducer is then used for storage and visualization purpose.

3.2.2 Correlation Analysis Using Map Reduce

Correlation analysis is performed on the fine grained processing of data set in the Map Reduce framework. The parameter set is different in their type and number in various hospital departments. The relationship between them is also varying based on diseases. Such relationships are examined in correlation analysis. The co-relation between parameters [11] are analyzed in two ways. It is arranged in two algorithms that is, inter correlation analysis and intra correlation analysis.

Intra-cluster Correlation Algorithm Within Cluster

In intra cluster correlation analysis the patient within the same department is clustered based on their resemblance. Each individual is a patient p in a department d where p€P and d€ DP. Hence each patient has a number of health parameters. However each parameter is not equally responsible for a particular disease. Therefore we have to find the correlation among health parameters of patients within a department DPi.

- Before performing correlation analysis we have to pre-process the data and it should be represented in a matrix format.
- The health parameters are stored in an intra-cluster parameter matrix. We separate the parameters and stored in a separate matrix for the analysis requirements.

The health parameter correlation value different from one patient to another due to the variance in the range of disease and severity of disease. The correlation analysis has different sub steps such as column mean, variance and standard deviation. All these sub steps are executed in map phases and intra-cluster correlation algorithm is executed in the reduce phase. Based on the resulting correlation values severity of disease can be calculated and high risk patients are cluster in to a group. The risk factor is in between the range [0, 1]. We had taken a threshold value within this limit to determine the high risk patients.

Algorithm 1: Intra-cluster correlation algorithm

Input: Patient health parameters

Output: i) Intra cluster correlation factor

1. Initialize total=0;
2. e=p;
3. **for** i=1 **to** e **do**
4. **for** j=1 **to** n **do**
5. $total_{ij}$=p;
6. **end for**
7. **end for**
8. U_p=total/x;
9. The step 10 to 17 executed U_p number of times
10. **for** i=0 **to** U_p **do**
11. **for** j=0 **to** n **do**

    i) Intra-cluster matrix (IaC[i][j]) formed Patient and its parameters are stored in matrix format.

12. **End for**
13. Find the column mean, mean=total/no of records
14. **End for**
15. Evaluate variance(vr), vr=$mean^2$/no of records
16. Find intra cluster correlation(cr)
17. **If** cr>= T **theni**
18. Ω_d={P};
19. **Enf if**
20. **Return** vr,sd,cr ,Ω_d;

According to the algorithm the total data collected are initialized. This step is necessary if we use both patients in department and BANs are used. This algorithm is implemented by ignoring BANs, but it can be use based on the requirements and source availability. The collected data is then representing in a matrix format. After that algorithm work to find the mean value of the parameters. Column mean of each parameter is calculated Then variance and standard deviation is calculated within other mappers. After computing mean, variance and standard deviation within mappers the results are shuffled and given to the reducers to achieve data locality during execution. Intra cluster correlation is executed within reducer function. The severity of disease determined from the correlation value.

Inter-cluster Correlation Analysis Between Cluster

Algorithm 2: Inter-Cluster Correlation algorithm

Input: Patient health parameters of two departments

Output: i) Inter-cluster correlation factor , ii) Newly classified patient list

1. Initialize total=0;
2. **for** i=1 **to** n1 **do**
3. **for** j=1 **to** n2**do**
4. Total amount of data collected
5. **end for**
6. **end for**
7. U_p=total/x;
8. The step 10 to 17 executed U^{ij}_p number of times
9. **for** i=0 **to** n1 **do**
10. **for** j=0 **to** n2 **do**
11. Intra-cluster matrix IaC[i][j]=[n1,n2]
12. **End for**
13. Find the column mean, mean=total/no of records
14. **End for**
15. Evaluate variance(vr), vr=mean^2/no of records
16. Evaluate standard deviation(sd), sd=sqrt(variance)
17. Find intra cluster correlation(cr)
18. **If** cr>= T **then**
19. Ω_d={P};
20. **Enf if**
21. **Return** inter-correlation factor, new patient cluster.

A threshold value is fixed. The patients with correlation value greater than the threshold are cluster into a new group. The group contains are high risk patients. Inter cluster correlation analysis is to find the similarity and dissimilarity between health parameters of different departments. For example cardiology department for heart disease and neurology department for neurological disease patients. Health parameters of patients of these departments are different in their number and type. The inter cluster correlation is to find the dependencies between these two departments parameters. And also high risk patients are grouped together based on the correlation value.

Input and output parameters are set before executing the algorithm. The total data collected are generate in an inter cluster matrix which contain all the parameters in both ith and jth departments. The column mean of all parameters of ith and jth departments is calculated. Variance and standard deviation is calculated within other map functions. The inter-cluster correlation factor is calculated in reducer () after completing the variance and standard deviations in different map functions. The intermediate results are shuffled between the reducers for the data locality. The highly influenced health parameters are identified and are grouped together. A threshold value is determined by compare with correlation values and the correlation value greater than the threshold, and then the patients with those parameters are grouped together. The newly classified group is high risk patients they need proper meditation and precautions.

4 Future Health Prediction

A modified future health prediction model is used here. The future health of a patient is predicted based on current health parameters. Here our new modified algorithm is capable of predicting one or more serious diseases instead of predicting any one disease. More number of correlated health parameters are analyzed so the accuracy of prediction is increased. Patient monitoring and understanding severity of serious disease is the main application of this model. Early detection of such disease leads to proper monitoring and treatment of patients.

Modified FHCP algorithm is executed after the execution of both intra-cluster and inter-cluster algorithms. The high risk patients are clustered as the output of inter-cluster correlation is taken for disease prediction. A flag is set as true for such high risk patients. The mean of correlated parameters of high risk patients is already calculated in previous algorithm. These mean and correlated parameters are compared. If all the correlated parameters show a higher value than mean it indicated that the patient may be the chance of that disease. Algorithm is work with different disease parameters parallely to find the chance to have any other disease. Algorithm shows a patient may have the chance of one or more disease. The efficiency of algorithm depends upon the input parameters. If more number of parameters the prediction is more accurate.

Algorithm 3: Modified FHCP Algorithm

Input: i) High risk patient list

Output: i) Prediction of one or more disease probability

1. Initialize probability=0

2. Find Intra-cluster correlation

3. Find Inter-cluster correaltion

4. if cr>threshold **then**

i)set the flag=true

4. If flag (true) **then**

5. for i=0 **to** l **do**

6. **for** j=0 **to** n **do**

7. **if** crparameter>Mean **then**

8. "Probabity of disease"

9. **end for**

10. end for

5 Performance Evaluation

The performance evaluation of algorithms is an important to determine the system performance. The evaluation process was done as a comparison. The patients are divided in to two groups of 50 patients. The algorithm is taken the two sets of data as input. Table 1 gives an idea about the parameter utilization in the system. It's a full utilization model. All parameters in the parameter list is taken for analysis in all algorithms so the system consider as full utilization model The data set collection phase is very important. A well arranged data set of clinical data increase the system performance and accuracy is higher if all the relevant parameters are included in it. All parameters included data set gives more correlated parameters with higher values of correlation.

Table 1. Parameter list of intra-cluster

Parameter	Value
No of patient in dataset 1	50
No patients in dataset 2	50
Utilization model	Full utilization

The Fig. 2 shows the result evaluation of intra-cluster correlation algorithm with two sets of patients. The result shows that almost all patient parameters having the correlation value greater than .75 are the most correlated patients. The smaller correlation values show that parameters have no correlation. Algorithms give similar results with two sets of data so the algorithm performance is good and accurate. The efficiency of the system increased if more number of parameters with higher correlation values.

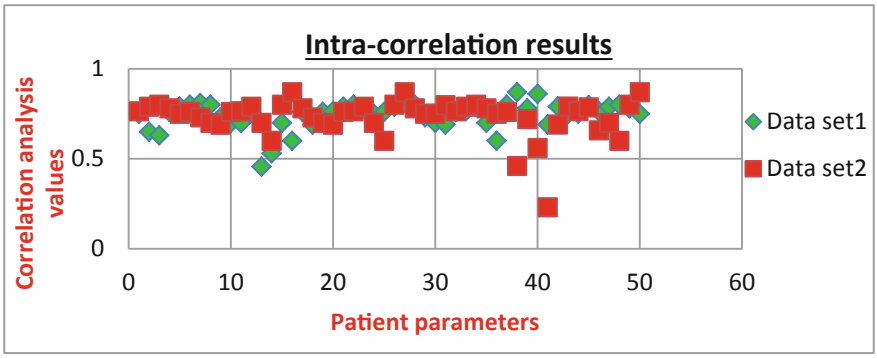


Fig. 2. Intra-cluster correlation result evaluation

Figure 3 shows the evaluation results of inter- cluster correlation algorithm. Result analysis is performed by applying three data sets as the algorithm. The algorithm shows similar results with all data sets. The results greater than .75 are more correlated patients and small results shows poor correlation between them. Accuracy of algorithm is 99 because which give accurate result for almost all parameters.

Modified future health prediction algorithm is tested with two different disease data sets. Algorithm predicts both diseases accurately. The prediction rate of both disease increased by increasing number of patient data that is shown in Fig. 4. The result shows algorithm is capable of working with any number of disease data set will give better prediction results. Results shows Modified FHCP capable of prediction one or more disease prediction which increases the application level of system in health care environment.

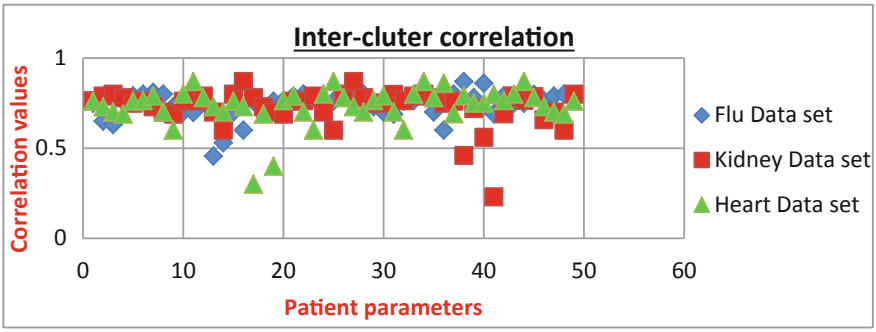


Fig. 3. Inter-cluster correlation result evaluation

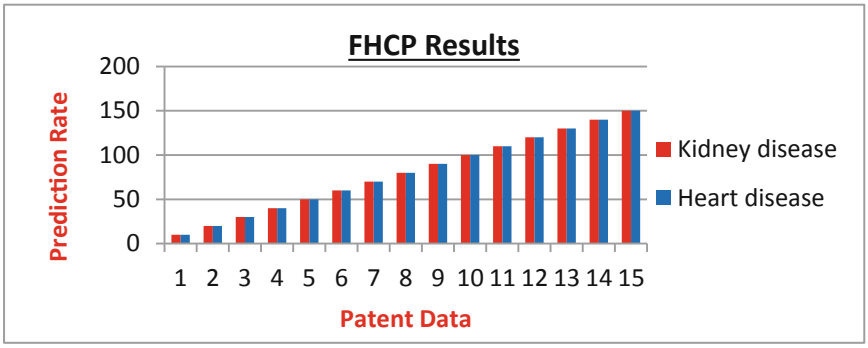


Fig. 4. Modified FHCP results

6 Conclusion and Future Work

This is a modified FHCP system. There are three algorithms are used inter-cluster intra-cluster algorithms for correlation analysis and modified FHCP for future health prediction. Here the application of FHCP is tested by modified algorithm to predict one or more serious diseases. The system offer many advantages in health care environment. Increased number of health parameters are effectively analysed there for the prediction is more accurate than previous works. Emergency department monitoring is the future work which increase the advantages in health care. The performance evaluation shows satisfiable results.

Acknowledgement. All author states that there is no conflict of interest.
Data set collected from this website: "http://www.kaggle.com".

References

1. Sahoo, P.K., Mohapatra, S.K., WU, S.-l.: Analyzing heath care big data with prediction for future health condition. IEEE Access **4**, 9786–9799 (2017). E-ISSN:2169-3536
2. Wu, C.H., Tseng, W.C.: Data compression and by temporal and spatial correlation in body area sensor network; a case study in Pilates motion recognition. IEEE Trans. Mob. Comput. **10**, 1459–1472 (2010)
3. Taylor, R.A., et al.: Prediction of in hospital mortality in emergency department patients with sepis: a local big data-driven machine learning approach. Department of Emergency Medicine, Yale University, Mar 2016
4. Sang, F., Cao, J., Khan, S.U., Li, K., Hwang, K.: A task level adaptive mapping frame work for real-time streaming data in health care application. Future Gener. Comput. Syst. 43–44 (2014)
5. Patel, M., Wang, J.: Application, challenges, prospective in emerging body area networking technologies. IEEE Wirel. Commun. **17**, 80–88 (2010)
6. Bates, D.W., Saria, S., Ohno-Machado, L., Shah, A., Escobar, G.: Big data for health care: using analytics to identify and manage high risk and high cost patients. Res. Artic. Health Aff. **33** (2014)
7. Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S.: The internet of things for healthcare: a comprehensive survey. IEEE. Trans. Content min. **3**, 2169–3536 (2015)
8. Raghupathy, W., Raghupathy, V.: Big data analytics in health care: promise and potential. Health Info. Sci. Syst. **7** (2014)
9. Lin, K., Xia, F., Wang, W., Tian, D., Song, J.: System design for big data application in emotion-aware health care. IEEE Access **4**, 6901–6909 (2016). E-ISSN:2169-3536
10. Tawalbeh, L.A., Mehmood, R., Benkhilifa, E., Song, H.: Mobile cloud computing model and big data analysis for health care applications. IEEE Access **4**, 6171–6180 (2016). E-ISSN:2169-3536
11. Yu, Z., et al.: Incremental semi supervised clustering ensemble for high dimensional data clustering. IEEE Trans. knowl. Data Eng. **28**, 701–714 (2016)
12. Dehury, C.K., Sahoo, P.K: Design and implementation of a novel service management framework for iot devices in cloud. J. Syst. Softw. **119**, 149–161 (2016)
13. Wang, W., Ying, L.: Data locality in map reduce : a network perspective. In: IEEE 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton), 30 Sept, 3 Oct 2014. **E- ISBN:** 978-1-4799-8009-3
14. Lee, M., Han, X.: Complex window query support for monitoring streaming data in wireless body area network. IEEE Trans. Consum. Electron. **53**, 1710–1718 (2011)

Data Science for Internet of Things (IoT)

M. Devi[1], R. Dhaya[1(✉)], R. Kanthavel[2], Fahad Algarni[3], and Pooja Dixikha[4]

[1] Department of Computer Science, King Khalid University, Sarat Abidha Campus, Abha, Kingdom of Saudi Arabia
{devinov6, dhayavel2005}@gmail.com
[2] Department of Computer Engineering, King Khalid University, Abha, Kingdom of Saudi Arabia
kanthavel2005@gmail.com
[3] Department of Computing and Information Technology, University of Bisha, Bisha, Kingdom of Saudi Arabia
fahad.a.algarni@gmail.com
[4] Department of ECE, Sona College of Technology, Salem, Tamilnadu, India

Abstract. The term data science has been floating around as a popular terminology among social media applications globally. The associated device called IoT generates more than 2.5 quintillion bytes of statistics step by step, which could basically impact the business shapes. There is no doubt that the rising technology of IoE (Internet of Everything) is dependent on Data Science concept. The Industrial Internet of Things (IIoT) which makes up a good proportion of IoT tries to analyze the data they record and turn the data into meaningful information. In customary Data Science, the investigation is static and confined being used. The information that is got may not be refreshed so the outcomes accomplished in the wake of preparing may not be shrewd or usable. Then again, since IoT information is being got continuously, the investigation supplement the most recent market designs which permits making this investigation more significant and wise when contrasted with customary ones. Additionally, as more innovation layers are included or incorporated with IoT, it turns out to be harder to structure and process the huge numbers of approaching information. So truly, Data Scientists do need to up their aptitude with the end goal to grasp IoT-created information. As the engaging quality of IoT expands a flood of information lies later on. It is bound to the change the manner in which has seen Data Science for quite a while. The blast in information isn't just going to require better foundation however more astute Data Scientists. Information Science for IoT can help overcome some wide-reaching difficulties in order to make more precise choices. This paper initiates to fulfill the readers to let identify the effective utilization of data science in IOT Platform in upcoming Era as IoT Opportunities for Data science as secured manner.

Keywords: Data science · Internet of things · Internet of everything · Information science

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 60–70, 2020.
https://doi.org/10.1007/978-3-030-37051-0_7

1 Introduction

IOT has the new rule for the future, which is going to be, "Anything that can be connected, will be connected.

Data Science Process is a responsive data science procedure to deliver analytics solutions and bright applications professionally. The following contents explain the approaches of data processing. Data Pre-processing: It is a practice that is used to convert the raw data into a clean data set. The raw data format which is collected from various sources is not viable for the analysis. Data scientists applied the strategy to get more appropriate for what they need to do with it. There are some fundamentals steps to be taken in data pre-processing such as (i) Data cleaning (resolving irrelevant data) (ii) Data Integration (data amalgamation from multiple databases /data cubes) (iii) Data Transformation (Shape the data using normalization and aggregation procedure) (iv) Data Reduction (data volume reduced without affecting the analytical results) (v) Data discretization (Numerical attributes replacing with nominal one).

2 Data Science Subdomain for IoT

The data science utilizing IoT will be managed extravagantly and gigantically for different real time applications that have been associated with real time data and computing advancements are as per the following

-Cognitive Computing: Cognitive computing extends this investigation approach to manage districts that were difficult to reach by progressively customary gadgets like business understanding and estimations [3].

-Real time Processing: Real time data processing includes a nonstop information process and yield of data. Real time data processing and analytics permits an association the capacity to make prompt move for those times when acting inside seconds or minutes is huge [4].

-Time Series data Analysis: Time series is a series of data that is filed in time arrange. The most well-known approach to picture time series data is to utilize a basic line outline, where the level hub plots the augmentations of time and the vertical hub plots the variable that is being estimated.

-Geo spatial Data Analysis: Geospatial data science meets various essential rising innovation and financial advancement challenges.

-Deep Learning: Traditional machine learning models have dependably been ground-breaking to deal with organized data and have been broadly utilized by organizations for credit scoring, beat expectation, purchaser focusing on, thus on. With regards to unstructured data such as pictures, content, voice and recordings, hand built highlights are times expending, weak and not versatile practically speaking.

-Edge Computing: Edge Computing alludes to calculation around the bend or edge in a system chart. Edge computing is likewise advantageous for the associations as it encourages them chop down costs that were prior acquired on exchanging data sets over a system [24].

3 Traditional Data Science Vs. IoT

By squeezing the association between these two data innovations down to its easiest frame, it comes down to time. Conventional data science, for instance, identifies with progressively basic procedures that encourage data accumulation and association. There is no expiry or approaching timetable to be worried about, generally [1]. While have to investigate and comprehend data as quickly as time permits, IoT is continuously, easy to utilize and apparently interminable. The ongoing variable is one of the noteworthy components that separate the two innovations. Both require high flag rates and preparing times, however IoT solely requires accumulated bits of knowledge and choices on the spot. To grow or draw out the time it takes for data handling, should diminish or moderate the general estimation of the data at the center of the innovation [23]. The Table 1 shows the comparison between traditional data and IoT Data.

Table 1. Comparison between traditional data and IoT Data

Subject	Traditional data	IoT data
Content	Created by human	Created by machine
Content consume	Based on the request	Pushing data
Content combine	Links	Operators
Value of the content	Answering the questions	Action and data
What was done	HTML and search engines	Data creation

Taxonomy: Figure 1 shows the taxonomy representation of data Science solutions for IoT systems. The first part of the taxonomy is the sources of data which are produced by public sector, private sector, Intelligent Transport Systems (ITS), Sensor

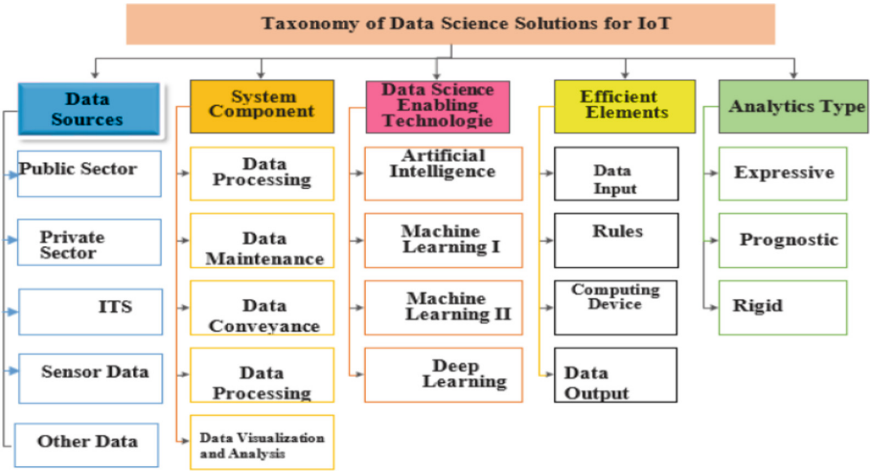


Fig. 1. Taxonomy of data Science solutions for IoT systems

data and other data sources. The second part of the taxonomy is system components which encompass of five parts explicitly data processing, data maintenance, data conveyance, processing of data and the final is data visualization and analysis. The third part of the taxonomy is enabling technologies of data science which may be related to IoT context, which are Artificial Intelligence, machine Learning I & II and Deep Learning [1]. The fourth part of the taxonomy is Efficient Elements supported for IoT contain four key elements, precisely, Data input, Rules for data maintenance, Computing device for processing purpose and data output. The last part of the taxonomy is analytic types are Expressive type, Prognostic type and Rigid type.

4 Open Research Problems in IoT for Data Science

IoT has a basic financial and social effect for the future development of information, system and correspondence advancements. It presents difficulties in mixes of volume, speed and assortment. A few enhanced advances, for example, computational insight and vast data can be consolidated to enhance data the executives and disclosure of information of huge scale mechanization applications. The greatest test exhibited by Big Data is the procurement of learning from IoT data [22]. It is basic to create foundations to dissect IoT data. Various IoT gadgets create consistent streams of data and analysts can create apparatuses to extricate significant information from these data utilizing mechanized learning procedures. Understanding data streams and examining them for significant information is a test and prompts Data Science. Machine learning calculations and computational insight methods are the main answer for handle vast IoT forthcoming data, the key advancements that are related with IoT [7]. Figure 2 shows the research problems in IoT and data Science.

Fig. 2. Research problems in IoT and data Science

5 Languages Used for Data Science

Data science is nonentity, but it is a "notion to merge statistics, data analysis and their connected approaches" in order to "know or recognize and examine authentic occurrences" through data. It pays methods and philosophies strained since numerous areas within the comprehensive parts of mathematics, statistics, information science, and

computer science. This arena is flattering more and more general with the arrival of Machine Learning all around us. In order to realize data science, might need to distinguish at least one of the programming languages [5]. There are many programming languages that are used for data science. Figure 3 shows the diagram representation of languages used in data science.

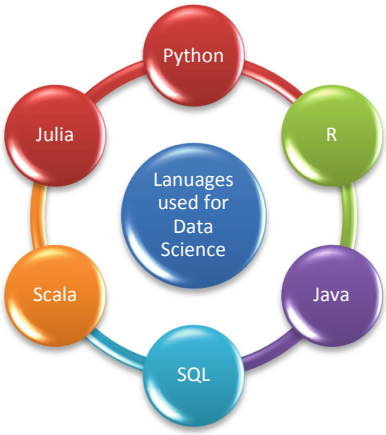


Fig. 3. Languages used for data science

- **Python:** Python is quickly picking up standard scheming and turning into an increasingly down to earth language to construct items. Python is a useful asset for medium-scale data handling. Python additionally has the benefit of a rich data network, offering tremendous measures of tool-box and highlights.
- **SQL:** Structured Query Language (SQL) is utilized to manage extensive databases. Specifically, it is useful in overseeing structured data.
- **Julia:** Julia has been intended to address all the numerical and computational needs; subsequently it is perfect for data researchers.

6 IoT and Data Relationship

Connection among IoT and Data processing every one of the data from IoT is a vocation in huge data. Different sorts and arrangements which may be organized, unstructured or semi-organized of data created from different gadgets and sensors in IoT are taken care of and changed by the assortment of Data accumulation [6]. The monstrous sum data started from IoT are ingested and put away by the "volume" of Data stacking. The close continuous preparing and investigation of gigantic data from IoT are performed in a favorable way by the "speed" of Big Data examination [13]. Likewise, the knowledge and bits of knowledge of savvy IoT objects are acknowledged and expanded by the "esteem" of Data. The equivalent is portrayed in Fig. 4 shows the relationship between IOT and Data.

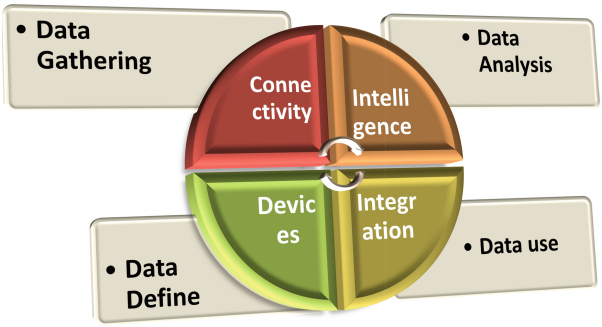


Fig. 4. Relationship between IOT and data

7 Challenges of IoT Applications in Data Science

Connection among IOT and Data science every one of the data from IoT is a vocation in huge data. Different sorts and arrangements of data created from different gadgets and sensors in IoT are taken care of and changed by the "assortment" of Big Data accumulation. The close continuous preparing and investigation of gigantic data from IoT are performed in an opportune way by the "speed" of Data Science analysis [8]. Likewise, the knowledge and bits of knowledge of savvy IoT objects are acknowledged and expanded by the appreciation of Data.

- **Data Storage and Analysis:** Because of the staggering expense of capacity, the first challenge is the capacity media and higher information or yield speed [21].
- **Knowledge Discovery and Computational Complexities:** Learning disclosure and portrayal is a prime issue in huge data and it incorporates a few optional fields, for example, confirmation, chronicling, organization, conservation, information recovery and portrayal. Because of the expansion in size of Data the current instruments may not be effective to process this data for significant information [9].
- **Scalability and Visualization of Data:** The most essential test for Data science methods is its adaptability and security. In the most recent decades analysts have focused on accelerate data examination and accelerate preparing. Data adaptability has turned out to be important for some, associations managing hazardous datasets, definitely when execution issues emerge. The target of data representation is to display the data in an increasingly proper manner, utilizing a few strategies of realistic hypothesis [20].
- **Poor data quality:** It's basic to maintain a strategic distance from manual data section where conceivable. Application mix instruments are one approach to computerize data passage and lessen the expansion of typographical mistakes, exchange spellings, and individual mannerisms from the data. Time spent 'preparing data' additionally avoids re-doing work down the line. When data is uniform and steady are prepared to begin removing the data needn't bother with. This is a fundamental advance to guaranteeing data quality, which conveys us to challenge number two [10].

- **Too much data:** Regardless of the present publicity around data science, an excess of data can really cause a large group of issues that counteract significant advancement. In these occasions, diminishing highlights and utilizing data determination procedures can help dispose of the commotion and slice through to what makes a difference most.
- **Data Structures:** Most sensors convey information with a period stamp and the vast majority of the information is exhausting with nothing occurring for a significant part of the time. While static cautions dependent on edges are a decent beginning stage for examining this information, they can't enable us to progress to indicative or prescient or prescriptive stages.
- **Multiple Data Formats together:** While time arrangement information have set up procedures and procedures for dealing with, the experiences that would extremely matter can't emerge out of sensor information alone.
- **Balance Scale and Speed:** The greater part of the genuine investigation for IoT will occur in the cloud, a server farm, or almost certain a half breed cloud and server-based condition. That is on the grounds that, regardless of the versatility and adaptability of the cloud, it may not be suited for situations requiring a lot of information to be handled progressively [11] (Table 2).

Table 2. Challenges of IoT applications in data science

Challenges	Actions
Data storage and analysis	Storage of Data and Analysis of Data; hard drives were utilized to store data; credited to the decent variety of data;
Knowledge discovery and computational complexities	Data Warehouses and Data centers; charge of putting away the data that is acquired from the working frameworks; computational multifaceted nature, vulnerability
Scalability and Visualization of data	Adaptability and security; Data adaptability has turned out to be important for some, associations managing hazardous datasets, definitely when execution issues emerge
Poor data quality	incorporate utilizing very much characterized industry principles and ceaseless irregularity discovery
Too much data	excess of data can really cause a large group of issues that counteract significant advancement
Data structures	connections between information pieces gathered at explicit interims of times
Multiple data formats together	Time arrangement information have set up procedures and procedures for dealing with, the experiences
Balance scale and speed	regardless of the versatility and adaptability of the cloud, it may not be suited for situations requiring a lot of information to be handled progressively

8 Ways to Spread Over Data Science Algorithms to IoT Data

One of the essential points of innovation has dependably been the improvement of human way of life and with the IoT, it is drawing nearer to accomplishment. In any case, to totally understand this objective, IoT needs data to offer improved encounters or find more up to date approaches to do this self-governing. That is the place Data Science and Machine Learning come enthusiastically [19]. For the proper use of Data Science systems, will have to characterize the data types [12]. When the data type is characterized, it may be ought to apply the correct calculation that falls in accordance with unmistakable data qualities.

9 Differences Between Data Science for IoT and Traditional Data Science

Data Science for IoT has resemblances but similarly certain noteworthy variances. Here are some variances among Data Science for IoT and Data Science [25].

- IoT and AI level for the Initiative
- Machines showing one another
- On-going preparing and IoT
- Real time labelling
- Real time accumulation
- Real time worldly connection
- Job of Sensor combination in IoT.

10 Impact of IoT on Data Science

Internet of things is a gathering of items that are one of a kind and can associate with the Internet [14]. These articles could be whatever can interface with the Internet and with one another so they can speak with one another. In any case, there is no detail about what these gadgets can do or can't do. A few contemplations of such gadgets are referenced beneath [2].

- The utensils can cooperate with individuals and with one another to impart
- These utensils are equipped for catching data
- These utensils ought to have the capacity to process
- Data Storage

These utensils have controllers to turn things ON or OFF

-Essentialness of IoT: The scan for IoT is picking up hugeness when contrasted with Big Data. There are different situations that should be concentrated to comprehend why this is being sought. There are different instances of shopper and modern applications that are set to change how function and speak with the world. To see how IoT has developed after some time, have to break down the publicity cycle [18].

-Difficulties with IoT: There is a great deal of difficulties in acknowledging IoT.

a. Inspire devices from various producers to speak with one another
b. Design prerequisites and correspondence routines
c. Privacy of Information

With the progression in IoT based application, there is a test in approving associated IoT applications, which incorporates its help for data volume, speed, assortment, and veracity [15]. The above Fig. 5 shows the impact on IoT on Data Science.

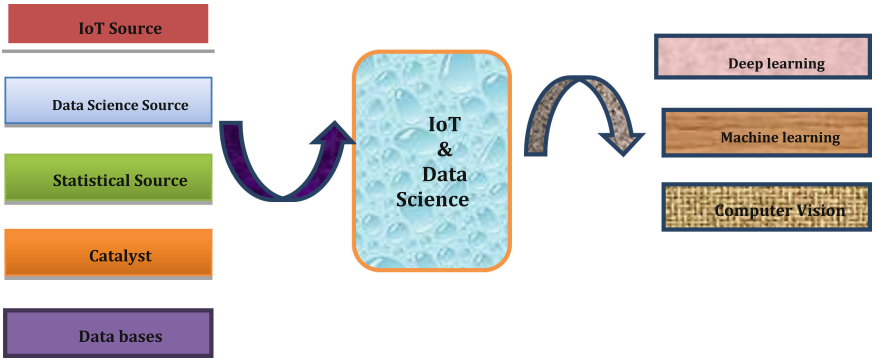


Fig. 5. IOT on data science impact

11 IoT Changing the Appearance Of Data Science

As the notoriety of IoT expands, a flood of data lies later on. It is bound to the change the manners in which have seen Data Science for quite a while. The blast in data isn't just going to require better foundation yet more intelligent Data Scientists. It will require a foundation that can dependably process a steady stream of complex data.

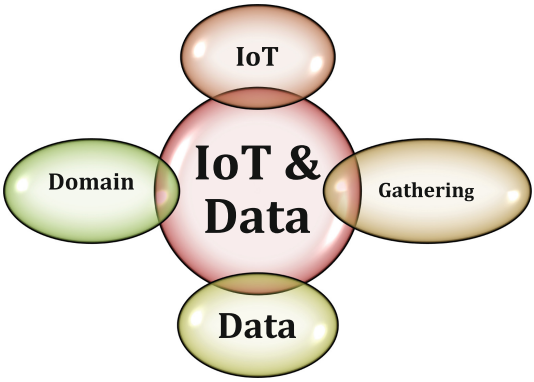


Fig. 6. Challenging appearance of data & IoT

What's more, it will be a genuine exercise in futility and cash on the off chance that can't utilize this flood of data to bode well out of it [17]. Hence, this discharge of data must to be an open door for data researchers. This Fig. 6 shows the challenging appearance of data & IoT

12 IoT Data Science for Altering the World

Data Science for IoT can help defeat some worldwide difficulties. It can help produce increasingly precise choices. This implies more intelligent answers for the purchasers around the globe. IoT likewise makes the worry of protection for individuals; however in the event that adds security advancements like Block-chain to IoT, which can understand numerous advantages [16]. IoT Data Science additionally permits incorporating computerized reasoning.

13 Conclusion

This paper focused on the Data Science for IOT in an elaborated manner. The differences between data science for IOT and traditional data science, impact of IOT on data science, challenges of IOT applications in data science, open research problems in IOT for data science and traditional data science versus the internet of things, Data Processing in Data Science Approaches, Data science Subdomain for IoT, languages supported for data science have been analyzed. The term Data Analytics has been well defined as a process which is used to examine big and small data sets with varying data properties to extract meaningful conclusions from these data sets. The processes in which the data science must undergo are data preprocessing, data visualization, predictive analysis, supervisory learning, un-supervisory learning, deep learning and computer vision. It is concluded that since IoT is among the most important foundations of fresh data, data science will offer a significant impact in constructing IoT applications more intelligent.

References

1. Abu-Elkheir, M., Hayajneh, M., Ali, N.A.: Data management for the internet of things: design primitives and solution. Sensors **13**(11), 15582–15612 (2013)
2. Riggins, F.J., Wamba, S.F.: Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics. In: Proceedings of 48th Hawaii International Conference on System Sciences (HICSS'15), pp. 1531–1540. IEEE (2015)
3. Cheng, B., Papageorgiou, A., Cirillo, F., Kovacs, E.: Geelytics: geo-distributed edge analytics for large scale iot systems based on dynamic topology. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 565–570. IEEE (2015)
4. Fang, H.: Managing data lakes in big data era: what's a data lake and why has it became popular in data management ecosystem. In: 2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 820–824. IEEE (2015)

5. Desai, P., Sheth, A., Anantharam, P.: Semantic gateway as a service architecture for iot interoperability. In: 2015 IEEE International Conference on Mobile Services (MS), pp. 313–319. IEEE (2015)
6. Hu, S.: Research on data fusion of the internet of things. In: 2015 International Conference on Logistics, Informatics and Service Sciences (LISS), pp. 1–5. IEEE (2015)
7. Schmidhuber, J.: Deep learning in neural networks: an overview. Neural Netw. **61**, 85–117 (2015)
8. Sun, Y., et al.: Organizing and querying the big sensing data with event-linked network in the internet of things. Int. J. Distrib. Sensor Netw. (2014)
9. Sun, Y., Yan, H., Lu, C., Bie, R., Zhou, Z.: Constructing the web of events from raw data in the web of things. Mobile Inf. Syst. **10**(1), 105–125 (2014)
10. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: a survey on enabling technologies protocols and applications. IEEE Commun. Surveys Tuts. **17(**4), 2347–2376 (2015). (4th Quart)
11. Mohammadi, M., Al-Fuqaha, A.: Enabling cognitive smart cities using big data and machine learning: approaches and challenges. IEEE Commun. Mag. **56**(2), 94–101 (2018)
12. Chen, M., Mao, S., Zhang, Y., Leung, V.C.: Big Data: Related Technologies Challenges and Future Prospects, Heidelberg. Springer, Germany (2014)
13. Tsai, C.-W., Lai, C.-F., Chiang, M.-C., Yang, L.T.: Data mining for internet of things: a survey. IEEE Commun. Surveys Tuts. **16(**1), 77–97 (2014). (1st Quart)
14. Fadlullah, Z.M., et al.: State-of-the-art deep learning: evolving machine intelligence toward tomorrow's intelligent network traffic control systems. IEEE Commun. Surveys Tuts. **19(**4), 2432–2455 (2017). (4th Quart)
15. Hu, H., Wen, Y., Chua, T.-S., Li, X.: Toward scalable systems for big data analytics: a technology tutorial. IEEE Access **2**, 652–687 (2014)
16. Xia, F., Yang, L.T., Wang, L., Vinel, A.: Internet of things. Int. J. Commun Syst **25**, 1101–1109 (2012)
17. Zaslavsky, A., Perera, C., Georgakopoulos, D.: Sensing as a service and big data. Proceedings of the International Conference on Advances in Cloud Computing (ACC) **2**, 1–8 (2013)
18. Lee, J., Ardakani, H.D., Yang, S., Bagheri, B.: Industrial big data analytics and cyber-physical systems for future maintenance & service innovation. Procedia CIRP **38**, 3–7 (2015)
19. Agarwal, D.: Difference between traditional data and big data, 6 (2016)
20. Mehta, Brijesh, Rao, UdaiPratap: Privacy preserving unstructured big data analytics: issues and challenges. Procedia Comput. Sci. **78**, 120–124 (2016)
21. Provost, F., Fawcett, T.: Data Science for Business-What you need to Know About Data Mining and Data-Analytic Thinking. O'Reilly (2013). ISBN 978-1-449-36132-7
22. Dhar, V.: Data science and prediction. Comm. ACM **56**(12), 64–73 (2013)
23. Mattmann, C.A.: Computing: a vision for data science. Nature **493**(7433), 473–475 (2013)
24. Tiropanis, T.: Network science web science and internet science. Comm. ACM **58**(8), 76–82 (2015)
25. Tinati, R., et al.: Building a real-time web observatory. IEEE Internet Comput. **19**(6), 36–45 (2015)

ECDSEC: An Efficient Group Key Management Scheme for Secure Data Sharing Among Mobile Users in Cloud Environments

S. Milton Ganesh[1(✉)] and S. P. Manikandan[2]

[1] University College of Engineering Tindivanam, Melpakkam, Villupuram District 604001, Tamilnadu, India
softengineermilton@gmail.com

[2] Sri Venkateswara College of Engineering, Pennalur, Sriperumbudur Taluk, Kancheepuram District 602117, Tamilnadu, India
spmanikandan@svce.ac.in

Abstract. The invention of cloud computing offers elastic storage services in pay-per-use policies and hence organizations store their data in cloud servers. A cybercriminal can hack the sensitive documents in the cloud and sell it for mere profit or a cloud server may be curious to learn the contents of documents. Though many works for securely distributing the keys to the mobile cloud users have been proposed, they are vulnerable to attacks and incur high computational and communication overheads. This research work addresses the security issues pertaining to secure group communication during the file upload and download over public clouds. This research is a pioneering attempt to securely transfer the keys, upload and download the documents from the cloud. The security analysis ascertains the effectiveness of the protocol and the experimental results confirm the efficiency of the proposed protocol.

Keywords: Cloud storage · Mobile user · Group key · Security
Confidentiality

1 Introduction

Cloud service providers offer services through private cloud, public cloud, hybrid cloud and community cloud. The application of cloud can be best understood whenever a user shares a sensitive document to other group members by uploading the document to the public cloud. In many cases, the group manager and the cloud service provider themselves will be curious to know the contents stored by the data owner in the cloud. In this context, maintaining the confidentiality of the documents prove to be a vital concern. To enhance the confidentiality of the data stored in the cloud servers, a secure access control mechanism is a major concern in public cloud networks. Many authors in the recent time and in the past have come out with novel access control based security mechanisms to secure the data stored in cloud servers.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 71–78, 2020.
https://doi.org/10.1007/978-3-030-37051-0_8

This research work has been organized such that Sect. 2 outlines the need for the proposed work. The proposed work is presented in Sect. 3. Section 4 analyzes the performance of the proposed protocol and Sect. 5 examines its efficiency against most of the known attacks in the literature. Section 6 provides a overview of the real time setup and effectiveness of the proposed protocol. Section 7 concludes this research work.

2 Literature Survey

A system for access control was proposed by Elisa et al. [1] which is based on policy design for XML documents and was implemented in JAVA. James et al. [2] proposed a scheme in which authorizations are specified with regard to role and not based on individual identities. At any point of time, a user may possess multiple privileges. A generic model of this scheme named Action Status based Access Control (ASAC) was proposed by Barker [3].

Group access is realized by encrypting an e-learning content through an encryption key composed of the parameters from all the users of the group with whom the document is to be shared. This key is dynamically generated for every user join or leave operation in the respective group. Whenever a new user joins or an existing user leave from the group, the encryption key must be updated in order to prevent the leaving or joining user from accessing the data or messages from the future or prior communications and a scheme in this regard was proposed by poovendran et al. [4]. Moreover, the issues which are part of securely distributing the group keys to the group users is studied by Kim et al. [5], Drira et al. [6] and Naranjo et al. [7] which led to the innovation of another new scheme in this direction [8]. The process of generating, distributing and maintaining the key is taken care of by key management schemes. There are many key management schemes being available in the literature proposed by Jeong et al. [9], Kim et al. [10] and Nabeel et al. [11]. Sridhar and Syms in 2016 [12] have introduced a novel hybrid mechanism based on group key registration technique to overcome the drawbacks of the previous protocols for the authentication of users in the cloud. Moreover, Praveena and Syms have developed a secure storage scheme for data to be stored in social networks using the proxy re-encryption scheme [13]. Thus, the security of the data stored in the cloud servers have become an immensely important concern. Based on the existing drawbacks as pointed above in the cloud storage scenario, the objectives of the proposed work are proposed as follows.

(i) To propose a novel group key management scheme for establishing a secure communication between a data owner and the group members for secure data exchange.
(ii) To reduce the overhead in group communication, by allowing a Group Manager to efficiently take care of the join and leave operations of the group members.

3 Proposed ECDSEC Scheme

The proposed system consists of four entities such as data owner, group users, group manager (GM) and the cloud server (CS). The mechanism of the proposed protocol is based on five phases such as system initialization, cloud server registration phase, group user registration phase, file upload phase and file download phase.

3.1 System Initialization

GM initializes the system by defining an additive cyclic group G_1 of prime order q. GM randomly selects two points $P, G \epsilon G_1$ and a random number $\beta \epsilon Z_q^*$. Followed by that, GM computes two new points such that $Y = \beta.G$ and $Z = e(P, G)$. Finally, GM publicly announces G_1, q, P, Y, Z.

3.2 Cloud Server Registration Phase

The CS and GM are involved in this phase to securely exchange the secret keys between them. The CS selects a public key PK_{CSP} and a private key SK_{CSP} from Z_q^* and computes $N = SK_{CSP}.P$. It sends a message to GM consisting of $PK_{CSP}, ID_{CSP}, N, r_1$ where ID_{CSP} is the identity of the CS, $r \epsilon Z_q^*$ is a random number. This message is sent as a plaintext over an insecure communication channel. GM receives the message from CS. GM computes $N = e(\beta.Y, X), O = \beta.Y$ and randomly selects his private and public keys PK_{GM} and SK_{GM} from Z_q^*. Then, GM sends $N, O, r, ID_{CSP}, PK_{GM}$ to the CS. CS verifies whether $e(O, N) \stackrel{?}{=} R$ in order to verify whether the reply has been received from the intended GM. The CS stores the public key PK_{GM} of the GM for further communications.

3.3 User Registration Phase

A user (group user or data owner) who wants to register himself with the GM for secure document upload to the CS, has to perform the following steps.

(i) The user randomly selects a public key PK_E and a private key SK_E from Z_q^* and computes $X = SK_E.P$. He sends a message to GM consisting of $PK_E, ID_i, ID_{Group}, X, v1$.

(ii) GM receives the message and sends $R, S, v_1, ID_i, PK_{GM}, ID_{Group}$ to the user.

(iii) The user computes the secret parameter $\alpha_i = \delta_i^{'} * r_i$ and sends $Enc_{PK_{GM}}(\alpha_i, ID_i, ID_{Group})$ to GM.

(iv) GM receives the message from user and decrypts it using his private key SK_{GM} and updates the cloud user list.

(v) CS decrypts $Enc_{PK_{CSP}}(CUL, ID_{Group}, ID_i, PK_E, v_2)$ sent by the GM using the private key SK_{CSP}. Then, CS checks whether the group with identity ID_{Group} exists and if one exists, then the new identity ID_i is added to the list. Else, a new list with this mentioned group identity is created in the cloud server.

Subsequently, CS selects a random number $CK_E \epsilon Z_q^*$ and sends $Enc_{PK_E}(CK_E, ID_i, v_2, PK_{CSP})$ to the group user with identity ID_i.

(vi) The user decrypts $Enc_{PK_E}(CK_E, ID_i, v_2, PK_{CSP})$ using the secret key SK_E and checks whether identity present in the message is same as the user's own identity. If successful, the user stores the secret key CK_E in its local database which is shared between the CS and the corresponding user and sends $Enc_{PK_{GM}}(ID_i, v_2)$ to GM.

(vii) GM decrypts the message and checks v_2. If successful, then it updates the *CUL* with the new identity of the user who is doing this registration process.

3.4 File Upload Phase

The data owner who owns the confidential document sends a request to GM as $Enc_{PK_{GM}}(ID_i, ID_{Group})$. GM decrypts the message from the data owner using his secret key SK_{GM} and sends $Enc_{PK_E}(ID_i, ACV_u)$ where ACV_u refers to the secret key vector $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \dots \\ \alpha_n \end{pmatrix}$ containing the secret keys shared by the members of the group with identity ID_{Group} in which n refers to the n^{th} member in the group. The data owner decrypts $Enc_{PK_E}(ID_i, ACV_u)$ using his secret key and randomly selects $\gamma \epsilon Z_q^*$ and computes $ek = e(P,P)^{\gamma}$. Also, the it encrypts the document as $Enc_{ek}(doc)$. Also, hides γ as $\gamma * \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \dots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \gamma\alpha_1 \\ \gamma\alpha_2 \\ \gamma\alpha_3 \\ \dots \\ \gamma\alpha_n \end{pmatrix}$ in which $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \dots \\ \alpha_n \end{pmatrix} = ACV_u$ and $\begin{pmatrix} \gamma\alpha_1 \\ \gamma\alpha_2 \\ \gamma\alpha_3 \\ \dots \\ \gamma\alpha_n \end{pmatrix} = ACV_g$. Here, $\gamma * ACV_u = ACV_g$. Finally, the data owner sends $Enc_{ek}(doc)$, ACV_g to CS as $ID_i, Enc_{CK_E}(ID_i, ID_{Group}, Enc_{ek}(doc), ID_{doc})$ to the CS. CS decrypts the message and retrieves the corresponding secret CK_E for the user with identity ID_i and decrypts the message. Thus, the user is able to store the document securely in the cloud server. Since the document is encrypted using the group key, the person who possesses the group key alone is able to decrypt it. In our case, neither the cloud server nor the group manager possess the group key and hence, the document can be decrypted only by the receiver. The enable the cloud server to identify the uploaded document from other documents stored in it, the identity of the document ID_{doc} is stored along with the document.

3.5 File Download Phase

The group user with identity ID_i sends a request to the CS for file download as $ID_i, ID_{Group}, Enc_{CK_E}(ID_i, ID_{Group}, ID_{doc}, v_3)$ such that $v_3 \epsilon Z_q^*$ refers to a random number. CS takes the ID_i of the group user and checks whether he is a member of the group represented by ID_{Group}. If the group user is ascertained that he is a member of the group, his corresponding secret key CK_E which is shared between the group user ID_i

and the CS is retrieved by the CS. CS decrypts $Enc_{CK_E}\left(ID_i, ID_{Group}, ID_{doc}, v_3\right)$ using the retrieved CK_E and verifies whether the user identity and group identity present in the decrypted content is the same as unencrypted identities. If successfully verified, CS sends $Enc_{CE_K}\left(ID_i, ID_{Group}, doc_i, Enc_{ek}(doc_i), Acv_g, v_3\right)$ to the group user. The group user decrypts the message $Enc_{CK_E}\left(ID_i, ID_{Group}, doc_i, Enc_{ek}(doc_i), Acv_g, v_3\right)$ using the secret key CK_E. Also, he computes $r_i^{'} * Acv_g = Acv_g^{'}$ which can be represented by $r_i^{'} * \begin{pmatrix} \gamma\alpha_1 \\ \gamma\alpha_2 \\ \gamma\alpha_3 \\ \dots \\ \gamma\alpha_n \end{pmatrix} = Acv_g^{'}$. The computation can be represented as below.

$$\begin{aligned} r_i^{'} * (\gamma\alpha_i) &= r_i^{'} * \gamma * (\delta_i^{'} * r_i) \\ &= \delta_i^{'} * \gamma * \left(r_i^{'} * r_i\right) \\ &= \delta_i^{'} * \gamma * (1) \\ &= \delta_i^{'} * \gamma \end{aligned}$$

Moreover, the group user makes the following computation as well in order to retrieve the group key.

$$\begin{aligned} \delta_i * (\delta_i^{'} * \gamma) &= \left(\delta_i * \delta_i^{'}\right) * \gamma \\ &= (1) * \gamma \\ &= \gamma \end{aligned}$$

4 Performance Evaluation

In this research, the data owner is left from any need for key updation which is automatically being taken care of by the GM. This improvement has a significant reduction in the need for computation if the group user is a mobile user which is a battery constrained device. During a user join or leave operation in the proposed protocol, the data owner is freed from the communication overhead also. The user who leaves the group sends the request $Enc_{PK_{GM}}\left(ID_i, ID_{Group}, \alpha_i\right)$ to GM and it does the necessary parameter removal and forwards the request to CS for further updation in the cloud server. The collusion attack is done by two or more users who left the group working co-operatively in order to retrieve the group key. Assume that, a user i has generated $\delta_i, \delta_i', r_i, r_i' \epsilon Z_q^*$ and user j has generated $\delta_j, \delta_j', r_j, r_j' \epsilon Z_q^*$ in order to be part of the group. But, after leaving the group, the two users exchange their credentials in an attempt to break the security and find the secret key γ. But, in the proposed protocol, the assumption has been made such that $\delta_i, \delta_i^{'}, r_i, r_i^{'}$ for all the users are all random numbers from Z_q^* and have nothing in common between them. Thus, though the users

try to collude, the scheme would resist a left user from acquiring the secret key γ successfully.

5 Security Analysis

The analysis of the proposed protocol is done based on the attacks and the efficiency of the proposed algorithm in resisting the attacks.

5.1 Forward Secrecy

The secret key is embedded in the access control vector as $\gamma * \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \dots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \gamma\alpha_1 \\ \gamma\alpha_2 \\ \gamma\alpha_3 \\ \dots \\ \gamma\alpha_n \end{pmatrix}$ in which γ is the secret key. The proposed method ensures forward secrecy by assuring that, a user who has left the group cannot access the documents belong to a group in which he is not a member.

5.2 Backward Secrecy

If m^{th} user joins the group at a time T, then the access control vector shall look like $\begin{pmatrix} \gamma\alpha_1 \\ \gamma\alpha_2 \\ \gamma\alpha_3 \\ \dots \\ \gamma\alpha_m \end{pmatrix}$ in which $\gamma.\alpha_m$ refers to the parameter intended for m^{th} user. But, before the inclusion of m^{th} user in the access control vector, it would be $\begin{pmatrix} \gamma\alpha_1 \\ \gamma\alpha_2 \\ \gamma\alpha_3 \\ \dots \\ \gamma\alpha_{m-1} \end{pmatrix}$ and thus, the m^{th} user cannot retrieve the secret key γ successfully. The context of ensuring the backward secrecy will hold true even if more than two users collude with each other in an attempt to break the security of the proposed ECDSEC algorithm.

5.3 Providing Security Over Insecure Communication Channels

Previous protocols exchanged secret keys between the data owner and the data users over insecure channels. But, in the ECDSEC scheme, with the efficient implementation of pairing based cryptography, the protocol securely exchanges the secret keys between the data owner, group user, group manager and the cloud server over insecure channels and this is the main objective of the proposed protocol.

5.4 Resistance to Collusion Attack

In the proposed protocol, the assumption has been made such that $\delta_i, \delta_i^{'}, r_i, r_i^{'}$ for all the users are all random numbers from Z_q^* and have nothing in common between them. Thus, though the users try to collude, the scheme would resist a left user from acquiring the secret key γ successfully.

6 Implementation

The proposed protocol incures less computational complexity measured in milliseconds due to the fact that, the user join operation keeps the data owner completely intact of it. A user who wishes to leave the group, sends a request to the group manager which in turn forwards the request to the cloud server after processing. The data owner is completely intact during the operation and this led to the enhanced performance efficiency. Only the group manager and the cloud server are part of the user join operation but not the data owner. Thus, the proposed protocol shows the minimum overhead among the protocols in the literature. As it is evident from the fact that, during the user join operation, the data owner is completely free from any computational overhead and the same is the case with the user leave operation as well. Hence, the proposed scheme performs better owing to its delegation of the maintenance of user leave and user join operations to the group manager.

7 Conclusions

This research work aims to securely distribute the group keys between the group manager, mobile users and the cloud service providers. The novel protocol, which is introduced in this research work enables a mobile user and a data owner to securely exchange the group keys in order to download the sensitive document from the public clouds. The protocol is an ideal candidate for implementing it in the real world scenario.

References

1. Bertino, E., Bonatti, A., Ferrari, E.: TRBAC: a temporal Role-Based Access Control Model. ACM Trans. Inf. Syst. Secur. **4**(3), 191–233 (2001)
2. Joshi, J.B.D., Rafae, B., Elisa, B., Arif, G.: Access-control language for multi-domain environment. IEEE Trans. Internet Comput. **8**(6), 40–50 (2004)
3. Barker, S.: Action-status access control. In: Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, pp. 195–204. ACM, Sophia Antipolis, France (2007)
4. Poovendran, R., Baras, J.S.: An information-theoretic approach for design and analysis of rooted-tree-based multicast key management schemes. IEEE Trans. Inf. Theory **47**, 2824–2834 (2001)

5. Kim, Y., Perring, A., Tsudik, G.: Group key agreement efficient in coummunication. IEEE Trans. Comput. **53**(7), 905–921 (2004)
6. Drira, K., Seba, H., Kheddouci, H.: ECGK: an efficient clustering scheme for group key management in MANET. J. Comput. Communications **33**(9), 1094–1107 Elsevier (2010)
7. Naranjo, J.A.M., Lopez-Ramosz, J.A., Casado.L.G.: A suite of algorithms for key distributions and authentication in centralized secure multicast environments. J. Computational Appl. Math. **236**(12), 3042–3051. Elsevier (2012)
8. Vijayakumar, P., Bose, S., Kannan, A.: Chinese remainder theorem based centralized group key management for secure multicast communication. IET Inf. Secur. IET **8**(3), 179–187 (2014)
9. Jeong, Y.S., Kim K.S., Kim, Y.T., Park, G.C., Lee, S.H.: A key management protocol for securing stability of an intermediate node in wireless sensor networks. In: 8th International Conference on Computer and Information Technology, pp. 471–476. IEEE (2008)
10. Kim, J.Y., Choi, H.K.: Improvements on Sun et al's conditional access systems in Pay-TV broadcasting systems. IEEE Trans. Multimed. 12, pp. 337–340 (2010)
11. Nabeel, M., Shang, N., Berino, E.: Privacy preserving policy-based content sharing in public clouds. IEEE Trans. Knowl. Data Eng. **25**(11), 2602–2614 (2013)
12. Sridhar, S., Smys, S.: A hybrid multilevel authentication scheme for private cloud environment. In: 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1–5. IEEE (2016)
13. Praveena, A., Smys, S.: Ensuring data security in cloud based social networks. In: Electronics. In: International conference of Communication and Aerospace Technology (ICECA), vol. 2, pp. 289–295. IEEE (2017)

Comparative Study on Deep Learning Frameworks for Object Detection

Elizebeth Kurian[1(✉)] and Justin Mathew[2]

[1] Computer Science and Systems Engineering, Saintgits College of Engineering, Kottayam, India
elizebeth.kurianl820@saintgits.org
[2] Saintgits College of Engineering, Kottayam, India
justin.mathew@saintgits.org

Abstract. Object detection is one among the major sub-domains of the computer vision which deals with the identification of objects of a pre-defined class. Recognition of object is imminent to identify numerous pertinent objects from an image or video. Several deep neural learning, machine learning based techniques are used for object detection in digital images and videos. This paper discusses a comparative study of some deep learning based object detection frameworks, and analysed on the benchmark mean Average Precision (mAP) and selected models are evaluated using PASCAL VOC 2007 dataset which is the standard image data set for object class identification and recognition. Among the selected detection models, PVANet has the highest mAP (84.9) with FPS 21.7 and is considered as the best object detection method.

Keywords: Computer vision · Object detection · Deep learning

1 Introduction

To visually sense the features of this world, human beings use their eyes and brains. Providing a similar or better capability to the computer is referred to as computer vision. Information from the images and videos can be automatically extracted and analysed using the computer vision. Computer vision aims at providing computers an automatic visual understanding of the world, several theoretical algorithms have been developed to achieve this. Machine Learning includes the computer vision where major algorithms are already being integrated with simple daily applications and business use cases. Facebook is using computer vision to recognize people in photos and perform numerous operations. Now-a-days, autonomous vehicles (AVs) rely on computer vision. AVs use computer vision to examine and choose a path of movement by inspecting multiple video inputs of the vehicle. Medical field is the prominent area where computer vision is applied. Diagnosis like reading x-rays, MRI scans, and other types of diagnostics are using image processing. Currently, personalized applications can be combined with computer vision without much effort.

The core applications of computer vision are object detection [1] and object classification. In object detection, a framework for identification will recognize a specific instance of an object, whereas, in object classification, a model has been trained on a

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 79–85, 2020.
https://doi.org/10.1007/978-3-030-37051-0_9

dataset of specific objects, this trained model classifies the new objects to the corresponding categories. Object Detection is achieved from the single object recognition to the multi-object recognition. Single object recognition can be stated as a problem of object classification as it identifies only one object from a single image. Following sections introduces the traditional object detection models and provides a brief note on deep learning and open datasets.

1.1 Traditional Object Detection Models

There are three stages in the traditional object detection models: selection of informative region, extraction of features, and their classification. In informative region selection, the whole image is scanned using a multi-scale sliding window and finds out all possible positions of the objects. This process is high-priced and leads to massive number of unnecessary windows. Feature extraction identifies objects in the image, Scale-invariant feature transforms [8], histograms of oriented gradients (HOG) [9], and Haar-like [10] features. It is hard to identify all kinds of objects due to the diverse appearance, illumination, and background of the images. To distinguish the target object from the other objects in the image, a classifier is essential. Support vector machine (SVM) [11], AdaBoost [12], and Deformable part-based model (DPM) [13] are some excellent classifiers.

1.2 Deep Learning and Open Datasets

Deep learning [2] is a sub-section of Machine Learning where knowledge is acquired through learning of data. It has formed a mainstream in the object recognition systems. With the emergence of deep learning, the issues in the traditional architectures of object detection are addressed. Convolutional Neural Networks (CNN) [7] is arguably the most popular deep learning architecture; in many research areas like classification of the image, image retrieval, image super-resolution reconstruction, facial identification, pedestrian recognition, video analysis, CNN has been widely used. Foundations of deep learning are dataset and neural network. Data required to carry out the experiment is referred to as dataset and extracting this data from real-time situations is a complex task, to reduce this issue various open source dataset are available. The accuracy of the neural network outcome relies on both the quality and size of the dataset.

Commonly used standard open datasets are ImageNet, COCO and PASCAL VOC. ImageNet dataset has 14 million surplus pictures with class annotations, also contains annotations of object locations and 20,000 categories of pictures are covered. ImageNet datasets are preferred in the research works such as image classification, object location, and object identification. “ImageNet International Computer Vision Challenge” (ILSVRC) [4] is a challenge based on ImageNet. Common Objects in Context (COCO) [5] is an open source dataset sponsored by Microsoft which includes more than 300,000 images encompassing 80 object categories. COCO is considered as the “standard” dataset for the performance of image semantic understanding as this dataset makes great advancement in segmentation recently.

In this paper, selected object detection frameworks are benchmarked based on mAP on the dataset PASCAL VOC (pattern analysis, statistical modeling and computational

learning visual object classes) [6]. mAP is the mean of the Average Precisions calculated over all the object classes of the challenge. PASCAL VOC is the very popularized and standardized image dataset for image classification, object identification, and segmentation. The PASCAL VOC 2007 (VOC07) dataset encompasses 20 classes (sheep, aeroplane, bicycle, boat, bus, car, motorbike, train, bottle, chair, dining table, potted plant, sofa, tv, person, bird, cat, cow, dog, horse) and contains a common set of tools for retrieving the datasets and notes. Compared with the previously mentioned ImageNet dataset, the size of the PASCAL VOC dataset is comparatively small and is fit for network-based programs. In PASCAL VOC 2007, all annotations are made available; new developments are the rise in the number of classes, the introduction of segmentation and person layout taster, annotations have been added with truncation flags, also evaluation measure changed to average precision.

2 Literature Survey

Fast R-CNN [14] is a Fast Region-based Convolutional Neural Network method for the detection of objects. It consists of several innovations to improve the speed of both training and testing, and also enhanced the precision of object detection. Fast R-CNN is compared with R-CNN [26] and SPPnet using the VOC07 and achieved a higher mAP. The object proposals are classified using the deep convolutional neural networks and is a fast update to R-CNN and SPPnet. R-CNN, SPPnet, and Fast R-CNN started from the identical pre-trained VGG16 network and use bounding-box regression. The results of VGG16 SPPnet are pre-determined and were taken from [15]. Single-scale training and testing were used by Fast R-CNN and achieved mAP 70.0% with FPS 0.5.

Faster R-CNN [16] has been developed by concatenating RPN and Fast R-CNN for object detection. Region Proposal Network (RPN) is a fully convolutional neural network that determines the objectness scores position and bounds of the object. Faster R-CNN uses RPN for object detection and RPNs are fully trained to produce extremely good region proposals. Faster R-CNN is a unified network and the RPN module tells the network where to look, thus it acts as the attention mechanism. Objects of a broad area of scales and their aspect ratios can be determined using Faster-RCNN. The Faster R-CNN using VGG-16 achieved 73.2% mAP with FPS 7 on the VOC07 test set.

Faster R-CNN [17] is based on residual learning framework to reduce the network training. Here VGG-16 has been replaced with ResNet-101. They are easier to optimize and achieved higher accuracy than previous ones. Here the layers are reformulated as learning residual functions and showed that Faster R-CNN has better performance on other detection methods. Both models are using the same detection mechanism, so better networks receive the gains. With FPS 5, object detection mAP is 76.4% on the VOC07 test set.

R-FCN [18] is the Region-based Fully Convolutional Network with fully convolutional layers which allows entire backpropagation for training and inference. The detection of an object from the image and their position are performed simultaneously. In R-FCN, all computations are shared on the whole image. R-FCN proposed position-sensitive score maps to solve the issue between translation-invariance detection and

classification of the image. This method is mainly used in Residual Networks (ResNets) [17]. For the 2007 Pa VOC, R-FCNs have achieved mAP score of 83.6%.

In YOLO [19], object detection is presented as a regression problem to the bounding boxes and their related class probabilities. Images are processed in YOLO real-time at the rate of at 45 frames per second. Another version of the network called Fast YOLO is also presented and its processing rate is 155 frames per second. YOLO faces issue with tiny objects that appear in groups and makes more localization errors compared to other object identification frameworks. YOLO is concerned with generalizing objects in new or unusual configurations as this model learns to predict the bounding boxes using the data. YOLO pushes mAP to 63.4% for VOC07 with FPS 45.

YOLO is prone to higher localization errors compared to other detection mechanisms. Moreover, YOLO has relatively low recall than other identification systems. An improved model of YOLO named YOLOv2 [20] overcame these issues; it is speedy, accurate and works as a good detector at small resolutions. YOLOv2 is ideal for low end GPUs, high frame rate videos, or multiple video streams as it works with high resolution at more than 90FPS with mAP almost comparable to Fast R-CNN. With operating above real-time speed, at high-resolution, YOLOv2 is an object detector with 78.6 mAP with FPS 40 on VOC07.

SSD [21] is the Single Shot MultiBox Detector for object identification using a single deep neural network and is used as a building block for huge models which require object detection phase. Multi-scale convolutional bounding box is used by the SSD and out-turns is connected to the multiple feature maps. Modeling the space of possible box shapes can be achieved from this. SSD removes proposal generation entirely and feature re-sampling stages or subsequent pixels and encompasses all calculations in one network. SSD can be easily indulged with other systems which require the component of detection and also it is easy to train. SSD512 model, for 512×512 input, outperforms Faster R-CNN in terms of accuracy on PASCAL VOC and achieves 76.9% mAP with FPS 19.

Feature Fusion Single Shot Multibox Detector (FSSD) [22], is the upgraded SSD method and has feature fusion module. Feature fusion module is filled with the features from different layers with different scales. Then convolutional layers are applied to fused feature map to generate pyramid features which will be fed to multi-box detectors to predict the final identification results. At the speed of 65.8 FPS, FSSD achieved 82.7 mAP on VOC07. This FSSD outperforms a lot of object detectors in both accuracy and efficiency.

A novel network structure called PVANet [23] reduces its redundancy by inheriting recent innovations including C. ReLU [25] and Inception structure and has more layers with fewer channels. PVANet achieved 84.9% mAP on VOC07 with FPS 21.7. PVANet is a light network which can able to perform complex vision tasks and can maximize the computational efficiency. Along with object detection, this new method can be used for semantic analysis and face recognition. PVANet is completely independent of network compression and quantization and thus modern compression and quantization methods are applicable to it.

For the training of region-based ConvNet detectors, Online Hard Example Mining Algorithm (OHEM) [24] is used. OHEM removes the hyper-parameters that are used in common. The effectiveness of the OHEM increases with the size and complexity of the

dataset; this shows a significant mark in the mAP performance on benchmark PASCAL VOC 2007 (78.9%).

3 Comparative Results

Comparison of different object detection methods on the dataset PASCAL VOC 2007 based on mAP is given in Fig. 1. Papers published within the past four years are chosen for study. Ten detection frameworks are selected and evaluated using the benchmark mAP.

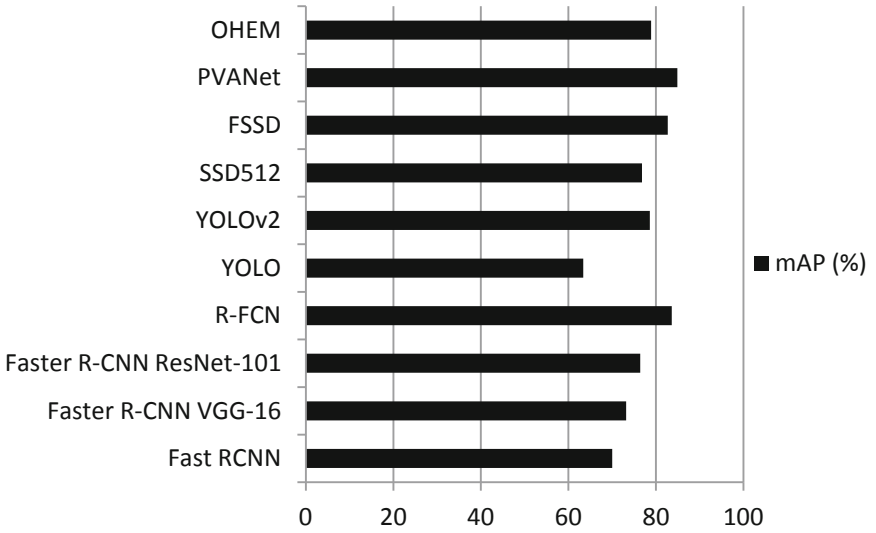


Fig. 1. mAP of detection methods on PASCAL VOC 2007.

In an overview, it is seen that PVANet is considered as the best object detection method and has the highest mAP (84.9) with FPS 21.7. Rapid training speed and higher accuracy advantages the PVANet as the superlative detection framework. R-FCN and FSSD are the other frameworks which hold the second and third position and were only at a small distance from PVANet. Localization errors of the YOLO has been overcomed by YOLOv2 and its mAP significantly surged about 15% than its previous version framework YOLO, which has the least mAP. A marginal increase in the mAP can be seen in the SSD512 and FSSD, i.e., mAP of 76.8 has been burgeoned to 82.7. Simple algorithm, OHEM gained 78.9 mAP on PASCAL VOC 2007. Faster R-CNN ResNet-101 is speedy than its antecedents Fast RCNN and Faster R-CNN VGG-16. Aforesaid mAP values stand on the strata VOC07 and vary according to other datasets.

4 Conclusion

Latterly, object detection has been a noteworthy discipline of exploration as it contains a plethora of information for semantic understanding regarding images and videos. Deep neural learning methods have acquired a great triumph in the domain of computer vision and object detection. A comparative study on various deep neural network object detection frameworks based on the results achieved on PASCAL VOC 2007 object classes has been stated in this paper. A few among the object detection methods within the past four years have been selected and found that PVANet object detection framework is foremost in the mAP. Computer vision has immense growth in the medical field due to its significant role in healthcare applications. Studies on the bigger perspective considering flow identification of tools from robotic assisted surgical strata can be done in the future to explore more on learning methods.

References

1. Felzenszwalb, P., Girshick, R., McAllester, D., Ramanan, D.: Object detection with discriminatively trained part-based models. IEEE Trans. Pattern Anal. Mach. Intell. **32**, 1627–1645 (2010)
2. Zhou, X., Gong, W., Fu, W., Du, F.: Application of deep learning in object detection. In: IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS), vol. 1, pp. 631–634, China (2017)
3. Deng, J., Dong, W., Socher, R., Li, L.J., Li, K., Fei-Fei, L.: Imagenet: a large-scale hierarchical image database. In: IEEE Conference on Computer Vision and Pattern Recognition, pp. 248–255 (2009)
4. Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., Huang, Z., Karpathy, A., Khosla, A., Bernstein, M., Berg, A., Fei-Fei, L.: Imagenet large scale visual recognition challenge. Int. J. Comput. Vis. **115**, 211–252 (2015)
5. Lin, T., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., Dollar, P., Zitnick, C.: Microsoft COCO: common objects in context. In: Computer Vision–ECCV, pp. 740–755. Springer International Publishing (2014)
6. Everingham, M., Van Gool, L., Williams, C., Winn, J., Zisserman, A.: The pascal visual object classes (voc) challenge. Int. J. Comput. Vis. **88**, 303–338 (2009)
7. LeCun, Y., Bengio, Y., Hinton, G.: Deep learning. Nature **521**, 436–444 (2015)
8. Lowe, D.: Distinctive image features from scale-invariant keypoints. Int. J. Comput. Vis. **60**, 91–110 (2004)
9. Dalal, N., Triggs, B.: Histograms of oriented gradients for human detection. In: 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05). IEEE (2005)
10. Lienhart, R., Maydt, J.: An extended set of Haar-like features for rapid object detection. In: Proceedings. International Conference on Image Processing, vol. 1, pp. I–I. IEEE (2002)
11. Cortes, C., Vapnik, V.: Support-vector networks. Mach. Learn. **20**, 273–297 (1995)
12. Freund, Y., Schapire, R.: A decision-theoretic generalization of on-line learning and an application to boosting. J. Comput. Syst. Sci. **55**, 119–139 (1997)
13. Xu, J., Ramos, S., Vazquez, D., Lopez, A.: Domain adaptation of deformable part-based models. IEEE Trans. Pattern Anal. Mach. Intell. **36**, 2367–2380 (2014)
14. Girshick, R.: Fast R-CNN. ICCV (2015)

15. He, K., Zhang, X., Ren, S., Sun, J.: Spatial pyramid pooling in deep convolutional networks for visual recognition. In: Computer Vision–ECCV 2014, pp. 346–361 (2014)
16. Ren, S., He, K., Girshick, R., Sun, J.: Faster R-CNN: towards real-time object detection with region proposal networks. IEEE Trans. Pattern Anal. Mach. Intell. **39**, 1137–1149 (2017)
17. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: CVPR (2015)
18. Dai, J., Li, Y., He, K., Sun, J.: R-FCN: object detection via region-based fully convolutional networks. In: NIPS (2016)
19. Redmon, J., Divvala, S., Girshick, R., Farhadi, A.: You only look once: unified, real-time object detection. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2016)
20. Redmon, J., Farhadi, A.: YOLO9000: better, faster, stronger. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2017)
21. Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C., Berg, A.: SSD: single shot multibox detector. In: Computer Vision–ECCV, pp. 21–37 (2016)
22. Li, Z., Fuqiang Z.: FSSD: feature fusion single shot multibox detector. In: CoRR (2018)
23. Hong, S., Roh, B., Kim, K., Cheon, Y., Park, M.: PVANet: lightweight deep neural networks for real-time object detection. In: NIPS 2016 Workshop on Efficient Methods for Deep Neural Networks (EMDNN) (2016)
24. Shrivastava, A., Gupta, A., Girshick, R.: Training region-based object detectors with online hard example mining. In: 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2016)
25. Shang, W., Sohn, K., Almeida, D., Lee, H.: Understanding and improving convolutional neural networks via concatenated rectified linear units. In: ICML (2016)
26. Girshick, R., Donahue, J., Darrell, T., Malik, J.: Rich feature hierarchies for accurate object detection and semantic segmentation. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 580–587 (2014)

An Adaptive Neighbour Knowledge-Based Hybrid Broadcasting for Emergency Communications

Manjusha Deshmukh[1(✉)], S. N. Kakarwal[2(✉)], and Ratnadeep Deshmukh[3(✉)]

[1] Computer Engineering Department, Pillai College of Engineering, Mumbai, India
mdeshmukh@mes.ac.in
[2] Computer Engineering Department, PES College of Engineering, Aurangabad, India
skakarwal@yahoo.com
[3] Computer Science Department, Dr. B.A.M. University, Aurangabad, India
rrdeshmukh.csit@bamu.ac.in

Abstract. In recent years, mobile ad-hoc networks have rooted their pillars for emergency communication owing to reasonable cost, diversity, and easiness of mobile devices. The mobile ad-hoc networks is a self-coordinated, distributed and infrastructure-less network of mobiles nodes. These characteristics of MANET enhanced the applicability of MANET in the field of emergency communication such as military and police operations, flood control and fire disaster management, etc. In MANET, a broadcast storm causes network problems as there are redundant broadcasts and packet collisions. Classical broadcast methods have motivated on evading broadcast storms by preventing some rebroadcasts. The further problem is the link breakages induced by node instability and their power exhaustion. In this research, we propose an adaptive neighbor knowledge-based hybrid broadcasting method to address these network problems. This method refines the counter threshold based on neighbourhood, mobility and energy of the node and makes use of the refined thresholds to make the broadcasting decision. The proposed method perform best as compared to AMECBB and TCBB by decreasing delay, packet dropping, and routing overhead and energy consumption.

Keywords: MANET · Broadcasting · Neighbour Knowledge-based routing, etc.

1 Introduction

Today, the cellular mobile network constructs the pillars of the existing communication system. In emergency circumstances, these cellular mobile networks could be disrupted during a natural disaster such as an earthquake, flood, tsunami, etc. or a man-made disaster such as terrorist attack, bomb blasts, etc. [1–3]. Furthermore, in inaccessible regions such as hills, mountains, etc., cellular mobile networks are not available due to inaccessibility of cellular signal. Ultimately, the mobile ad-hoc network offers

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 86–97, 2020.
https://doi.org/10.1007/978-3-030-37051-0_10

communication in the disaster-affected area and inaccessible areas for smooth conduction of rescue operations.

Mobile ad-hoc networks is a self-coordinated, distributed and infrastructureless network of mobiles nodes. In mobile ad-hoc networks, every node is constantly moving, producing alternative routes to be settled among the mobile nodes through a period of time. With the purpose to guarantee connectivity between mobile nodes in the absence of existing infrastructure, each mobile node in the mobile ad-hoc network acts as a router to accomplish routing operation. Hence, routing is an interesting operation. The continuously changing behavior and low power consumption of mobile ad-hoc networks energized many researchers to work on routing in mobile ad-hoc networks. These researchers are forced to use broadcasting to propagate emergency messages in disaster circumstances. Utmost routing protocols use flooding as a broadcasting mechanism for route discovery. Flooding accomplishes neighbourhood processing by rebroadcasting the acquired packet to neighbourhood nodes until it reaches the destination node. It is a very elegant approach to implement route discovery in mobile ad-hoc networks but suffers from broadcast storms [4, 5]. Classical broadcast methods have motivated on evading broadcast storms by preventing some nodes from rebroadcasts. These classical broadcast methods are categorized as counter-based and non-counter-based methods. The difference between these two methods lies in the decision parameter used to make a broadcast forwarding decision. The counter-based scheme aims to eliminate the number of broadcasts based on the number of broadcast packets received during the broadcast process from nodes neighbourhood. Therefore, in this research, we introduce a counter-based method to focus on the nodes vicinity in the network during the process of route discovery. This method accumulates the one-hop and two-hop neighbourhood information and then chooses the routes corresponding to the association between the one-hop and two-hop neighbours. Further, the mobility and power exhaustion of mobile nodes cause link breakages in the mobile ad-hoc networks [6]. In order to make a more robust method against link breakages due to mobility and energy exhaustion of the mobile nodes, the speed and the energy of the nodes are also taken into consideration to focus upon. The goal of our proposed method is to address the routing problems induced in MANET and enhance the performance by combining the classical broadcast methods.

The rest of this paper is arranged as follows. Section 2 describes classical broadcast methods used in the literature. Section 3 proposes an adaptive neighbour knowledge-based hybrid broadcasting method (ANKHB). Section 4 describes the performance study of proposed method evaluated through simulation and comparative analysis. Section 5 concludes the paper.

2 Related Work

The broadcast storm and link breakages problems have a significant impact on the lifetime of the network. In literature, many counter-based and noncounter based methods are exploited to address the routing problems induced in MANETs. The counter-based and non-counter based methods are further categorized corresponding to

the decision parameters used to make the broadcast forwarding decision such as neighbor-knowledge, distance, speed, and energy.

Neighbour-knowledge based methods: These methods are categorized as density based and vicinity based methods corresponding to the broadcast decision parameter. The density-based methods make use of local density (number of neighbours) measure and global density (total number of nodes in the network) measure to take the broadcast decision. These methods aim to reduce the broadcasts in the high-density network. In [7, 8], the authors proposed Density-aware Probabilistic method in which the broadcast forward probability is attuned to inversely proportionate to the local density and directly proportionate to the efficiency parameter adaptable to topological factors. In [9], the authors exploit the additional coverage by knowing the one-hop neighbours and global density measure i.e. the total number of nodes which eventually replaced in [10] by the average number of nodes in the network.

The vicinity based methods use the nodes vicinity in one-hop neighbourhood scope and two-hop neighbourhood scope as one of decision parameter to make the broadcast decision. These methods accumulate the one-hop and two-hop neighbourhood information and then take into account the association between the one-hop and two-hop neighbours to make broadcast decision making. In [11], the authors proposed three different variations of the vicinity based method. In the first variation, the broadcast forward probability is attuned according to the density of two-hop neighbors attained only through one-hop neighbors. This variation attempts to avoid lonely nodes. The second variation fixed the broadcast forward probability to the fraction of one-hop neighbors within two-hop neighbourhood scope. The third variation decided the broadcast forward probability to the fraction of two-hop neighbors within two-hop neighbourhood scope.

However, in another approach [12], Hyocheol Jeong, Jeonghyun Kim, Youngh wan Yoo proposed a family classification of nodes neighbours. The parent node and their one-hop neighbours are considered at first position whereas parent nodes two-hop neighbours are designated as child nodes that acquires the second position. Then they take into account the association with all their neighbours in order to decide broadcast forward probability. The broadcast forward probability induced is directly proportionate to the number of child nodes and inversely proportionate to the number of one-hop neighbours of the parent node.

In [13], the D. G. Reina, S. L. Toral, P. Jonhson, F. Barrero united density based and vicinity based approaches to flooding to address broadcast storms and link failure problems incurred due to the instability of the nodes. They proposed the forward neighbourhood measure in order to differentiate the density of nodes in two-hop neighbourhood vicinity to the one-hop neighbourhood vicinity. The forward probability is adjusted according to the forward neighbourhood measure of the previous and the current node. The forward probability is based on the implication that the density decreases if the forward neighbourhood measure of the current node is less than the forward neighbourhood measure of the previous node and vice-versa.

Distance based methods: These methods [14, 15] are categorized as Euclidean distance based and RSS based methods corresponding to the broadcast decision parameter. The goal of these methods is to decrease rebroadcasts by the selection of the

farthest nodes from the senders. Euclidean-distance based methods use the distance between the source and the destination nodes as the decision measure for the broadcast process provided with the support of the GPS system. The RSS based methods use the relative distance between the nodes as a function of the signal power.

Speed based methods: As mobile nodes are not limited by the speed, highly unstable nodes may cause drastic changes in the topology of MANET which in turn cause link breakages in the network. Hence, the objective of the speed based methods is to reduce redundant broadcasts by the choice of highly stable nodes to determine further steady routes [16–18] in the high-density network. These methods are intent to reduce link breakages in low-density networks of faraway dispersed nodes to induce less intermediate nodes for the route discovery process.

Energy based methods: Owing to the limited power capacity of the mobile nodes, the nodes possibly die out earlier in high-density networks to cause linkage breakages. Therefore, energy based methods aim to achieve network lifetime by the reduction of the rebroadcasts through the selection of strong nodes during route discovery [19, 20].

3 Adaptive Neighbour Knowledge-Based Hybrid Broadcasting Method

The ANKHB method gathers the one-hop and two-hop neighbourhood information and uses nodes vicinity in one-hop neighbourhood scope and two-hop neighbourhood scope as one of the decision parameters to ensure connectivity of the ad-hoc network. Moreover, the mobility and power exhaustion of mobile nodes also causes network link breakages in the mobile ad-hoc networks. Therefore to ensure long-lasting network lifetime, ANKHB have taken into consideration the speed and the energy of the mobile nodes. MANET can be represented as an undirected graph (M) of mobile nodes (N) linked through the edges (E) of the graph. The edge (N_i, N_j) exists if there is connectivity between node N_i and node N_j.

Neighbouring Knowledge Acquisition

Hello packets are used to acquire neighbor knowledge information from the network. The node sends the Hello packet to the nodes in its coverage. If the Hello reply is received from these neighbouring nodes within the constrained time then these nodes become the neighbouring nodes of that node. By the use of Hello message, when a node (N_i) receives a broadcast packet it performs the following

1. Initializes packet counter,
2. Constructs One-hop neighbour set (O) of node N_i,
3. Constructs Two-hop neighbour set (T) of node N*i*,
4. Constructs Common neighbour set (I) such that I (N_i) = O (N_i) $\cap$ T (N_i).

Stability and Energy Efficiency Estimation

Nextly, the stability, and energy fraction is estimated for the common neighbor set (I).

1. Stability (S) is computed as the ratio of the difference of maximum speed (S_{max}) and current speed (SN_i) to the maximum speed (S_{max}).
2. Energy Efficiency (E) is computed as the ratio of the energy of the node (EN_i) to the initial energy of node (E_{ini}).

Classifying Stability and Energy Efficiency

1. To specify the mobility of the MANET, stability type (S_{ty}) is evolved as Condition ($S > S_{uth}$).

$$\begin{array}{ll} S_{ty}\ :\ \text{if condition} = \text{True}; & S_{ty} = \text{More Stable} \\ \quad\ \text{Otherwise}; & S_{ty} = \text{Unstable} \end{array}$$

2. Also, stability type (S_{ty}) is evolved as Condition (S_{lth}) < S < (S_{uth})

$$\begin{array}{ll} S_{ty}\ :\ \text{if condition} = \text{True}; & S_{ty} = \text{Stable} \\ \quad\ \text{Otherwise}; & S_{ty} = \text{Unstable} \end{array}$$

3. To specify the energy efficiency of the MANET, energy efficiency type (E_{ty}) is evolved as condition ($E > E_{th}$).

$$\begin{array}{ll} E_{ty}\ :\ \text{if condition} = \text{True}; & E_{ty} = \text{Strong} \\ \quad\ \text{Otherwise}; & E_{ty} = \text{Weak} \end{array}$$

Assigning Thresholds and Broadcasting

The counter thresholds are dynamically set as per the energy efficiency and stability of the network in spite to make broadcast decision making. The refinement of the thresholds decides the number of transmissions allowed in the network. The ANKHB refines counter threshold to decide counter thresholds (C_{th}) as High, High Moderate, Low Moderate and Low from two conditional attributes viz., S_{ty} and E_{ty}. The refinement is methodized as follows in Table 2. Then based on stability and energy efficiency type it constructs the following:

1. Highly stable set (HS), strong set (ST), weak set (W) and, stable(SB) of node N_i.

2. Common neighbour set of highly stable and strong nodes (M) such that M (N_i) = HS (N_i) $\cap$ ST (N_i)

Thus, it decides preferences to form stable routes which makes the use of stability and energy efficiency of the mobile nodes. If the packet counter reaches counter threshold (C_{th}) then the packet is dropped otherwise transmitted (Table 1).

Table 1. Characteristic refinement table

No.	S_{ty}	E_{ty}	C_{th}
1	Highly stable	Strong	High
2	Highly stable	Weak	High moderate
3	Stable	Strong	Low moderate
4	Otherwise	Otherwise	Low

4 Performance Study

This section describes comparative methods, evaluation setup and performance measures used for evaluation of the proposed protocols.

4.1 Comparative Methods

The performance of the ANKHB is evaluated by comparing the proposed method with the AMECBB and TCBB methods.

AMECBB The adaptive, mobility-aware energy-efficient, counter-based broadcasting (AMECBB) is a hybrid probabilistic method of packet counter and neighbor knowledge, speed and energy-based methods. AMECBB refines the counter thresholds based on the network, speed, and energy of mobile nodes which forms the platform for rebroadcast probability estimation. The substantial accomplishments obtained by AMECBB to address MANET issues are:

1. AMECBB provides a robust method to achieve efficient route discovery by reducing the overall energy consumption of the network to increase the durability of the network.
2. Retransmissions are constrained by introducing a random delay which indirectly avoids packet dropping due to collision falloff.

TCBB It is a novel counter-based broadcasting method using TOPSIS multicriteria decision-making that determines whether to broadcast according to a set of parameters. It focuses on three main decision parameters of the mobile node viz., the neighborhood, mobility, and energy. The rebroadcast probability function is constructed by mapping three decision parameters into a single parameter. The weights of these criteria reflect their relative importance in the decision-making process. The significant achievements obtained by TCBB as a means to address MANET issues are:

1. TCBB offers effective route discovery which involves the neighbourhood propagation and multi-criteria decision making to achieve guaranteed delivery by the reduction in the redundant broadcasts.

2. Re-transmissions are controlled by the TOPSIS Multi-criteria decision-making which estimates the performance of each alternative by relatively simpler mathematical computation to reduce the latency of the route discovery.

4.2 Evaluation Setup

This section aims to evaluate the performance of an adaptive neighbour knowledge based hybrid broadcasting (ANKHB) method using the NS-2 Simulator (NS-2.34). The parameters used in the following simulation experiments for Mobile Ad-hoc network are listed in Table 2. The network has a constant transmission range of 250 m. The MAC layer scheme follows the IEEE 802.11 MAC specification. The movement pattern of each node follows the random way point model. The two-ray ground reflection model which considers both the direct path and a ground reflection path as a radio propagation model. The transceiver of MANET is configured with Omni directional antenna. The mobile nodes move over the terrain size of 1000*1000. The simulation was performed for the network of 100 nodes over the varying simulation times of (75, 100, 125, 150, 175, 200).

Table 2. Simulation parameters

No.	Parameter	Value
1	Network area	1000*1000
2	Transmission range	250 m
3	Simulation time	350 s
4	Traffic pattern	CBR(UDP)
5	Number of nodes	100
6	Pause time	25 ms
7	Routing protocol	AMECBB, TCBBB, ANKHB
8	MAC protocol	IEEE 802.11
9	Mobility model	Random way point mobility model
10	Propagation model	Two ray ground
11	Anteena	Omni directional

4.3 Performance Measures

The measures used to evaluate the effectiveness of the proposed method are the Packet dropping ratio, total consumed energy, delay, normalized routing overhead and throughput.

Packet Dropping Ratio The packets are dropped in the network if they fail to reach to the destination because of congestion in the network. The congestion occurs in the network because of redundant re-transmissions. The packet dropping ratio can be defined as the ratio of the number of packets dropped to the total number of packets sent. Therefore, it is desirable to have smaller packet dropping ratio. Figure 1 shows the graph of packet dropping ratio versus time. The packet dropping ratio were

increased from the low simulation time to the high simulation time for the comparative as well as proposed protocol. Indeed,

ANKHB performed better than AMECBB and TCBB by reducing dropping ratio by an additional 15% and 40% respectively.

Delay In order to reach from the source to the destination, the packet travels through the number of intermediate nodes. Delay is defined as the total time required by a packet to travel from the source to the destination. A lower delay means better performance. Figure 2 presents a graph of the delay versus time. There is no significant increase or decrease in delay over the increasing simulation time for the ANKHB. Truly, ANKHB outperformed AMECBB and TCBB in reducing the delay by an additional 63% and 56% respectively. As more the number of re-transmissions are condensed in our proposed method the overall routing process speeds up.

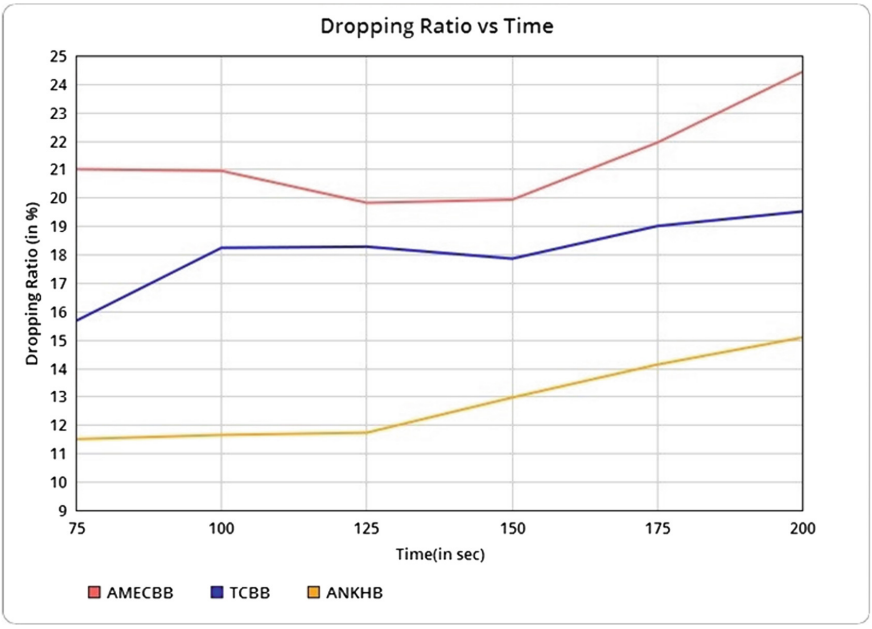


Fig. 1. Packet dropping ratio versus time

Total Energy Consumed Total energy consumption is defined as the difference between the current and initial energies of nodes. A lower total energy consumption means better performance for a proposed scheme. Figure 3 shows a graph of the total consumed energy versus the simulation time, emphasizing that total consumed energy increased over increasing simulation time when using the proposed method as well as comparative methods. In fact, ANKHB decreased the total energy consumption by more than 53% compared to the AMECBB method and 46% compared to TCBB method. As nodes vicinity and energy has a considerable impact on the number of the

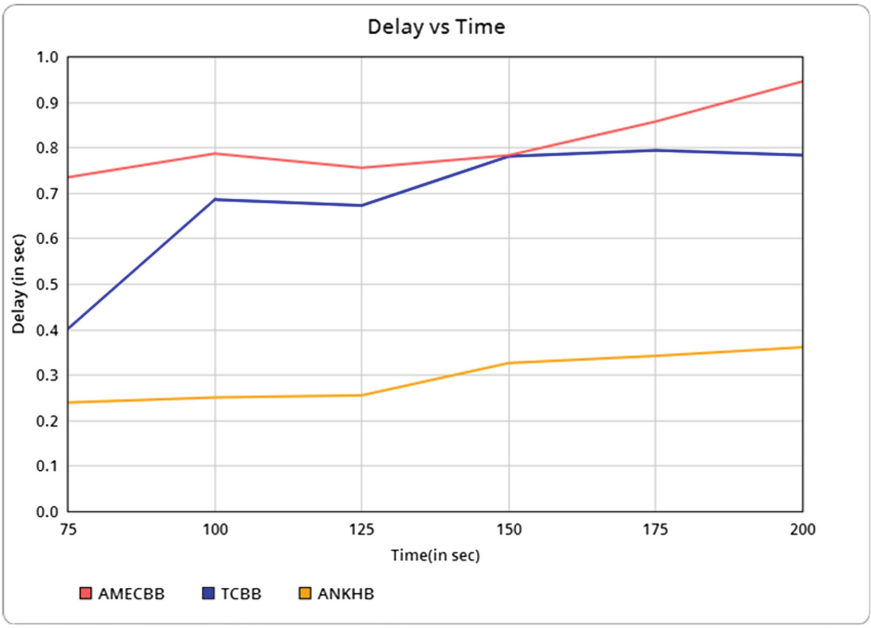


Fig. 2. Delay versus time

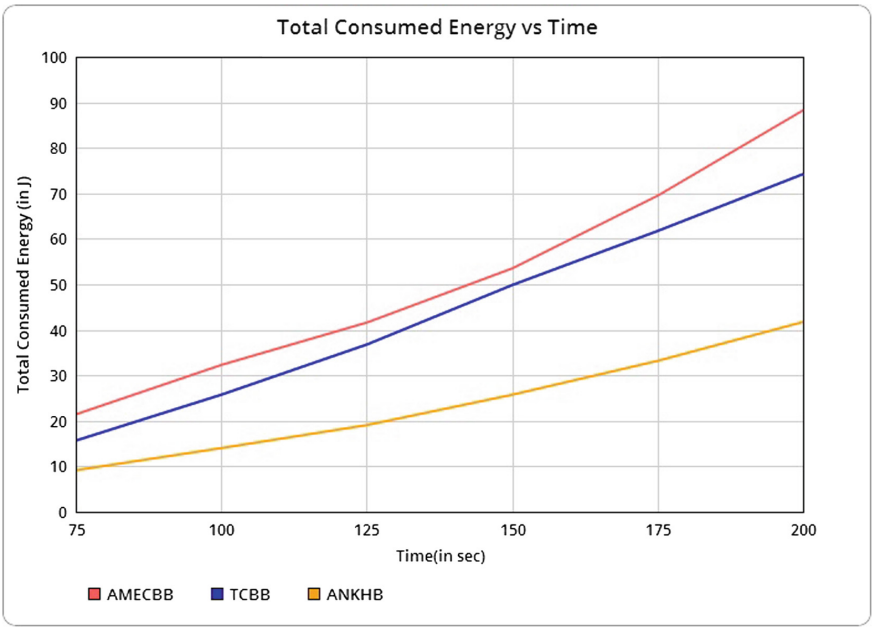


Fig. 3. Total consumed energy versus time

re-transmission in our proposed scheme the overall energy consumption is reduced more compared to comparative methods.

Normalized Routing Overhead The continuous changing position of the mobile nodes has an impact on the routing overhead of the network. To overcome this issue, ANKHB attempts to limit the selection of highly stable nodes providing long term connectivity. Figure 4 shows a graph of the normalized routing overhead versus the simulation time. The normalized routing overhead was decreased at the start of the simulation time then it remained stable for the proposed method as well as comparative methods. Indeed, ANKHB outperformed AMECBB and TCBB in reducing the normalized routing overhead by an additional 9% and 3% respectively.

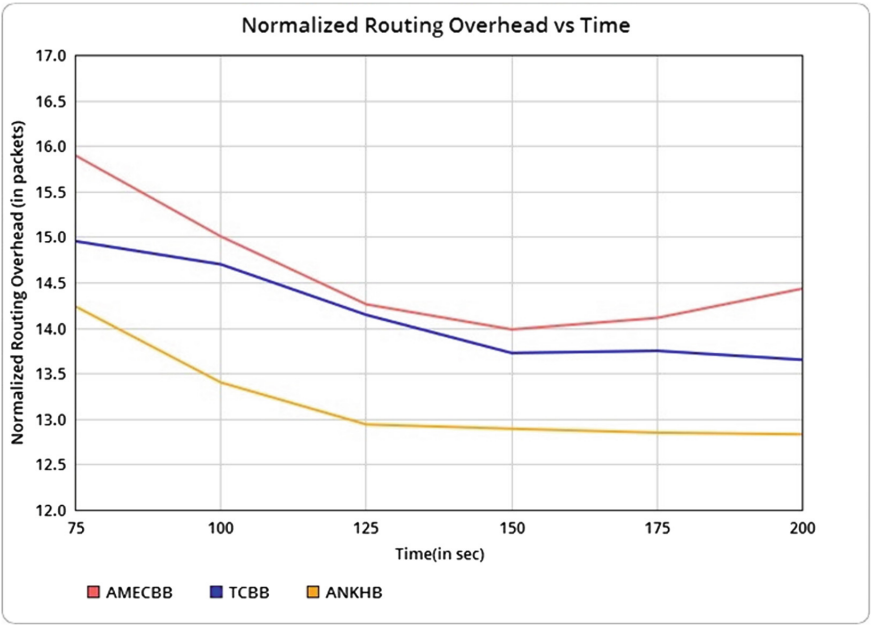


Fig. 4. Normalized routing overhead versus time

5 Conclusion

In this research, an adaptive neighbour knowledge based hybrid broadcasting method was proposed which dynamically refines the counter thresholds based on nodes vicinity information, speed, and energy of the mobile nodes to address the issues of MANET. ANKHB method accumulates the one-hop and two-hop neighbourhood information and then take into account the association between the one-hop and two-hop neighbours to make broadcast decision making. It considers the common set of nodes to act as forwarder nodes for route discovery process to reduce link failures. The dynamic nature of MANET incurs high routing overhead in the network. To reduce routing

overhead, ANKHB attempts to limit on the selection of highly stable nodes of the common set of nodes. The performance evaluation revealed that ANKHB outperformed over AMECBB and TCBB. In fact, ANKHB decreased the normalized routing overhead by more than 9% compared to the AMECBB method and 3% compared to TCBB method as well as reduced the delay by an additional 63% and 56% respectively. Further, energy consumption was reduced by 53% when compared with AMECBB and by 46% when compared with TCBB.

References

1. Jyoti Grover, Ashish Jain, N. S. Chaudhari. Ahmed Y. Al-Dubai: Unmanned Aerial Vehicles operated Emergency Ad hoc Networks. In: 7th International Conference on Communication Systems and Network Technologies. IEEE (2017)
2. Anjum, S.S., Noori, R.M., Anisi, M.H.: Review on MANET based communication for search and rescue operations. Int. J. Wirel. Pers. Commun. **94**(1), 31–52 (2017). (Springer)
3. Reina, D.G., Toral, S.L., Barrero, F., Bessis, N., Asimakopoulou, E.: Modelling and assessing ad hoc networks in disaster scenarios. J. Ambient Intell. Humaniz. Comput. **4**(5), 571–579 (2013). (idUS)
4. Ni, S.Y., Tseng, Y.C., Chen, Y.S., Sheu, J.P.: The broadcast storm problem in a mobile ad hoc network. In: 5th Annual ACM/IEEE InterNational Conference On Mobile Computing and Networking (MobiCom). ACM (1999)
5. Tseng, Y.C., Ni, S.Y., Shih, E.Y.: Adaptive approaches to relieving broad-cast storms in a wireless multihop mobile ad hoc network. Trans. Comput. **52**(5), 545–557 (2013). (IEEE)
6. Fazio, F., Guerriero, F., Fazio, P.: Link stability and energy aware routing protocol in distributed wireless networks. Trans. Parallel Distrib. Syst. **23**(4), 713–726 (2012). (IEEE)
7. Cartigny, J., Simplot, D.: Border node retransmission based probabilistic broadcast protocols in ad-hoc networks. In: 36th Annual Hawaii International Conference on System Sciences (HICSS 03). IEEE (2003)
8. Scott, D.J., Yasinac, A.: Dynamic probabilistic retransmission in ad hoc networks. In: Proceeding of the International Conference on Wireless Networks (ICWN04). (2004)
9. Zhang, X.M., Wang, E.B., Xia, J.J., Sung, D.K.: A neighbour coverage-based proba-bilistic rebroadcast for reducing routing overhead in mobile ad-hoc networks. Trans. Mob. Comput **12**(3), 424–433 (2013). (IEEE)
10. Ejmaa, A.M.E., Subramaniam, S., Zukarnain, Z.A., Hanapi, Z.M.: Neighbour-based dynamic connectivity factor routing protocol for mobile ad-hoc network. J. IEEE Access. **4**, 8053–8064 (2016). (IEEE)
11. Ryu, J.P., Kim, M.S., Hwang, S.H., Han, K.J.: An adaptive probabilistic broadcast scheme for adhoc networks. In: Conference on High speed Networks and multimedia communications, pp. 646–654. IEEE (2003)
12. Jeong, H., Kim, J., Yoo, Y.: Adaptive broadcasting method using neighbor type information in wireless sensor networks. Sensors **11**(6), 5952–5967 (2011). (NCBI)
13. Reina, D.G., Toral, S.L., Jonhson, P., Barrero, F.: Hybrid flooding scheme for mobile ad hoc networks. IEEE Commun. Lett. **17**(3), 592–595 (2013). (IEEE)
14. Wisitpongphan, N., Tonguz, O.K.: Scalable broadcast strategies for ad hoc routing protocols. In: 1st International Symposium on Wireless Pervasive Computing, pp. 1–6. Springer (2006)
15. Wisitpongphan, N., Tonguz, O.K., Parikh, J.S., Mudalige, P., Bai, F., Sadekar, V.: Broadcast storm mitigation techniques in vehicular ad hoc networks. IEEE Wirel. Commun. **14**(6), 84–94 (2007). (IEEE)

16. Khamayseh, Y., Darwish, O., Wedian, S.: MAAODV mobility aware routing protocols for mobile ad hoc networks. In: Conference on Systems and Networks Communications, IEEE (2009)
17. Yassein, M.B., Al-hassan, A.A., Taye, Z.A.: Performance analysis of the effects of network density and network mobility on velocity based. In: Conference on Systems, Signals and Devices (SSD), pp. 1–7. IEEE (2010)
18. Khalaf, D.M.B., Al, A.Y., Abed, M.: New velocity aware probabilistic route discovery methods for MANET. In: 20th Conference on Software, Telecommunications and Computer Network (SoftCOM), pp. 1–6. IEEE (2012)
19. Shivashankar, H.N., Varaprasad, G., Jayanthi, G.: Model and protocol for energy efficient routing over mobile ad hoc networks. Transact. Emerg. Top. Comput. **2**(2), 192–197. (2012). (IEEE)
20. Zhu, J., Wang, X., Trans. Mob. Comput. **10**(11), 1546–1557 (2011). (IEEE)

Traffic Congestion Control Using Hierarchical Decision Model

Suprit Atul Gandhi, Vinay Prakash Desai(✉),
Akshay Sameer Abhyankar, and Vahida Attar

Department of Computer Engineering and Information Technology,
College of Engineering, Pune, Maharashtra, India
{gandhisal5.comp, desaivpl6.comp, abhyankarasl5.comp,
vahida.comp}@coep.ac.in

Abstract. Nowadays, due to the advancement in engineering and technology, the number of vehicles has been increased drastically. So, there is a need for proper management of traffic in order to maintain the smooth functioning of the cities and nation as a whole. Though various techniques are evolved for traffic object detection, it has been used for managing the traffic. The project focuses on developing an efficient algorithm for controlling the traffic signal lights. It uses a hierarchical decision-making model, providing local decisions based on statistics, and global decisions based on pattern learnt at a higher level. Situations like emergency arrival and accidents would be handled by the global nodes' network. The decision taken would be communicated to the self-automated cars for their future decision.

Keywords: Vehicle traffic · Hierarchical model · Random forest · Online machine learning · IoTivity stack · Simulation · Smart cities

1 Introduction

Traffic congestion is one of the biggest problems faced by almost all metropolitan cities. Even developing cities and other small towns are facing similar issues. In a recently conducted survey, it has been observed that people spend around 90 min per day travelling. This not only causes fatigue and inconvenience, but we also go through huge financial loss. This is a huge and alarming problem. Traffic congestion is caused by many different issues like poor quality roads or narrow roads, accidents, and most importantly vehicle density. Vehicle density on the road is slowly increasing which portray the breakdown of transportation base. For a common man, time is the most precious thing. Hence it is necessary to have an efficient real-time system that ensures a smooth flow of traffic.

Our current signals are static i.e. they work according to predefined time at any given moment of the day. For example, a signal will be green for 30 s at 11 pm and at 10 am. The difference is that at night 30 s are enough for all the cars to pass through but at 10 am during office hours, the number of cars that pass through 30 s is not significant so at such times the timer should be increased [1]. So, we need a dynamic system to monitor the timing of signals. In our paper, we have proposed a system where

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 98–106, 2020.
https://doi.org/10.1007/978-3-030-37051-0_11

centrally-controlled traffic signals and sensors regulate the flow of traffic through the city in response to demand. Our system focuses on better traffic management by considering the very specific detail of the real-time condition of roads and then try to optimize the traffic flow [2]. The point is to determine the traffic density on each side of the road by calculating the number of vehicles at traffic signal zone at regular interval of time by using Image processing techniques. The data is collected and then fed to a local controller which then communicates with the global controller. At the local level, the traffic poles will communicate with each other through the centre node, which would then take the decision. The global node would take decision-based on the patterns learnt so far [3, 9].

In most of the cities in India, CCTV cameras are already deployed at every intersection which reduced our extra hardware requirement. The cameras can capture car and pedestrian density along with car speed. On top of this, it can also detect an ambulance and accidents which cause major congestion. But this is just one of the solutions [4, 10]. There are also other solutions proposed to tackle the congestion issue. A similar type of approach is proposed in Optical Information System. The developed real-time algorithms for image processing in this system extracts traffic data all the time and in any weather condition [5, 11–13]. Another solution to reduce congestion is by ride sharing. Instead of one man going in one car, other people going to the same office on the same route can share his ride. Which will reduce the number of cars on the road and reduce pollution to some extent. This comes under Travel Demand Management (TDM) i.e. strategies that increase travel choices to people [6–8].

It is seen that existing solutions to reduce the congestion problem have varied efficiency levels, due to a number of factors. In order to increase efficiency, our proposed solution is as follows.

2 Proposed Solution

We propose a hierarchical decision model to control traffic congestion. In the model hierarchy consists of majorly two types of controllers:

1. Local Controller
2. Global Controller

2.1 Local Controller

It is responsible for the decision making of a traffic signal at intersection or roundabouts. It does take it into account the traffic parameters of the adjacent or neighbouring intersection. At the local level, a set of rules will be provided to the controller and depending upon the circumstances the local controller will make decision-based on static rules provided.

Traffic parameters for decision making at the local level are as follows:

- Current traffic density per lane (for example traffic density includes a number of vehicles)
- Current pedestrian density

- Average waiting time of vehicles and pedestrians
- Information about congestion from neighbouring nodes
- A decision from the global controller.

1. Get Snapshots from every Camera associated with an Edge registered with Node Controller.

C: Camera, E: Edge, CD: Car Density, CWT: Car Waiting Time, PD: Pedestrian Density, PWT: Pedestrian Waiting Time

Let it be C1: E1 → (CD1, CWT1, PD1, PWT1)
C2: E2 → (CD2, CWT2, PD2, PWT1)
C3: E3 → (CD1, CWT1, PD1, PWT1) and so on for the entire map.

2. Convert data into Data frame using conversion function:

a. Classify CDi and PDi into Very High, High, Medium, Low, Very Low of Density Class
b. Classify CWTi and PWTi into Very High, High, Medium, Low, Very Low of Waiting Time Class.

3. Decision:

Acquiring information from the above data frame along with Neighbouring Controller's and Global Controller's Decision, the time period of each signal is decided. This decision is modified when an ambulance or an accident is detected.

2.2 Global Controller

Two or more than two local controllers comes under the global controller. The global controller takes a smart decision based on the current states of all the local controller under it. The behaviour of those local controllers will now depend on each other. More the level of the global controller more is the scope of the area covered by it. By taking into account about the previous decisions made by the local controller using static rules and by observing the change in parameters (mentioned above), the global controller will learn and try to optimize the traffic flow further by giving decisions to the local controller. A potential Machine Learning model for Global Controller could be Decision Tree, Random Forest Algorithms. In our proposed solution we are aiming at controlling traffic congestion using the Random Forest Algorithm. The pros of using Random Forest over Decision Tree is as follows:

- For decision tree there must be optimal choice identified at each node, this makes the model greedy i.e. it takes the most optimal decision at each step but does not take into the account the global optimum.
- Decision Trees generally face the problem of overfitting.
- Random forest is a collection of the decision tree. They limit overfitting without increasing error due to bias.
- Random forest also reduces variance by training on different samples of data.
- Random forest works well on missing data with maintained accuracy.

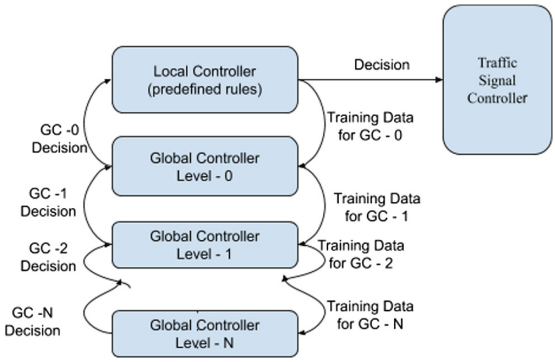


Fig. 1. Block diagram for the flow of decisions in the hierarchical model

In Fig. 1, the flow of data (decisions) among various controllers is shown. As seen from the above figure, the traffic data first passes through the local controller where the decisions are taken based on the rules that are predefined to control the traffic congestion at the local level only. Further, the data is passed to the Global Controller Level - 0. It is trained using the Random Forest Algorithm on various parameters such as vehicle traffic density, pedestrian density, traffic waiting time and so on. Depending upon the traffic handled by the local controller and producing the new traffic states, this data will be used by the Global Controller to train the model using the Random Forest Algorithm.

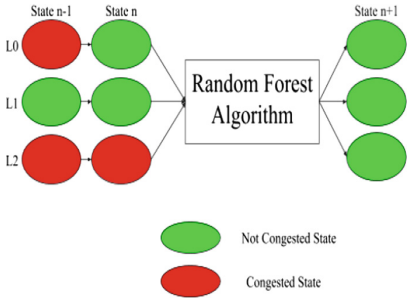


Fig. 2. Training for global controller

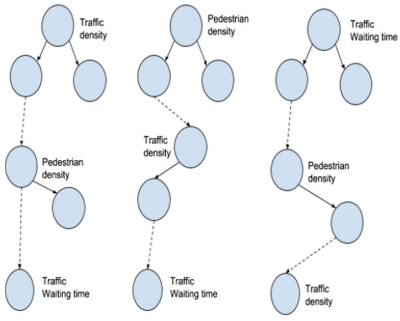


Fig. 3. Random forest implementation

In Fig. 2, *State n-1* represents the traffic condition before the decision being taken by the previous level controller and *State n* consists of traffic condition after the decision was taken by the previous level controller. This serves as the training data for a subsequent global controller. The Global controller performs the random forest algorithm in the way given below.

Random Forest will generate the tree similar to the one given in the Fig. 3 and the results obtained through various trees will be taken into consideration, thereby reducing the probability of overfitting.

3 Simulation

3.1 Simulator Setup

The Simulator module of the project is used for testing the performance, response ratio, reliability and other factors of the proposed algorithm. The simulator has been designed to map closer to real-world situations. The simulator module can be broken into two parts: One dealing with creation dynamic traffic and failing situations, and others dealing with communication with the respective Local Controller modules for getting decisions. Both the parts work independently of each other, thus allowing us to test the performance accurately.

3.1.1 Simulation Element

In this part, vehicle traffic is generated randomly, which travel around the map by taking their own decisions at various points. Each traffic generated can be of three types:

1. Normal: traffic following the traffic rules.
2. Misbehaving: traffic which does not follow any traffic rules or signal.
3. Emergency: traffic indicating ambulance, fire brigade, and other things for which roads must be cleared urgently.

Accidents like situation are generated randomly on any road in the simulator. This would stop any car coming towards the accident point. Accidents are cleared after some time. Same as an accident, congestion situations also occur in the module.

The camera module captures the road details and sends it to the respective local controller. Data sent by the camera includes traffic density, average speed, the presence of pedestrian for crossing the road, the presence of accident and ambulance. The simulated traffic signal pole just signals the current signal provided by the local controller. Failure of traffic signal pole, as well as camera, has been also simulated.

3.1.2 Communication Element

The simulator module is also responsible for communication with the respective local controller. For establishing communication, the simulator initially queries the local controller manager for getting socket address of each local Controller. After initializing each camera and traffic signal pole with a socket address, each component starts their communication with the local controller independently.

Following are screen views of the simulator:

1. Screen for Logical map and simulated traffic:
   The intersection of roads are represented as nodes in graphs and road are represented by edges in the graph. Traffic flows are represented by small boxes. Red boxes indicate misbehaving traffic, one which does not follow the traffic signal and blue boxes indicate ones those who follow the traffic signals. The slider is used to control the speed of traffic and pedestrian generation (Fig. 4).

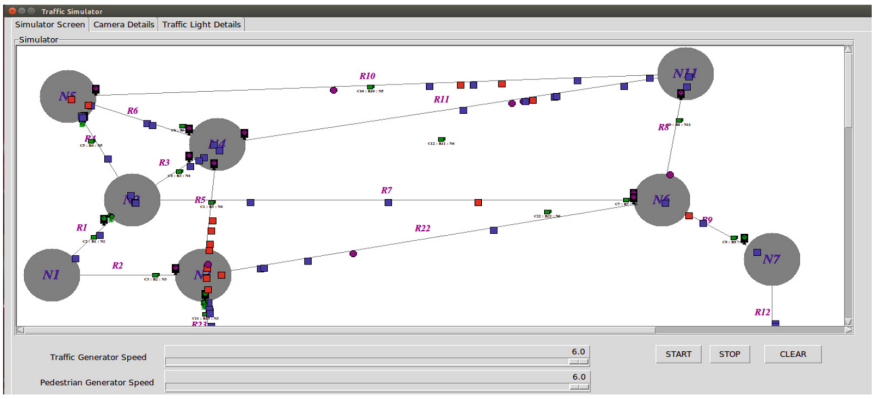


Fig. 4. Logical map view

2. Screen showing camera-view at each road
   The graph of each camera indicates the values of various captured parameters with respect to time. Buttons are provided to stop a camera capturing indicating failure of a camera (Fig. 5).

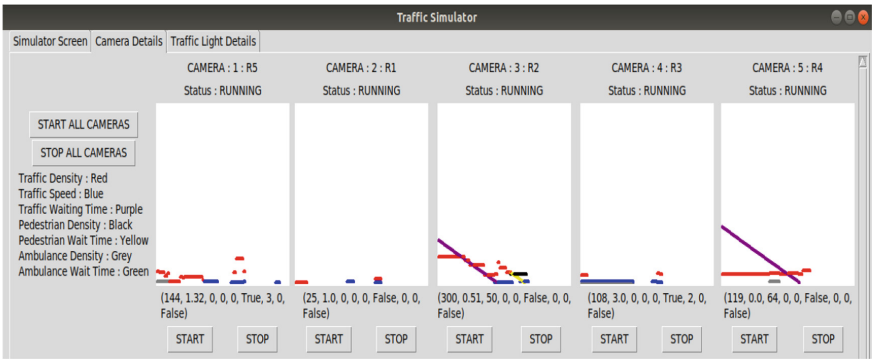


Fig. 5. Camera view in simulator

3. Screen showing traffic signal pole status
   Each traffic signal poles are current status provided in this screen. S is for Stop, P for Pedestrian and each number indicating the edge number in the graph (Fig. 6).

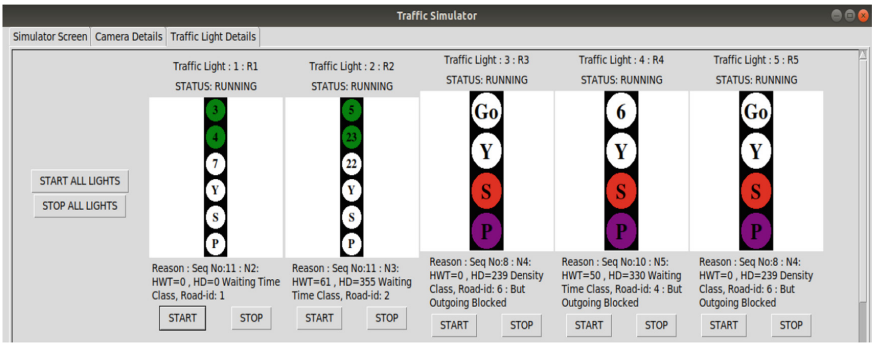


Fig. 6. Signal status in simulator

4 Results

The impact of local and global can be seen in the following graphs captured by the camera (Fig. 7).

Table 1. Legends used in cameras' graph

Parameters	Colours
Traffic average speed	Blue
Traffic waiting time	Purple
Pedestrian density	Black
Pedestrian waiting time	Yellow
Ambulance density	Grey
Ambulance waiting time	Green
Traffic density	Red

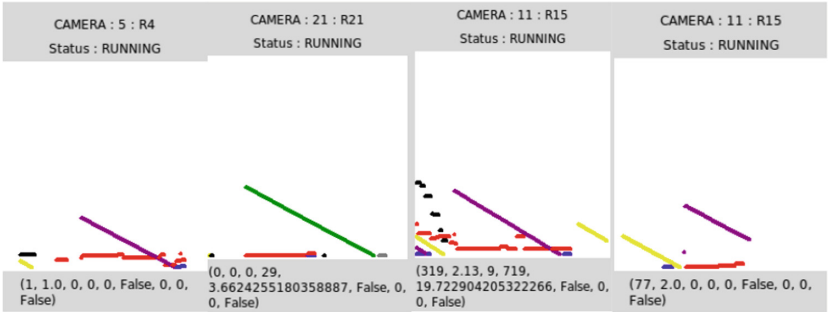


Fig. 7. Camera view of simulator screen

In the camera view, as represented from the above set of images, the time varies according to the horizontal line (X-axis) and the density count is shown using a vertical line (Y-axis). In Camera 11 and Camera 5, the traffic waiting was increasing initially, but after some point the graph breaks and waiting time almost becomes negligible. This shows that the traffic waiting time was reduced which further can be said that traffic congestion was controlled (Table 1).

In Camera 21, the ambulance waiting time was increasing but later the waiting time for ambulance diminishes to zero and in Camera 11 the pedestrian waiting time is also reduced, which shows that the traffic is fully under control of our system.

5 Conclusion

This project aims at controlling urban traffic congestion. The proposed solution effectively reduces traffic congestion and tries to optimize the flow of traffic. This type of traffic control system is highly required in a country like India where the population density is so high which ultimately results in a very high density of vehicles on road. This model is also useful for Smart Cities implementation.

References

1. Carsten, D., et al.: A traffic object detection system for road traffic measurement and management
2. Teodorović, D., Dell' Orco, M., Teodorović, D., Dell' Orco, M.: Mitigating traffic congestion: solving the ride-matching problem by bee colony optimization. Transp. Plan. Technol. **31**(2), 135–152 (2008)
3. Sanchez-Medina, J.J., Galan-Moreno, M.J., Rubio-Royo, E.: Traffic signal optimization in "La Almozara" district in Saragossa under congestion conditions, using genetic algorithms, traffic microsimulation, and cluster computing. IEEE Trans. Intell. Transp. Syst. **11**(1), 132–141 (2010)
4. Alpatov, B.A., Babayan, P.V., Ershov, M.D.: Vehicle detection and counting system for real-time traffic surveillance. In: 2018 7th Mediterranean Conference on Embedded Computing (MECO), pp. 11–14, BUDVA, MONTENEGRO, June 2018
5. Srinivasan, D., Choy, M.C., Cheu, R.L.: Neural networks for real-time traffic signal control. IEEE Trans. Intell. Transp. Syst. **7**(3) (2006)
6. Tahmid, T., Hossain, E.: Density based smart traffic control system using canny edge detection algorithm for congregating traffic information. In: 2017 3rd International Conference on Electrical Information and Communication Technology (EICT), pp. 1–5, Khulna (2017)
7. Ki, Y.K., Heo, N.W., Choi, J.W., Ahn, G.H., Park, K.S.: An incident detection algorithm using artificial neural networks and traffic information. In: 29th International Conference 2018 Cybernetics & Informatics (K&I), Lazy pod Makytou, Slovakia, Jan. 31–Feb. 3 2018
8. He, J., Bresler, M., Chiang, M., Rexford, J.: Towards robust multi-layer traffic engineering: optimization of congestion control and routing. IEEE J. Sel. Areas Commun. **25**(5), 868–880 (2007)

9. Van Phu, C.N., Farhi, N., Haj-Salem, H., Lebacque, J.: A vehicle-to-infrastructure communication based algorithm for urban traffic control. In: 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), pp. 651–656, Naples (2017)
10. IoTivity Open Source Project Announces Preview Release. Linux Foundation. Accessed 14 Jan 2015
11. Liaw, A., Wiener, M.: Classification and regression by randomForest. R news **2**(3), 18–22 (2002)
12. Rodriguez, J.J., Kuncheva, L.I., Alonso, C.J.: Rotation forest: a new classifier ensemble method. IEEE Trans. Pattern Anal. Mach. Intell. **28**(10), 1619–1630 (2006)
13. Van Essen, B., Macaraeg, C., Gokhale, M., Prenger, R.: Accelerating a random forest classifier: Multi-Core, GP-GPU, or FPGA?. In: 2012 IEEE 20th International Symposium on Field-Programmable Custom Computing Machines, pp. 232–239, Toronto, ON (2012)

A Proposed Blockchain Model to Enhance Student Knowledge

P. V. Siva Kumar[1], Sriramudu[2], Chaitanya Palli[2], J. Adarshavathi[2], and Padmavathi Guddeti[2(✉)]

[1] Department of CSE, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India
sivakumarpasupuleti@gmail.com
[2] CRRAO AIMSCS, HCU Campus, Hyderabad, India
sriram4b0@gmail.com, adarsha94l@gmail.com, padmagvathi@gmail.com, chaitanya@crraoaimscs.res.in

Abstract. As the education becomes more competitive in nature, students need to learn many other subjects or courses by interest or need. We identified the multidisciplinary knowledge of the students and created interested groups based on the grades or points obtained through questionnaire. But this learning happens through online, in order to maintain security of the student information, we have proposed a blockchain model SIBC(Student Interest Blockchain). This model is useful to identify the student interests and creates a platform to fulfill the student interest along with his regular course. It was proposed to maintain separate blocks for each specialization area, and the student can join any one of the block based on the points got in the questionnaire. Each block consist of students, faculty experts, industry experts, alumni of that institution and all other resources available are helping the students to enhance his knowledge in that particular area.

Keywords: Architectures for educational technology system · Computer mediated communication · Distributed learning environments · Interactive learning environments

1 Introduction

The blockchain technology is very useful for the decentralized database. Most of the blockchain applications are suitable for payment processing, to monitor supply chain, data sharing, land registrations, medical, and military. Now a days almost all the transactions in the world are digital via some network. And the persistent problem raised is the credibility of the transactions, how and when it took place and all. To arrive at a solution there are few methods like writing in a personal dairy, a more advanced way is emailing to self and let it unopened and few enterprises use more elaborative ways of verifying involving team of people. All these methods involve verification and/or by more people which effects the integrity of the data. Authentic time stamping blockchain technology was discussed in [1, 2] to avoid tampering of the document originality particularly its date. Blockchain (BC) operates as a peer-to-peer

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 107–115, 2020.
https://doi.org/10.1007/978-3-030-37051-0_12

network using proof-of-work to record a public history of transactions, [3]. First blockchain technology was discussed in, [3] for network of peer to peer which applies proof of work to maintain public record of transactions, due to this, attacker cannot make any changes if maximum CPU power is under the control of honest nodes. Blockchain has two components securing data and recording every value virtually. Without BC it is difficult to monitor, identify the ownership or transfer of ownership.

In the Finance sector there are many functions like payments and remittance of money transitions either nationally or internationally. It is necessary to provide the security and transparency for the transactions. Here the Blockchain Technology helps to provide the security and transparency for the financial transactions. But the disadvantages of BCT in finance sector is Risk and Volatility [4, 5]. In the Government sector there are many activities are happening like land registrations, vehicle registrations, bill payments like power bill payment, house tax payments and so on. There is a possibility of fraud in many places of the activities. For example, in the land registration it may possible for multiple registrations or illegal registration of lands. To overcome these problems, the Blockchain Technology helps to control fraud activities and provide the transparency in the system [6, 7].

In the Health sector also, it is necessary to maintain the security and transparency for the medical reports and medicine details to control the fake medicine in the market. The Blockchain Technology helps here to control the fake medicine. It is also very important to provide the security for data and storage of files. If the data or files stored on distrusted system or cloud environment that can be acces by anybody. To provide the security for such data or files the Blockchain Technology can use. In Education Sector also the Blockchain Technology used to prevent the duplicate certificates or provide the security for the online courses or student information [8, 9]. They are many applications of IoT like insurance sector, manufacturing systems and so on, IoT devices will help to enable message exchanges between two parties by using smart contracts. The Blockchain Technology helps to provide the authentication between two parties and provide the security.

In BC technologies for security aspects cryptography play major role. The main Cryptographic functions used in BC are hash functions and digital signatures. *Hash functions* are used to represent for the current state of BC to ensure immutable. All the information (amount transferred, address and timestamping) is combined into the mathematical formula to hash called transaction ID. Transaction ID is a hash value used to identify or inform the transaction happened. All the blocks are linked back to previous hashes to generate new block and form a chain to the first or genesis block. There is a consensus rule in BC. *Consensus rules* are specific set of rules that nodes on the network will ensure a block follows when validating that block and the transactions within it. Getting consensus agreement means unanimous acceptance between nodes on the network for a single data value. *Digital signatures* are used for authentication which are part of security on a blockchain. Literature related to blockchain technologies were discussed in [10–13]. Applications of Blockchain technologies beyond cryptocurrency discussed in [14]. BC for social impact, IoT, e-governance, energy industry, economy, real estate and management were discussed in [15–22] respectively. Bitcoin [12] used as cryptocurrency which uses SHA256 [23, 24] as hash function, ECDSA [25] and multisignature [26] for authentication and bullet proofs as consensus [27, 28] algorithm. Blockchain architecture can understand from Fig. 1 [29]. The recent years have

been seen major and remarkable development in the field of digital payments and its technologies. Block-chain is a revolutionary technology, it promises to secure the data, image, video, transactions, and even resources [30–34].

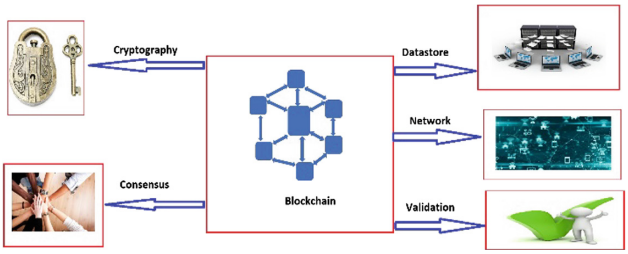


Fig. 1. Blockchain architecture

2 Motivation of Proposed Model

Motivated by the literature and application potential of the BC models, we want to apply BC to education. Now a days, competition is very high in the education field. It is very difficult for the student to get the admission in their interested engineering branch and institution. The student will get an admission in the institution based on the entrance examination or grade obtained. After clearing the entrance examination, the student needs to select the engineering branch and institution for the admission.

In the admission process the academic institute will be graded as top-grade institutions, good grade institutions and normal grade institutions based on the faculty, infrastructure, placements and other facilities for the students. Generally, in the admission process the best grade students have the choice to select any branch of engineering course in any top-ranking institution, whereas the good grade students have a choice to select any branch of engineering course in normal grade institution or they may get some of the engineering course in the top graded institution of not their preference. And the poor grade students have a chance to get any branch of engineering course in the normal grading institution of not their preference. In some cases, students may get good ranked institution but the branch is not their choice or some students may get the branch of their choice but not the institution or some students may get the admission where the branch and institution were not their choice. Whatever the reason, every student who enters into the Institution with by choice or by chance, the student needs to complete his engineering course without losing of his own interest. Many students are having the interest to learn the advanced courses or to learn the other branch courses or interested in fine arts like music, dance…etc. or social services along with their own course to fulfilment the market needs, placements or self-improvement. By considering the interest of the students, it is suggested to the Institution to create separate interest groups by each branch and offer these courses for all students of that Institution. If the student fulfils the minimum requirements of interest group then he may join into that interest group. Apart from his regular course of study, the student can

complete his desired course simultaneously. So, it is important to consider the interest of the student and provide a platform to fulfil their interest along with their regular course.

Motivated by the importance of multidisciplinary knowledge or learning capability of the student we started our research with 1000 first year engineering students known as freshmen engineers consists of all engineering branches related to one institution.

Step-1: 1000 freshmen engineers of all branches answered questiner1 (Q1) and questiner2 (Q2) related to their interest in Computer Science Engineering (CSE) and Electronic and Communication Engineering (ECE) respectively. Q1 and Q2 consists of 20 questions which can capture the learning capacity of the student. And student can enter into their interested group if they got 75% or more points in the questioner. Out of 1000 students 214 students got more than 75% points in only CSE, 72 students got more than 75% points in only ECE and 690 students got more than 75% points in both CSE & ECE were qualified questioners. After entering into ECE or CSE interested group, student can enhance knowledge through proper guidance like videos, online courses and interaction with the concern faculty available in that group.

Step-2: After entering the interest branch like CSE or ECE again the one more questioner need to be answered by the student. Here the questioner consists of all the specialization of that branch for example if the CSE interested group questioner will consist of the questions from all its specialization like Artificial intelligence, Data Science, Computer and Network Security, mobile and web computing To narrow down to the core specializations i.e., to enter into Level-2, they have to answer questioner and must qualify with 50% points.. In specializations students can learn more precise information and practical implementation. In Level-2 they have to learn their specialization in systematic way i.e., (1) Theoretical information (2) Numerical examples (3) Practical Learning (4) Interaction with the experts from industry(5) Mini Project. To go to the Level-3, they must complete mini project in their specialization which can be monitored by faculty and industry. Then they can go to Level-3.

Step-3: Institution will identify the experts from Alumni, research and development, Software, Specialization related Industry and Academia. In Level-3 student can interact with alumni and industry people. So they can understand the industrial needs, current status of research in that area, new programming languages and enhance their knowledge in that area. Our study extended to interested groups in the engineering branches like CSE, ECE, EEE (Electrical and Electronics Engineering, ME (Mechanical Engineering), and CE (Civil Engineering).

But in these groups, all the learning activities are happening through online process. After identify the student interest in this model and added into the corresponding block. Block can have the information about the students, faculty, alumni and industry experts related to that block. To provide the security for the information blockchain model can be a better one to follow. It can avoid entry of untrusted party. Initially, this model can be applied to one institution and later it can be implemented to group of institutions. The proposed blockchain architecture can be understood from Fig. 2.

3 Proposed SIBC for Academic Institution

Blockchain is originally devised to enable currency transactions to be carried out in trustless environment. However, if we considered the students and their interested area other than core branch process as the currency, blockchain technology can potentially be applied to the students in one university or institution and this can be extended to group of institutions. In this blockchain, we are considering one university or institution where the students can admit into the different branches like civil (B1), electrical (B2), computer science (B3), mechanical (B4) and so on through entrance examination. One blockchain will be created for each branch so that all the students of that branch will be connected in that block. Like that we will create separate block for each branch of engineering. After admission the students in the respective branch, the University or institution will provide unique registration or admission number for the student.

The University or institution broadly identify the interest groups like computers, electronics, electrical like that. Based on the questionnaire collected from the student, the university or institution authorities will decide in which interest group the student can join. The department will identify the thrust area of that branch and create sub interest groups in those areas. For example, the computer science department identified the thrust areas like Artificial Intelligence, Machine Learning, and Deep Learning and so on. Apart from these core branch interest groups, the institution will also identify some interest groups like music, dance, social service, entrepreneur and so on to fulfil the student interests. Each interest group will have one faculty mentor. The University or institution will conduct one examination or questionnaire to identify the student interest. This questionnaire helps to decide in which area the student is interest to join. In this process the core branch student can join directly to the interest group without taking this questionnaire. For example, the computer science student can directly join into the computer science interest group whereas the other branch students need to take the questionnaire process. Based on the questionnaire, classification of the interested branch block is done using machine learning classifiers. Based on the answers given in the questionnaire, the department will decide which interest group is suitable for the student to join. Then the department permits him to join in that interest group. Here we will create blockchain for each interest group. We will create the separate blockchain for alumni students of the university or institution. Here we divide the alumni students into different groups based on their working field like academic, research, industry, software industry and so on. Here we can create blockchain model for all alumni groups and linked with the interest groups of the university or the institution as shown in Fig. 3. With this each interest group block will have the students, faculty mentor and alumni students related to that interest. Any student in the respective block, will know about the other student details of his own stream or other stream. Since the duplication of student details is highly possible, we are using SHA-256 [23, 24] as Proof of work consensus algorithm to add a new student into the block. For authentication of the students in each block multi signatures [26] are proposed for this environment. Here one blockchain will be created for all the interested groups, so that each student details like his interest group and which branch he is belonging to will be maintained and shared to other members of the block. One blockchain will be created for each interest

group with all its sub groups. Because of this blockchain each student of one particular interest group will know about the other student details in that block. After completion of the course all the students are added in to the alumni group. Each alumni student can be a member of any one of these sub groups. Here also one blockchain will be created for the alumni group and all its sub groups. Because of this blockchain each alumni student will know about the details of the other alumni student details where he is working and other details. We want to extend this model to identify the student difficulties and problems in terms of medical or psychological. The two categories of students who are having medical problems (hereditary problems or due to habits etc.) and psychological problems (family problems, less interest in technical education etc.). By identify the student health problem and taking extra care by the institution will be helpful to the student to overcome from his heath problem and complete his studies.

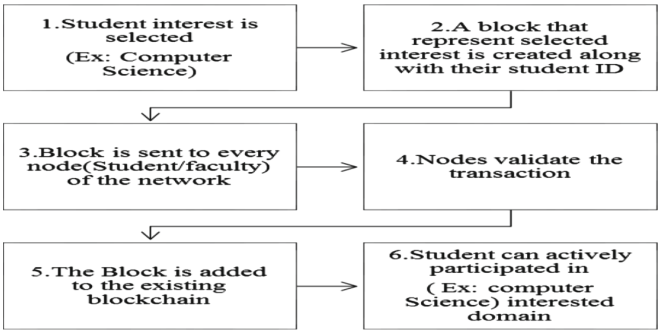


Fig. 2. Proposed SIBC (Student Interest Blockchain) architecture

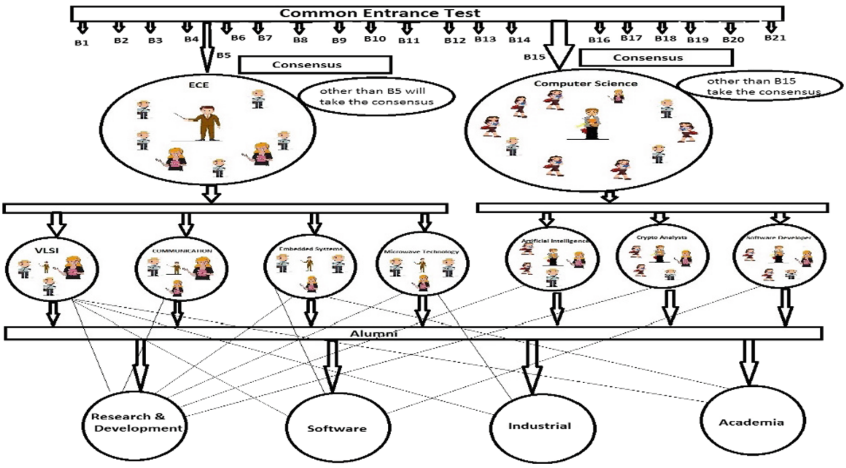


Fig. 3. Proposed blockchain SIBC in academia

4 Conclusion and Future Work

In this proposed model, the faculty mentor evaluate the student talent and identify the interest of the student were discussed. If the student fulfils the minimum requirements of that interest group, then the student allowed to join into that group and interact with the group to enhance his/her knowledge along with his regular course. In this paper we proposed BC model for one Institution based on technical specializations and we want to extend our research to identify the student interest in extracurricular activities and medical & psychological problems and enhance their knowledge through SIBC model. As a future work, this model can be extend to group of institutions or University where number of institutions affiliated to that University and enhance the student's knowledge and make them to expose to the world.

Compliance with Ethical Standards. All author states that there is no conflict of interest. We used our own data. Humans/aniamls are not involved in this research work. We used our university students and got approval from the university.

References

1. Haber, S., Stornetta, W.S.: How to time-stamp a digital document. J. Cryptol. **3**, 99–111 (1991)
2. Bayer, D., Haber, S., Stornetta, W.S.: Improving the efficiency and reliability of digital time-stamping. Sequences, vol. 2, pp. 329–334 (March 1992). ISBN 978-1-4613-9325-2
3. Nakamoto, S.: Bitcoin P2P e-cash paper (31 Oct. 2008). https://bitcoin.org/bitcoin.pdf
4. Yoo, S.: Blockchain based financial case analysis and its implications. Asia Pac. J. Innov. Entrep. **11**(3), 312–321 (2017)
5. Aras, S.T., Kulkarni, V.: Blockchain and its applications–a detailed survey. Int. J. Comput. Appl. (0975–8887) **180**(3) (2017)
6. Alketbi, A., Nasir, Q., Talib, M.A.: Blockchain for government services–Use cases, security benefits and challenges. In: 15th Learning and Technology Conference (L&T) (2018)
7. Ølnes, S., Ubacht, J., Janssen, M.: Blockchain in government: benefits and implications of distributed ledger technology for information sharing. Gov. Inf. Q. **34**(3), 355–364 (2017). Elsevier
8. Chen, G., Xu, B., Lu, M. et al.: Exploring blockchain technology and its potential applications for education. Smart Learn. Environ. **5**(1) (2018). http://doi.org/10.1186/s40561-017-0050-x. Springer
9. Turkanović, M., Hölbl, M., Košič, K., Heričko, M., Kamišalić A.: EduCTX: A Blockchain-Based Higher Education Credit Platform. Digital Object Identifier. IEEE Access (2018). https://doi.org/10.1109/ACCESS.2018.2789929
10. Link-1:https://www.ibm.com/cloud/garage/architectures/blockchainArchitecture
11. Link-2:https://www.zignuts.com/blogs/how-blockchain-architecture-works-basic-understanding-of-blockchain-and-its-architecture/
12. Vujičić, D., Jagodić, D., Ranđić, S.: Blockchain technology, bitcoin, and Ethereum: a brief overview. In: 17th International Symposium INFOTEH-JAHORINA (INFOTEH) (2018)
13. Conte de Leon, D., Stalick, A.Q., Jillepalli, A.A., Haney, M.A., Sheldon, F.T.: Blockchain: properties and misconceptions. Asia Pac. J. Innov. Entrep. **11**(3), 286–300 (2017). https://doi.org/10.1108/APJIE-12-2017-034

14. Miraz, M.H., Ali, M.: Applications of blockchain technology beyond cryptocurrency. In: Annals of Emerging Technologies in Computing (AETiC). International Association of Educators and Researchers (IAER), vol. 2, no. 1, pp. 1–6 (1 Jan. 2018). Print ISSN: 2516-0281, Online ISSN: 2516-029X. http://aetic.theiaer.org/ archive/v2n1/p1.pdf
15. Al-Saqaf, Walid, Seidler, Nicolas: Blockchain technology for social impact: opportunities and challenges ahead. J. Cyber Policy **2**(3), 338–354 (2017)
16. Yeow, K., Gani, A., Ahmad, R.W., Rodrigues, J.J.P.C., Kwangman, K.: Decentralized consensus for edge-centric internet of things: a review, taxonomy, and research issues. IEEE Access, pp. 1513–1524 (2018)
17. Bohme, R., Christin, N., Edelman, B., Moore, T.: Bitcoin: economics, technology, and governance. J. Econ. Perspect. **29**(2), 213–238 (2015)
18. Mattila, J., Seppala, T., Naucler, C., Stahl, R., Tikkanen, M., Badenlid, A., Seppala, J.: Industrial blockchain platforms: an exercise in use case development in the energy industry. The Research Institute of the Finnish Economy, vol. 43 (2016)
19. Pilkington, M.: Blockchain technology: principles and applications. In: Olleros, F.X., Zhegu, M. (eds.) Research Handbook on Digital Transformations. Edward Elgar (2016)
20. Swan, M.: Blockchain: blueprint for a new economy. O'Reilly Media, Inc. (2015)
21. Karamitsos, I., Papadaki, M., Al Barghuthi, N.B.: Design of the blockchain smart contract: a use case for real estate. J. Inf. Secur. **9**, 177–190 (2018). https://doi.org/10.4236/jis.2018.93013
22. Crokell, H.H.: Specialization and international competitiveness. In: Etemad, H., Sulude, L.S. (eds.) Managing the multinational subsidiary. Croom-Helm, London (1986). Book chapter style
23. Sun, W, Guo, H., He, H., Dai, Z.: Design and optimized implementation of the SHA-2(256, 384, 512) hash algorithms. In: 7th International Conference on ASIC, IEEE xplore (2007)
24. Sahni, N.: A review on cryptographic hashing algorithms for message authentication. Int. J. Comput. Appl. **120**(16) (2015)
25. Lamba, S, Sharma, M.: An efficient elliptic curve digital signature algorithm (ECDSA). In: 2013 International Conference on Machine Intelligence and Research Advancement. IEEE xplore
26. Maxwel, G., Poelstra, A., Seurin, Y., Wuille, P.: Simple schnorr multi-signatures with applications to bitcoin. https://eprint.iacr.org/2018/068.pdf
27. Swanson, T.: Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems 2015
28. Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J.J.: Blockchain contract: a complete consensus using blockchain. In: 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), p. 577–578. IEEE (2015)
29. Muzammal, M., Qu, Q, Nasrulin, B.: Renovating blockchain with distributed databases: an open source system. In: Future Generation Computer Systems, vol. 90, pp. 105–117 (2019)
30. Chouhan, L., Songara, A.: Blockchain security for wireless multimedia networks. In: Cryptographic and Information Security Approaches for Images and Videos. CRC Press (2018)
31. Biswas, K., Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: IEEE 18th International Conference on High Performance Computing and Communications (2016)
32. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**(4) (2018)

33. Tian, F.: An Agri-food supply chain traceability system for China based on RFID & blockchain technology. In: 13th International Conference on Service Systems and Service Management (ICSSSM) (2016)
34. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for IoT security and privacy: the case study of a smart home. In: 2nd IEEE PERCOM Workshop On Security Privacy And Trust In The Internet of Things (2017)

Heuristic Solutions Supported by GPON for Future Telecommunication Optical Network

Jasmeena Singh(✉) and Amit Kumar Garg

Department of Electronics and Communication Engineering, Deenbandhu Chotu Ram University of Science and Technology, Murthal 131039, India
jasmeenasingh8816@gmail.com, garg_amit03@yahoo.co.in

Abstract. This paper has illustrated the comparison of various modulation formats with and without FBG. It is seen that internet service providers are looking for new ways to satisfy customer's requirements related to quality, bandwidth, speed, and security. Optical access network proves to be the crucial broadband network to satisfy the demands such as video communication, cloud computing, data mining. The most common optical access network is the PON and the most promising is GPON (Gigabit Passive Optical Network). In this paper, a general study on GPON is done with FBG and without FBG. For the distance of 100 km and bitrate 2.5 Gbps analysis of GPON has been done. Role of FBG as dispersion compensator and multiplexer has also been analyzed. The outcome shows that NRZ with uniform FBG shows better results.

Keywords: Passive optical network · Gigabit passive optical network · ODN · FBG (Fibre bragg Grating) · AON

1 Introduction

Recently, the metropolitan network has experienced large demands related to greater bandwidth, long haul transmission, high speed, and privacy. In order to satisfy this demand, service providers are looking for an efficient network with minimum investment and maximum revenue. Digital Subscriber Lines such as Very High-Speed DSL (VDSL) proved to be cost-effective but can operate over limited distance and provides symmetric data rates of 100 Mbps [1]. Performance of DSL degrades as the distance between customer and digital subscriber line access MUX (DSLAM) (300 m) increases. In order to support high data rates, increasing demands of bandwidth and distance and low latency, fiber optic communication proves to be promising for FTTH and telecommunication network as well. The first low loss fiber was invented in 1970 after this fiber communication developed rapidly. Internet service providers migrated from UTP network to the optical network in order to satisfy the demands of higher bandwidth and data throughput. The basic telecommunication network consists of services, core area, access area, and user area. Core and aggregation together form the transport network [2]. The earlier optical network covers core area but now it covers access part too. FTTH is one of the major fiber optic communication network

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 116–125, 2020.
https://doi.org/10.1007/978-3-030-37051-0_13

configuration used to provide triple-play services (data, voice, video) to customers. FTTH is capable of providing fixed telephone and interactive applications. For various services such as transactional video on demand, High Definition Television, bioinformatics, internet-based applications and more, the optical network provides high reliability, high bandwidth throughput, decreased revenue and EMI tolerance. For these demands, fiber optic communication provides three ways of communication- Point to point, Point to Multipoint (Active Optical Network), Point to Multipoint(Passive Optical Network). The comparisons of P2P, P2MP (AON) and P2MP (PON) communication technologies are given in Table 1.

Table 1. Comparison of various existing telecommunication technologies:

Technology name	Pros	Cons
P2P	High speed, high capacity, dedicated	High development cost, expensive, smaller distance
P2MP (AON)	High capacity	Developing, operating and maintenance cost is high, management and centralization is required, active components required
P2MP (PON)	High capacity, flexible, scalable, low operating and maintenance cost, uses passive elements	Protection methods are required and chances of fault in OLT

PON has been used as it provides higher bandwidth, co-existence with next-generation PONs, longer distance (20 km), easy upgrading and broadcasting in downstream, passive splitters. For this PON proves to be desirable [4]. PON works in tree topology so as to maximize the coverage area with minimum network splits and hence maximizing the power. There are three main technologies of PON-APON/BPON, EPON, and GPON. APON and BPON is defined in IEEE802.3 and ITU-T G.983 respectively and provides the bitrates up to 1244 Mbps. EPON is defined in IEEE802.3.ah and capable of providing bitrates of 1.25 Gbps for both upstream and downstream. GPON is defined as ITU-T G.984.x and is capable of providing symmetric data rates and provides security, long reach, flexibility, and higher split ratio [5]. GPON is superior to other PON technologies [6]. In this paper, the study of the downlink part alone is done [13–15]. In this paper, FBG along with various modulation formats has been used and analyzed. Section 2 will provide an overview of GPON, Sect. 3 will discuss FBG, Sect. 4 provides simulation setup and results, and Sect. 5 will provide a final conclusion and remarks.

2 GPON

GPON uses TDM service; deliver multiple services with multiple QoS, supports multipattern services such as voice, data, and video. GPON supports split ratio up to 1:128, provides security with Advanced Encryption Standard and GPON Encapsulation Method (GEM) (8 level priority). GPON can support multiple users per one ONT. If a user requires more than one port, the mini router can be used. GPON have the capability to provide services to each and every user according to the demand i.e. bandwidth will be allocated according to the payment done by the user (government tariff policy of channel selection these days). The redundant bandwidth can be provided to corporate users due to their high bandwidth requirements. In the telecommunication network, GPON uses various methods such as SIP, and H.248 in order to provide telephone services [2]. GPON is superior to GEPON as it can serve 64 users with speed up to 2 Gbps downstream and GEPON supports 32 users with 1 Gbps downstream [15]. GPON supports seven different speed combinations (Fig. 1, Table 2).

Table 2. GPON upstream and downstream speeds

Upstream direction	Downstream direction
2.4 Gbps	2.4 Gbps
1.2 Gbps	2.4 Gbps
622 Mbps	2.4 Gbps
155 Mbps	2.4 Gbps
1.2 Gbps	1.2 Gbps
622 Mbps	1.2 Gbps
155 Mbps	1.2 Gbps

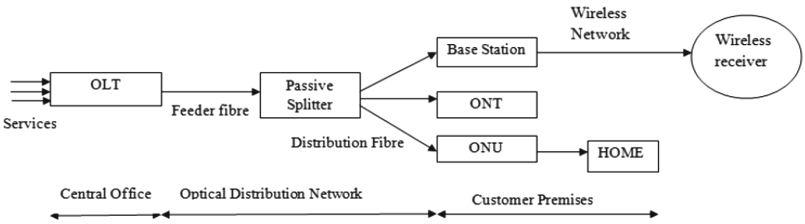


Fig. 1. Proposed gigabit passive optical network for future transport network

There are four main components of GPON - OLT, ONU, ODN, passive Splitters.

OLT resides at local exchange and connects one system card for onboard configurations, one line card for incoming internet and many GPON cards. It works at −48 vDC. OLT allocates bandwidth, perform traffic scheduling and control buffers. In ODN there are different classes such as A, B, B+, C, C+. GPON uses B+ class which

supports 64 users for 20 km. ONU depends upon class used. WDM triplexer modules separate the three wavelengths i.e. 1310 nm, 1490 nm, 1550 nm. Media Access Controller provides isolation between different upstream bursts. Passive splitter has the following characteristics - small dimension, highly reliable, low insertion loss, network survivability, uniformity, and broad operating wavelength [12]. Also, the GPON system unavailability can be given as:

$$System\ unavailability,\ U_{sys} = \frac{MTTR}{MTBF} \tag{1}$$

MTBF = Mean Time Between Failure
MTTR = Mean Time to Repair
Un-availabilities of GPON which can be restored:

$$U_{OLT-GPON} = U_{TX} + U_{RX} + U_{OC} + U_{Splitter} + U_{OS} \tag{2}$$

$$U_{sys} = U_{OLT} + U_{FF} + U_{OS} + U_{Splitter} + U_{DF} + U_{ONU} \tag{3}$$

Here, TX = Transmitter, RX = Receiver, OC = optical Circulator, OS = Optical Switch, FF = Feeder Fibre, DF = Distribution Fibre Availability of GPON:

$$A_{sys} = 1 + U_{sys} \tag{4}$$

3 Fiber Bragg Grating

FBG is a low-cost wavelength specific filter, which acts as a band rejection filter. It is based on Fresnel reflection. FBG reflects the wavelength satisfying the Bragg condition from the rear interface which results in a peak in reflection spectrum and transmits the residual wavelengths from the front interface.

For this Bragg wavelength is:

$$\lambda_b = 2n\bigwedge \tag{5}$$

Here, n is an effective refractive index, $\bigwedge$ is a grating period. In an optical fiber, FBG creates a periodic variation of the refractive index along the optical fiber axis. FBG provides high spectral efficiency, low polarization sensitivity, low insertion loss [18–20]. FBG has been used as dispersion compensator which is wideband and tunable. FBG found to be effective in filtering, add-drop multiplexing, gain flattening of EDFAs in WDM based transmissions and also used in laser diodes [16–20].

4 Simulation Setup and Results

Optical Line Terminal is the transmitter section of GPON. It consists of a Pseudo Random Bit Sequence Generator scrambles data. Bitrate considered for this is 2.5 Gbps. The input signal is modulated using Continuous Wave laser have a wavelength of 1310 nm and 1400 nm and input power of 4 dBm and 5 dBm respectively. Various pulse modulation formats have been used in the simulation. Optical Distribution Network uses single mode optical fiber for a distance of 100 km has been used. Uniform Bragg Grating has been used as it provides the periodic refractive index, quasi-distributed sensing and uniform grating period. Also, the passive optical splitter has been used for analysis. Optical Network Terminal consists of receiver section having Bessel optical filter, optical attenuator, LPF, and Avalanche Photodiode, 3R regenerators and BER analyzer has been used so as to estimate Q- factor, BER, and Eye Diagram. The simulation setup for various modulation formats has been designed and the effect of FBG on modulation formats has also been analyzed.

The simulation setup using FBG and without FBG has been shown in Figs. 2 and 3.

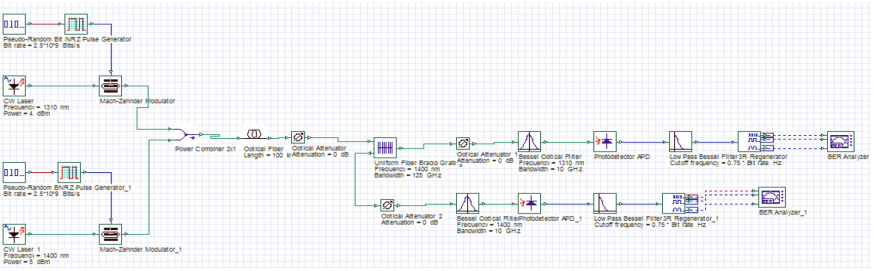


Fig. 2. Simulation setup for 1310 nm and 1400 nm using uniform FBG

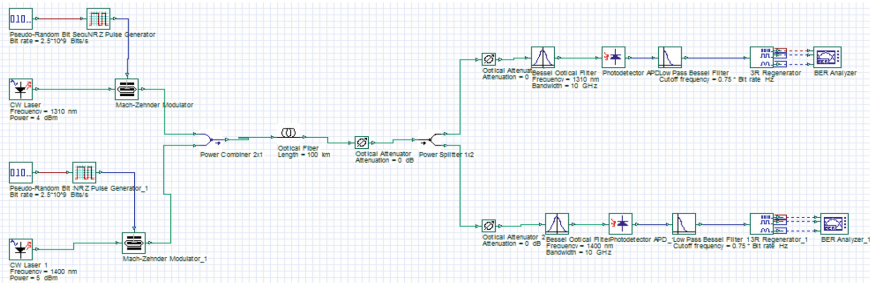


Fig. 3. Simulation setup for 1310 nm and 1400 nm using a passive optical splitter (1:2)

Simulation setup for nonreturn to zero pulse generator has been shown in both cases. For, different modulation formats NRZ pulse generator has been replaced with other modulation formats such as Return to Zero, Pulse Amplitude Modulation (PAM),

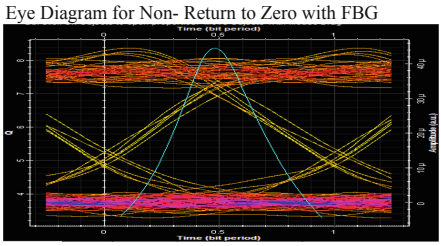


Fig. 4. Q-factor vs time for NRZ using 1310 nm

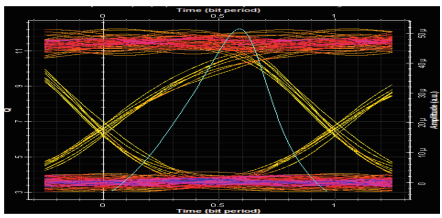


Fig. 5. Q-factor vs time for NRZ using 1400 nm

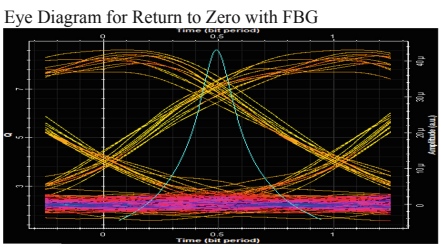


Fig. 6. Q-factor vs time for RZ using 1310 nm

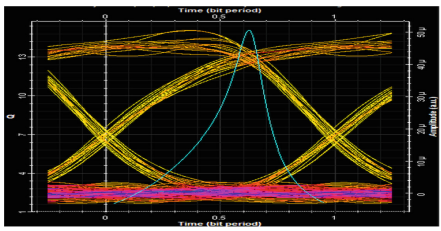


Fig. 7. Q-factor vs time for RZ using 1400 nm

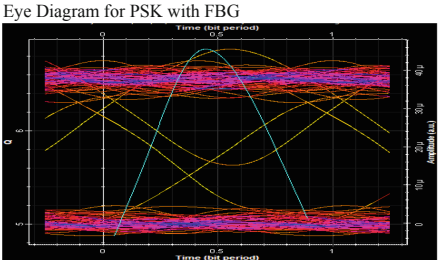


Fig. 8. Q-factor vs time for PSK using 1310 nm

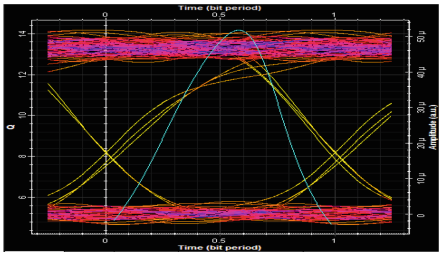


Fig. 9. Q-factor vs time for PSK using 1400 nm

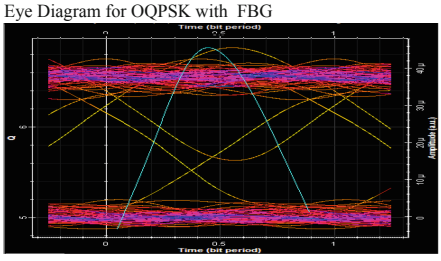


Fig. 10. Q-factor vs time for QOPSK using 1310 nm

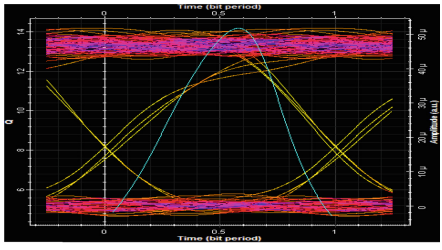


Fig. 11. Q-factor vs time for OQPSK using 1400 nm

Eye Diagram for NRZ without FBG

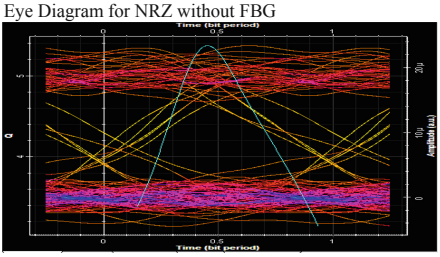


Fig. 12. Q-factor vs time for NRZ using 1310 nm

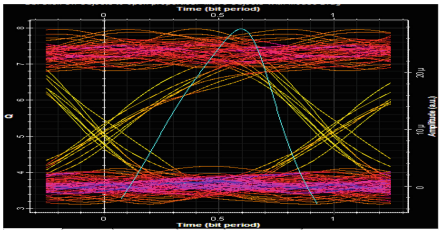


Fig. 13. Q-factor vs time for NRZ using 1400 nm

Eye Diagram for RZ without FBG

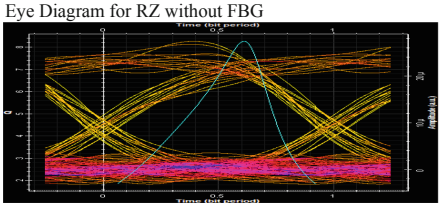


Fig. 14. Q-factor vs time for RZ using 1310 nm

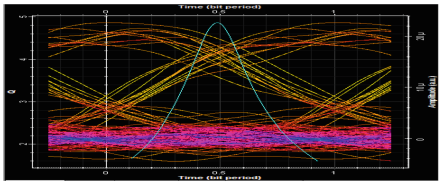


Fig. 15. Q-factor vs time for RZ using 1400 nm

Eye Diagram for PSK without FBG

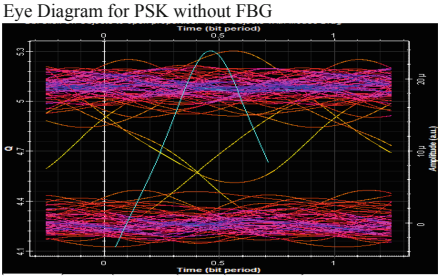


Fig. 16. Q-factor vs time for PSK using 1310 nm

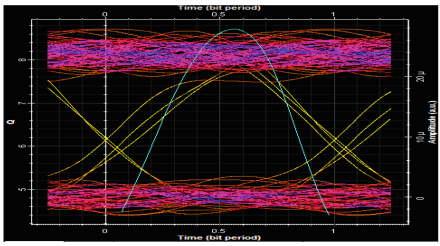


Fig. 17. Q-factor vs time for PSK using 1400 nm

Eye Diagram for OQPSK without FBG

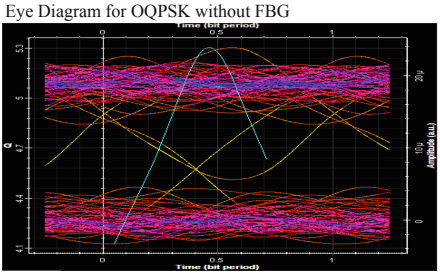


Fig. 18. Q-factor vs time for QOPSK using 1310 nm

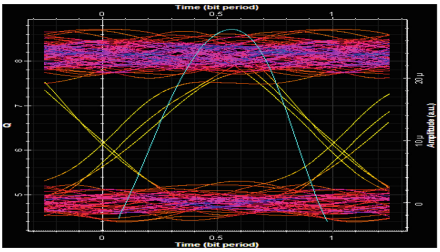


Fig. 19. Q-factor vs time for OQPSK using 1400 nm

Table 3. Q-factor and BER with FBG

Modulation formats	Q-factor (1310 nm)	Q-factor (1400 nm)	Bit error rate (1310 nm)	Bit error rate (1400 nm)
NRZ	8.367	12.247	2.44598e-017	7.73658e-035
RZ	8.61172	15.079	2.56291e-018	8.98943e-052
PSK	6.874	14.171	2.96033e-012	6.8543e-046
OQPSK	6.874	14.171	2.96033e-012	6.8543e-052
PAM	2.527	2.621	0.00546	0.00423
QAM	1.955	2.598	0.0234	0.00422

Table 4. Q-factor and BER without FBG

Modulation formats	Q-factor (1310 nm)	Q-factor (1400 nm)	Bit error rate (1310 nm)	Bit error rate (1400 nm)
NRZ	5.371	7.97291	3.52079e-008	7.30461e-016
RZ	4.862	8.26001	4.13427e-007	5.725e-017
PSK	5.303	8.716	5.57017e-008	1.41716e-018
OQPSK	5.303	8.716	5.57017e-008	1.141716e-018
PAM	2.245	2.348	0.0100	0.0094
QAM	1.689	2.390	0.0436	0.0081

Phase Shift Keying (PSK), Quadrature Amplitude Modulation (QAM), Orthogonal Quadrature Phase Shift Keying (QPSK), Minimum Shift Keying (MSK), Differential Phase Shift Keying (DPSK). In this setup single mode, the optical fiber of 100 km length has been considered. Layout bitrate is 2.5 Gbps. FBG wavelength is 1400 nm, which is to be dropped while transmitting 1310 nm of wavelength. Three parameters have been analyzed Eye Diagram, Q-factor, Bit Error Rate (BER).

Eye Diagram for various modulation formats without FBG has been shown in Figs. 4, 5,6, 7, 8, 9, 10, 11 and with FBG in Figs. 12, 13, 14, 15, 16, 17, 18, 19.

The corresponding Q-Factor and BER have been summarized as (Tables 3 and 4).

From the above tables, it has been seen that Q-Factor is improved, BER decreases, and eye-opening increases for various modulation formats. Analysis of using two wavelengths has been done. It can be analyzed using a set of wavelengths with uniform FBG and TWDM technique in FTTH network.

5 Conclusion and Future Scope

Various modulation formats have been analyzed on the basis of Q-Factor, eye height, and BER. It has been observed for the distance of 100 km NRZ have maximum Q-Factor and minimum BER. It has been observed that FBG act as a dispersion compensator as Q-Factor of modulation formats has been improved and BER decreases. Also, the role of add-drop MUX has been analyzed as it is used to drop the wavelength

of 1400 nm. Hence, it may be used for long haul transmission applications. FBG can be used to decrease the insertion loss and polarization sensitivity. FBG can be deployed in order to increase the data rate, distance, and quality of the signal transmitted. İn future, we plan to analyze the effect of FBG and channel spacing in WDM and TWDM system in GPON using various modulation formats.

References

1. Alobaida, H.: Current and future FTTH technologies. J. Wirel. Netw. Commun. **7**(2), 35–40 (2017)
2. Selmanovic, F., Skaljo, E.: GPON in telecommunication network. In: International Congress on Ultra Modern Telecommunication and Control Systems and Workshop (ICUMT). IEEE (2010)
3. Hamza, M.E.G., et al.: Enhancement of gigabit passive optical highspeed network using fiber-to-the-home. In: 2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), 978-1-5386-4123-1/18/$31.00 ©2018 IEEE
4. Kadhim, D.J., et al.: Design and implementation of a practical FTTH network. Int. J. Comput. Appl. **72**(12), 0975–8887 (2013)
5. Kaur, K., et al.: GPON—a review. IJARCCE **5**(7) (2016)
6. Rokkas, T., et al.: Economics of time and wavelength domain multiplexed passive optical networks. J. Opt. Commun. Netw. **2**(12) (2010)
7. Kaur, B., et al.: Design and simulation of GPON networks over different FBG techniques. IOSR J. Electron. Commun. Eng. **12**(3), 47–52 (2017)
8. De Andrade, M., et al.: Evaluating strategies for the evolution of passive optical networks. IEEE Commun. Mag. 176–184 (2011)
9. Effenberger, J.: The XG-PON system: cost effective 10 Gbps access. J. Lightwave. Tech. **29** (4), 403–409 (2011)
10. Luo, Y., et al.: Time-and wavelength-division multiplexed passive optical network (TWDM-PON) for next-generation PON stage 2 (NG-PON2). IEEE J. Lightwave Tech. **31**(4), 587–593 (2013)
11. Prat, J., (ed.) *Next-Generation Passive Optical Networks*. Research Towards Unlimited Bandwidth Access. Springer, Dordrecht (2008)
12. Cvijetic, N.: OFDM for next-generation optical access networks. IEEE/OSA J. Lightwave Tech. (2012). (Invited tutorial, To appear Feb)
13. Sugumaran, S., et al.: Performance analysis of 2.5 Gbps downlink GPON. Int. J. Electric. Eng. **7**(1), 43–51 (2014)
14. ITU-T recommendation G.984.1, Gigabit-capable passive optical networks (GPON) General characteristics. International Telecommunication Union (2003)
15. Adhikary, A., et al.: A project report on downstream transmission performance of GPON. Asian J. Adv. Res. Rep. **1**(1), 1–11 (2018)
16. Riant, I.: Fiber Bragg gratings for optical telecommunications. C R Phys. **4**, 41–49 (2003)
17. Kumar, S., et al.: A comprehensive review on fiber bragg grating and photodetector in optical communication networks. J. Optic. Commun. (2019)
18. Kumar, K., et al.: Performance analysis of dispersion compensation using Fiber Bragg Grating (FBG) in optical communication. Int. J. Curr. Eng. Technol. **4** (2014)
19. Dabhade, S.S., et al.: Fiber bragg grating and phase conjugator as dispersion compensator. Int. J. Adv. Electric. Electron. Eng. (IJAEEE) **1** (2012)

20. Ahlawat, D., et al.: Performance evaluation of proposed WDM optical link using EDFA and FBG combination. J. Optic. Commun. (2018). https://doi.org/10.1515/joc-2018-0044
21. Irfan Anis, M., et al.: Evaluation of advanced modulation formats using triple play service in GPON based FTTH. IEEE (2015)

An IoT Based Weather Monitoring System Using Node MCU and Fuzzy Logic

Meenakshi Srivastava(✉) and Rakesh Kumar

Department of CSE, M.M.M. University of Technology,
Gorakhpur 273010, U.P, India
srivastavameenakshi05@gmail.com, rkiitr@gmail.com

Abstract. Weather monitoring is a systematic method that gives us detailed information about the weather of our surrounding environment. This device basically monitors the different weather parameters such as temperature, humidity, and rain. The heart of the device is Node MCU (12E). In this paper, three sensors are used namely temperature and humidity sensor (DHT11) and rain sensors have been used, which is connected to Node MCU. When the code is uploaded on Arduino IDE, the board is connected and the sensors start working. All monitored data are stored in thingspeak platform. We use another approach to calculate rain value by the use of IoT & its platform and fuzzy logic to set the weather condition easily for their users. Finally, we compare and analyze both rain value by the use of a different method and the performance of rain value is analyzed on the basis of a different method.

Keywords: Internet of things (IoT) · Weather monitoring · Fuzzy inference system

1 Introduction

Now-a-days, Weather monitoring plays an important role in atmosphere which gives us knowledge about the weather in our surrounding environment [1]. Weather station is a place located either on sea with a tool and appliances for estimating environmental conditions to give us knowledge and information for atmosphere forecast. The measurement taken includes environment parameter such as temperature, humidity, rain, pressure and so on. In comparison of past days, the procedure of studying the environment parameter became simple because of technological progress. For detecting the weather condition of our surrounding environment, we use sensors and actuator. According to the use of this device, the overall result will be corrected and the whole organization will be consuming less power. IoT (Internet of things) is a tangible technology that can be used in data centre [2]. Figure 1 shows that IoT (Internet of things) connects the whole world at particular place. As per the evaluation of technological specialist 50 billion physical objects or sensors will be connected in IoT by 2020. Example of IoT (Internet of things) devices such as smart health, smart homes such as smart TV among so on. As said earlier, IoT is not only Human-Human interaction; it is also Human-physical device communication.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 126–137, 2020.
https://doi.org/10.1007/978-3-030-37051-0_14

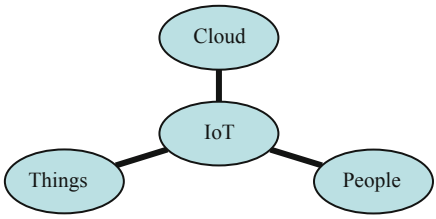


Fig. 1. IoT (Internet of Things)

This paper proposed a model of application IoT. This paper as well as monitor the weather parameter such as temperature, humidity, rain and upload this environment parameter value to cloud platform thingspeak using Node MCU. All analysed or monitored data are store in cloud platform. The main concept of paper all weather parameter sensors are connecting to Node MCU, Which is heart of device. We use C language and the code is written in Arduino IDE and uploads the data by the Node MCU, once the code is upload the board is connect to Node MCU then Its start working. Another we create second model this is fuzzy model for rain condition. We calculate the predicted rain value using fuzzy logic rule and by the use of fuzzy rule we achieve a better performance and then we compare and analysis both model on the basis of monitored rain value and predicted rain value.

The objective of this paper is as follows:

1. Calculate weather parameter such as Temperature, Humidity, Rain through Node MCU and different sensor.
2. Stored weather parameters data on online IoT platform.
3. To set the fuzzy rule to achieve better performance and more accuracy.
4. To compare and analysis both rain condition.

Rest of the paper is organized as follows. Section 2 explains the related work. System architecture is given in Sect. 3. Section 4 explains implementation setup in detail. Result and Discussion are given in Sect. 5. Finally, Sect. 6 contains the conclusion & future scope of this paper.

2 Related Work

Abraham et al. [2] give an IoT solution for the remote environment. Ram et al. [3] proposed a IoT based data logger system. It works on advance result for detecting the environment condition at a specific place. In 2016 Ibrahim et al. [4] proposed to build a cost effective environment monitoring device using Raspberry-Pi. In this he takes data from environment through sensor and uploads the data on web browser. In 2016, Kodali and Mandal [1] worked on weather station in which the station provide us information about the neighbouring environment and give alert to the user. In 2016 Meana-Llorian et al. [5] worked on IoT platform and fuzzy logic to control inside temperature of outside temperature condition in which he work on fuzzy logic and IoT (Internet of Things) related platform. Maksimovie et al. [6] worked on monitoring and

detecting the fire in which he proposed a fuzzy logic based fire monitoring and detecting system based on sensors. Kaur et al. [7] proposed a model to achieve automatic employee performance appraisal based on raw data monitor from Internet of things. Manjunatha et al. [8] present a multi-sensor data fusion algorithm in which he work on WSN using fuzzy logic for the event detection. Adiwijaya et al. [9] present a rainfall forecasting system using genetic algorithm. Suwardi et al. [10] proposed a rainfall prediction system using neuro-fuzzy model. Jaladi et al. [11] present a short range wireless technology in which she proposed a sensor logging model in environment monitoring. She works on zigbee protocol and raspberry pi. Mois et al. [12] given a 3 IoT (internet of things) based wireless sensor network in which he work on smart communication environment system.

Adhy et al. [13] proposed a Rendeng allocation in which his aim to test usability of Rendeng application. Rending application result has down in concept of efficiency. Rending has developed for some user.

3 System Architecture

Figure 2 shows that system architecture of weather monitoring. The sensor node is the main part of system architecture. Node MCU is a main part of proposed model and all sensors like temperature, humidity and rain are connected to this Node MCU. It is the heart of the device.

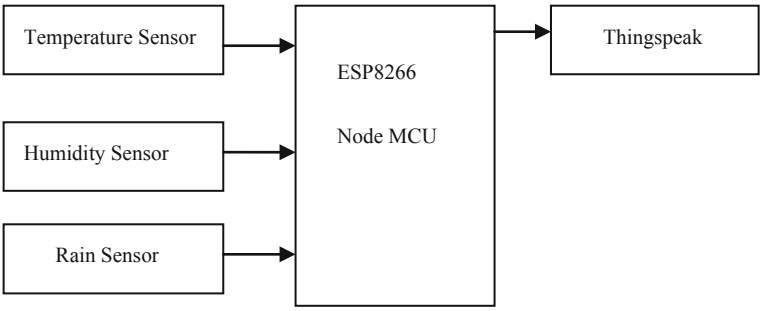


Fig. 2. Block diagram of weather monitoring system

3.1 Node MCU

Node MCU [14] network architecture is open for modification. Node MCU is a kit/board. It exists of Wi-Fi module. Node MCU board normally comes in market in black color only. In this board have an analog pin and digital output pin. It can be programmed through Arduino IDE. After it programmed the Node MCU board is connected and starts working. All sensors connect to Node MCU and monitor all environment data and send the data to IoT platform thingspeak through Wi-Fi module. Disk space of node MCU is 4 Mbytes (Fig. 3).

Fig. 3. Node MC

3.2 DHT 11(Temperature & Humidity Sensor)

DHT 11 is a temperature and humidity sensor. It monitors the temperature of surrounding environment. DHT11 temperature sensor consists of 4 pin. Pin 1 is GND, Pin 2 is Data pin, and Pin 3 is Voltage pin. Pin 1 is connected to GND, pin 2 is connected to node MCU data pin and pin 3 connected to 3.3 V. Pin 4 is left pin. DHT11 is monitor the temperature from range 0 °C–50 °C. DHT11 is monitoring the Humidity from range 20%–90% (Fig. 4).

Fig. 4. DHT11 sensor

3.3 Raindrop Detection Sensor

Rain sensor can detect the rain of our surrounding environment [15]. Rain sensor has a 4 Pin and 2 loop pin. In Rain sensor Pin 1 is A0 (Analog output), pin 2 is digital output, Pin 3 is GND and Pin 4 is Vcc. First loop pin is (+), it is a sensor board A, second loop pin is (−). It is also a sensor board B. In this module, analog output pin is measure moisture and when moisture exceeds then it gives digital output pin. In this module rain board and control board are different (Fig. 5).

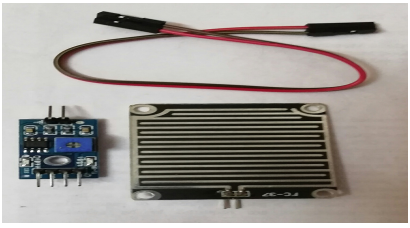


Fig. 5. Rain sensor

3.4 Thingspeak

Thingspeak is a analyze, visualize IoT platform [16]. It give the permission to analyses and visualize live environment parameter such as temperature, humidity, data flow in cloud. In 2010 thingspeak was firstly start through ioBridge (Fig. 6).

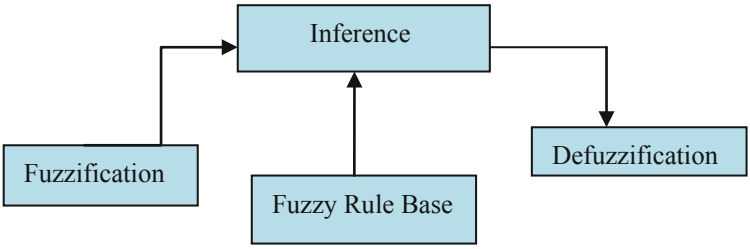


Fig. 6. Block diagram of fuzzy inference system

Fuzzifier: It is a procedure of changing input or crisp value to fuzzy value. Fuzzifier is based on the type of the strategy of inference engine similar to composition or disjunction rule based system [17]. Fuzzifier can be explaining as a plotting from an observed input place to fuzzy tag in a universe of identified input universe of discourse. In simple way we said that fuzzifier is electronic component. This fuzzifier module changes the numeric or crisp input to fuzzy input value.

Rule Evaluation: Fuzzy rule evaluate using a sequence of IF-THEN rule. In fuzzy rule evaluation:

IF Z is A and

IF W is B Then Z, W is variable.

Fuzzy rule is main idea in fuzzy logic. Some example of this rule is:

If Temperature is High, Humidity is low then Rain is low.

If Temperature is low and humidity is high then rain is high.

Defuzzifier: It is a procedure of changing fuzzy input value into the numeric or crisp input value. It is a procedure of producing a measurable result in crisp input, given fuzzy element and their associative membership function. Fuzzifier holds up the application of many fuzzifier methods and changes the crisp input value to fuzzy value. Knowledge base is mixture of rule evaluation. It is made upon the transformation of the numerical value to fuzzy data.

4 Implementation and Setup

For Model 1:

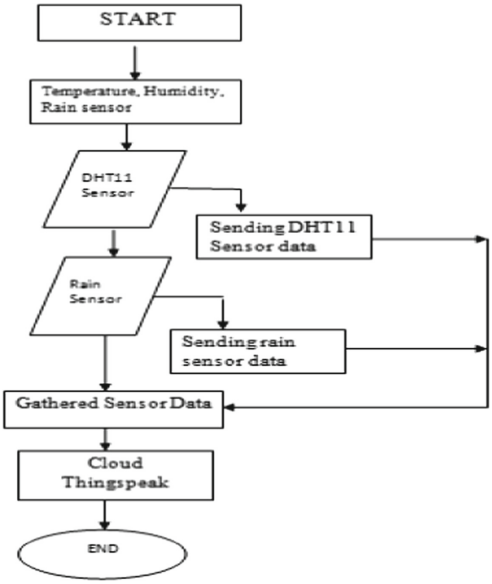
4.1 Hardware Components

1. Node MCU
2. Temperature and Humidity Sensor (DHT11)
3. Rain Sensor.

4.2 Software Components

1. Arduino IDE
2. Wi-Fi
3. Thingspeak.

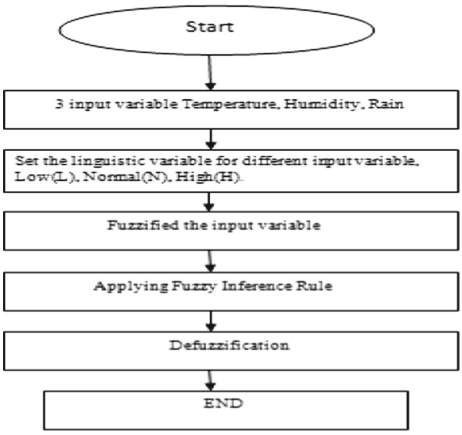
Flow Chart:



Based on the architecture shown in Fig. 2 we have build a right model that the model exist of many sensor and other hardware module and their functionality shown in system architecture. In this monitored model we use Node MCU is an electronic device for monitoring and storing the monitored data in cloud platform. We use Arduino IDE for processing. In this flow chart firstly we use Node MCU as a microcontroller. We use three different sensors for temperature, humidity and rain. Node MCU is a core of the model and all weather parameter related sensor are connected to node MCU. Data is uploaded through accessible Wi-Fi. When the code is

uploaded node MCU is connected to Wi-Fi and all connected sensors will start working. Wi-Fi is used to transfer the data to cloud in a thingspeak platform. All monitored value will be stored in thingspeak according to real time and plot graph in thingspeak utilizes the real time monitored data.

For Model 2:



In this model 2 flow chart, firstly we use three weather parameters Temperature, Humidity and Rain. We create proper fuzzy model for rain condition. In fuzzy logic model there are two fuzzy operation are performed, Fuzzification and Defuzzification. In fuzzifier every crisp input convert into fuzzy input for using membership function for two input and one output data. For temperature and humidity membership function is Low(L), Normal(N), High(H) and for rain membership function is Low(L), Normal (N), High(H), then we set the ranges according to the membership function or linguistic values. There are 3 input and 3 membership function then rule is.

IF Temperature is high, humidity is low THEN rain is low.

IF Temperature is low, humidity is normal THEN rain is low.

For overall fuzzy calculation MATLAB FIS used. All the processing is done in MATLAB Fuzzy logic tool box. Then lastly apply Defuzzification method. In Defuzzification method, we change the fuzzy output in crisp output. In implementation process we setup two model. According to these two model we analysis the rain condition. We compare monitored rain value to fuzzified rain value.

5 Result and Discussion

5.1 For Model 1 Result

See Figs. 7 and 8.

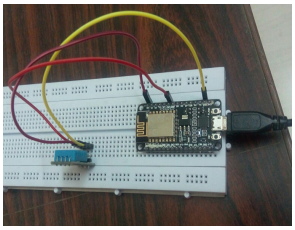


Fig. 7. Hardware setup

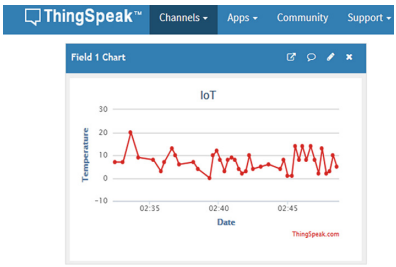


Fig. 8. Temperature result

5.1.1 Humidity and Rain Result

See Figs. 9 and 10.

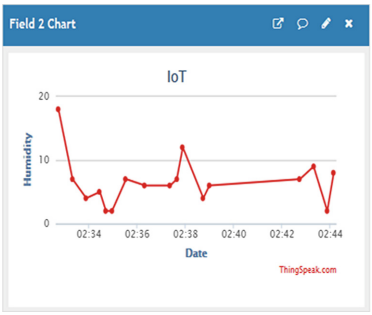


Fig. 9. Humidity result

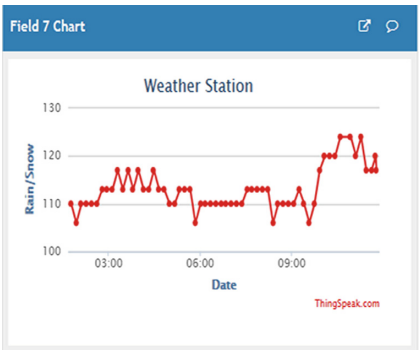


Fig. 10. Rain result

5.2 For Model 2 Result

In this model 2 we use historical data for minimum and maximum value of temperature and humidity. In this model we use MATLAB Fuzzy tool Box. Using this we apply different method (Table 1).

Table 1. Input parameters with its labels

S.no.	Parameter	Linguistic labels
1.	Temperature	Low (L), Normal (N), High (H)
2.	Humidity	Low (L), Normal (N), High (H)
3.	Rainfall	Low (L), Normal (N), High (H)

The maximum and minimum number of chances by recognizing every rules according to weather parameter is 7 rules. Since all 3 input has 3 membership degree. The 7 rules are:

If (temperature is low) and (humidity is high) then (chances of rain is high).

If (temperature is normal) and (humidity is normal) then (chances of rain is normal).

If (temperature is high) and (humidity is high) then (chances of rain is high).

If (temperature is low) and (humidity is low) then (chances of rain is low).

If (temperature is low) and (humidity is normal) then (chances of rain is low).

If (temperature is high) and (humidity is normal) then (chances of rain is low).

If (temperature is normal) and (humidity is high) then (chances of rain is high).

Chances of rain can be calculated by Fuzzy logic tool box (Table 2).

Table 2. Input parameters with its range

Parameter	Level
Temperature (°C)	Low: 0–10.8
	Normal: 10.8–21.8
	High: 20.04 to >28
Humidity (%)	Low: 0–31.3
	Normal: 31.6–48.1
	High: 48.3 to >68

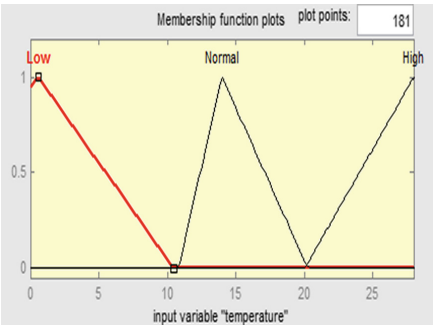


Fig. 11. Membership function for temperature

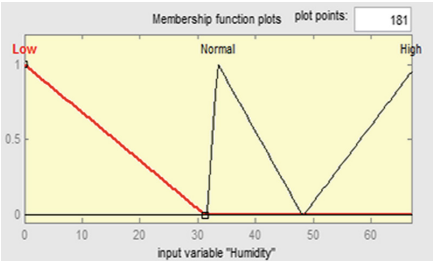


Fig. 12. Membership function for humidity

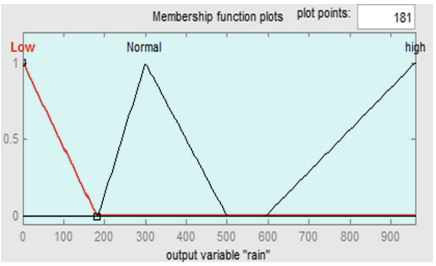


Fig. 13. Membership function for rain

In this Figs. 11, 12, 13 we use MATLAB fuzzy tool box. We have made and designed membership function. Inputs of our model are temperature, humidity as they are weather parameter that effects rain value. Output variable are consider the fuzzy set. The input parameter is managed by fuzzy if-then rule (Figs. 14, 15, 16).

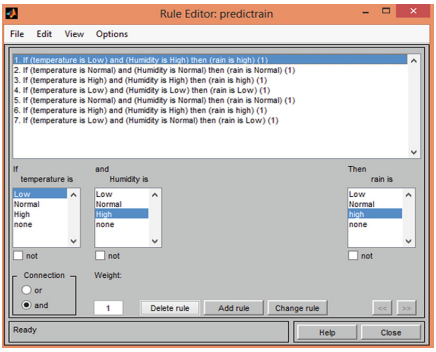


Fig. 14. Fuzzy logic system rule base

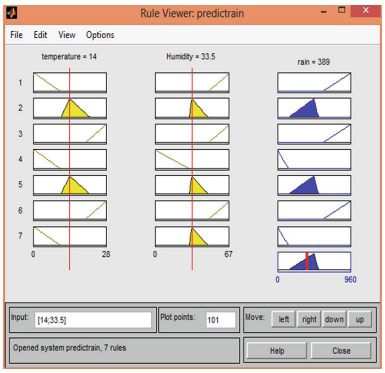


Fig. 15. FIS rule view

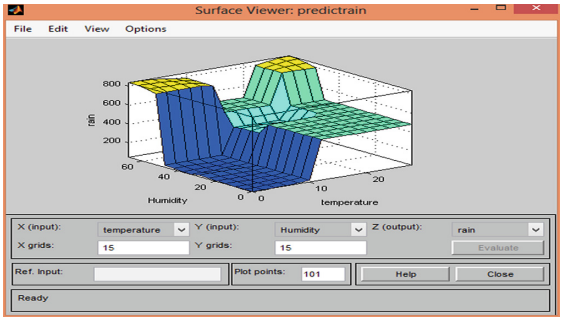


Fig. 16. FIS surface view

Different output can come from these model, when input value is different than output is also different, as temperature is low and humidity is high then chances of rain is high. In Table 3 we can see our simulated rain result by combining different input parameter (Table 4, Fig. 17).

Table 3. For different input evaluated results

Temperature (° C)	Humidity (%)	Output (mm)
14	33.5	388.53
20.2	36.2	298
21.4	35.6	347.24
17.6	43.6	264

Table 4. Comparison result

Monitored rain value	Predicted rain value
127	388.53
124	298
120	347.24
117	264

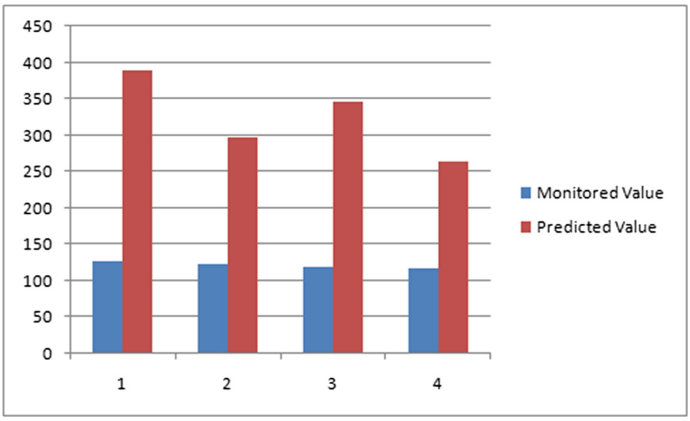


Fig. 17. Analysis result

6 Conclusion and Future Scope

This paper has developed an IoT (Internet of Things) solution for real time weather monitoring applications by the use of cost-effective sensor and other components. The monitored data was shown on thingspeak platform. Next, we present IoT together with fuzzy logic approach to calculate the rain value. According to both monitored and fuzzified rain value, we achieve a best performance for rain condition. In future we can add GPS in the model, so that the location of our neighboring environment will be mailed. We use some different environment parameters in the model.

References

1. Kodali, R.K., Mandal, S.: IoT based weather station. In: 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). IEEE (2016)
2. Abraham, S., Beard, J., Manijacob, R.: Remote environmental monitoring using internet of things (iot). In: 2017 IEEE Global Humanitarian Technology Conference (GHTC). IEEE (2017)
3. Ram, K.S.S., Gupta, A.N.P.S.: IoT based data logger system for weather monitoring using Wireless sensor networks. Int. J. Eng. Trends Technol. **32**(2), 71–75 (2016)
4. Ibrahim, M., et al.: Internet of things based smart environmental monitoring using the Raspberry-Pi computer. In: 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC). IEEE (2015)
5. Meana-Llorián, D., et al.: IoFClime: the fuzzy logic and the Internet of Things to control indoor temperature regarding the outdoor ambient conditions. Futur. Gener. Comput. Syst. **76**, 275–284 (2017)
6. Maksimovic, M., et al.: Developing a fuzzy logic based system for monitoring and early detection of residential fire based on thermistor sensors. Comput. Sci. Inf. Syst. **12**(1), 63–89 (2015)

7. Kaur, J., Kaur, K.: A fuzzy approach for an IoT-based automated employee performance appraisal. Comput. Mater. Continua **53**(1), 24–38 (2017)
8. Manjunatha, P., Verma, A.K., Srividya, A.: Multi-sensor data fusion in cluster based wireless sensor networks using fuzzy logic method. In: IEEE Region 10 Colloquium and the Third ICIIS, Kharagpur, India (2008)
9. Adiwijaya, F.N.: A rainfall forecasting using fuzzy system based on genetic algorithm. In: 2013 International Conference of Information and Communication Technology (ICoICT)
10. Surwardi, A., Takenori, K., Shuei, K.: Neuro-fuzzy approaches for modeling the wet season tropical rainfall. J. Agric. Inf. (2006)
11. Jaladi, A.R., Khithani, K., Pawar, P., Malvi, K., Sahoo, G.: Environmental monitoring using wireless sensor networks (WSN) based on IOT. Int. Res. J. Eng. Technol. **4**(1) (2017)
12. Mois, G.: Analysis of three IoT-based wireless Sensors for environmental monitoring. IEEE Trans. Instrum. Measur. **66**(8), 2056–2064 (2017)
13. Adhy, S., et al.: Usability testing of weather monitoring on a web application. In: 2017 1st International Conference on Informatics and Computational Sciences (ICICoS). IEEE (2017)
14. https://en.wikipedia.org/wiki/NodeMCU
15. https://wiki.eprolabs.com/index.php?title=Raindrop_Sensor
16. https://en.wikipedia.org/wiki/ThingSpeak
17. Indrabayu, N.H., Pallu, M.S., Achmad, A.: A new approach of expert system for rainfall prediction based on data series. Int. J. Eng. Res. Appl. **3**(2), 1805–1809 (2013)

Android Based Ripening Stage Identification for Peppercorns

K. J. Mythri(✉), N. Divya Ravi(✉), Poojitha, M. Prajna, and M. R. Pavan Kumar

Alva's Institute of Engineering and Technology, Mangalore, Karnataka 574225, India
divyaravi2007@gmail.com

Abstract. India is an agricultural country with over 58% of income is earned through agro-based environment. Out of all, the major crop produced in India is Black pepper. The production of black pepper has played a very important role in enhancing the economic growth of our country. To help in enhancing the production and the export of black pepper from India, this study proposes a method to detect the ripening stages of peppercorns. An android application is developed to predict the maturity and ripeness of the peppercorns. This will help the cultivators to produce peppercorns as per the global market requirement.

The pepper images, representing various stages of maturity are collected from various agricultural resources. These images are trained and classified by extracting, the color features like RGB value. The training and classification is done using Support Vector Machine Algorithm. SVM classifies the images into three classes. The images in these classes are used as the dataset to further identify the maturity or ripen stage of the peppercorns in the input image captured by the android application.

Keywords: Peppercorns · Agriculture · Maturity · Image processing · SVM algorithm

1 Introduction

Black Pepper is one of the most priced spices in the world. It is known to add flavor and taste to any bland food. Black pepper is also extensively used for its medicinal value in curing digestive issues, bronchitis, improving blood circulation etc. Manufacturers are focusing on continuous new product innovations such as essential oils, black pepper spray and fragrances. Recent research shows that there will be a significant impact on growth of the global market for black pepper. In 2017 global black pepper market was approximately valued at more than 3,700 million US$, which is estimated to increase at a CAGR of 6.1% over the forecast period to reach more than 5,700 million US$ by the end of 2024 [1].

In India, Kerala is the largest producer of black pepper. However, the tropical climate in major parts of the India is suitable for the cultivation of this popular spice. According to the department of agriculture, the harvesting time of black and white peppercorn in India, comes in the month of December and January, which does not

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 138–145, 2020.
https://doi.org/10.1007/978-3-030-37051-0_15

coincide with the harvest period of other major pepper producing countries in Asia [2]. Figure 1 shows the harvesting period of all the major pepper producing countries in Asia. Increasing the production of black pepper during this time would be favourable for the economic growth of our country.

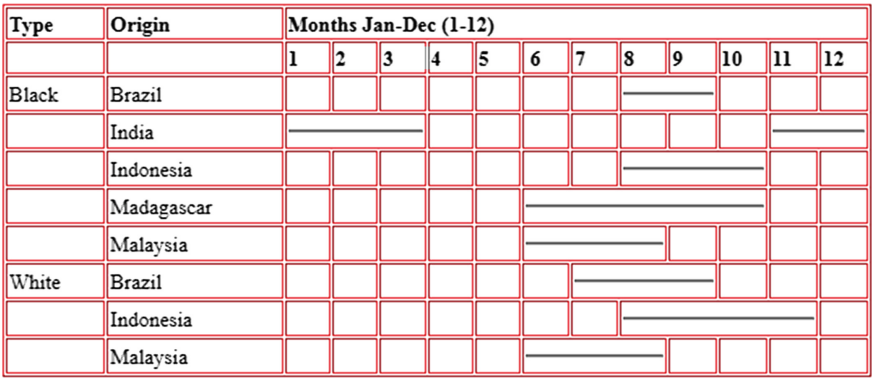


Fig. 1. Harvesting calendar of pepper producing countries in Asia [2].

Peppercorns are the fruits from the plant called Piper Nigrum. There are black, green and white peppercorns, which simply indicate the different ripen stages of the same peppercorn. Harvesting the peppercorns at the right stage of maturity is necessary for producing different kinds of pepper products with good colour, appearance, weight and taste [3]. Table 1 shows the optimum maturity stage needed for different pepper products at maturity. Here the canned peppers are immature, fresh (green) peppercorns [4].

Table 1. Optimum maturity stage needed for pepper products [4]

Product	Stage maturity at harvest
Canned pepper	4–5 months
Dehydrated green pepper	10–15 days before maturity
Oleoresin and essential oil	15–20 days before maturity
Black pepper	Fully mature & 1–2 berries start turning yellow to red in each spike
Pepper powder	Fully mature with maximum starch
White pepper	Fully ripe

There is a need for simple, easy and cost effective technique for identifying the ripening stages of the peppercorns. Smart phones are nowadays widely used for solving real time problems related to agriculture and industries. This paper discusses on developing an android application to identify the maturity stage of the peppercorns and

also predict the time required for the peppercorns to reach the next ripen stage and thereafter fully ripen stage. The system would help the cultivators to predict the time needed for ripening and hence plan a better marketing strategy to increase sales and profit.

2 Literature Survey

Lim and Gopal [5] developed an automated harvest system, based on computer vision to classifying the ripe peppers in a farmhouse. Firstly, a pepper detection algorithm was used to identify the area of interest from the image captured. The area of interest was determined by extracting the features like color, intensity and orientation. This actually gives the exact coordinate position of the pepper in the given image. Next the region containing the red color components were identified, as they are more likely to be the ripe pepper region. Lastly active contour method is applied to the extracted red region for form extraction. This is followed by the testing step to confirm the identification of ripe pepper region. Hence a fully automated harvest system was developed to identify and classify ripe peppers in the farm.

Ji et al. [6] a machine based computer vision system for harvesting apple. Here the images of the apple farm are captured using a color charge coupled device. The basic principle of color charge couple device is to represent the pixel value in the image in the form of an electrical charge. The electrical charge here determines the intensity of the color. However the main point here is to identify the intensity of red color value in the input image. In the meantime the images are processed to remove the noise, image segmentation method is used to identify edges. Once the color and shape feature is extracted from the images, the color quality is thoroughly investigated to identify and classify ripen apple for harvest. An improvised SVM algorithm was used for ripen apple classification.

Rupanagudi et al. [7] introduced an economical method for identifying the maturity stage of tomato. The six stages of tomato ripening process include immature green mature green, breaker, turning, red ripe, and overripe. The image processing algorithms were used to identify these six important stages of ripening. Simulink, integrated with Matlab was used to design model based image detection algorithm for identifying the ripen stage. An overall 98% of accuracy was obtained in successful classification.

Salunkhel et al. [8] used two methods to classify Alphonso mangoes. The two methods are based on the two color models: RGB and HSV respectively. In the RGB model, the classification is done based on the color intensity levels of Red, Green and Blue pixel in the images, while in the HSV model, the Hue, Saturation, Value is used to represent colors, which is quite similar to the way humans perceive color. Both the methods are insensitive to the ambient light quantity, if the images are taken under normal light conditions. Compare to the manual methods, the RGB and HSV method precisely gave 90.4% and 84.2% accuracy.

Dadwal et al. [9] developed a system where basically three steps were used to determine the threshold level for some selected parameters in the images. The steps include histogram equalization, image segmentation, and relative estimation of segmentation based on parameters. The training set was created for determining the

appropriate threshold value. The three steps were applied to any input image, and the parameters were compared with the threshold to detect the maturity of fruits or vegetables in the input image.

Gokul et al. [10] developed a system that utilizes the spherical shape of the sweet lime to detect the fruit and volume of the sweet lime to detect its ripeness. The radius here plays a major role in identifying the sweet lime in the pictures. Radius calculated can be used to determine the maturity level also. Volume is approximately measured based on the RGB color ratio.

Saadl et al. [11] developed a strategy to classify banana into three classes ripe, unripe and overripe depending on the histogram RGB value. Artificial Neural technique was used for effective classification. 32 training sample images were collected for applying the ANN algorithm. 28 images were used in the testing phase. Out of 28, images 25 images were accurately classified.

Kipli et al. [12] developed an application to predict the ripeness of banana. Here sample images representing three different ripen state of banana is sent through Google Cloud Vision Application Programming interface. The Google Cloud platform is used to analyze the attributes of the images. Thus a database is formed. For any input image of banana, the application compares the attributes with the database and the image is thus classified into either of the three states unripe, ready and overripe. Image processing and data mining algorithms are utilized.

3 Methodology

The proposed method identifies the maturity or ripeness stage of the peppercorns using image processing and SVM algorithm. The Fig. 2 shows the steps involved in the proposed system. The method involves two phases. The first phase is called the training phase and the second phase is called the testing phase. The basic steps involved in both the phases are Image Acquisition, Pre-processing, Feature Extraction and Classification using SVM algorithm.

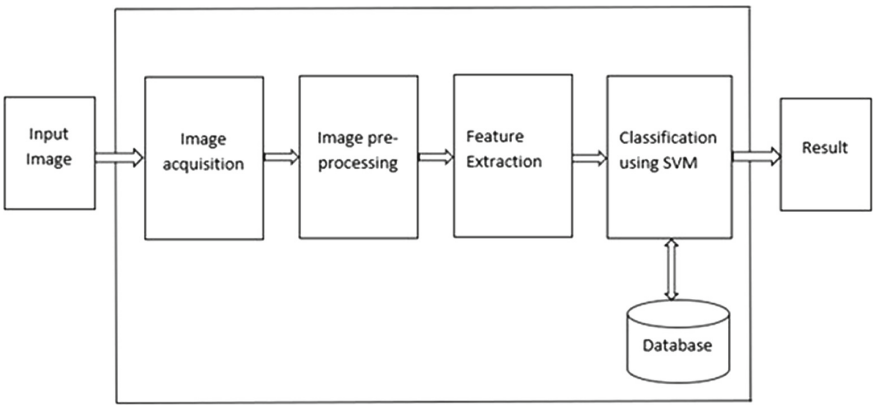


Fig. 2. Proposed system design.

In the training phase, the images representing various stages of maturity or ripeness of peppercorns were collected from authorized agricultural resources [13]. Around 50 images representing 4–5 months maturity stage of peppercorns, 45 images representing 6–7 months maturity stage, and 55 images representing 8 months fully ripe red peppercorns were collected. These datasets were pre-processed using histogram equalization and then the image processing methods were used to extract the RGB features. Based on the average value calculated on these features, the datasets were classified into three classes using SVM algorithm. The three classes here represent the three stages of maturity of the peppercorns. The 4–5 months mature green peppercorns represents class C1, the 6–7 months maturity stage peppercorns represents class C2 and fully ripe red peppercorns represents class C3. The images in these classes form the trained dataset and are stored in the database. These images will be further used in the testing phase to identify the maturity stage of the peppercorns in the input image captured through the Android App developed. The following steps explain the testing phase in details.

A. Image Acquisition and Collection

In this stage the image of black pepper fruit is captured through the camera of the smart phone.

B. Image Pre-processing

In pre-processing, histogram equalization is used as the primary method for noise reduction, cropping and smoothing of the input image. Edge detection and shape detection is carried out as the secondary method for pre-processing.

C. Feature Extraction

In the proposed method, image processing technique is used to extract the RGB value of the pixels in the input images. The Red, Green and Blue value of the pixels in the images determines the color intensity of the given image. The average of the R, G and B component of each pixel in an image is calculated. The Average RGB value is a threshold value or descriptor. The following are the equations for computing the average of the R, G, B component of an image, where I is the image, w - width of image I, h - height of image I, $I(x, y)$ - the pixel of image I at row y, column x, $R(p)$, $tt(p)$, $B(p)$ - the red, green and blue color component of pixel p, r_a, g_a, b_a - the average red, green and blue component of image I_a and (I_a, I_b) - the distance measure between image I_a and I_b.

$$r = \sum_{x=1,y=1}^{x=w,y=h} \frac{R(I(x,y))}{w \times h} \tag{1}$$

$$g = \sum_{x=1,y=1}^{x=w,y=h} \frac{G(I(x,y))}{w \times h} \tag{2}$$

$$b = \sum_{x=1,y=1}^{x=w,y=h} \frac{B(I(x,y))}{w \times h} \tag{3}$$

The equation for distance measure of image I_a and I_b is calculated using the weighted Euclidean distance. The distance between two exact images will be 0 and the distance between two most dissimilar images will be 1 depending on the range of RGB i.e. from 0–255.

$$d(I_a, I_b) \sqrt{\frac{(r_a - r_b)^2 + (g_a - g_b)^2 + (b_a - b_b)^2}{3}} \tag{4}$$

D. Classification

In classification the images are classified using SVM (Support Vector Machine) algorithm. The distance measure calculated is used as the threshold value, to decide the class to which the input test image belongs. Since SVM is the binary classification method as a research it can be applied even for the multiple classes. So here the test images would belong to the class, based on the closest match to the cluster class C1, C2 or C3. The Fig. 3 represents the test image that closely matches to class C1, Fig. 4 represents the test image that closely matches to class C2, Fig. 5 represents the test image that closely matches to class C3.

4 Experimental Results

The android application is developed using Java and by implementing the MVC architecture. The trained datasets are stored in the cloud platform. The Fig. 6 shows the snapshot of the android application. Both, images from the gallery and real time images of peppercorns captured from the smart phone camera were tested and accurately classified. The proposed system provides an accuracy of approximately 80%. Out of ten images tested for classification, eight images were accurately classified into its corresponding class, thereby efficiently identifying the maturity or ripen stage of the peppercorns.

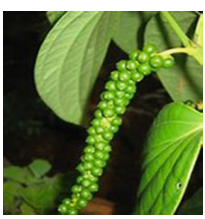


Fig. 3. Class C1

Fig. 4. Class C2

Fig. 5. Class C3

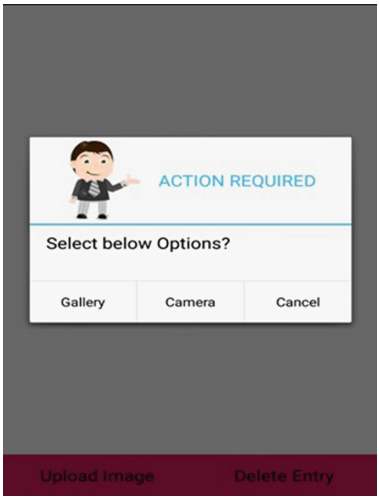


Fig. 6. Snapshot of android application

5 Conclusion and Future Work

The proposed framework will be useful for peppercorns cultivators to efficiently identify the maturity stages of the peppercorns. This is necessary in order to harvest the peppercorns at the right stage of maturity and thereby produces quality pepper products for sale and export. In future work, the system could be developed to predict the time required to reach the next stage of maturity. Also, this method can be applied to predict the maturity of the other fruits.

References

1. https://www.persistencemarketresearch.com/market-research/black-pepper-market.asp
2. https://www.nda.agric.za/docs/Infopaks/pepper.htm
3. http://nhb.gov.in/NHBDPR/Black_Pepper_DPR.pdf

4. https://pepperindia.com/pepper_products.html
5. Lim, K.H., Gopalai, A.A.: Robotic vision system design for black pepper harvesting, Department of Electrical and Computer Engineering Curtin University, Sarawak Campus Miri, IEEE. glkhann@ieee.org, alpha.agape@ieee.org. 978-1-4799-2827-9/13/$31.00
6. Ji, W., Zhao, D., Cheng, F., Xu, B., Zhang, Y., Wang, J.: Automatic recognition vision system guided for apple harvesting robot. Comput. Electric. Eng. **38**(5), 1186–1195 (2012)
7. Rupanagudi, S.R., Ranjani, B.S., Nagaraj, P. and Bhat, V.G.: A cost effective tomato maturity grading system using image processing for farmers. In: IEEE International Conference on Contemporay Computing and Informatics. IEEE (2014). ISBN: 978-1-4799-6629-5/14/$31.00
8. Salunkhe, R.P., Patil, A.A.: Image processing for mango ripening stage detection: RGB and HSV method. In: Third International Conference on Image Information Processing. IEEE (2015). 978-1-5090-0148-4/15/$31.00
9. Dadwal, M., Banga, V.K.: Color image segmentation for fruit ripeness detection: a review. In: 2nd International Conference on Electrical, Electronics and Civil Engineering (ICEECE'2012), Singapore, 28–29 April 2012
10. Gokul, P.R., Raj, S., Suriyamoorthi, P.: Estimation of Volume and Maturity of Sweet Lime Fruit using Image Processing Algorithm. In: IEEE ICCSP Conference. IEEE (2015). 978-1-4799-8081-9/15/$31.00
11. Saad, H., Ismail, A.P., Othman, N., Jusoh, M.H., fadzlina Naim, N., Ahmad, N.A.: Recognizing the ripeness of bananas using artificial neural network based on histogram approach. In: 2009 IEEE International Conference on Signal and Image Processing Applications (2009). 978-1-4244-5561-4/09/$26.00
12. Kipli, K., Zen, H., Sawawi, M.: Image processing mobile application for banana ripeness evaluation. IEEE (2018). 978-1-5386-8369-9/18/$31.00
13. Zonal Agricultural and Horticultural Research Station, Brahmavar-576213, Udupi District

Energy Efficient Heterogeneous Wireless Sensor Networks - Recent Trends & Research Challenges

H. R. Manjunath[1(✉)] and C. D. Guruprakash[2]

[1] Sri Siddhartha Academy of Higher Education, Sri Siddhartha University, Tumakuru, Karnataka, India
manjunathdvg@gmail.com
[2] Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India
cdguruprakash@gmail.com

Abstract. In recent times, Heterogeneous Wireless Sensor Networks (HWSNs) are gaining increasing interest from various research communities due to their potential applications in large number of domains such as environmental applications, area surveillance and health monitoring. However, the performance of a HWSN primarily depends on a set of critical decision parameters including robustness, security, connectivity and efficient usage of energy and so on. Specifically, one of the most important research challenges is, enhancing the network lifetime of HWSNs, so that the object monitoring activities can be conducted without any interruptions. More specifically, Energy usage in a network is an essential factor, which directly influences the lifetime of the given network. In contrast, efficient energy utilization within a network can be achieved by means of grouping the nodes into clusters using effective clustering algorithms. In this paper, an overview of HWSNs is presented along with the different state-of-the-art techniques used for implementing energy efficient clustering strategies. Furthermore, this article also explores the future key directions and highlights the research challenges that need to be addressed in achieving energy efficient clustering in HWSNs.

Keywords: HWSN · Energy efficiency · Clustering in HWSNs

1 Introduction

In the past few decades, there is an bigger research curiosity in the possible uses of Wireless Sensor System (WSN) in variety of field including border security surveillance, disaster management, and surveillance of battle field and so on [1]. Generally, Wireless sensor system (WSN) consists of small sensors/nodes having capabilities such as sensing, calculation and communications. These sensors collect data by sensing their environment, collect the sensed facts to figure useful information and send out it to the base location or the adjacent node for further processing. However, sensor nodes are limited in power, memory, computational capacities and specifically shorter life span. One of the strategies is to extend the lifetime of WSN is to incorporate a definite percentage of sensor nodes outfitted with additional energy sources, by means of

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 146–151, 2020.
https://doi.org/10.1007/978-3-030-37051-0_16

building the WSN as heterogeneous WSN (HWSN) in terms of energy. Due to this incorporation of additional sensor nodes, HWSNs stay alive for a longer time, as compared to homogeneous WSNs, which is sufficiently demonstrated in the literature in terms of many present schemes for heterogeneous wireless sensor networks (HWSNs) such as SYLPH [1] and EEHC [2]. Researchers of WSN believe that, if nodes are non-homogeneous having some of the nodes with different energy levels, might extend the lifetime of a WSN and its reliability to a greater extent [3].

Generally, there are three types of resource heterogeneity may exist in HWSN-based sensor nodes, namely computational heterogeneity, link heterogeneity and energy heterogeneity.

Computational heterogeneity indicates that, few of the mixed nodes consist of more potent microprocessor and more memory compared with the other regular nodes. Link heterogeneity represents, some of the nodes in HWSN have more bandwidth and longer distance network transmission capabilities compared to the other normal nodes. Energy heterogeneity denotes that, some of the heterogeneous nodes are line powered or battery replaceable. Energy heterogeneity is considered as the most important heterogeneity among all the three types of resource heterogeneities, since both the computational heterogeneity and link heterogeneity mainly depends upon consumption of amount of energy resources. In addition, the effectual position of heterogeneous nodes in the sensor network significantly reduces average energy consumption and also increases network lifetime as well as reliability of data transmission. Due to these reasons, HWSN have broader applications than homogeneous WSNs. However, due to their replace ability of nodes, one of the major challenges in HWSN is dealing with effective consumption of energy in order to extend the network life span in complex heterogeneous network environments.

2 Literature Survey

Clusters are the organizational unit for WSNs. A WSN can be able to changed in size by gather together the sensor nodes into groups i.e. clusters. Every cluster have got a head, which is called as the cluster head (CH), which may be selected by the sensors in a bunch or pre allocated by the network designer. In the literature, a no. of clustering algorithms are introduced for designing HWSNs, which in turn can enhance scalability, data communication as well as efficient energy utilization.

For example, Smaragdakis et al. [4] discuss stable election protocol (SEP), which uses heterogeneity concept. As per this procedure, a node can become a cluster head based on weighted election prospect, which uses a function of the residual energy of the nodes in order to make sure consistent usage of node energy. The fundamental network of the SEP considers two levels of heterogeneity namely advanced nodes and normal nodes. However, the energy of the superior node is somewhat advanced than the ordinary nodes and their count is lesser than that of the normal nodes due to the bigger cost factor.

Li et al. [5] introduced the distributed energy efficient clustering DEEC protocol by considering 2-level and multilevel heterogeneous WSN. In this multilevel non homogeneous network plan, the energy of each sensor node is arbitrarily assigned from

a given energy time. However, in this group all nodes are having diverse levels of energy because of arbitrary allotment. Due to these reasons, this multilevel non homogeneous network model is hardly of any use, since designing sensor nodes of large number energy levels may not be nearly viable.

Mao et al. [6] presented an efficient data assembly algorithm known as (EDGA) for heterogeneous WSNs that considers 3 levels of non uniformity by introducing 3 forms of nodes: traditional, advanced, and super nodes. However, the performance of this approach is slightly less due to the fact that, the vitality of a propelled hub is higher than that of a normal node and the vitality of a super hub is higher than its counterpart propelled hub.

Recently, in 2014, two distributed protocols namely, single-jump vitality productive bunching convention (S-EECP) also, multi-bounce vitality proficient grouping convention (M-EECP) are introduced by Kumar [7]. In S-EECP, the cluster heads are chosen by a weighted likelihood dependent on the proportion between remaining vitality of every hub in examination with the normal vitality of the system. But, M-EECP uses a greedy method to take care of the single source most brief issue to locate the most brief way from each bunch head to the BS.

Farouk et al. [8] presented a stable and vitality proficient grouping (SEEC) convention followed by the extension of multi-level SEEC. Zhou et al. [9] presented a technique based on bunching convention vitality scattering forecast and bunching the board (EDFCM), which uses two-level network composed of super hubs and normal hubs. In this method, the best number of gatherings calculated using LEACH. Also, a mathematical energy consumption model to compute the weighted likelihood of hub for choosing bunch head node is employed. However, the technique achieves slightly less performance, since the computation of normal vitality utilization at the next round of organize causes deviations in practice, which might form an ideal value.

Chand et al. [10] conducted a study of heterogeneous HEED protocol. It considers three parameters, namely residual energy, hub thickness, and separation. The authors used fuzzy logic techniques to determine the cluster heads. However, if cluster heads are not ready to speak with one another, then the data may be lost.

In 2015, Xiao et al. [11] detailed a cell-grouped calculation known as CC-HEED for energy efficiency in HWSNs. Though the performance of this approach is better, yet power consumption constrains limit the output rates, since cell nodes in cell-shaped areas are assembled together to collect the data in each cell region by taking into account power utilization model.

Very recently in 2016, Singh et al. [11] introduced a novel vitality proficient bunching convention (NEECP) for expanding the system lifetime in WSNs. This strategy chooses the bunch heads effectively with a movable detecting range and performs information total utilizing anchoring approaches. It likewise stays away from transmission of excess information by utilizing a repetition check work for improving the system lifetime. However, the performance of this scheme is slightly poor, due to the limitations of aggregation functionalities.

3 HWSNs - Network Model

HWSN in general, consists of multiple sensors with different processing capabilities as well as initial energy. Since, each node in a HWSN has staggered control choices; it can consume different energy levels per round during their ordinary execution depending upon its present power level. Further the connection quality and bundle loss rate are primary performance bottleneck issues in HWSN, which needs to be tackled with at most care, in convoluted remote situations. In addition, the node interferences can occur among hubs and clusters. In this way, the heterogeneous WSN with considerable amount of limitations is continuing as one of the potential research domain in the recent few decades (Fig. 1).

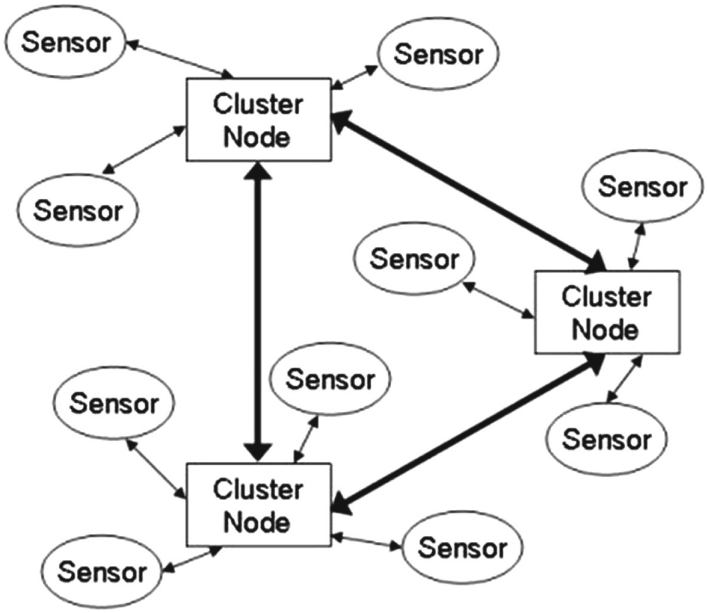


Fig. 1. Example two-layered heterogeneous WSN for energy efficiency

4 Future Research Challenges

In the current writing, though various techniques are introduced to achieve energy efficient clustering, yet few of the research challenges are not yet completely solved, which need to be addressed in future are as summarized below:

A. Computing ideal number of cluster heads:
In the literature, most of the techniques select the cluster head in a predefined way. However, achieving the ideal number of bunch heads is essential to ensure the least energy dissipation in the network so that the power consumption is reduced to extend the life of the network.

B. Maximize network lifetime:
In HWSN, the sensors are resource constraint and dependent on batteries as source of energy, due to which maximizing the lifetime becomes an important concern in HWSN design.

C. Cluster size:
In HWSN, balanced number of cluster members can distribute the load of cluster head uniformly. Since, if the cluster head is overburdened, this can cause more energy consumption and early death of nodes, which needs to be resolved.

D. Ignoring residual energy, geographic location information:
In the existing algorithms less focus is given towards remaining energy as well as geographic location of nodes, which prove to be very effective while selecting cluster heads. Therefore, incorporation of residual energy and geographic location information may significantly enhance the energy utilization of nodes in terms efficient clustering process.

E. Reduce the Energy Spent per Round:
This measurement is related to the total energy used in routing messages in a round. It is a measure of the short term which can be intended to improve the energy efficiency of nodes in any HWSN.

F. Effective Low-Duty Cycle Operations in Idle States of Nodes:
In general, from the data sensing point of view, the To collect environmental data from the field, sensor nodes should remain in active state, whereas sensor nodes are expected to be powered off periodically for energy conservation concerns. To solve this issue, effective low duty-cycled operations need to be employed, where In order to save energy consumption in idle conditions, each node periodically switches between sleep mode and wake mode.

G. Uniformity in Cluster head distribution:
In the literature, though cluster head distribution is focused more, yet suitable metrics for computing uniformity in cluster head distribution are completely unexplored, which might result in longer network lifetime.

5 Conclusion

Only just, more popular are heterogeneous wireless sensor networks (HWSNs) among various research communities due to their potential applications in large number of domains such as environmental applications. Specifically, one of the most important research challenges is, enhancing the network lifetime of HWSNs. However, Energy usage in a network is an essential factor, which directly influences the lifetime of the network.

On the other hand, efficient energy utilization in a network can be achieved by means of grouping the nodes into clusters using effective clustering algorithms. In this paper, an overview of HWSNs is presented along with the different state-of-the-art techniques used for implementing energy efficient clustering strategies. Further, future key directions and research challenges are highlighted in this article which could be beneficial for achieving energy efficient clustering in HWSNs.

References

1. Dudek, D., Haas, C., Kuntz, A., Zitterbart, M., Krüger, D., Rothenpieler, P., Pfisterer, D., Fischer, S.: A wireless sensor network for border surveillance. Int. J. Embed. Netw. Syst. **7**, 303–304 (2009)
2. Corchado, J.M., Bajo, J., Tapia, D.I., Abraham, A.: Using heterogeneous wireless sensor networks in a telemonitoring system for healthcare. IEEE Trans. Inf. Technol. Biomed. **14** (2), 234–240 (2010)
3. Kumar, D., Aseri, T.C., Patel, R.B.: EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks. Comput. Commun. **32**(4), 662–667 (2009)
4. Smaragdakis, G., Matta, I., Bestavros, A.: SEP: a stable election protocol for clustered heterogeneous wireless sensor networks. In: 2nd International Workshop on Sensor and Actor Network Protocols and Applications, pp. 1–11 (2004)
5. Li, Q., Qingxin, Z., Mingwen, W.: Design of a distributed energy efficient clustering algorithm for heterogeneous wireless sensor networks. Comput. Commun. **29**(12), 2230–2237 (2006)
6. Mao, Y., Liu, Z., Zhang, L., Li, X.: An effective data gathering scheme in heterogeneous energy wireless sensor networks. In: Proceedings of the IEEE International Conference on Computational Science and Engineering, vol. 1, pp. 338–343 (2009)
7. Kumar, D.: Performance analysis of energy efficient clustering protocols for maximising lifetime of wireless sensor networks. IET Wirel. Sens. Syst. **4**(1), 9–16 (2014)
8. Farouk, F., Rizk, R., Zaki, F.W.: Multi-level stable and energy-efficient clustering protocol in heterogeneous wireless sensor networks. IET Wirel. Sens. Syst. **4**(4), 159–169 (2014)
9. Zhou, H.B., Wu, Y.M., Hu, Y.Q., Xie, G.Z.: A novel stable selection and reliable transmission protocol for clustered heterogeneous wireless sensor networks. Comput. Commun. **33**(15), 1843–1849 (2010)
10. Chand, S., Singh, S., Kumar, B.: Heterogeneous HEED protocol for wireless sensor networks. Wirel. Pers. Commun. **77**(3), 2117–2139 (2014)
11. Xiao, G., Sun, N., Lv, L., Ma, J., Chen, Y.: An HEED-based study of cell-clustered algorithm in wireless sensor network for energy efficiency. Wirel. Pers. Commun. **81**, 373–386 (2015)
12. Singh, S., Chand, S., Kumar, R., Malik, A., Kumar, B.: NEECP: novel energy efficient clustering protocol for prolonging lifetime of WSNs, IET Wirel. Sens. Syst. (2016)

A Novel Security Scheme of Temporal-Key Based Encryption Policy in Sensor Applications

M. N. Premakumar(✉) and S. Ramesh

Department Electronics & Communication, Dr. AIT,
Bengaluru, Karnataka, India
premakumar1976feb@gmail.com

Abstract. The contribution of Wireless Sensor Network (WSN) towards commercial sensing application is tremendously progressing day-by-day. However, it is still shrouded by security problems owing to less practical applicability of existing research solutions as well as inherent nature of resource constrained nodes. Key management in encryption technique is one of the most frequently exercised techniques; however, it lacks the robustness against various attacks due to flawed in design principle of dependable parameters in construction security solution. Therefore, the proposed system introduced a novel temporal key-based mechanism that is meant for strengthening the encryption operation. The study also offers higher flexibility to include different encryption algorithm for scaling the security feature based on different vulnerability over the challenging environment of WSN.

Keywords: Wireless sensor network · Security · Encryption · Temporal keys · Clustering techniques · Energy efficiency

1 Introduction

Due to the sensing mechanism that is cost efficient, a high degree of attention is attracted towards Wireless Sensor Network (WSN) area [1]. The WSN based issues are addressed with several solutions in various segments [2–4]. Regardless of the numerous research-based techniques available, the research community is yet to address several security issues associated with WSN [5–8]. Execution of a strong cryptographic protocol is a major challenge in sensor nodes as WSN imposes several security issues in this context [9]. The memory constraints and low computational capabilities does not allow execution of prospective encryption algorithms from other networks in sensor nodes [10]. This imposes a great challenge in designing an encryption system that is light weight and can balance the computational complexity and strong security features. Public key encryption is commonly used in encryption mechanism as management of key plays a major role in this domain. Several loopholes are also associated to encryption of public key. The performance of computation-communication in WSN is compromised whereas strong security is provided by public key encryption. The lack of assurance towards compromise of keys or additional

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 152–161, 2020.
https://doi.org/10.1007/978-3-030-37051-0_17

protection in public keys is a substantial loophole in public key encryption. Based on multiple factors like energy and distance for protection of public keys, several adversaries are filtered. A novel mechanism for this purpose is introduced in this paper.

2 Related Work

A brief of the literature containing recent trends towards addressing the WSN based security issues and related research is presented in this section. Aissani et al. [11] used the process of re-keying for management of micro key in WSN. Burg et al. [12] emphasized on the security issues in IoT devices. The paper also rendered that in cyber-physical systems, implementation of WSN does not provide adequate security. Gandino et al. [13] discussed the solution to reduce the computational complexity using hierarchical approach for management of master key. Gopalakrishnan et al. [14] performed secure routing with chaotic approach that was independent of pre-shared keys. Enhancement of security measures with an emergency key of special form is presented by Gope and Hwang [15] using a unique mechanism for exchanging of keys. Haghighi et al. [16] studied the use of analytical modeling for addressing wormholes. Huang et al. [17] focused on strengthening of the authentication system using the group key management concept. Kesavan et al. [18] considered the WSN based mobility aspects for managing the security issues using clustering to perform processing of dynamic keying. Other than this, other security addressing approaches like randomization, composite key distribution, time and energy management, linear programming, identification of attack, encryption of public-key, optimization, multifactor authentication and so on [19–30] are studied by several researchers.

3 Problem Description

Irrespective of numerous studies towards key management and cryptographic approaches towards securing WSN, there are yet two potential problems that are unaddressed e.g. (i) existing key management techniques are based on some model/equation that if compromised damages the entire network system, (ii) consideration of dependable parameters to construct encryption algorithm were not much focused other than conventional random/prime numbers. Therefore, research problem can be stated as “developing highly dynamic dependable parameters for constructing a novel secure approach for strengthening the key management in WSN is computationally challenging task”. The next section outlines about the proposed research methodology in order address this identified research problem.

4 Proposed Methodology

The design implementation of the proposed system is carried out using analytical research methodology. Figure 1 highlights the proposed scheme of secure communication in WSN with a novelty of implementing temporal key factors as the core backbone of the encryption approach used.

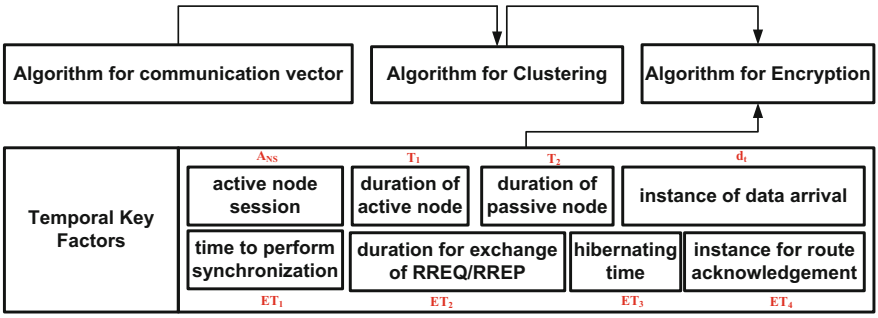


Fig. 1. Proposed scheme

The proposed system aims to develop a novel temporal key-based mechanism for offering secure communication in WSN. Initially a communication vector is constructed using shortest routing approach followed by dynamic and user-defined cluster formation. Finally, a flexible encryption approach is introduced that uses different attributes of temporal keys. The novelty/robustness of proposed system is that none of the parameters used for temporal keys can be even compromised or extracted by the adversary as they are highly dynamic in order and at the same time they are also large in number. A matrix-based mechanism is introduced in order to formulate hops and clusters where different forms of encryption algorithm can be implemented depending upon the criticality of the data to be forwarded. The next section discusses about the design of algorithm and its logic of implementation.

5 Algorithm Implementation

The design and development of the proposed algorithm is based on the fact that is a need of a novel security system that can offer an efficient balance between communication performance as well as security performance in WSN. The research aim is implemented using three different research objectives sequentially viz. Algorithm for Constructing communication vector, Algorithm for clustering, and Algorithm for applying encryption. The briefings of these algorithms are as follows.

5.1 Algorithm for Constructing Communication Vector

This algorithm is responsible for setting up normal communication vector between two sensor nodes. The algorithm takes the input of S_A (Simulation Area) and N (Number of Sensors), which after processing gives the output of c_{vec} (communication vector).

(i) Operation of Algorithm: The algorithm performs a random distribution of all the N

Algorithm for Constructing Communication Vector

Input: S_A, N

Output: c_{vec}

Start

1. (x, y)→S_A. rand(N)
2. **For** i=1:N
3. α=β≤r
4. d=euc[N(x,y)-BS(x,y)]
5. **If**d<r
6. α((I,N+1),(N+1,i))=1
7. **End**
8. α→0
9. xy→[N(x,y), BS(x,y)]
10. c_{vec}→Apply f_1(α, xy, I, N+1)

End

sensors with (x, y) being the position of the sensor (Line-1). For all sensors (Line-2), the algorithm checks for a variable β which is basically a matrix storing all the spatial information of the sensors with each other. If the value of β is found to be less than coverage r than it can be assumed that these set of nodes are having large number of connections with each other (Line-3). Further Euclidean's distance function *euc* is applied between the sensor node with position N(x, y) and base station with position BS (x, y) in order to obtain distance *d* (Line-4). A connection matrix α is formed if distance *d* is found to be less than coverage *r* (Line-5). Therefore, Line-6 shows the process of establishing connection among all the neighboring nodes. Finally, the diagonal value of the distance matrix is made zero (Line-8). Further, a matrix *xy* is formulated in order to connect base-station and current sensors (Line-9). Finally, a shortest routing protocol function f_1(x) is applied with an input arguments of connection matrix α, matrix with position information of current sensor with base station, and all sensor information.

(ii) Security Benefit of Algorithm: In order to perform secure routing, it is essential that a proper accountability of the entire sensor should be retained in order to perform security validation. Normally, such information is retained over hop table that is borne by an individual sensor. Hence, the beneficial factor of this algorithms are (i) it retains all sensor node identity-based as well as hop-based information and maintains a record in the form of dynamic memory system called as connection matrix, (ii) it offer shortest routing using f_1(x).

5.2 Algorithm for Clustering

Clustering plays an essential role in performing communication system. Apart from energy-efficient data aggregation, it has also bigger contribution towards retaining higher security. A controlled mechanism of maintaining number of clusters is one of the best mechanisms to triangulate the adversary, which unfortunately doesn't exists in any of existing approaches of clustering. Therefore, the proposed clustering algorithm formulates clusters on the *demand* of user/application unlike an automated mechanism of existing system. The algorithm takes the input of τ (number of target cluster) which after processing lead to generate of shortlisted nodes under specific clusters G_{id} (cluster ID).

(i) Operation of Algorithm: For all the sensors (Line-1), the proposed system first

Algorithm for Clustering
Input: τ
Output: G_{id}
Start
1. **For** i=1:N
2. $\rho_{1node} \rightarrow h_1(i)$
3. **If** (ρ_{1node}!=N+1)
4. $\rho_{2node} \rightarrow h_2(h_1)$
5. $h_2(i) \rightarrow \rho_{2node}$
6. **End**
7. **End**
8. **For** i=1: τ
9. **If**i< τ
10. getID→Ridx((i-1).N/τ)+1, (i).N/τ)
11. **Else**
12. getID→Ridx((i-1).N/τ)+1, end
13. **End**
14. Gid(getID)=i
15. **End**
End

obtains single hop $h_1(x)$ information for all the sensors (Line-2) and retain all this information in a matrix ρ_{1node} (Line-2). In case of presence of more number of hops (Line-3), the algorithm constructs double hops from single hop $h_1(x)$ itself (Line-4) and this results in final two hops matrix i.e. ρ_{2node} (Line-5). The algorithm then takes the input of number of cluster and generates a random identity R_{idx} from all the existing sensors (Line-8 and Line-9). For all the number of clusters (Line-9), the algorithm extracts an identity of all the nodes using the expression shown in Line-10 and Line-11 in order to finally confirm the identity of all nodes under demanded number of clusters (Line-14).

(ii) Security Benefit of Algorithm: Normally, the presence of attacker node will be either within a cluster or outside of it. However, it is more likely that adversary position will be definitely within the reach of one of the cluster. Hence, proposed algorithm benefits by restricting the process of generating number of clusters on the demand of user/application and hence cannot be controlled by any adversary. Therefore, number of clusters can be retaining low with coverage of all the sensors. This is the best way to

minimize the search time of validation of member nodes within or outside of a cluster. Moreover, it generates a random identity of each member node as well as cluster node and retains under a secured matrix Gid, which is completely inaccessible to adversary. Therefore, even without using any form of cryptographic approach till this step, the proposed system offers significant level of data integrity as well as confidentiality.

5.3 Algorithm for Applying Encryption

This is the final step of proposed system which offers resistivity against lethal adversaries. This algorithm offers the proposed framework to implement different kinds of encryption algorithm in order to secure the data packet. The algorithm takes the input of A_{NS} (active node session), f_{size} (size of frame), T_1 (duration of active node), T_2 (duration of passive node), d_t (instance of data arrival), ET_1 (time to perform synchronization), ET_2 (duration for exchange of RREQ/RREP), ET_3 (hibernating time), ET_4 (instance for route acknowledgement), *pr* (priority), and *data* (data packet), which after processing yields *e* (Encrypted data).

(i) Operation of Algorithm: This part of the algorithm considers various temporal-key based security system parameters, which ensures that it retains record of each instance of communication with respect to active and passive mode. The mechanism of compute temporal factor is illustrated in result section. The algorithm generates an arbitrary index in order to generate arbitrary instances of data being arriving within the networks. The algorithm also ensures that in case of faster propagation of attack, it must complete its process of data aggregation by fast forwarding all important data. For this purpose, the algorithm computes the data arrival time *dt* and *pr* to obtain cardinality of all the important messages (Line-3). The next part of the algorithm is all about obtaining specific temporal instance *dt* randomly (Line-4) using some predefined constant *flag* (Line-4). Finally, an encryption function *enc* is applied over the data that is sorted by the *dt* in its prior step followed by encryption all the other data.

Algorithm for applying encryption
Input: A_{NS}, f_{size}, T_1, T_2, d_t, ET_1, ET_2, ET_3, ET_4, pr, data
Output:*e*
Start
1. init A_{NS}, fsize, T_1, T_2, dt, pr
2. compute ET_1, ET_2, ET_3, and ET_4
3. $Card_{impmsg} \rightarrow (dt*pr)/100$
4. $dt(dt(r_{idx}(1:Card_{impmsg}))) \rightarrow flag$
5. E→Enc(data) and compute E
End

(ii) Security Benefit of Algorithm: In existing system, the encryption algorithm encrypts almost all the data but doesn't schedule the encryption cycle based on time factor. Therefore, the novelty factor of this algorithms are (i) it offers highly flexible encryption operation where any form of encryption algorithm can be used, (ii) the complete encryption operation is scheduled primarily for important data packet and then for other packets so that it can protect all the sensitive data packet, (iii) it offers data integrity, confidentiality, non-repudiation, and privacy too, (iv) the algorithm is equally valid for any forms of attacks in WSN.

6 Results Discussion

As the proposed system offers solution towards security problems in WSN, where it offers higher degree of flexibility to incorporate any form of security approaches, therefore, it is essential to assess the effectiveness of it. The proposed study chooses the performance parameters of remnant energy of sensor node as well as processing time to assess the security implementation in MATLAB. According to last algorithm discussed in prior section, the proposed system uses temporal keys based security approach where it initializes A_{NS} as 0.2 and f_{size} as 1 s. It computes $T_1 = A_{NS}.\ f_{size}$ and $T_2 = (1 - A_{NS}).\ f_{size}$, ET_1 is considered as 20–30% of T_1, ET_2 is considered as 80–90% of T_1, ET_3 is considered as 80–90% of T_2 and ET_4 is considered as 20–40% of T_2. The proposed system is compared with existing secure and energy efficient routing strategy SecLEACH [31] and LS-LEACH [32]. The analysis is carried out by combination of three different encryption algorithms i.e. RSA [33], AES [34], and SEA [35].

The outcome exhibited in Fig. 2 shows some interesting outcomes which is required to understand thoroughly. An impartial simulation over MATLAB over similar test variable has resulted in Fig. 2 which visually shows that LS-LEACH with SEA and LS-LEACH with RSA offers better residual energy. Similarly, SecLEACH with AES also offers a good residual energy in comparison to proposed system. However, a logical justification is that proposed system offers more better and prac-

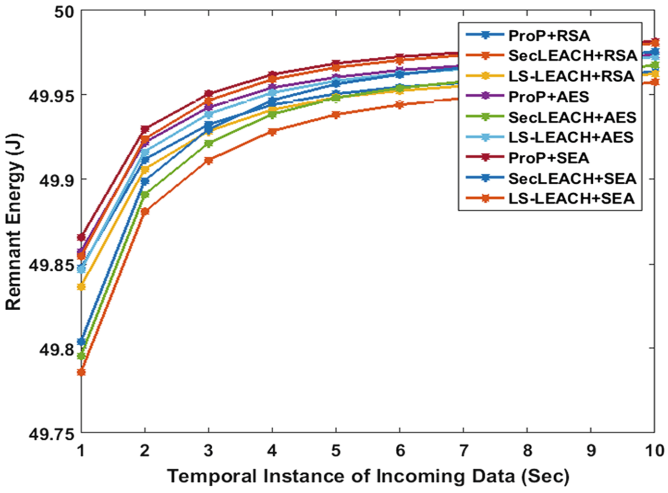


Fig. 2. Comparative analysis of remnant energy

tically efficient energy reduction compared to both the existing system for three reasons: (i) proposed system is completely free from location of complex encryption algorithm inclusion and it can be changed at any point of time, however, there is no alteration possible in SecLEACH or LS-LEACH; therefore, it is good from security viewpoint, (ii) both the existing system don't have any control over number of cluster formation; however, proposed system has potential control over cluster formation

number, and (iii) proposed system offers swapping of active and passive mode to offer better energy control during encryption, and none of such flexibility existing in SecLEACH or LS-LEACH. Hence, from this ground, residual energy of proposed system offers practical outcome in contrast to existing system.

The above numerical outcome in Table 1 showcase that proposed system offers better result when used with SEA algorithm as well as AES algorithm. However, it also offer better outcome when used with RSA. The prime reason behind this is proposed system doesn't use any form of iterations in order to constructs routes. A very progressive routing scheme has been presented that result in progressive finding of short, secure, and energy efficient route using temporal key-based approach unlike existing system.

Table 1. Comparative analysis of time

System	Security	Encryption time(s)	Processing time(s)
SecLEACH	RSA	1.282	5.267
	AES	0.687	2.871
	SEA	0.582	2.548
LS-LEACH	RSA	0.989	4.871
	AES	0.788	4.172
	SEA	0.687	4.082
ProP	RSA	0.765	2.521
	AES	0.449	0.987
	SEA	0.492	0.879

7 Conclusion

The present paper introduced one cost effective security approach to show a better possibility of introducing flexibility in using encryption protocols over secure routing mechanism. The energy calculation has been carried out using standard benchmarked first order radio-energy model and when compared with existing system with various combinations, it shows that proposed system offers higher security from maximum key-based attacks in WSN with faster response time. The future work will be towards strengthening key-distribution mechanism as a continuation of it.

References

1. Xu, G., Shen, W., Wang, X.: Applications of wireless sensor networks in marine environment monitoring: a survey. Sensors **14**(9), 16932–16954 (2014)
2. Kobo, H.I., Abu-Mahfouz, A.M., Hancke, G.P.: A survey on software-defined wireless sensor networks: challenges and design requirements. IEEE Access **5**, 1872–1899 (2017)

3. Ruiz, M., Alvarez, E., Serrano, A., Garcia, E.: The convergence between wireless sensor networks and the internet of things; challenges and perspectives: a survey. IEEE Latin Am. Trans. **14**(10), 4249–4254 (2016)
4. Kumar, A.A., Ovsthus, S.K., Kristensen, L.M.: An industrial perspective on wireless sensor networks—a survey of requirements, protocols, and challenges IEEE Commun. Surv. Tutorials **16**(3), 1391–1412 (2014)
5. AlMheiri, S.M., AlQamzi, H.S.: Data link layer security protocols in wireless sensor networks: a survey. In: 2013 10th IEEE International Conference on Networking, Sensing and Control (ICNSC), Evry, pp. 312–317 (2013)
6. Khedim, F., Labraoui, N., Lehsaini, M.: Dishonest recommendation attacks in wireless sensor networks: a survey. In: 2015 12th International Symposium on Programming and Systems (ISPS), Algiers, pp. 1–10 (2015)
7. Elgenaidi, W., Newe, T., O'Connell, E., Mathur, A., Toal, D., Dooly, G.: Reconfiguration of neighbouring nodes in coastal monitoring wireless sensor networks based on leader node recommendation. In: 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), Barcelona, pp. 0348–0352 (2017)
8. Tomić, I., McCann, J.A.: A survey of potential security issues in existing wireless sensor network protocols. IEEE Internet Things J. **4**(6), 1910–1923 (2017)
9. Grover, J., Sharma, S.: Security issues in wireless sensor network—a review. In: 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 397–404 (2016)
10. Yegireddi, R., Kumar, R.K.: A survey on conventional encryption algorithms of cryptography. In: 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, pp. 1–4 (2016)
11. Aissani, S., Omar, M., Tari, A., Bouakkaz, F.: μKMS: micro key management system for WSNs. IET Wirel. Sens. Syst. **8**(2), 87–97 (2018)
12. Burg, A., Chattopadhyay, A., Lam, K.Y.: Wireless communication and security issues for cyber–physical systems and the internet-of-things. Proc. IEEE **106**(1), 38–60 (2018)
13. Gandino, F., Ferrero, R., Montrucchio, B., Rebaudengo, M.: Fast hierarchical key management scheme with transitory master key for wireless sensor networks. IEEE Internet Things J. **3**(6), 1334–1345 (2016)
14. Gopalakrishnan, B., Bhagyaveni, M.A.: Anti-jamming communication for body area network using chaotic frequency hopping. Healthc. Technol. Lett. **4**(6), 233–237 (2017)
15. Gope, P., Hwang, T.: A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Trans. Ind. Electron. **63** (11), 7124–7132 (2016)
16. Sayad Haghighi, M., Wen, S., Xiang, Y., Quinn, B., Zhou, W.: On the race of worms and patches: modeling the spread of information in wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **11**(12), 2854–2865 (2016)
17. Huang, M., Yu, B., Li, S.: PUF-assisted group key distribution scheme for software-defined wireless sensor networks. IEEE Commun. Lett. **22**(2), 404–407 (2018)
18. Kesavan, V.T., Radhakrishnan, S.: Cluster based secure dynamic keying technique for heterogeneous mobile wireless sensor networks. China Commun. **13**(6) 178–194 (2016)
19. Li, Z., Wang, H., Fang, H.: Group-based cooperation on symmetric key generation for wireless body area networks. IEEE Internet Things J. **4**(6), 1955–1963 (2017)
20. Moara-Nkwe, K., Shi, Q., Lee, G.M., Eiza, M.H.: A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. IEEE Access **6**, 11374–11387 (2018)

21. Oliveira, L.M.L., Rodrigues, J.J.P.C., de Sousa, A.F., Denisov, V.M.: Network admission control solution for 6LoWPAN networks based on symmetric key mechanisms. IEEE Trans. Ind. Inf. **12**(6), 2186–2195 (2016)
22. Shim, K.A.: BASIS: a practical multi-user broadcast authentication scheme in wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **12**(7), 1545–1554 (2017)
23. Shin, S., Kwon, T.: Two-factor authenticated key agreement supporting unlinkability in 5G-integrated wireless sensor networks. IEEE Access **6**, 11229–11241 (2018)
24. Tian, F., et al.: Secrecy rate optimization in wireless multi-hop full duplex networks. IEEE Access **6**, 5695–5704 (2018)
25. Al-Turjman, F., Kirsal Ever, Y., Ever, E., Nguyen, H.X., David, D.B.: Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks. IEEE Access **5**, 24617–24631 (2017)
26. Wu, J., Ota, K., Dong, M., Li, C.: A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. IEEE Access **4**, 416–424 (2016)
27. Yildiz, H.U., Ciftler, B.S., Tavli, B., Bicakci, K., Incebacak, D.: The impact of incomplete secure connectivity on the lifetime of wireless sensor networks. IEEE Syst. J. **12**(1), 1042–1046 (2018)
28. Zhang, J., Tao, X., Wu, H., Zhang, X.: Secure transmission in SWIPT-powered two-way untrusted relay networks. IEEE Access **6**, 10508–10519 (2018)
29. Zhao, J.: Topological properties of secure wireless sensor networks under the q - composite key predistribution scheme with unreliable links. IEEE/ACM Trans. Netw. **25**(3), 1789–1802 (2017)
30. Zheng, G., et al.: Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks. IEEE J. Biomed. Health Inf. **21**(3), 655–663 (2017)
31. Oliveira, L.B., Wong, H.C., Bern, M., Dahab, R., Loureiro, A.A.F.: SecLEACH—a random key distribution solution for securing clustered sensor networks. In: Fifth IEEE International Symposium on Network Computing and Applications (NCA'06), Cambridge, MA, pp. 145–154 (2006)
32. Alshowkan, M., Elleithy, K., Alhassan, H.: LS-LEACH: a new secure and energy efficient routing protocol for wireless sensor networks. In: 2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications, Delft, pp. 215–220 (2013)
33. Burnett, S., Paine, S.: *RSA Security's Official Guide to Cryptography*, McGraw Hill Professional (2001)
34. Daemen, J., Rijmen, V.: *The Design of Rijndael: AES—The Advanced Encryption Standard*. Springer Science & Business Media (2013)
35. Standaert, F.X., Piret, G., Gershenfeld, N., Quisquater, J.J.: SEA: A scalable encryption algorithm for small embedded applications. In: International Conference on Smart Card Research and Advanced Applications. Springer (2006)

A Survey on Next Generation Networks

Veeragandham Sree Vaishnavi(✉), Y. Mohana Roopa, and P. L. Srinivasa Murthy

Computer Science and Engineering, Institute of Aeronautical Engineering, Hyderabad, India
vaishnavipvan@gmail.com, ymohanaroopa@gmail.com, plsrinivasamurthy@gmail.com

Abstract. Now-a-days the networks which are wireless are characterized through a constant range policy assignment. A big part of the allocated range is used occasionally and based on the physical area differences inside usage of allocated ranges degree is fifteen percent-eighty five percent with an excessive differences in time. A confined attainable range and incapability within the ranges utilization lead to a brand-new designed named as Next Generation Network (xG network) and also cognitive radio network.

Keywords: Networks · Wireless · Next generation networks · Range · Cognitive radio network

1 Introduction

Due to the restricted attainable ranges and incapability within the range utilization lead to a brand-new designed named as Next Generation Networks. It can be defined below.

"Next-Generation Network is a network which is a packet-based capable of offering assistance which include the services by telecommunication and use more than one communication technique to communicate parallely. The Quality of Service will allow delivery of technology for which carrier-connected capabilities were impartial by beneath lying carrier-relationed technologies".

Now-a-days the networks which are not wired are managed in a way of constant range mission coverage, that is the range is managed by using the groups which are governmental which are allocated to the holders who are licensed offering more time based on the large physical areas. Additionally, a big part of the constant range which is used occasionally is shown in Fig. 1. The usage of a spectrum is focused more on positive quantities of a range where as a tremendous quantity of the range will be remained as not utilized.

NeXt Generation (xG) communication networks will offer excessive bandwidth to mobile clients through heterogeneous wi-fi design and techniques of accessing the dynamic spectrum. The ineffective use of a prevailing range may get progressed via opportunistical entry for a licensed bands without interference of users who are existing now. The next generation network are imposing number of challenges because of the spectrum which is having a wide range and also numerous applications of requirements of the quality of services. These differentiations ought to be caught and changing

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 162–171, 2020.
https://doi.org/10.1007/978-3-030-37051-0_18

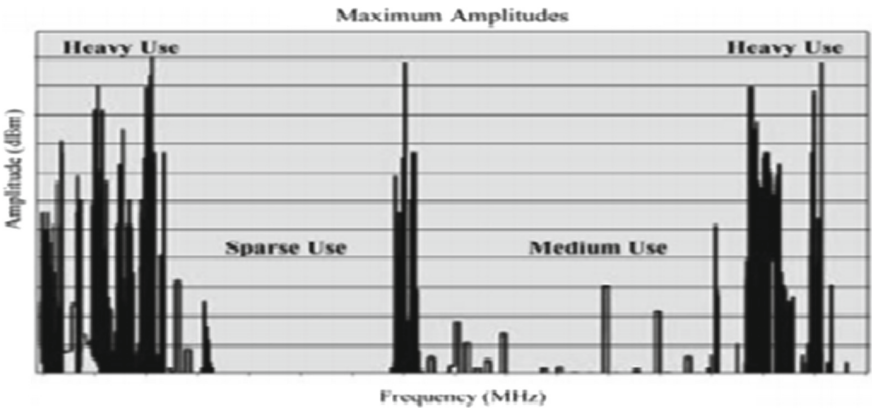


Fig. 1. Spectrum utilization

randomly as the terminals of the mobile will move between the architecture of those which are not wired alongside the spectrum pool which is available [1–3].

2 Next Generation Network Architecture

The existence of the wireless network architecture will lead to differentiation in case of spectrum policy and communication technology. And more a little part of spectrum which are wireless have been licensed for the different reasons but still there are few

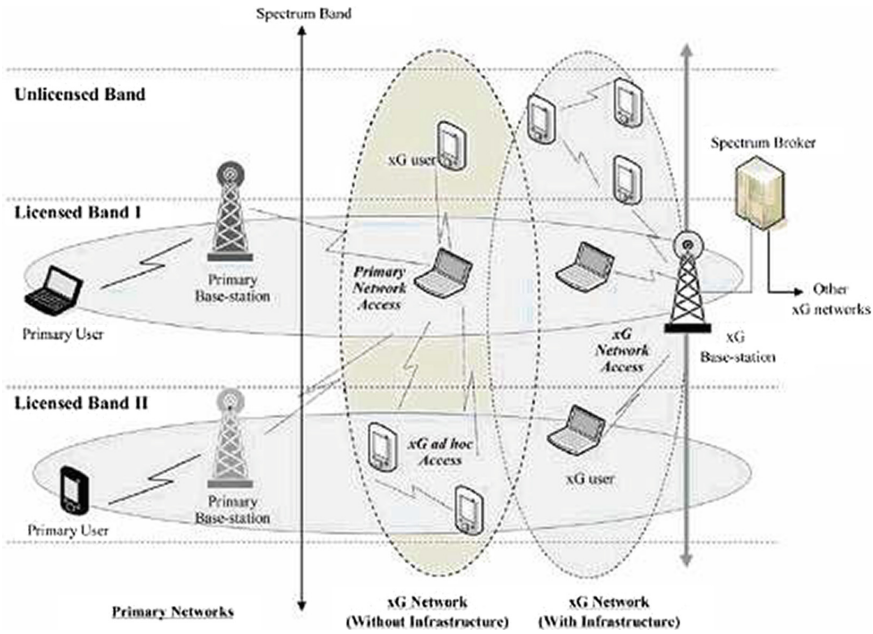


Fig. 2. xG network architecture

bands which are remained as unlicensed. To develop the communication protocol, a transparent explanation of Next Generation Network design is needed. The architecture of Next Generation Networks are divided into two types they are the primary networks and xG networks as shown in the Fig. 2.

- *Primary Networks*:
  The current infrastructure of the network which is existing can be called as a primary networks which is having an access to the band of the section which is certain. Example of the primary network are the networks which are cellular and also the networks which are TV broadcast. A primary network elements are discussed below:

  1. Primary users: Primary users are users who are having a license to drive in a band of a spectrum which is certain. These accesses are controlled by elementary base-stations and so these access will not get effected by any of users who are unlicensed. The elementary users doesn't require modifications for co-existing with the current base stations which are xG and the next generation clients.
  2. Primary Base-Stations: The elementary base-stations is also known as the licensed base-stations which are licensed has constant designed component for network which is having a base-stations which are licensed trans-receiver systems present inside cellular systems. This principles, this primary stations aren't having any next generation capacity to share it with the next generation clients. But it will request for having the estate and the xG protocol for Next Generation users of elementary access of network.

- *xG network*:
  The Next Generation Network (xG network) is also referred to as the cognitive radio, the network which is secondary and also the network which is unlicensed. It is not having a licensed band for functioning in particular band. Here the access of the spectrum is done in a manner which is opportunistic. The xG network will arrange the infrastructure and the ad hoc networks which are shown in the Fig. 2. A xG network elements are shown below:

  1. xG user: It is not having any license. Therefore, the additional functions are necessary for sharing the licensed spectrum band.
  2. xG base stations: It is constant designed component having xG network capabilities. This base station will provide one hop connection to the users of the xG without the access of the spectrum license. By this, the network can be accessed by the user of xG.
  3. Spectrum Brokers: Spectrum Brokers can also be known as scheduling servers. It is a network which are central and that will make a major role in distributing resources of spectrum to different xG networks. This spectrum broker is having a capacity to connect with each other and will serve as a manager for the spectrum information for enabling the existence combinedly with the multiple xG networks.

As referred to the above xG Architecture it is mainly divided into three types: primary networks and xG network. And there again xG networks are based on infrastructure xG network and the other one is networks which are ad-hoc. These were functioned below the heterogeneous environments which consists both the bands which are licensed and the bands which are unlicensed. The xG user can interact one another by the multi-hops manner otherwise by using base-stations. xG network consists of three heterogeneous kinds of access networks which are explained below:

1. xG network access: In this kind the xG user can use the base-stations by basing on both the licensed and the unlicensed.
2. xG hoc access: It is used to communicate with others by using the hoc connection.
3. Primary networks access: In this section the xG users can use the elementary base stations by the band which is licensed [4].

3 xG Network Functions

As we can see the above architecture we can come to know that the xG architecture is operated based on the licensed bands or the unlicensed bands. By this the functionalities of the next generation networks will vary based on the licensed and unlicensed band users. This section, we will discuss about the xG networks in licensed band and unlicensed band.

3.1 xG Networks on Licensed Bands

As seen in the Fig. 1 there get exists still the holes of the spectrum which are unused in the bands of license. Thus, the next generation networks are moved to explore holes of the spectrum through techniques of cognitive communication. This design is shown in Fig. 3 where next generation networks exists along with elementary network in the similar location and also on similar band spectrum. There exists the number of challenges to the next generation network because of these elementary users. But main aim of next generation networks is for providing best spectrum which is available and also licensed bands functions were used for identifying primary users. The holes of spectrum which is having the capacity of channel are dependent on primary users. Hence interference issue of the primary users are very important in the architecture. If the primary users are visible in spectrum bands which are involved by xG user then the xG user should move from the present spectrum and go in search of the new spectrum immediately which is referred to as the spectrums handoff.

3.2 xG Networks on Unlicensed Bands

The policies of open spectrum which had initiated in the industrial scientific and medical (ISM) bands has been very attractive to many of the technologies and also for the innovative uses. Due to this it has been interfered in many of the multiple different

kinds of the networks where the efficiency of the industrial scientific and medical band is getting decreased. But finally the capability of the access to open spectrums and quality services will provide depending upon degree by which radio could be planned for designing for allocating the spectrum efficiently. The next generation network could be designed for operating upon the unlicensed band so it efficiently can be improved in the particular portions of spectrum. Since in this there are no licensed users everyone are having the same accessing right for the spectrum band. Number of next generation networks exist in the same portion and communicate with each other in the same portion of the spectrum. In this unlicensed architecture the next generation networks focuses mainly on the next generation users. Variant to the operations of the licensed band here the spectrums handoff doesn't get altered by elementary users. Whatever it is, here everyone are having the same right for accessing the spectrum and the xG users must compete with one another in the similar licensed band. If number of xG community operator's live within the similar unlicensed bands, the equal sharing of spectrum between them is essential [5].

4 xG Networks Applications

The applications of xG networks are discussed below:

- *Leased Networks*: The primary network will provide an opportunity for accessing its license spectrums with an agreement with the third person that it should provide the good quality services for the elementary user [11]. Considering an example, the elementary network can rent accessing rights of its spectrum for the mobile virtual network operator and also regional community for broadband access.
- *Cognitive's Mesh Networks*: The wireless network are becoming a cost-efficient technology. As it is becoming the cost-efficient it is providing the broadband connectivity [12]. As the density of the network gets increased then the applications will require more higher output and then the mesh networks requires the higher capacity for meeting the requirement of application. The cognitive radios will allow bigger amount of spectrums, the next generation network are used by mesh networks in urban cities. Considering an example, coverage areas of the next generation network can be increased by the meshed wireless backboned network of the infrastructure link which are established by the Cognitive access point (CAP) and also the Cognitive Relay Node (CRN). The capacities of this CAP is connected through the access of broadband to Internet which is shared over the bigger areas with CRN. The next generation networks are having the capability for adding the contemporary or the permanent spectrums for the infra-structure links which are used for activating in case of the highest traffic loads.
- *Emergency Networks*: The another area of the next generation networks are the public safety and the emergency networks [13]. If there is a case of the natural disasters, during that period there may be temporarily disability of the network and also the communication infrastructure may get damages at that times there is a need for establishing these emergency networks. These networks deals with the very important information, good communication must be possible with the minimum

latency. Additionally, these communication requires the sufficient quantity of the radio spectrum for sake of handling the more volume of the traffic like voices, videos and also data. The next generation network will allow to use present spectrums without any need of the framework and it will maintain the interaction priority and also the responding time.

- *Military Networks*: The interesting application of the next generation networks is a military's radio environment [14]. The next generation networks enables the military radio to select the arbitrary, modulation and the coding schemes and the Intermediate frequency bandwidth (IF). And also the military networks are having the need of the next generation networks for the protection and the security during the tough situations. These next generation networks allows the military personnel for performing the handoff's for locating the protective band spectrum.

5 Challenges of Next Generation Networks

- *Challenges of Routing*

Routing is playing an important role but it is an unexplored problem in the Next Generation Network. Specially in the xG network with number of hop interaction necessities, the precise characteristic of the open spectrums phenomenon necessitate novel's routing algorithm to be developed. Research on the Next Generation Network is elementarly on the spectrums sensing technique and the spectrums sharing solution. We emphasize the need for the purpose routing algorithm in open spectrums environment constitutes a major matter in Next Generation Networks.

A principal layout choices for routings in xG network is the combination in between the routing and also the spectrum control. The random spectrum that's not continuous in conditions of both the time and area necessitate a technique. Simulation based comparisons are carried out for cross-layered and decouple techniques for routings and spectrum managements. The consequences in both works results that a cross-layered solutions that construct route and determine the working spectrums at the every time for every hops that outperform a method in sequence where routes are choosen without depending on the spectrum allocations.

The internal dependency between the routes selection and the spectrum's management is inquired. Firstly, the routes selection and the spectrum's management method were proposed. In the strategy, the routes selection is done without depending on the spectrum's management by using the shortest path algorithm. In this strategy the routing layer will discover path to the selected routes. As usual the spectrum management is performed on each hop. The source-based routing strategy is operated by using a global outlook of network to display the upper bound in attainable performance. The simulations in each reveal that cross-layer approach is high quality for routing in xG networks since the availability of spectrum precisely impacts the end-to-end act. These two results for routing in xG networks transparently display that cross-layer approaches together consult the route and spectrum which are necessary for the Next Generation Networks.

Another precise project for routing in xG networks is the reformed equipment for analytical assessment of routing protocols. Traditionally, routing protocols for ad hoc networks are analysed by the usage of graph models [6].

- *Challenges of transport layer*

Transport protocols constitute an unexplored field for xG networks when you consider that there exist no work on this location yet. Many solutions have been suggested to make better the performance of the TCP and UDP in the conventional wireless networks in recent years. These studies concentrate on the mechanism to restrict the performances degradation of the TCP and UDP that rise up due to the wireless link errors and the access delays. However the Next Generation Networks are imposing the unique challenges on the transport layer as described below:

The performances of the TCP depends upon the packet loss probability and the round trip time (RTT). Wireless link errors and the packet loss probability is not only depending on the access technology, but also it depends upon the frequency which is in use, the interference level and the bandwidth which is available. Therefore the wireless TCP and UDP constructed for the existing wireless access technologies can't be used in the dynamic spectrum assignment based Next Generation Networks [7].

- *Challenges of the QOE in the Next Generation Networks*

In the Next Generation Networks the voice, multimedia and data services will be assembled into solely networked platform. This will increase the complexity of the underlying services of the wireless network and also the optical networks. Though they all are combined into a single platform they must be cost efficient and also the resources efficient so that the users may get satisfied. Hence, now the service providers are shifting their concentrations from the network Quality of Services (QOS) to the form of user Quality of Experience (QOE) which will describe the act of the network from the perspective of the user. Sometimes the high quality of services can result in the Quality of experience but it cannot reach up to the highest mark of the Quality of Experience. Optimizing the Quality of the Experience includes the factors such as application levelled Quality of the Services, the surroundings which are nearer to the customer networks, based on the factors of the users and the ability of the final equipment.

The end to end Quality of the experience will depends upon the outcome effects of the entire system including the network systems, terminals, the surroundings which are nearer to the customer surroundings and the users. To ensure the Quality of the Experience of all the vertical network layer operations are needed to performed basing on the user's real time of the Quality of Experiences. To achieve all this goals there is a need to address many of the challenges like Quality of Experience measurement, management, diagnosing and also the monitoring.

Hence, here we propose the two important components of the end-to end quality of experience. Those are the Quality of Experience or the Quality of the Services reporting act which is installed at the TE. And the other one is the managing component of the Quality of Experience which are installed at the sources and the networks. The Quality of the experiences and the Quality of the Services reporting components will measure the QOE/QOS performances received by the users and report them back to the sources and the networks. The components of the management of the Quality of Experience

will receive the report and make the necessary modifications to the transport functions and rearranging the parameters of the application-layer to maximize the user Quality of Experience. As the networks are maximizing the network independently and locally of their users, the end-to-end Quality of Experiences can be implemented in the Next Generation Network that is composite in the nature. And the end-to-end Next Generation Network still is having many challenging issues, and it will receive great attention from both the industry and the academia which will give that means which will generate a revenue and also the growth of a competitive service vendors.

- *Challenges of the Next Generation Mobile Networks*

In today's environment the users of the mobile network are looking forward for the speed connectivity of the 5G network and where the service vendors are going through challenges in complying with connectivity needs without huge capital investments. Hence, a new technique came into the existence which is known as Network Function Virtualization (NFV) which can solve the problem of the service vendors and also which will change the infrastructure of the tele-communication to make it more cost-efficient.

The Network Function Virtualization aim is to change the tele-communicational industry by separating the network functionalities from the underlying notified hardware. The NFV is providing all the benefits for the tele-communication industry hence all the network based engineers and the researchers are using this technique to have a smooth way in the industry of tele-communication. Though it is providing a good challenges in the tele-communication industry it is facing many technical challenges hence the tele-communication services providers, the academic researchers, IT organizations are finding a new approaches to overcome this problem. The Network Function Virtualization is also used to make less the transactions which are occurred on the physical networks [8].

- *Challenges of the Network Management for the Next Generation Networks*

The current management of the network have been divided into the two types they are ITU-T's recommendations for Telecommunication Management Network (TMN) and IETF's straightforward Network Management Protocol (SNMP) that favors the Internet Protocol networks. Public Switched Telephone Network, Public Switched Data Network, Public Land Mobile Network and the Wireless Local Area Networks etc. these are the functions which are targeted more on the networks which are not dependent. All these approaches will be included into a single Internet Protocol based infrastructure which are going to be considered as the Next Generation Networks in the coming days. But the complexity of the Next Generation Network will bring a great challenges to the management of the network.

As the Next Generation Networks are deriving from the tele-communication networks and the Internet Protocol based infrastructure, the management architecture and the control are completely different from each other and will be acting separately between the Quality of Service enabled transport or the enabled network domain and the object-oriented application with assigning environment process. Due to the stress arising from the development of the rapid technology and the competition along with the fresh perception of the Next Generation Networks will generate a important

challenges in the fields of the administration, operation and managing the maintenance of the services and the networks.

- *Challenges of the Mobile Ad Hoc Networks*

In the coming 10 years, there comes a lot of changes in the Internet which will be operated by the rapid increase of mobile devices or wired personal computers or the existing systems. The wireless appliances on the Internet includes the Laptops, mobile phones, computers, media players etc. and also there are embedded sensors which are used to sense and control the objects. As now the usage of the computing devices and the wireless networks are playing a very important role. The internet will act as an interface between the people and their surroundings. Controlling the objectives and events of the Internet will again leads to the new methods which are integrated with the lifestyle of people and their surroundings. The potential impact of the long run wireless web is incredibly vital as a result of the network combines the ability of computation, search engines and databases within the background with the immediacy of information from mobile users and sensors within the foreground. The flow of data and the interaction between the mobile users, the supporting computer's infrastructure are completely different as compared to that of the today's applications of the Internet such as email, messages, worldwide web etc. For supporting all these requirements in a global networking there is a need of bringing the major changes [9].

- *Challenges of the Next-Generation wireless sensor networks*

The wireless sensor networks have gained a worldwide attention in the recent years particularly in the area of development of the smart sensor. The wireless sensor networks are having a potential to the replacement of the wired networks. These wireless sensor networks can provide the risk analysing data. Mainly it can help the farmers to analyse the risk before only like frost damages occurring on the crop, changes in the climate and making the farmer to get awareness about these changes and making his crop safe by analysing what damages can occur to his crops if there is a drastic change in the climate. Not only in the field of agriculture but also the wireless sensor networks are also used in the medical field as well as for building the secured buildings with low cost in the developed countries [10].

6 Conclusion

The next generation networks are evolved for solving the contemporary wireless network problem issues on account of the confined available spectrum and inefficiency in the usage of spectrum by exploring the prevailing wireless spectrum opportunistically. Next Generation Networks (xG) are also known as the Cognitive Radio Network as well as the Dynamic Spectrum Access. The next generation networks are supplied with the intrinsic capacities of the cognitive radio which provides a final spectrum-awareness communication model in the wireless communication. In this survey, the next generation architecture, applications and challenges are discussed.

References

1. Akyildiz, I.F., Lee, W.Y., Vuran, M.C., Mohanty, S.: NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey. Comput. Netw. **50**, 2127–2159 (2006). Elsevier
2. Zhao, J., Zheng, H., Yang, G.H.: Distributed coordination in dynamic spectrum allocation networks. IEEE (2005). 1-4244-0013-9/05
3. Weiss, T.A., Jondral, F.K.: Spectrum pooling: an innovative strategy for the enhancement of spectrum efficiency. IEEE Radio Commun. Mag. **42**(March), 8–14 (2004)
4. Darpa, X.: The XG architectural framework V1.0 (2003)
5. Cao, L., Zheng, H.: Distributed spectrum allocation via local bargaining. In: Proceedings of IEEE Sensor and Ad Hoc Communications and Networks (SECON) 2005, pp. 475–486, September 2005
6. Xin, C.: A novel layered graph model for topology formation and routing in dynamic spectrum access networks. In: Proceedings of IEEE DySPAN 2005, pp. 308–317, November 2005
7. Akan, O.B., Akyildiz, I.F.: ATL: an adaptive transport layer for next generation wireless internet. IEEE J. Sel. Areas Commun. (JSAC) **22**(5), 802–817 (2004)
8. Chowdhury, N.M.K., Boutaba, R.: Network virtualization: state of the art and research challenges. IEEE Commun. Mag. (2009). University of Waterloo
9. Yang, H., Luo, H., Ye, F., Lu, S.W. and Zhang, L.: Security in mobile ad hoc networks: challenges and solutions. IEEE Wirel. Commun. (2004)
10. Gungor, V.C., Lu, B., Hancke, G.P.: Opportunities and challenges of wireless sensor networks in smart grid. IEEE Trans. Indus. Electron. **57**(10) (2010)
11. Stine, J.A.: Spectrum management: the killer application of ad hoc and mesh networking. In: Proceedings of IEEE DySPAN 2005, pp. 184–193, November 2005
12. Akyildiz, I.F., Wang, X., Wang, W.: Wireless mesh networks: a survey. Comput. Netw. J. **47**(4), 445–487 (2005)
13. Maldonado, D., Lie, B., Hugine, A., Rondeau, T.W., Bostian, C.W.: Cognitive radio applications to dynamic spectrum allocation. In: Proceedings of IEEE DySPAN 2005, pp. 597–600, November 2005
14. Murty, R.: Software-defined reconfigurability radios: smart, agile, cognitive, and interoperable. Technology@ Intel Mag. **84** (2003)

The New Approach for Creating the Knowledge Base Using WikiPedia

Prasad E. Ganesh[1(✉)], H. R. Manjunath[1], V. Deepashree[1], M. G. Kavana[1], and Raviraja[2]

[1] Alva's Institute of Engineering and Technology, Moodbidre, Mijar, Karnataka, India
gprasadl78l43@gmail.com, manjunathdvg@gmail.com
[2] Swiss Re, Bengaluru, India

Abstract. Wikipedia is recognized as one of the largest repositories in the Web. The term knowledge base was in connection with the expert systems as it is the part of Artificial Intelligence. A knowledge base can be created for any entity. The existing system like YAGO, MediaWiki tries to convert Wikipedia into a structured database to provide a vast knowledge base across the domains. It is very difficult to get the information which we want across the domains. So, the solution would be to get a systematic automated approach to build a knowledge base using Wikipedia on entity which we are interested in. The proposed system provides a knowledge base built upon the location as its entity. The system is feeded with seed data, by using these seed data it traverse through the Wikipedia graph and builds knowledge base using similarity measurement between seed data and traversed upcoming pages of wiki graph. Any expert AI systems uses gold standard knowledge base to take any decisions.

Keywords: Natural language processing · Knowledge base · Entity linking

1 Introduction

As digital libraries are regularly increasing in volume, makes it more easy access to the content or information. But it makes it more difficult for a researcher to get a particular information. In that Wikipedia is a large-scale source of network, having all information through the collaboration of contributors. Wikipedia contains information in hierarchical level as articles, link between articles, categories of same kind of articles, multiple language linking etc.

Most records we tend to get from the web in everyday existence is within the style of texts. These texts contain an outsized range of named entities (e.g. person, organization, and place) that are the essential components of texts. However, these entities are extremely ambiguous, thus we want to link them to associate degree existing content in order that folks will apprehend what the entities ask and perceive the texts a lot of properly.

A Knowledge base (KB) could be a special reasonably information for sophisticated structured and unstructured information utilized by automatic processing system. In general, a Knowledge base isn't a static assortment of data, but a dynamic resource.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 172–178, 2020.
https://doi.org/10.1007/978-3-030-37051-0_19

The cognitive content construction must extract data like entities and relationships between entities from net texts and add them to the cognitive content. Before filling, the foremost necessary step is to clear up those entities extracted by the system. We have a tendency to decision this method as named entity linking or entity linking. Entity linking could be a task of linking named entities in net texts to their corresponding entities in an exceedingly cognitive content (e.g., DBpedia, and YAGO). The proposed system aims at creating a knowledge base which solves ambiguity of recognizing a place if the place is searched using its alias name and helps in retrieving all possible information about that location.

2 Literature Survey

Beevi and Deivasigamani [1] presented a novel way to deal with the making of information base by extracting knowledge from unstructured web documents. Pre-processing techniques, similarity and redundancy techniques were performed on the extracted documents. The extricated information is sorted out and changed over to XML archives which was then stored in the information base. Though the system is effectively conveyed in genuine condition, refinement is possible in knowledge extraction and representation processes.

Maree et al. [2] Proposed a framework for programmed information base development from heterogeneous information sources including space explicit ontologies, universally useful ontologies, plain messages, picture and video inscriptions which are naturally extricated from site pages. In the proposed framework a few data extraction procedures were integrated to naturally make, enhance and stay up with the latest. Despite the fact that the made information base is utilized to discover arrangements between heterogeneous ontologies in the ecological and agrarian spaces, further expansion al ontologies from online metaphysics vaults on the web can be misused to en-rich and grow the inclusion of the learning base.

Nastase and Strube [3] proposed an approach to derive a large scale and multilingual by misusing a few features of Wikipedia. They described how to expand upon the Wikipedia's current system of classifications and articles to automatically find new relations and their occurrences.

Ma and Zhang [4] proposed the novel approach called economical manifold ranking (EMR) to interchange the normal similarity activity techniques that are unable to replicate the $64000 similarity between completely different modalities of knowledge. Though EMR technique will exploit structure of knowledge to ranking and is additional stable and correct than the normal ways that however as a result of the dimension of the information are going to be lost when the various modalities of knowledge are projected to the common feature area, the performance

Of the rule will be reduced. Thus, the EMR rule is combined with the DNN ways to attain the higher performance for cross-media retrieval.

Saad and Kamarudin [5] concentrated on ascertaining semantic likenesses among sentences and playing out a near examination among recognized comparability estimation systems. They used a large lexical database of English known as WordNet to figure the word-to-word se-mantic likeness. The consequence of the exploration

inferred that the Jaccard and Dice performs better in estimating semantic closeness between sentences.

Trisedya and Inastra [6] explored a few sentence alignment methods which are been used before for another domain and also to check whether the Wikipedia can be used as one of the resources for collecting parallel corpora of some languages. They had used two approaches of sentence alignment by treating Wikipedia as both parallel corpora and comparable corpora which gave positive results. Though the system gave positive results for two particular ethnic languages, it could not give an expected result when tested for other ethnic languages.

Effendi et al. [7] constructed an interpretation corpus dependent on different rudimentary tasks (insertion, deletion, substitution and reordering operations in a publicly supporting stage to produce multi-rework sentences from a source sentence. These rudimentary reword tasks can be used for various applications. Though the system gave good performance for several applications further it can be improved for the utilization by other applications including summarization and machine translation.

Gupta et al. [8] proposed a method for analyzing interlanguage interfaces alongside divert page titles and link text titles and it additionally sifted through off base interpretation applicants utilizing design coordinating. They proposed the utilization of page parameters to give a relativity between the sought string and the interpretation hopefuls. The technique was helpful for particular do-principle explicit terms since exactness and inclusion were superior to anything the bilingual.

Content corpus approach. The framework can be additionally created by including the India dialects which are absent in the online lexicons and by breaking down and discovering some more parameters for better execution.

Whang et al. [9] proposed definite investigation of semantic corpus construction advancements, and proposes another website page deduplication calculation dependent on TF-IDF and word vector separate. The method has established the semantic corpus of common language under cloud administration stage. Though the system proposed an calculation to sift through the non-repetitive corpus put away in HBase and can powerfully store learning in discourse acknowledgment, further it can be improved by optimizing the web joins evacuation calculation and web content duplication expulsion calculation.

Nothman et al. [10] have exhibited a strategy for consequently creating named substance explained message in various dialects from Wikipedia, in light of marking each cordial connection with the element sort of the objective article. The approach was highly effective and efficient for creating NER models in resource-scarce langauges. By using domain-oriented article classification and sentence selection, the method has been utilized for fast development of substance explained corpora specifically spaces however has saddled labeling just the four CoNLL NER types disregards Wikipedia's di-section inclusion of specialized and prevalent areas. Wu et al. [11] introduced the troubles and uses of element linking and fixated on the most approaches to manage those issues. They conjointly listed data bases, datasets and also the analysis criterion and a few challenges on the entity linking. As per their analysis content is employed in substance connecting frameworks are disconnected data or extracted from the net database anyway ailing in programmed update system. To upgrade the exactness of substance connecting, a few frameworks misuse some propelled models to manage this

drawback, as genuine AI models anyway that has higher time quality. In this manner, the framework is frequently improved by executing the approaches to adjust exactness and registering quality.

3 Methodology

The proposed system takes locations name or its alias name as an input and retrieve the Wiki-Pages of the location. Then all the categories under that location is retrieved. Later similarity measurement algorithm is applied to the current page and seed page, if the similarity is greater than 85% then that page is added to the database. Finally the API is created which can be used for the location based applications (Fig 1).

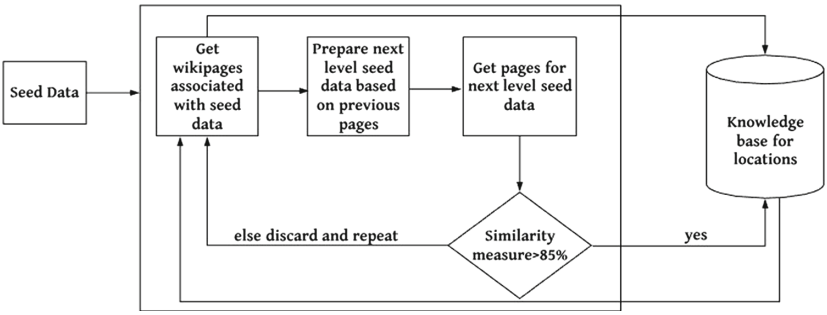


Fig. 1. Block diagram for proposed system

The proposed system process as follows:

- Initially, the seed data is prepared manually by storing the location name, its corresponding Wikipedia URL and seed categories in the database. If the wikipages and categories under the pages are describing about a place or a location, then it is considered as a seed data candidate.
- When user runs the system, creates knowledge base for seed data by fetching the Wiki-page basic details using query API, extract alias names using query API and extract the files and multilingual data using the additional mediawiki queryAPI. The location is covered according to geo coordinates (i.e., latitudes and longitudes).
- Whatever the seed data that have been taken in L1, pages of categories are displayed through API. For L2 data considering sub categories of L1 data comparing with similarity measurements with result more than 85% will be considered as L2 seed data.
- The final product will be the knowledge base for the location.

4 Results and Discussion

4.1 Experimental Setup

- The proposed system uses mongo dB which is an open-source document database and leading NoSQL database. Mongo DB is used to store mainly two collections: Seed categories and Wiki_pages.
- Python 3.7 is the platform to run the proposed system.
- Microsoft Excel Sheets are used to store the seed categories which are collected manually (Fig. 2).

Title	Url	Seed_categories
Karnataka	https://en.wikipedia.org/wiki/Karnataka	South India
Bagalkot	https://en.wikipedia.org/wiki/Bagalkot	Cities and towns in Bagalkot district,Cities in Karnataka
Bengaluru Urban	https://en.wikipedia.org/wiki/Bangalore_Urban_district	Districts of India
Belagavi	https://en.wikipedia.org/wiki/Belgaum	Forts in Karnataka,Tourism in Karnataka,Former capital cities in India,Smart cities in India,Cities and towns in Belgaum district
Bellari	https://en.wikipedia.org/wiki/Bellary	Municipal corporations in Karnataka
Vijayapur	https://en.wikipedia.org/wiki/Bijapur	Tourism in Karnataka
Chamarajanagar	https://en.wikipedia.org/wiki/Chamarajanagar	Cities and towns in Chamarajanagar district
Chikballapur	https://en.wikipedia.org/wiki/Chikkaballapur	Cities and towns in Chikkaballapur district
Chitradurga	https://en.wikipedia.org/wiki/Chitradurga	Cities and towns in Chitradurga district
Dakshina Kannada	https://en.wikipedia.org/wiki/Dakshina_Kannada	Tulu Nadu
Davanagere	https://en.wikipedia.org/wiki/Davanagere	Cities and towns in Davanagere district
Dharwad	https://en.wikipedia.org/wiki/Dharwad	Cities and towns in Dharwad district
Haveri	https://en.wikipedia.org/wiki/Haveri	Western Chalukya Empire,Cities and towns in Haveri district
Kodagu	https://en.wikipedia.org/wiki/Kodagu_district	Proposed states and territories of India
Kolar	https://en.wikipedia.org/wiki/Kolar	Cities and towns in Kolar district
Koppal	https://en.wikipedia.org/wiki/Koppal	Cities and towns in Koppal district
Mandya	https://en.wikipedia.org/wiki/Mandya	Cities and towns in Mandya district
Raichur	https://en.wikipedia.org/wiki/Raichur	Cities and towns in Raichur district
Ramanagara	https://en.wikipedia.org/wiki/Ramanagara	Climbing areas of India
Shivamogga	https://en.wikipedia.org/wiki/Shimoga	Cities and towns in Shimoga district
Tumakuru	https://en.wikipedia.org/wiki/Tumkur	Cities and towns in Tumkur district
Udupi	https://en.wikipedia.org/wiki/Udupi	Cities and towns in Udupi district,Populated coastal places in India,Port cities in India
Yadgiri	https://en.wikipedia.org/wiki/Yadagiri	Cities and towns in Yadgir district
Guntur	https://en.wikipedia.org/wiki/Guntur	Mandal headquarters in Guntur district
Kadapa	https://en.wikipedia.org/wiki/Kadapa	District headquarters of Andhra Pradesh
Krishna	https://en.wikipedia.org/wiki/Krishna_district	Districts of Andhra Pradesh
Kurnool	https://en.wikipedia.org/wiki/Kurnool	Cities in Andhra Pradesh

Fig. 2. Excel sheet for seed data

4.2 Results

The proposed system is efficient than the existing system which fails to identify whether the searched entity is place or a person. The proposed system redirects into the correct page when the place is searched by its alias names. This system has a common API which replaces the different APIs needed for different format of data (text, image, video and so on) and it resolves the language problem by supporting multi languages. Figure 3 represents the incremental knowledge base constructed by the system showing all the seed categories of various locations.

Figure 4 represents database stored in mongo dB which is extracted from the seed categories and provides the information of the location to the user when they search for the location by its alias name.

```
Saved seed_categorie :Forts in Karnataka pagetitle :  Mirjan Fort
Saved seed_categorie :Forts in Karnataka pagetitle :  Mudgal
Saved seed_categorie :Forts in Karnataka pagetitle :  Mundargi
Saved seed_categorie :Forts in Karnataka pagetitle :  Nadivi
Saved seed_categorie :Forts in Karnataka pagetitle :  Nandi Hills, India
Saved seed_categorie :Forts in Karnataka pagetitle :  Pavagada
Saved seed_categorie :Forts in Karnataka pagetitle :  Raichur fort
Saved seed_categorie :Forts in Karnataka pagetitle :  Sadashivgad
Saved seed_categorie :Forts in Karnataka pagetitle :  Savandurga
Saved seed_categorie :Forts in Karnataka pagetitle :  Sira, Karnataka
Saved seed_categorie :Forts in Karnataka pagetitle :  Srirangapatna fort
Saved seed_categorie :Forts in Karnataka pagetitle :  Tekkalakote
Saved seed_categorie :Forts in Karnataka pagetitle :  Uchangidurga
Saved seed_categorie :Forts in Karnataka pagetitle :  Vanadurga Fort
Saved seed_categorie :Forts in Karnataka pagetitle :  Yadagiri
Saved seed_categorie :Tourism in Karnataka pagetitle :  Agumbe
Saved seed_categorie :Tourism in Karnataka pagetitle :  Aihole
Saved seed_categorie :Tourism in Karnataka pagetitle :  Badami
Saved seed_categorie :Tourism in Karnataka pagetitle :  Bagalkot district
Saved seed_categorie :Tourism in Karnataka pagetitle :  Belgaum
Saved seed_categorie :Tourism in Karnataka pagetitle :  Belur, Karnataka
Saved seed_categorie :Tourism in Karnataka pagetitle :  Bijapur
Saved seed_categorie :Tourism in Karnataka pagetitle :  Bidar
Saved seed_categorie :Tourism in Karnataka pagetitle :  Dandeli
Saved seed_categorie :Tourism in Karnataka pagetitle :  The Emerald Route
Saved seed_categorie :Tourism in Karnataka pagetitle :  Golden Chariot
Saved seed_categorie :Tourism in Karnataka pagetitle :  Gommatagiri
Saved seed_categorie :Tourism in Karnataka pagetitle :  Gopinatham
Saved seed_categorie :Tourism in Karnataka pagetitle :  Jamboti
Saved seed_categorie :Tourism in Karnataka pagetitle :  Kanakachalapathi Temple, Kanakagiri
Saved seed_categorie :Tourism in Karnataka pagetitle :  Kanakagiri
Saved seed_categorie :Tourism in Karnataka pagetitle :  Kanakagiri Jain Shri kshetra
Saved seed_categorie :Tourism in Karnataka pagetitle :  Karnataka State Tourism Development Corporation
Saved seed_categorie :Tourism in Karnataka pagetitle :  Kodagu district
Saved seed_categorie :Tourism in Karnataka pagetitle :  Kokrebellur
Saved seed_categorie :Tourism in Karnataka pagetitle :  Lakkundi
Saved seed_categorie :Tourism in Karnataka pagetitle :  Lal Bagh
Saved seed_categorie :Tourism in Karnataka pagetitle :  Madikeri
Saved seed_categorie :Tourism in Karnataka pagetitle :  Mandagadde Bird Sanctuary
Saved seed_categorie :Tourism in Karnataka pagetitle :  Pattadakal (town)
Saved seed_categorie :Tourism in Karnataka pagetitle :  Sakleshpur
Saved seed_categorie :Tourism in Karnataka pagetitle :  Saundatti
Saved seed_categorie :Tourism in Karnataka pagetitle :  Shivaganga
Saved seed_categorie :Tourism in Karnataka pagetitle :  Shravanabelagola
Saved seed_categorie :Tourism in Karnataka pagetitle :  Sirsi, Karnataka
Saved seed_categorie :Tourism in Karnataka pagetitle :  Somanathapura (town)
Saved seed_categorie :Tourism in Karnataka pagetitle :  Somwarpet
```

Fig. 3. Incremental knowledge base

	_id ObjectId	title String	url String	summary String	content String	categories Array
1	5c9a4d685f38a62f84884077	"South India"	"https://en.wikipedia.org/wiki/	"South India is the area includ	"South India is the area includ	[] 25 elements
2	5c9a4d6c5f38a62f84884078	"Andhra Pradesh"	"https://en.wikipedia.org/wiki/	"Andhra Pradesh () (pronunciati	"Andhra Pradesh () (pronunciati	[] 27 elements
3	5c9a4d6f5f38a62f84884079	"Karnataka"	"https://en.wikipedia.org/wiki/	"Karnataka (Karnāṭaka) is a sta	"Karnataka (Karnāṭaka) is a sta	[] 23 elements
4	5c9a4d715f38a62f8488407a	"Kerala"	"https://en.wikipedia.org/wiki/	"Kerala () is a state on the so	"Kerala () is a state on the so	[] 28 elements
5	5c9a4d745f38a62f8488407b	"Lakshadweep"	"https://en.wikipedia.org/wiki/	"Lakshadweep (; ISO: Lakṣadvīp	"Lakshadweep (; ISO: Lakṣadvīp	[] 23 elements
6	5c9a4d775f38a62f8488407c	"Puducherry"	"https://en.wikipedia.org/wiki/	"Puducherry (, literally New To	"Puducherry (, literally New To	[] 21 elements
7	5c9a4d7a5f38a62f8488407d	"Bharatanatyam"	"https://en.wikipedia.org/wiki/	"Bharatanatyam (Tamil: பரதநாட்ய	"Bharatanatyam (Tamil: பரதநாட்ய	[] 14 elements
8	5c9a4d7c5f38a62f8488407e	"Carnatic music"	"https://en.wikipedia.org/wiki/	"Carnatic music, Karnāṭaka saṃg	"Carnatic music, Karnāṭaka saṃg	[] 14 elements
9	5c9a4d7f5f38a62f8488407f	"Cinema of South India"	"https://en.wikipedia.org/wiki/	"The Cinema of South India is u	"The Cinema of South India is u	[] 6 elements
10	5c9a4d825f38a62f84884080	"Coastline of Andhra Pradesh"	"https://en.wikipedia.org/wiki/	"The Coastline of Andhra Prades	"The Coastline of Andhra Prades	[] 6 elements
11	5c9a4d845f38a62f84884081	"Coastline of Tamil Nadu"	"https://en.wikipedia.org/wiki/	"The Coastline of Tamil Nadu is	"The Coastline of Tamil Nadu is	[] 7 elements
12	5c9a4d875f38a62f84884082	"Coromandel Coast"	"https://en.wikipedia.org/wiki/	"The Coromandel Coast is the so	"The Coromandel Coast is the so	[] 28 elements
13	5c9a4d8a5f38a62f84884083	"South Indian cuisine"	"https://en.wikipedia.org/wiki/	"South Indian cuisine includes	"South Indian cuisine includes	[] 11 elements
14	5c9a4d8c5f38a62f84884084	"Dravidian architecture"	"https://en.wikipedia.org/wiki/	"Dravidian architecture is an a	"Dravidian architecture is an a	[] 10 elements
15	5c9a4d8f5f38a62f84884085	"Earliest color films in South	"https://en.wikipedia.org/wiki/	"The South Indian film industry	"The South Indian film industry	[] 6 elements
16	5c9a4d925f38a62f84884086	"Economy of South India"	"https://en.wikipedia.org/wiki/	"Economy of South India after i	"Economy of South India after i	[] 5 elements
17	5c9a4d955f38a62f84884087	"Geography of South India"	"https://en.wikipedia.org/wiki/	"The Geography of South India c	"The Geography of South India c	[] 5 elements

Fig. 4. Mongo dB database

5 Conclusion and Future Work

Any AI system which is location-based application can use the proposed system's API to access the information of that location along with its categories. The proposed system works only for the Indian places. The ambiguity of redirecting to the exact page is resolved when the location is searched by its alias names.

In future, the system can be developed for locations all over the world and Knowledge graph can be constructed by using this knowledge base. Currently the system is using similarity measurement algorithm which can be replaced with other

Machine Learning process to get more accuracy. Further the knowledge base can be created for multi entity which closely related or for multilingual so that this knowledge base can be used for translation also.

References

1. Beevi, J. H., Deivasigamani, N.: A new approach to the design of knowledge base using XCLS clustering. In: Proceedings of IEEE International Conference on Pattern Recognition, Informatics and Medical Engineering, pp. 14–19 (2012)
2. Maree, M., Alhashmi, S.M., Belkhatir, M., Hawit, A.: Automatic construction of a domain-independent knowledge base from heterogeneous data sources. In: Proceedings of IEEE International Conference on Fuzzy Systems and Knowledge Discovery, pp. 1483–1488 (2012)
3. Nastase, V., Strube, M.: Transforming wikipedia into a large scale multilingual concept network, pp. 62–85. Elsevier (2012)
4. Ma, S.Q., Zhang, H.: Efficient manifold ranking for cross-media retrieval. In: 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), pp. 335340 (2018)
5. Saad, S.M., Kamarudin, S.S.: Comparative analysis of similarity measures for sentence level semantic measurements of text. In: Proceedings of IEEE International Conference on Control System, Computing and Engineering, pp. 90–94 (2013)
6. Trisedya, B.D., Inastra, D.: Creating Indonesian-javanese parallel corpora using wikipedia articles. In: Proceedings of IEEE, pp. 239–245 (2014)
7. Effendi, J., Sakti, S., Nakamura, S.: Creation of a multi paraphrase corpus based on various elementary operations. In Proceedings of IEEE Conference of the Oriental Chapter of International Committee for Coordination and Standardization of Speech Databases and Assessment Technique (O-COCOSDA), pp. 177–182 (2017)
8. Gupta, A., Goyal, A., Bindal, A., Gupta, A.: Meliorated approach for extracting bilingual terminology from wikipedia, world academy of science, engineering and technology. In: Proceedings of 11th IEEE International Conference on Computer and Information Technology, pp. 78–85 (2008)
9. Wang, S.Z., Zhang, Q.C., Zhang, L.: Natural language semantic corpus construction based on cloud service platform. In: Proceedings of IEEE International Conference on Machine Learning and Cybernetics, pp. 670–674 (2017)
10. Nothman, J., Ringland, N., Radford, W., Murphy, T., Curran, J.R.: Learning multilingual named entity recognition from Wikipedia, Elsevier, pp. 151175 (2012)
11. Wu, G., He, Y., Hu, X.: Entity linking: an issue to extract corresponding entity with knowledge base. In: Proceedings of IEEE, vol. 6, pp. 6220–6231 (2018)
12. Tehseen, M., Javed, H., Shah, I.H., Ahmed, S.: A light- weight key negotiation and authentication scheme for large scale WSNs. In: Recent Trends and Advances in Wireless and IoT-enabled Networks, pp. 225–235. Springer (2019)
13. Sun, S., Au, K.S., Li, Y., Barber, P.: Systems and Methods for Authentication. US Patent Application 16/159,235, filed 14 Feb (2019)

Ethereum Based IoT Architecture

Sandeep B. Kadam[1(✉)] and Shajimon K. John[2]

[1] Department of Electronics and Communication Engineering, Saintgits College of Engineering, Kottayam, Kerala, India
sandeep.bkadam9@gmail.com
[2] Saintgits College of Engineering, Kottayam, Kerala, India
shajimon.k@saintgits.org

Abstract. Internet of Things (IoT) is expanding exponentially due to the manufacturing of cheaper electronics and high-speed communication. Blockchain technology has paved way for the introduction of digital cryptocurrency called bitcoin. The blockchain is one of the four main technologies that have enabled cryptocurrency. Conceptually blockchain is a distributed digital ledger that stores data in blocks, which are cryptographically linked with the previous blocks. This makes blockchain immutable. Blockchain has gained its popularity in the scientific community with the success of bitcoin and ever since researchers are trying to adopt this technology to other areas in order to solve problems beyond the smart sectors like Internet of Things (IoT), supply chain and so on. In our research work, we adopt blockchain in IoT and implement ethereum based IoT architecture for securing the IoT network. We have implemented a two-node ethereum network where transactions are made at the expense of ether and each transaction is verified by the miner using the smart contract written in the ethereum network.

Keywords: Internet of things · Blockchain · Ethereum · Smart contract · Raspberry pi

1 Introduction

Internet of Things is the basis of intelligent buildings, intelligent energy systems, intelligent transport systems and intelligent Healthcare, which are key elements of developing cities that are smart [1]. The trust, identity and the security serves as the most fundamental requirement for having a speedy as well as a safe implementation of the Internet of things solutions. The blockchain address the following three apprehensions and integrates the all forms of the internet of things under one frame work. This approach also defines the different roles of each IoT device built on its features and performance requests because it fulfils the vision of the mobile edge of consumer electronics.

Current IoT architectures are centralised architectures and are vulnerable to single node failure. If an attacker can get access to the centralised cloud, then the data that resides in the cloud is vulnerable. At present, there no efficient way to detect these. Another threat to the centralised architecture is DDoS attacks [2, 3]. A DDoS attack is when an attacker directs a huge volume of data to the central unit which makes it hard

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 179–184, 2020.
https://doi.org/10.1007/978-3-030-37051-0_20

to process the data and the original request for processing by a client node is thus denied. Centralised cloud-based architectures are trust-based which leads to privacy issues [4]. IoT data contains sensitive data about the user and storing the same in a third party doesn't ensure the safety of the data [5]. There is no mechanism to check if the data has been copied to a third person without knowledge of the owner of the data. These issues can be addressed by incorporating blockchain into the IoT architecture.

The blockchain is a digital leger that can store data which are cryptographically hashed. The blockchain is circulated to all the nodes in the network which means the same copy of data is stored in all nodes [6]. Data is stored in blocks which are cryptographically hashed with the previous block. These two properties of blockchain make it immutable and immune to single node failure. Blockchain on an abstract level is a linked list where each list is linked to the previous list. In blockchain, the list is called as a block since it contains multiple number of information. The blockchain is implemented either in structure data type or in JSON format. Blockchain was first used in bitcoin by Satoshi Nakamoto in 2008 [7].

Ethereum is blockchain technology which is an open software platform that allows developers to create and implement decentralized applications. Ethereum can store code in the blockchain, unlike bitcoin. A smart contract is simply an expression used to define a computer code that can enable the exchange of money, content, property, securities or anything of value. When executed in the blockchain, a smart contract develops a computer program that runs automatically and runs automatically when explicit conditions are met. Since smart contracts work in the blockchain, they are executed precisely as intended, with no opportunity of censorship, downtime, fraud, or third-party intrusion [8].

This paper describes the IoT infrastructure based on Gateway-oriented communication technology which incorporates ethereum blockchain for securing the network. A local ethereum private chain is created and a smart contract is deployed on to the chain which validates the transactions and the devices from which the data is generated. We propose how low power end devices can be connected to the network and how data from these devices can be validated.

2 Proposed Architecture

In our IoT-Blockchain architecture, we include a gateway between low power IoT devices. Low power IoT devices are incapable of handling blockchain due to their low power and limited memory. Gateway is a small computer system that handles all the transactions to and from the IoT devices [7]. Copy of ethereum blockchain resides inside this gateway. Gateways act as miners in this architecture and they validate transactions that occur in the network [9]. IoT gateway will be discussed in detail in the upcoming sections (Fig. 1).

2.1 Blockchain

It is a decentralized ledger positioned in a P2P core. System nodes produce and transmit transactions uninterruptedly. As expected, a blockchain contains of

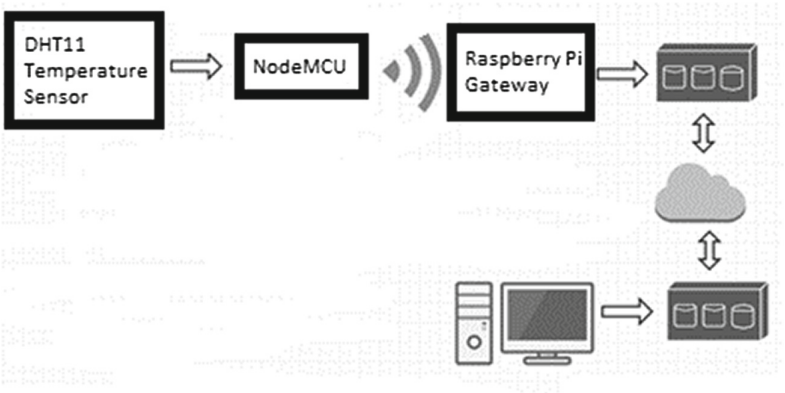


Fig. 1. A simple block diagram of IoT-blockchain architecture

cryptographically bound blocks and timestamped pools of transactions. Nodes repetitively check system blocks to oppose malicious invaders attempting to falsify or falsify dealings. Every dealings in the blockchain is aided with cryptography in Fig. 2, shows the detail structure of the blockchain.

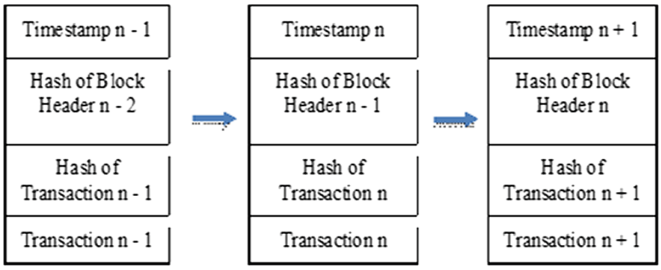


Fig. 2. Structure of blockchain

In customary schemes that are based on a block-chain, the miner will identify the following block by framing a solution to the mathematical problem that is difficult to compute, but easily verifiable. On identify the new block by farming the solution for the complex problem, the identified block is projected as the proceeding block to the network and assigned under the minor. The broadcast strategy retains the co-ordination among the pairs using the consensus.

A type of block chain called Etherum uses the smart contract to relate the individuals connected with the block chain in a particular transaction. The code for the smart contract in the Etherum is usually complied using the Etherum-VM. It allows one to completely program the bit coin capacities and control and execute as per it is programmed. The decentralized nature enables all who are connected to it to access the information from anywhere [10].

2.2 Types of Blockchain Nodes

Miners: Miners are definite nodes that cumulate block transactions and execute algorithms of the consensus which meet requirement of the system to achieve a benefits in terms of finance [11]. Miners process a transaction that happens in the network and controls all incoming and outgoing transactions. Miners practice consensus algorithms such as Proof of Work (PoW) to authorize a transaction in the network. In the PoW consensus, the miners in the network have the uppermost computing power [7].

Full nodes: ensures the complete downloading of the block-chain and an uninterrupted authentication for all the transactions, framework without trust and distributed. Adequate storage and manipulating capability is mandatory to execute a complete node.

Thin clients: ensures the downloading of the blocks header that contains the transaction hashes alone. Consequently, it is probable to intermingle with the blockchain by least storage and calculation necessities. Thin clients don't mine a block. They can store a portion of the blockchain due to the memory and processing limitations.

2.3 İmplementation

In our paper, we have used a raspberry pi as a gateway that connects a temperature sensor to the ethereum blockchain. We have implemented a two-node network where the raspberry pi acts as the gateway and host to store ethereum private chain. A smart contract is deployed on the private chain which only accepts data only from the temperature sensor connected to nodemcu. The filtration is done using ip address filtering. The contract only accepts data from the specified ip address only [12]. Nodemcu is connected to the raspberry pi via Wi-Fi. Block Diagram of the connection is shown in the figure. The gateway acts as a full node and an Ubuntu machine is used as miner which mines the transactions. This is done because of the limited RAM of raspberry pi. Both the Linux machine and raspberry pi are synchronized in real time and are connected over the internet. We are controlling a LED on raspberry pi using the temperature sensor value by spending ether for each transaction.

2.4 Procedure for Deploying Ethereum Private Chain on Raspberry Pi

- Install prerequisites to run ethereum private chain on Ubuntu machine and raspberry pi. Nodejs, Web3 and git are installed in both machines.
- Pull go-ethereum from GitHub and clone the same on both the machines and build.
- Create a genesis block and synchronise both machines with the private ethereum chain.
- Create a smart contract that will interact with the temperature sensor and raspberry pi led status using javascript and run the application.
- Use the ethereum wallet to check the status of the led and temperature sensor.

3 Evaluation

Memory consumption of the architecture can vary with synchronisation speed. In our configuration, miner node uses 1.5–2 GB of memory which is practically the equal as full node while thin clients use around 200 MB of memory. The data rate in blockchain systems be determined on several metrics and differs according to the employment. In bitcoin network, a block is created in every 10 min. For the ethereum network, there is no limit for the size of a block and is dependent on the gas limit for validating a block. We have set an average gas limit as 20,000 gases which mean a block can contain 224 transactions. Although transaction performance is weak to support large-scale deployment, it is essential to keep in mind that businesses are produced only by the gateways of the internet of things and each gateway can hold 100's of 1000's of IoT components.

4 Conclusion

Internet of Things enables smart cities, intelligent transportation, intelligent medical care and so on. Blockchain integration with IoT will make IoT data fault tolerant and immune to DDoS attacks. In this paper, we have tried to implement an IoT architecture integrating ethereum private blockchain. Though the speed of operation and large scale integration is limited in this particular architecture, it points to a promising future of integrating blockchain or similar technologies with IoT for making the existing IoT devices more secure and faster.

References

1. Yaqoob, I., et al.: Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE Wirel. Commun. **24**(3), 10–16 (2017)
2. Alaba, F.A., et al.: Internet of things security: a survey. J. Netw. Comput. Appl. **88**, 10–28 (2017)
3. Aikat, J., et al.: Rethinking security in the era of cloud computing. IEEE Secur. Priv. (2017)
4. Ali, M.S., et al.: Applications of blockchains in the internet of things: a comprehensive survey. IEEE Commun. Surv. Tutor. (2018)
5. Jing, Q., et al.: Security of the internet of things: perspectives and challenges. Wirel. Netw. **20**(8), 2481–2501 (2014)
6. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Whitepaper (2008). (2009)
7. Dorri, A., Kanhere, S.S., Jurdak, R.: Towards an optimized blockchain for IoT. In: Proceedings of the Second International Conference on Internet-of-Things Design And Implementation. (2017). (ACM)
8. Zhang, Y., et al.: Smart contract-based access control for the internet of things. IEEE Internet Things J. (2018)
9. Özyılmaz, K.R., Yurdakul, A.: Designing a blockchain-based IoT infrastructure with Ethereum, Swarm and LoRa (2018). arXiv preprint arXiv:1809.07655
10. Dannen, C.: Solidity programming. In Introducing Ethereum and Solidity, p. 69–88. Springer (2017)

11. Dorri, A., et al.: Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops) (2017). (IEEE)
12. Aung, Y.N., Tantidham, T.: Review of Ethereum: smart home case study. In: 2017 2nd International Conference on Information Technology (INCIT) (2017). (IEEE)

Motorbike Helmet with Heads-Up Display Navigation and Fall Detection System

Ritik Gupta[1], Rashmi Singh[2(✉)], Vaibhav E. Pawar[1], and Shital V. Patel[2]

[1] Department of Information Technology, Bharati Vidyapeeth, Navi Mumbai, India
guptaritikr@gmail.com, vaibhav.e.pawar@gmail.com

[2] Department of Mechanical Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai, India
rashmissingh97@gmail.com, virshitl974@gmail.com

Abstract. Globally, there is an upward trend in the use of two-wheelers, both for transport and recreational purposes. This has led to an increase in the demand for a safety device that can act more than a cushioned wall between the wearer and the point of impact. The proposed solution is an Advanced Helmet with features like a Head-Up Display which would provide Distraction free Navigation and a Fall Detection system that could potentially reduce the number of deaths in road accidents by allowing faster Emergency Response through Accurate Location information being provided within minutes of the incident.

Keywords: Navigation · Head up display · HUD · Fall detection · GPS · Google maps · Emergency safety · Internet of things

1 Introduction

Road Safety is one of the major concerns in the developing world. Strict rules and regulations have been introduced by governing bodies for all vehicle users to ensure the safety of all commuters. Even though there has been an evolution in the services provided to motorists, be it for safety or for navigational assistance, motorcyclists are yet to receive any such benefits in a universal and affordable fashion. Motorcyclists who take long road trips or commuters who travel along solitary roads suffer from a lack of proper support for Navigation which may cause distractions while driving. Concern has also been voiced for a dependable post accident alert system which could help those in need of aid possibly avoid death from common causes like blood loss. Accident victims are also often subjected to the indifference of passersby due to mistrust owing to the criminal activities performed under this pretext.

Motorcyclists who often travel long distances on their bikes are at a relatively higher risk of falling victims to road accidents due to no emergency features or navigational support being provided in their existing safety gear. Using phones to perform mundane tasks like request navigational support, exponentially increases the chances of an accident while driving due to the amount of distraction it introduces. It also requires

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 185–193, 2020.
https://doi.org/10.1007/978-3-030-37051-0_21

the rider to shift their attention between things while driving, because the application that are being used are not meant to be used while on the move. They present information in a manner which requires the user to carefully analyze the information being presented in order to make a logical decision about their journey, therefore increasing the cognitive load, which is an additional hazard. In case of accidents, the victims sometimes remain unassisted for extended periods of time which can lead to unnecessary complications or may even result in death.

2 Study of Existing Work

According to data released in 2016 [1], 43 deaths occurred per day, 28 of which were comprised of two-wheeler riders. The fatality rate has also gone up from 21.6 deaths per 100 accidents to 31 deaths per 100 accidents between 2005 and 2017 with this number continuing to grow. States in India which contributed to this data have also stated that one of every five bike occupants who died in crashes were not wearing helmet and their total number was 10,135. To identify the underlying issues and public opinion on why wearing helmets was not considered a necessity when driving two wheelers despite being required by the law to do so, a survey was conducted with over 100 willing participants from a multitude of varying backgrounds [2]. This survey also provides insightful information on the most preferred safety measure which is taken by people and the features that would make them more likely to wear a helmet.

In 2007, a group of three students from the University of California introduced the idea for an Active Heads-Up Display which would warn the car user when they were over-speeding. The group made use of a laser based wide area windshield display and after experimenting with different display styles and by conducting tests they were to conclude that their system helped achieve a 42% decrease in the amount of time required by users to slow back down to the legal speed limit. However, based on eye tracking information it was inferred that the display had potential to be more distracting than helpful due to the users checking their speed constantly [3].

This was followed by publishers from Honda Research Institute USA who moved from Direct Displays to Augmented Reality based interfaces which would not only inform the user of the navigation hints that they needed in their field of vision, but also allow them to gauge the distance between them and the next turn. The experimenters recorded visuals, overlaid their HUD on top of it and presented them to test subjects. Their design while allowing clearer instructions on empty and open roads can also be viewed as occlusive and distracting on busy roads with objects overhead that require attention. Based on test results, many users found the display helpful but an almost equal amount of users raised concerns regarding the cognitive load it would bring. AR visuals were also shown to have failing effects in studies conducted by the references that they used [4].

Finally in 2018, a group of students from Graduate School of System Design and Management, Keio University in Yokohama, Japan presented their research on a Navigational System for Motorbikes. They adopted a different, more human-Centered approach towards head-up displays by projecting the information on the visor attached to the front of the motorcycle. This approach allowed for more information to be

displayed and did not modify the helmet in any way, thereby not compromising the safety of the rider. They performed tests on a virtual reality based setup [5]. In a condition of riding a motorcycle at maximum of 30 km/h, the presenting information timing shall be 40–55 m prior to the upcoming crossroad [6], the presenting information position shall be Lower Left or Lower Right [7], and the presenting information quantity shall be not more than 5 letters of Hiragana [8].

3 Proposed Solution

3.1 System Architecture Diagram

Figure 1 describes the proposed architecture. The Raspberry Pi will have 3 main functions namely: The Navigation App, The Location App and the Emergency Monitor App. Their individual functions will be detailed in the sections that follow. The Raspberry Pi and the Android Smartphone communicate using Wireless Fidelity Ad Hoc Protocols or WiFi Hotspot. The Raspberry Pi and the SSD1306 module together act as a Navigation Display System. Further, The Raspberry Pi is interfaced with the 6 degree of freedom Controller (GY-521 MPU-6050 3-axis 6-DOF Gyro & Acceleration Sensor Module) using I^2C interface.

Rasspberry Pi Zero [9]. Is a single board computer which features a 1 GHz single core CPU, with the capability to run Linux based operating systems. The Raspberry Pi Zero W has an integrated WiFi chip which can be used to connect it to the internet. It also comes with double row GPIO (General Purpose Input Output) pins which can be used for interfacing it with a variety of I/O devices. In our case, it is going to be the 0.9 inches SSD1306 OLED Display Module and the GY-521 MPU-6050 Sensor Module. We will be installing Debian-based Raspbian OS on the Raspberry Pi and use the Luma library for interfacing it with the SSD1306 display module. Luma is a python library which provides a drawing canvas which is similar in function to the Python Imaging Library or Pillow, and other functionality to support drawing primitives and text-rendering capabilities for small displays on different types of microcontrollers. It is also highly compatible with all flavors of Raspberry Pi running Python 2.7-3.5.

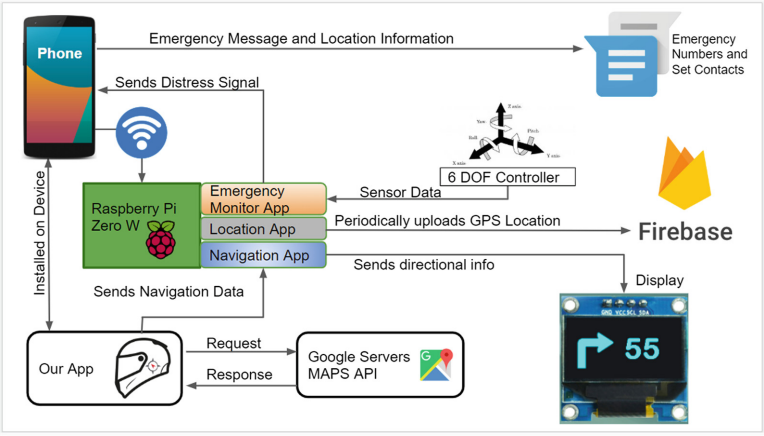


Fig. 1. System Architecture Diagram

SSD1306 OLED Display module. This OLED Display Module measures 0.96" which is very compact and can easily be accommodated inside a motorbike helmet. The advantage of using an OLED Display is that it offer more brightness in less amount of electricity due to the absence of the requirement for a backlight, which is present in LCD displays. This module supports both SPI and I^2C protocols of communication. This module also supports viewing angles of greater than 160° which would allow the user to view the screen from any angle.

Firebase Realtime Database [10]. It is a cloud-hosted real-time NoSQL database. It makes use of WebSocket which is much faster than regular HTTP connections and provides an API that allows developers to store and sync data across multiple clients. The data is stored in JSON format, synced across connected devices in milliseconds, and available even if the app goes offline.

GY-521 MPU-6050 3-axis 6-DOF Gyro and Acceleration Sensor Module [11]. This is GY-521 MPU-6050 3-axis 6-DOF Gyro Accelerator Sensor Module. GY-521 MPU-6050 6 axis attitude gyro is a 6 degree of freedom (DOF) device which incorporates an MPU6050 accelerometer and gyro chip, and HMC5883L digital compass. The MPU6050 devices combine a 3-axis gyroscope and a 3-axis accelerometer on the same silicon together with an onboard Digital Motion Processor (DMP) capable of processing complex 6-axis MotionFusion algorithms. The parts integrated 6-axis MotionFusion algorithms access external magnetometers or other sensors through an auxiliary master I^2C bus, allowing the devices to gather a full set of sensor data without intervention from the system processor.

3.2 Shell Design

A normal helmet consists of the Outer Shell, Inner Lining and the Visor. Due to the extra components added to the Helmet, a new design is constructed which will feature a more Aerodynamic design along with improvements that make the helmet much more visible at night time to other drivers. The components will be properly housed between the outer shell and the inner lining with ventilation slots to allow for ventilation of any excess heat (Fig. 2, Table 1).

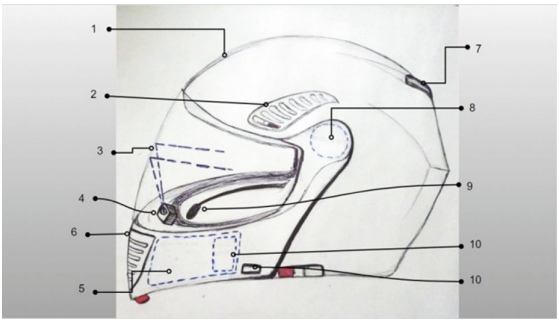


Fig. 2. Proposed6 Design of The Unit

Table 1. Functions of Corresponding Parts of the Proposed Design

1	Lightweight, Aerodynamically sound, polycarbonate shell	6	Cooling Vents for Electronic components
2	Adjustable air vents for ventilation	7	Reflector for better nighttime visibility
3	The position of Reflection which won't Distract or Distort the view field	8	Audio output device for navigational hints
4	Pop Up Display module	9	Microphone for voice command
5	The processing unit and 6 DOF Accelerometer Sensor Module	10	A. Rechargeable Power module 2600 mAh and B. USB charging port

3.3 Fall Detection System

The MPU-6050 is the chosen chip for monitoring user orientation and change in acceleration while driving. Due to the protocol of communication being I^2C, this device works out-of-the-box with the Raspberry Pi Zero W. The data received from the sensor will be checked at each second. Through trial and error, a set of values have been determined which are only observed when a person is falling and in a position from which the driver cannot recover safely. The program continually monitors the output generated by the MPU6050 chip for these values (Figs. 3, 4).

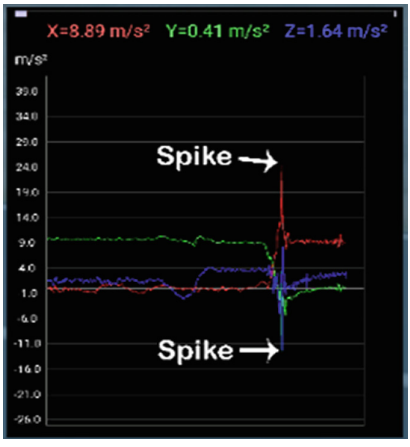


Fig. 3. Visualisation of accelerometer values

Fig. 4. Sample emergency message

In case a fall is detected by the system, a notification appears on the phone of the user saying that a fall has been detected by the system. The user can deny the detected fall by tapping on it. In case the user interacts with the generated notification within a set amount of time, any further emergency actions will no longer occur and the system

will go back to monitoring for any further falls. In case the user does not interact with the notification within 30 s the system initiates Emergency Action. In this case, the user's emergency contacts will be sent a message notifying them of the fall along with GPS coordinates of the user which is arranged into a convenient Google Maps Navigation URL and urges them to ascertain the information by calling the person as soon as possible. At this point, the text on the notification changes to state that the emergency has been reported to the emergency contacts. If the user interacts with this message, they get the option to send out an 'All-OK' text to the same contacts from their own device. This feature has been included to avoid any panic which may be caused if the user is unable to interact with the notification in time.

3.4 System Methodology

Once the user launches the companion application, they are greeted with a wizard informing them of the major features that are included in the application. Following this wizard, a sign in UI is present. Users get the option to use their existing Google Account credentials to register/login to the application or use their email for the same. This has been provided to reduce the information load of remembering a new set of credentials on the user. If the user registers a new account they are presented with a form asking some basic personal information as well as medical information which can be useful in case of an accident. Authentication of users and Storage of personal data is done via Firebase. The user is then requested to provide the necessary permissions and switch on their mobile hotspot so a connection can be established between the Smart Phone and the Raspberry Pi (Figs. 5, 6).

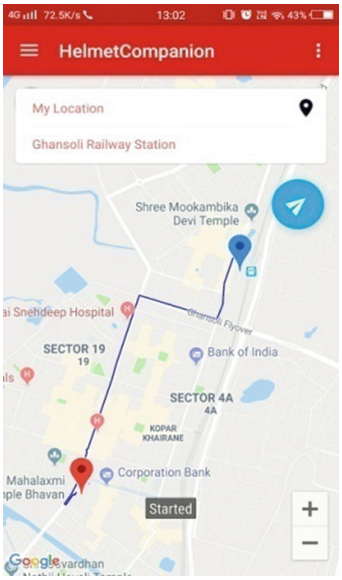


Fig. 5. Map view of companion app

Fig. 6. Helmet prototype with navigation cue

In the next screen, a custom interface similar to Google Maps will be provided using which the user can search for the destination they want to go to and the route they want to take to get there. A location icon is also present, upon pressing which, the map will zoom in to their current location. When both source and destination have been provided, a route will be calculated between the two locations and shown to the user traced on the map. On pressing the Go button, user's location will be periodically uploaded to Firebase Servers to assist in finding the user in case of a mishap. The Navigation application will then inform the user periodically about their location being updated in the database. This is meant to help remind the user of the application being active in the background.

4 Conclusion

Based on a few tests conducted with many users over the course of 2 months, many different potential issues with the system were identified and promptly fixed. One such issue was users being unable to respond to the notification in time due to being on a moving vehicle which needed to be safely stopped in case an emergency was detected wrongly. This led to panic in users as there was no way to send a rectification message in the early prototype. Hence, the feature of sending an All-OK text message directly from the notification was introduced. This feature boosted user willingness to try out the system, since mistakes could be just as easily rectified. The amount of information to be displayed was chosen based on different studies conducted by authors who have previously worked on this subject. User productivity was observed to be highest with the most minimal information being displayed as unlike existing smart phone applications which provided information which required more time and attention to process, this system gave them exactly what they needed.

5 Future Scope

Recent efforts taken by the Road Transport Ministry of India are proof that the government has recognized the need of an update to Motorbike Helmets that are ISI compliant and provide more comfort to the wearer [12]. This project is meant to enhance the current amount of functionality provided by motorbike helmets through several useful additions however, it should be noted that these additions are completely optional. They do not affect the normal functioning of the safety device. The entire electronic system is fit in the jaw section and can be made removable as well as user replaceable for faster emergency aid. Wi-Fi hotspot is used for maintaining the connection between the modules in the helmet and the Android Smartphone as it allows for the creation and monitoring of several connections at once. It would be however, much more energy efficient to use Bluetooth 4.0 for this purpose as only a single connection needs to be maintained and it will be within the operational range for Bluetooth. The Fall Detection System introduced in this prototype can be isolated as an independent set of modules comprising of the hardware and the software parts. The Algorithm can

be used for several other applications like Care Systems for the Children and the Elderly.

A 'Safe' Voice Communication System can be implemented which will allow the user to receive calls and talk to the caller, provided the vehicle has been completely stationary for a set duration of time. This system will disconnect calls if the user attempts to move the vehicle while a call if going on, to prevent any illegal activities or misuse of the system. It can be implemented with the help of additional modifications like a highly accurate location sensor which can distinguish between a stationary and moving user or using a sensor to judge if the user is moving.

The fall detection system was tested for accuracy and it detected each and every type of conventional fall which it was tested for. However, fall intensity could further be detected in the system. This functionality will be included in the next prototype and introduce a range of new features with it. Testing this system with more users in different situations can provide us with better insights and more useful data to make a more safety driven project.

References

1. The Times of India: In 2016, not wearing helmets, seat belts killed 43 a day by D. Dash, 14 Aug (2017). https://timesofindia.indiatimes.com/city/delhi/28-bikers-without-helmets-died-daily-in-2016/articleshow/60050999.cms
2. Survey About Motorbike Helmets and Road Safety (Google Forms). https://docs.google.com/forms/d/1t9hZU8xkxRliHZrKaNEfKCscjFYPa-kw8G_GY6Y4wtU/edit#responses
3. Cheng, S., Doshi, A., Trivedi, M.: Active heads-up display based speed compliance aid for driver assistance: a novel interface and comparative experimental studies. In Intelligent Vehicles Symposium (IEEE, June 2007), pp. 594–599 (2007)
4. Bark, K., Tran, C., Fujimura, K.: Victor Ng-thow-hing, personal navi: benefits of an augmented reality navigational aid using a see-thru 3D volumetric HUD. In: Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications,17–19 Sep. Seattle, WA, USA (2014). https://doi.org/10.1145/2667317.2667329
5. Ito, K., Nishimura, H., Ogi, T.: Motorcycle HUD design of presenting ınformation for navigation system. In: 2018 IEEE International Conference on Consumer Electronics (ICCE), 29 March. Las Vegas, NV, USA (2018). https://doi.org/10.1109/icce.2018.8326113
6. Ito, K., Nishimura, H., Ogi, T.: Evaluation of the information presentation timing for motorcycle head-up display. Transactions of the JSME (in Japanese) **853**, 17–00113 (2017). (in Japanese)
7. Ito, K., Tateyama, Y., Nishimura, H., Ogi, T.: Evaluation of the position to present information using the head-up display for motorcycle. Trans. Hum. Interface Soc. **4**, 435–442 (2016). (in Japanese)
8. Ito, K., Tateyama, Y., Nishimura, H., Ogi, T.: Evaluation of information amount to present for motorcycle head-up display. Transactions of the JSME (in Japanese) **830**, 15–00203 (2015). (in Japanese)
9. Raspberry Pi Zero W-Raspberry Pi. https://www.raspberrypi.org/products/raspberry-pi-zero-w

10. Firebase Realtime Database. https://firebase.google.com/docs/database/
11. MPU-6050 | TDK. https://www.invensense.com/products/motion-tracking/6-axis/mpu-6050/
12. The Times of India: Design-less bulky motorcycle helmets, adapt them to women's hairstyles: Govt. panel by D. Dash 7 Apr (2017). https://timesofindia.indiatimes.com/india/design-less-bulky-motorcycle-helmets-adapt-them-to-womens-hairstyles-govt-panel/articleshow/58060851.cms

A Crypto-Blocking Approach for the Security Paradigm for Aadhar Towards Privacy Preservation on Cloud Infrastructure

Chhaya S. Dule[1(✉)], H. A. Girijamma[2], and K. M. Rajasekharaiah[3]

[1] Department of Computer Science and Engineering, K G Reddy College of Engineering and Technology, Hyderabad, Telangana, India
chhaya0671@gmail.com
[2] Department of Computer Science and Engineering, RNS Institute of Technology, Bangaluru (VTU Belgaum), Bangaluru, India
girijakasal@gmail.com
[3] Faculty of Information Technology, AMITY Institute of Higher Education, Quatre Bornes, Mauritius
drrajcse2014@gmail.com

Abstract. In the world various methods are being adopted to create a systematic identification for their citizens. In year 2009, UIDAI a government body of India initiated a 12-digit number called Aadhar number, which is generated out of biometric and demographic fusion of an individual and their identity. In order to ensure a highest level of data protection as well as privacy preservation of the Aadhar card propagation through a network, it requires an efficient model of security that becomes synchronous with the cloud infrastructure. This paper initially investigates the existing approaches and their limitations towards the Aadhar card security proposes a security model namely ECrypto-AaDhaar based on the cryptography approach synchronous to the cloud architecture. The privacy preservation of the AAdhar card associative demographic and biometric information is performed considering a statistical crypto-blocking operation prior propagating it through the network in the context of cloud infrastructure. The study later also presented an experimental analysis to demonstrate the performance of ECrypto-AaDhaar technique from a time complexity perspective.

Keywords: Aadhar · Image cryptography · Statistical Crypto-blocking mechanism

1 Introduction

The primary objective of the Aadhaar is to facilitate the government schemes to the Indian citizens by integrating people's identity as biometric, their demographic details, bank account, cell phone number with government application portals [1]. One of the most popular schemes is already realized includes cooking Gas subsidy payment directly to the consumer bank account [2]. These steps cut down the effect of middleman and enable good governance to eradicate corruption- Aadhaar is here to stay.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 194–203, 2020.
https://doi.org/10.1007/978-3-030-37051-0_22

Currently Aadhaar is mandatory to almost 139 schemes of the government [3]. As of now approximately 1.19 billion resident of India which is almost 93% of India's pollutions are enrolled with the system along with their 10 fingers, 2 irises, face in reposit [4]. Similar approaches are being encourages by other countries to make these kinds of initiation more globally extensible and useful. Table 1 shown few examples for the countries.

Table 1. Country wise Program

Country	India	Brazil	GHANA	Indonesia	Malaysia
Program	UDDAI	(Abrid).	(NIA)	eKTP	MyKad

The applications connected with the Aadhaar require higher level of availability, connectivity, scalability, authentication, authorization and fault tolerance in the system design which is achieved by setting up the eco-system to the cloud. The facilitation along with cloud can take the government schemes to the remotest place of the country, therefore the framework shall be robust enough. All these goes to the good part of the system, but what about the protection guarantee of privacy of an individuals whose biometric data is a part of the system? The right to privacy of Indian citizens, government drafts and preventive actions are still in ambiguous and initial phases that brings the focus of study to work on the security aspects of Aadhaar Card [5] The Aadhaar Act 2016 says that the identity of an individual for any purpose will be established by the Aadhar Number [6], that has propagated service-oriented architecture (SOA) to build new business models like TrustID to identify many blue color professionals. In Feb 2017, A consent-based trust-platform in India namely Ongrid provisions a complete information that includes Aadhar Number, Name, date of Birth, Mobile, Gender and Aadhaar Address those are very critical and private information for the banking frauds [7].

Section 2 describes the applications based on the Aadhar and the methodologies adopted for the security, Sect. 3 described an architectural model for the security paradigm of Aadhaar over cloud synchronization, Sect. 4 discusses results and finally the conclusion in Sect. 5.

2 Review of Literature

The evolution of various Internet of Things (IoT) based applications, social networking and Aadhaar like systems are facilitating large amount of data rather with qualifying characteristics it may be kept under the Big Data category also. In our extensive survey on study of the security measures for Bigdata in cloud reveals the security model and trend of the research in the domain of privacy preservations [1, 2]. In this paper the major focus in on security models for Aadhaar. The total number of publications found in the IEEE Xplore a digital library till September 2018 were found only 27conference papers and one journal/magazine. Moreover, this area of research is less explored when the specific problem of Aadhaar privacy preservation is concerned.

A recent work in a similar direction by Padmavathi et al. [8], introduced a computational system, in order to secure the automated ration distribution. Here, the authors have mostly emphasized to build an interactive approach of smart card enabled ration circulation where Aadhaar card plays a crucial role. It replaces the conventional ration card by replacing it with a novel approach of RFID based Aadhaar transaction system where, it contains all the demographic an bio-metric attributes associated with an individual. The design analyses followed by an experimental set up are exhibited from a theoretical point of view. Lastly a statistics of analysis of ration beneficiary with respect to consumption pattern is also highlighted.

Mishra [9] also introduced a mathematical approach which is modeled in order to formulate an AAdhar based smart card system. The study mainly exploited the design and executional limitations associated with existing watermarking techniques. Thereby to achieve the intended security goals with an efficient potential economic development, this AAdhar conceptualization id done to a significant aspect where all the money transactions related activities can be secured. The contextual proposal associated with [9] influences the economic growth of Indian Railway System, where it targets to implement verification of passenger details in a ticketless manner. For this, a simplified authentication method using Aadhaar databases anticipate boosting up the contributory aspects of local trains in generating maximum share in revenue. The authors also claimed that this can lead to a better prospect, where the execution of smart railway system can be visualized in practice.

Shah [10] mostly focused on the low-cost implementation Raspberry Pi supported bio-metric systems which can be used in Aadhaar-card management systems. On the other hand Halvi and Soma [11] conceptualized a cloud assisted bio-metric system which authenticates facial data with extra-layer of security features. The authors claim that the system is scalable and achieves 96% accuracy when Aadhar card images are considered for authentication. In the study of Illakiya et al. [12], a secure voting system is introduced where Aadhaar card and bio-metric sensor attributes authorize security of each vote. The presented solution targeted to be implemented on cloud storage enabled platforms with efficient bio-metric solutions.

On the basis of above explored critical study, it is thoroughly observed that although very few research attempt made, where Aadhaar card attributes play a crucial role but most of them lacks efficiency in terms of scalability and robustness. It is also found that not a single research study till date talk about securing Aadhar attributes with a higher-level crypto-blocking approach prior processing it to the cloud storage as the futuristic IoT applications are much more exposed and vulnerable in every layer in-network processing. Thereby, this current issue is needed to be addressed and there is a need of developing a cost-effective solution which can fill this gap in a significant manner.

3 System Model: ECrypto-AaDhaar

The existing Aadhar data model is on centralized database [13] which is not effective enough from various viewpoints (1) Higher ownership cost, (2) Bandwidth optimization limitation, (3) Risk of location-based security etc., thus the data need to be kept on

the cloud infrastructure to overcome all these bottlenecks. Most importantly the model for the privacy preservation as it is facing some legal conflict too[AR2] because there is no open draft about the privacy preservation. In odder to overcome the treats on the biometrics and unique ID stored in a central data servers the proposed model provisions cryptographic mechanism to push the data to the cloud.

3.1 Aadhaar Input Model

This subsystem of ECrypto-AaDhaar provisions various compressed image format (A_0) of Aadhaar input to be security transmitted to the cloud infrastructure (C). The local reposit A_0 description, $A_d = A_p \cup A_n$. The initial digitization of A_d gives vector $dA = [edA_{i,j}]_{dim=3}$, having R(dA), G(dA), B(dA) as RGB format. The down sampled preprocessed dA is shown in Fig. 1

$$I = \begin{bmatrix} dA_{11} & dA_{12} & \dots & dA_{1j} \\ dA_{21} & dA_{22} & \dots & dA_{2j} \\ dA_{31} & dA_{32} & \dots & dA_{3j} \\ dA_{i1} & dA_{i2} & \dots & dA_{ij} \end{bmatrix}_{Dim=3}$$

Down sampled preprocessed Digital Aadhaar (dA)

Fig. 1. Aadhaar input for security after preprocessing

The preprocessed image dA which is also uniformly resized for the ease of computation, further considered as an input to the secondary sub-system termed as protector module.

3.2 Aadhaar Protector Model

In this subsystem, a protector image (pI) is considered and intended to maintain the authenticity and integrity of the preprocessed digitized Aadhaar image dA. pI is located in the local reposit P_d in a specific compressed format, which is, initially located using two unique attributes such as P_p and P_n where $P_d = P_p \cup P_n$. pI further digitized into a vector called dp = $[edP_{i,j}]_{dim\ =}$ 3 and resized.

The resized image will have R(dp), G(dp), B(dp) as RGB format. The following Fig. 2 exhibits the resized protected image mathematical expression along with its visual outcome.

$$pI = \begin{bmatrix} dp_{11} & dp_{12} & \ldots & dp_{1j} \\ dp_{21} & dp_{22} & \ldots & dp_{2j} \\ dp_{31} & dp_{32} & \ldots & dp_{3j} \\ dp_{i1} & dp_{i2} & \ldots & dp_{ij} \end{bmatrix}_{Dim=3}$$

Protected Image and its mathematical representation (pI)

Fig. 2. Resized and digitized protected image

The protector model and input models both are analytically designed on the basis of different operational entities where Digitization is performed to represent a physical image with digitized numerical form which is illustrated as follows:

3.2.1 Sampling

In this process of numerical computation where the physical image entities are subjected to undergo through a procedure in order to intensify its values within a finite range. In sampling process the input image is sampled on the basis of a fixed number of samples.

3.2.2 Quantization

In this computational step the measured sample valued ate replaced with an integer point. The proposed ECrypto-AaDhaar, here reduces the computational steps by representing the array of pixel entities with an uniform pixel attribute which basically consume very lesser memory space. The quantization process also computed the digitized elements with respect to 2^n –multi-level objective where n can be 256 gray (8bits/pixel) or 32 gray levels (bits/pixel) (Fig. 3).

The protector image of the individual here, works as a cover image (C_I) which hides the actual Aadhaar data entities considering a Statistical structuring model followed by an encoding process in the context of cloud enabled networks which is illustrated as follows:

3.3 Statistical Structuring Model

This part of ECrypto-AaDhaar subsystems incorporates a novel statistical notion of probability distribution (PD) by means of a Quantile function execution. The PD process is evaluated with respect to a Specific value of distribution quintiles. During this phase of the *statistical structuring and modeling*, the considered pre-processed digitized image attributes associated with both *I* and *pI* get converted into double precision form from unsigned integer 8. The transformation of precision format result in a highly balanced numerical representation which do not impose much

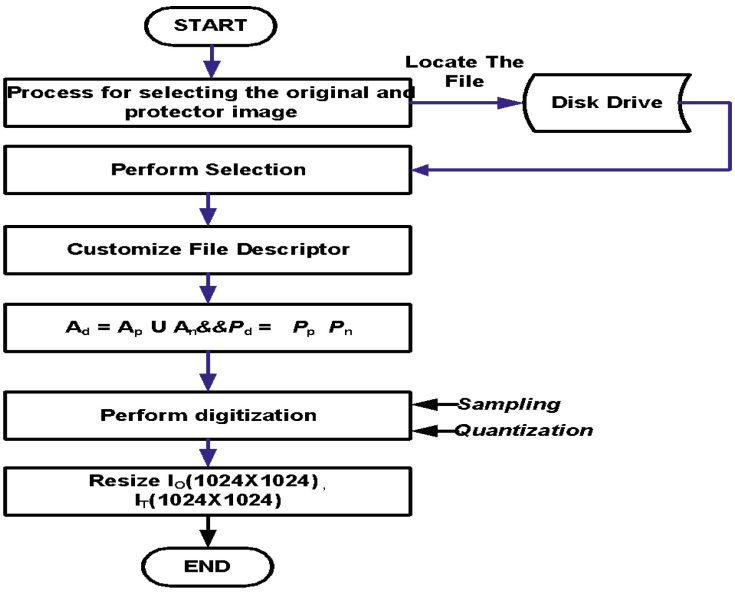


Fig. 3. Flow Design of Image Selection Process

computational overhead to the system in terms of space complexity. Statistical structuring also efficiently handles the memory out of range problems, which mostly occurs when a big floating point number is computed. Thereby, transformation of precision of data controls the negative effect of complexity up to a significant extent. During this phase of the design, the precision attributes of both I and pI get converted into double to reduce the time and space complexity of this structuring and modeling process, which has a significant impact on speeding up the process of encoding in cloud environment. The following work flow is designed considering the computational steps associated with the ECrypto-AaDhaar: Statistical Structuring model (Fig. 4).

During this statistical blocking process, ECrypto-AaDhaar evaluate the statistical measurement which is standard deviation (β) oriented, where the alpha-Quantile value (Q_α) is defined with respect to a specific range. The statistical measurement of β w.r.t Q_α is stored into a matrix called alpha-MAT where the structure of the data attributes associate Q_α can be explored. Finally β by means of proper ordering and reshaping of image data *I* and its *pI* is executed and also the value for index of each attribute get stored.

3.4 Analysis of Pixel Transformation Modeling

This computational design process enables a reversible transformation schema of pixel entities with respect to three different attributes such as Transformation factor Tf, Run-off Pixel Entity (Rp) and Minor Pixel Entity (Mp). Here the value of Tr always should be even and the value of $Lp < 0$. This phase of the execution basically performs a block based transformation to encode the image attribute and the original image further get

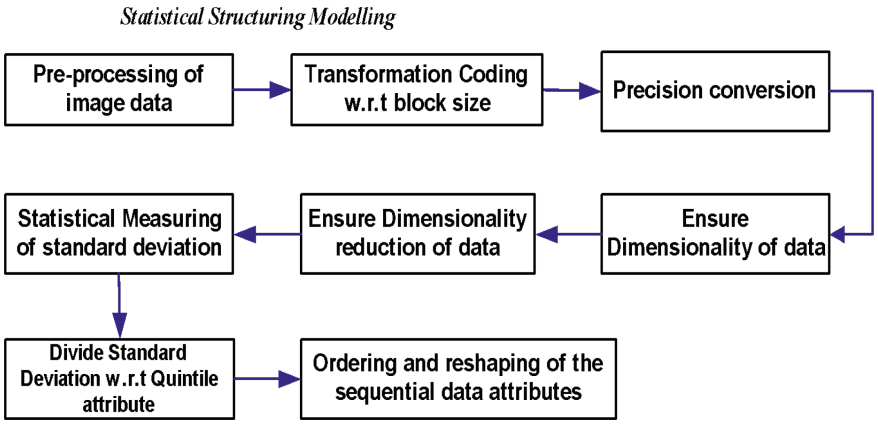


Fig. 4. Work Flow associated with Statistical Structuring Modeling process

encrypted and ECrypto-AaDhaar process a computationally efficient encoding mechanism to protect Aadhaar I under pI. Finally the encrypted file ε_f = Encrypt (I ∪ pI) is propagated to the networking pipeline in the context of cloud.

3.5 Experimental Assessment of ECrypto-AaDhaar

The extensive simulation of the proposed ECrypto-AaDhaar, under goes through a computational execution supported with a 64-bit windows machine. The extensive simulation is performed in a numerical computing platform with respect to different parameters. The simulation set-up exclusively require computational resources with minimum of 4 GB of internal memory and 1.2 GHz processing speed. The study in the first attempt design an simulate the ECrypto-AaDhaar computational process and further the outcome obtained, got validated on the basis of a processing time analysis where two other woks of Liang et al. [14] and Rad et al. [15], who have worked on the similar direction has been considered for the comparison.

The Fig. 5 exhibits a comparative performance analysis, where the performance of the proposed ECrypto-AaDhaar is validated with respect to the assessment of time complexity. As the work of Liang et al. [14] and Rad et al. [15] also addressed the similar security problem of image data in cloud environment, thereby it has got significance in terms of baselines and direction of research.

A thorough analysis of the study of Rad et al. [15] reveals that they have emphasized on enhancing the presented encryption procedure from a complexity view point. The study performed mainly attempted to reduce the computational time of their encoding approaches in the context of cloud enabled parallel computing support. On the other hand the approach of Liang et al. [14] also focused on formulating a secure image retrieving approach for cloud environment.

A closer interpretation of the above Fig. 5 shows that ECrypto-AaDhaar accomplishes the image security requirements with very processing time (Sec) as compared to the other two baselines. The outcome in terms of processing time is found having more

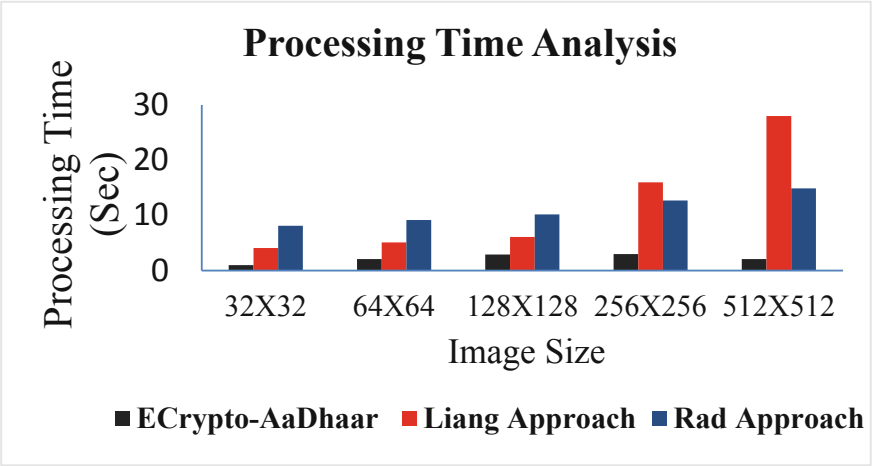


Fig. 5. Time Complexity Analysis

consistency in the case of ECrypto-AaDhaar as it reduces the cost of computation by introducing a statistical modeling of β computation. The time complexity here in this context evaluated with respect to different size/dimension of the input image which are 32 x 32, 64 x 64, 128 x 128, 256 x 256 and 512 x 512 RGB or gray-scale image components. The digitization process followed by statistical structuring also added more value to the proposed ECrypto-AaDhaar from a complexity view point.

The crypto-blocking operation of ECrypto-AaDhaar also reduces the space complexity where the variable of input image size increases. Liang et al. [14] and Rad et al. [15] both work do not impose a consistent processing time when the data size increases. It is also observed that in that for the image dimension of (512 x 512) Liang et al. [14], takes more time for the execution as compared to Rad et al. [15].

The space complexity is also reduced in the proposed study by incorporating precision and block-coding which does not appear in the other two works. The prime novelty of this work is it has reduced the complexity of crypto-blocking operation without compromising the security aspects of Aadhar image encoding. Thereby it can be said that the proposed approach balances the equilibrium between the cloud security requirements and the time complexity. Here security requirements are imposed towards preserving the integrity of Aadhar demographic and biometric attributes.

4 Conclusion

Security in the context of cloud computing and big data has certainly gained a much attention from the researchers. Although, there exist a lots of contribution in the line of big data security but most of the solutions do not meet the requirement of time complexity which has a significant impact on the economic growth. A thorough investigational study also exhibited a fact that not a single research work has been carried out towards preserving the high dimensional Aadhar card image attributes not in India or

abroad. Thereby addressing this open research problem, the proposed study has introduced a novel cryptography based security approach namely ECrypto-AaDhaar, which considers high-dimensional AAdhar image attributes such as demographic and biometric information associated with an individual and attempt towards protecting it with higher level of security without compromising the cost of computation. The extensive design and analysis of the proposed ECrypto-AaDhaar is carried out in a numerical computing environment and the outcome has been justified with respect to time complexity viewpoint. The comparative performance analysis shows that ECrypto-AaDhaar accomplishes scalability and robustness even though the dimensionality of image data increases. It also archives consistency during execution of data which has not been observed in the other two cases. Thereby, the ECrypto-AaDhaar ensures its adaptability into futuristic cloud enabled IoT solutions for securing Aadhar data attributes.

Response:

The abstract of the paper is sent to CoSIT -Dubai Conference for the paper selection process. But the registration of the paper could not happen because of certain unavoidable circumstances. But still, the abstract is published on the website as information to the authors. I requested the conference coordinator to delete the page from the website from last 4 months but no response from them. But, Now that link is disabled.

Acknowledgement. All author states that there is conflict of interest.
We used author photo(s) in the Fig. 1 and 2.
We used our own data.

References

1. Sharma, S.A.S.B.S.: Privacy and security of aadhaar: a computer science perspective
2. Dixon, P.: Health Technol. **7**, 539 (2017). https://doi.org/10.1007/s12553-017-0202-6
3. Ramanathan, U.: Blundering along, dangerously, Frontline India, 28 April (2017). http://www.frontline.in/cover-story/blundering-along-dangerously/article9629188.ece?homepage=true
4. https://www.indiatimes.com/technology/news/how-does-aadhaar-compare-with-other-id-systems-in-the-world-how-to-secure-its-leaky-database-276972.html
5. Dule, C.S., Girijamma, H.A.: Guaging the effectivity of existing security measures for big data in cloud environment (2017)
6. Dule, C.S., Girijamma, H.A.: Content an ınsight to security paradigm for bigdata on cloud: current trend and research. Int. J. Elect Comput. Eng. (IJECE) **7**(5), 2873–2882 (2017)
7. Silhavy, R., Silhavy, P., Prokopova, Z., Senkerik, R., Kominkova O.Z. (eds.): Software Engineering Trends and Techniques in Intelligent Systems. CSOC 2017. Advances in Intelligent Systems and Computing, vol 575. Springer (2017)
8. Padmavathi, R., Azeezulla, K. M., Venkatesh, P., Mahato, K.K., Nithin, G.: Digitalized Aadhar enabled ration distribution using smart card. In: 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT), pp. 615–618. IEEE (2017)

9. Mishra, K. N.: AAdhar based smartcard system for security management in South Asia. In 2016 International Conference on Control, Computing, Communication and Materials (ICCCCM), pp. 1–6. IEEE (2016)
10. Shah, D. K., Bharadi, V. A., Kaul, V. J., Amrutia, S.: End-to-End Encryption Based Biometric SaaS: Using Raspberry Pi as a Remote Authentication Node (2015)
11. Halvi, A.K.B., Soma, S.: A robust and secured cloud based distributed biometric system using symmetric key cryptography and microsoft cognitive API (2017)
12. Illakiya, S., Karthikeyan, U.M.,Velayutham, Devan, N.T.R.: E-voting system using biometric testament and cloud storage. In: 2017 Third International Conference on Science Technology Engineering and Management (ICONSTEM), pp. 336–341. Chennai (2017)
13. Sujith kumar, S,K.M.Y., Pravan, V., Sumathy, Thejeswari, C.K.: Novel approach for Smart Indian Railways. In: 2017 2nd International Conference on Computing and Communications Technologies (ICCCT). Chennai (2017)
14. TLiang, H., Zhang, X., Cheng, H., Wei, Q.: Secure and Efficient Image Retrieval over Encrypted Cloud Data. Security and Communication Networks (2018)
15. Rad, P., Muppidi, M., Jaimes, A. S., Agaian, S. S., Jamshidi, M.: A novel image encryption method to reduce decryption execution time in cloud. In: 2015 9th Annual IEEE International Systems Conference (SysCon), pp. 478–482. IEEE (2015)

PMI-IR Based Sentiment Analysis Over Social Media Platform for Analysing Client Review

Jyoti Patel(✉), Rahul Dubey, and Rajeev kumar gupta

Department of Computer Science and Engineering, Sagar Institute of Science and Technology, Bhopal, India
jyotibpatel1994@gmail.com

Abstract. Social media is an emerging platform where people share their opinion about any national or global issue. This opinion attract marketing and research team to analysis people sentiment over social media for their marketing of their product. The reviews of end user over social media play an important role to show the quality of products. This paper discus the analysis and the evaluation of the sentiment based on the customer review s that are available in the online for presenting the sentiment based review for the products by using point wise mutual information of opinion word. The Results shows that using modified approach gives improved efficiency on feature-based sentiment analysis.

Keywords: Sentiment analysis · NLP · Crawler · POS

1 Introduction

The analysis that is based on the sentiment is field that studies he humans feelings based on the opinions given by them. It aims in delivering more useful information regarding the human assumption on a particular area. early work in sentiment analysis appears in 2002 by Turney [1] and Pang [2], they proposed conceptual methods that applied on online reviews to detect the polarity of the individual review. Sentiment classification is also useful in business intelligence applications where user inputs and feedbacks can be processed, analysed and summarized to improve the business strategies.

2 Sentiment Analysis

Sentiment analysis is a part of Natural Language Processing (NLP). It is a field of Computer Science and Artificial Intelligence that provides interaction between computers and natural language written or spoken by humans. Natural language text could be social media contents, blogs, speech, or reviews. The purpose of NLP is to train computers to learn and understand natural language. Many task performed by NLP on natural language such as parts-of-speech tagging, stop words removal, Named Entity Recognitions, word and sentence segmentation, parsing, Information retrieval, Information extraction, subjectivity identification et.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 204–212, 2020.
https://doi.org/10.1007/978-3-030-37051-0_23

Sentiment analysis is not favorable subject for researcher before 2000; very less work has done before the evaluation of Web 2.0. This is because much less opinion contents available on the internet. Social media, blogs and shopping portals provide online platform to people to express their sentiments. Therefore huge opinion contents are available in digital forms. In 2002 Pang, Lee and Vaithyanathan [2] and Turney [1] proposed sentiment analysis methods that extract and classify the text contents as positive or negative. Since then many methods and studies has been proposed and developed by researchers to make sentiment analysis more applicable at industry level. In this chapter we discuss the different levels of SA and tasks that need to perform SA.

2.1 Components of Sentiment Analysis

- **Crawler:** This tool views all the review available in the web page and retains them. The reviews viewed are retained in a particular format called the indexing files. The indexing files keeps in reserve the review in the form of a book index with the page of the content displayed in it.
- **Preprocessing:** This step ensure the minimizing of the memory usage, by deducing the stop word in the content applying the algorithm of the stemming.
- **POS Tagging:** utilized for the assigning of the tags for the adverbs, nouns and the adjectives.

2.2 Semantic Orientation

The supervised or the unsupervised learning is utilized in enumerating the words semantic orientations.

2.3 Categories of Classification for Sentiment

(i) Supervised-Learning
(ii) Unsupervised-Learning.

(i) Supervised Learning (SL)
The SL hold labelled data sets for training, each training set has a pair of inputs and the output that are desired. The SL serves as type of machine learning for producing useful information's form the data set provided for training. There are few supervisory learning methods available which implies on text contents, these methods also called machine learning methods, these methods are used to build sentiment classifier for specific domains (Fig. 1).

(ii) Unsupervised Learning (UL)
There are few unsupervised learning methods available which used to detect subjective information from the text contents. These are machine learning methods that use statistical data acquired by using Information Retrieval systems.

Sentiment analysis applications are totally dependent on natural language processing techniques. Natural (human) language connects humans with computers. People these days largely express their sentiments in natural language especially in

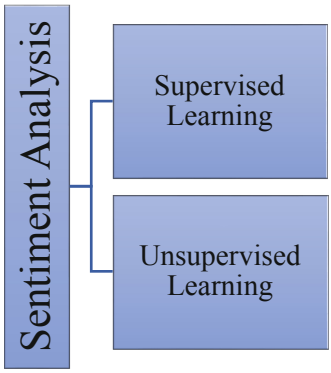


Fig. 1. Basic Sentiment Classifications technique

English (also in other languages [27]). Now day's huge amount of digital text data generated daily on internet because of social media, blogs, online shopping sites, discussion forums, online news etc. Most of these digital platforms have sentiment oriented contents. Many companies, governments and organizations use this data for the improvement of facilities and services. Natural language processing plays a crucial role in analyzing and processing text contents. Many techniques and tasks of NLPs used to extract the opinions. There are many sentiment tools like SentiWordNet [10], SentiStrength [19], Sentic Net 2.0 [28] also available which exploit the concept of natural language processing. Language processing tasks allows preprocessing that requires detecting the different features/aspects from the review text. NLP techniques help in subjectivity classification by identifying the subjective statements. Machine learning NLP algorithms investigate many statistical methods, decision making annotation to extract opinion-oriented expressions that contains sentiments.

3 Natural Language Processing

The NLP being a significant section of the artificial intelligence enables the computer to learn like humans. the latest advancement in the NLP is the methods of corpus. A corpus is set of documents that contain large set of training examples. Statistical methods used in NLPs in many tasks like word sense identification, generating grammars and parsing tree, also in finding mutual information between sentiment oriented words. Instead of writing rules by hand coding statistical methods take the inputs from the large set of training set and generate the results based on the probabilistic decisions. Each of these input are attached with real valued weights. Applying probabilistic decisions on input weights generates relative certainty of the many different possible solutions of problems.

WordNet is another machine learning tool available, is an online lexical reference system. This NLP tool contains English nouns, adverbs, adjectives and verbs organized into a synonym set. This tool used in many NLP research and techniques.

4 Literature Review

Gregory and Pasi [11] the author elaborates the significance and the procedure of the unsupervised learning over the supervised learning.Wu et al. [12] the author discusses the "Phrase Dependency Parsing for Opinion Mining" Kin [13] the paper discusses the "A Method for Opinion Mining of Product Reviews using Association Rules" Hamed and Javad [14] e-business market search engines plays an important role because of their efficient methods to find requested products quickly. Presenting a framework to extract the relative information from shopping websites helps search engine to provide better services. Search engine's components like crawler, indexer, database and graphical user interface provides effective tool for web user behavior. Crawler crawls into websites to get the useful information; indexer stores the crawled information into indexed files which fasten speed of search engine. Crawlers working on graph search algorithms treat web pages as nodes and hyperlinks as edges. Suggested framework improves efficiency by taking advantage of multiple processes, threads and asynchronous resources. We observe that improving efficiency of search engine by integrated framework helps to find helps to mine into product information.

Ye et al. [15] envision that semantic oriented based approach suggested by Turney can be used in other languages like Chinese or other languages. Tagging of words is similar by using POS tagger. Semantic oriented based classification methods are able works fine for Chinese language similar to English classification methods. We found that estimation of SO of two-word phrases of Chinese language using the pmi-ir method is same.

5 Proposed Work

The aim of the analysis and the evaluation based on the sentiment is to provide a summary based on the sentiment of the reviews presented in the webpage by the customers who visit the site. The study progresses as shown below.

Collecting product reviews or Web Crawler

To collect product reviews from e-commerce site we write a program called web crawler or web spider [14] which crawls into web pages and copy reviews and ratings of different products. These reviews and ratings are posted by users who bought products from shopping website. A web crawler is a program that can access the html contents of web page and can download the contents from web page like images, audio, hyperlinks or texts. It is possible to copy texts or images from html tags like < p > tag, < title > tag or < body > tag and < image > tag. Most of the web search engines use web crawling technique to improve the searching methods for finding efficient results. Web crawler helps search engines to update its large web database. It can download all web pages or can re-visit to pages for web processing by search engine. In our web crawler we scrap into only those html tags in which reviews, ratings of products and title of web page are stored. These reviews, ratings and title are stored in special repository or heap of memory called Inverted indexing files [19]. An inverted file is a special data structure which provides a word based mechanism for

indexing text documents. It arranges the text documents in such a manner so they can be searched easily and speedily. An inverted indexed file contains two parts first is *dictionary* which stores all the distinct words in lexicographic order from text documents and second is *posting list* which contains all the information of each word of *dictionary* like text position, number of occurrence, document ID. An inverted indexed files system is most effective structure for storing and searching the large collections of text data.

In our thesis we download the reviews and ratings using web crawler and store them in inverted files so it can be easily searched when required. The mechanism of crawler based on the TFIDF (term frequency- inverse document frequency) where TF represents the word occurrence in text documents and IDF represents document IDs in which that particular word occur. Figure 2 shows the mechanism of web crawler.

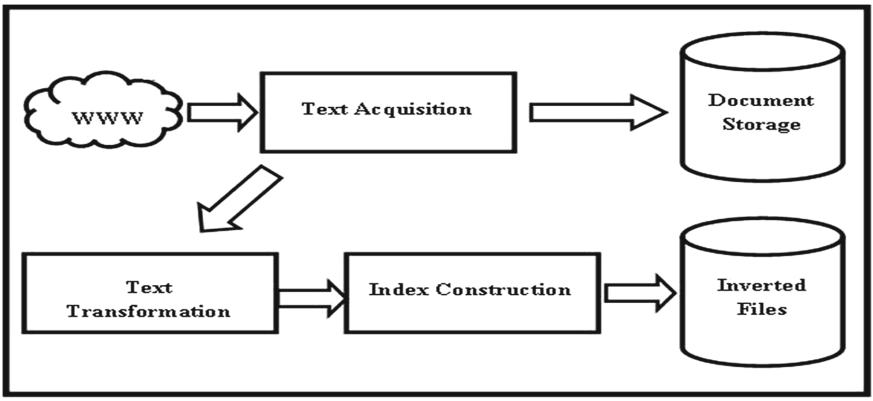


Fig. 2. Web crawler working

5.1 Text Acquisition and Document Storage

This allows downloading the necessary ratings and the reviews that are available in the website utilizing the topic based crawler that concentrates only on the specified pages in the web. The downloaded documents are stored in the document storage in the compressed form.

5.2 Text Transformation

Text documents are tokenized into index terms used for indexing and searching. Index terms are individual words. These words are arranged in lexicographical order in *dictionary*. Number of occurrence of terms their position in documents and other information is stored in *posting list*. Mapping between these two and both list are stored in inverted indexed files. It is much like metadata of text documents. Tokenization used to identify each index term.

5.3 Finding Review Sentences

We envision our work by finding those sentences where four specific features are mentioned in reviews for that product. These four specific features/aspects are *camera, battery, price* and *processor.* More important is that all four features are nouns. Most of features of products are nouns so they can be easily extracted from the large collection of reviews using POS tagger technique. All four features are common in mobiles, tablets and laptops. We choose these four features because they are frequently mentioned in product reviews and are the most discussed feature of products in reviews. The reason for finding the review sentences is that only those sentences will be processed where these four features are mentioned and other sentences will be discarded.

5.4 Parts-of Speech Tagging and Opinion Phrase Extraction

We used POS tagger on review sentences to tag the individual words. Tagging helps to access each word separately and can identify opinion oriented words. We found that combining two consecutive word express strong sensible sentiments. For example "very good", "not bad", "amazing quality", "high price", these two word phrases are extracted from review sentences. Turney [1] suggest in his research that combining two consecutive words like nouns with adjective or nouns with adverbs or adjective with verbs it is possible to extract opinion oriented phrases. These phrases describe the subjectivity and characteristics of the products. Following the patterns suggested by Turney [1].

5.5 Semantic Orientation of Phrases (Modified PMI-IR Method)

Semantic orientation of each phrase is measured by using pmi-ir method. SO is the mutual information between phrases and reference word set. This word set has 18 positive and negative words. These reference words are combined with all the extracted phrases and stored in text files. We choose 18 different positive and negative words to calculate the SO instead of using only "excellent" and "poor". These reference words display highest level of positivity and negativity.

6 Result Analysis

This work found that among 48 relevant outputs 38 outputs have positive sentiments about features that means strength of positivity (Average SO) of these feature is greater than threshold value. Similarly 10 features have negative sentiments whose strength of negativity (Average SO) is less than threshold value. The Fig. 3 shows the overall performance of our featured based sentiment analysis (Fig. 4).

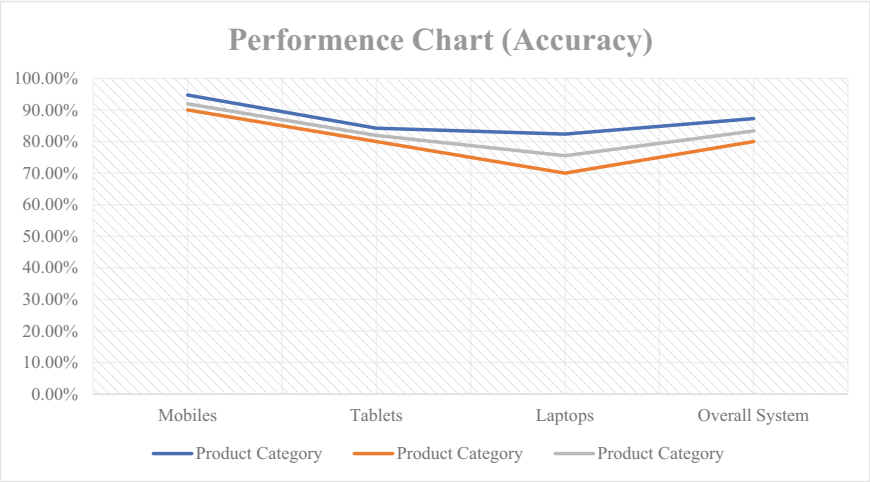


Fig. 3. Resultant Accuracy Graph

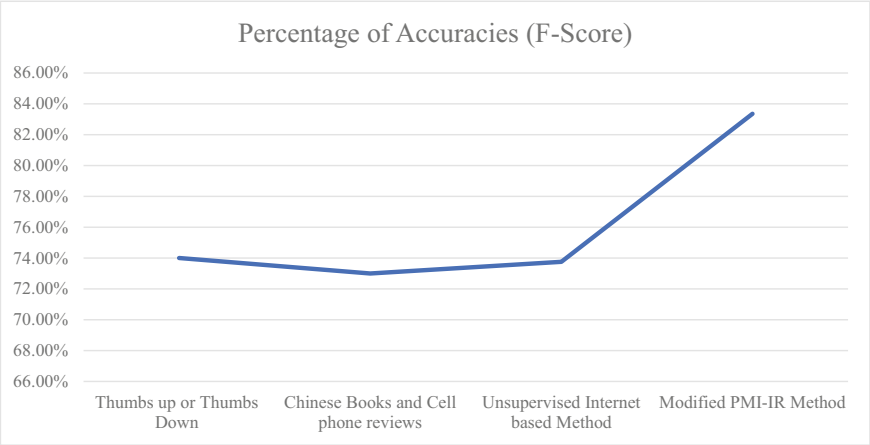


Fig. 4. F Score

7 Conclusion

Our study presents an unsupervised modified PMI-IR method of classifying opinions of features of online products as positive or negative. Sentiment analysis is currently hot topic between the researchers because of its usability in e-commerce sites and social media. Increasing use of internet and social media platform gives people to express their sentiments online. Implementation of tasks of sentiment analysis using NLP techniques makes it more challenging and interesting. The overall performance of our study is comparable to the results of semantic oriented based approach in the earlier

studies for product reviews analysis [19, 20], which range from 70% to 85%. Our system acquires 83.35% accuracy using modified pmi-ir method which is quite good as compared to other sentiment analysis approaches.

References

1. Singla, Z., Randhawa, S., Jain, S.: Sentiment analysis of customer product reviews using machine learning. In: 2017 International Conference on Intelligent Computing and Control (I2C2), pp. 1–5. Coimbatore (2017)
2. Zhang, Z.Q., Li, Y.J., Ye, Q.: Law rob sentiment classification for Chinese product reviews using an unsupervised internet based method. In: 2008 International conference on Management Science and Engineering USA (2008)
3. John, R., Julie T.: Unsupervised sentiment classification of English movie reviews using automatic selection of positive and negative sentiment items (2010)
4. Bing, L.: Sentiment analysis and opinion mining Bing Liu. Sentiment Analysis and Opinion Mining, Morgan & Claypool Publishers (2012)
5. Jindal, N., Bing, L.: Mining Comparative Sentences and Relations Copyright ©2006 American Association for Artificial Intelligence
6. Mike, T., Kevan, B., Georgios, P., Di, C.: Sentiment strength detection in short informal text journal of the american society for information science and technology, **61**(12): 2544–2558 Copyright © (2010)
7. Feldman, S.: NLP Meets the Jabberwocky: Natural language processing in information retrieval online may 1999 copyright © Information Today, Inc. (1999)
8. Santorini, B.: Part-of-speech tagging guidelines for the penn treebank project (3rd revision, 2nd Printing), technical report, Department of Computer and Information Science, University of Pennsylvania (1995)
9. Taboada, M., Brooke, J., Tofiloski, M., Voll, K.: Maite Taboada's SO-CAL program, Lexicon-based methods for sentiment analysis c 2011 association for computational linguistics, vol. 37 no. 2 (2011)
10. Mullen, T., Collier, N.: Incorporating topic information into sntiment analysis models, National Institute of Informatics (NII). Tokyo Japan
11. Gregory, G., Pasi, T.: What is a word, what is a sentence? Problems of Tokenization, https://www.researchgate.net/publication/2360239 Rank Xerox research center April (1994)
12. Wu, Y., Zhang, Qi., Xuanjing, H., Wu, L.: Phrase dependency parsing for opinion mining. Proceedings of the 2009 Conference on Empirical Methods in Natural Language Processing, pp. 1533–1541, Singapore, 6–7 Aug (2009). (c 2009 ACL and AFNLP)
13. Kim, W.Y., Joon, S.R., Kim, K.I., Kim, U.M.: A method for opinion mining of product reviews using association rules ICIS 2009, 24–26 Nov, 2009. Seoul, Korea Copyright © 2009 ACM 978-1-60558-710-3/09/11. (2009)
14. Turney, P., Littman, M.L.: Unsupervised sentiment classification of English movie reviews using automatic selection of positive and negative sentiment items. National Research Council Canada Institute for Information Technology (2002)
15. Ye, Q., Li, Y., Yiewn, Z.: Semantic oriented sentiment classification for chinese products reviews: an experimental study on books and cell phone reviews tsinghua science and technology, pp 797–807, vol 10, no. 18 (2005). ISSN 1007-0214 07/05
16. Anil K.K.M., Rajasimha, N., et. al.: Analysis of users' sentiments from kannadaweb documents.In: 11th International Multi-Conference on Information Processing IMCIP-2015 (2015)

17. Cambria, E., et al.: SenticNet 2: a semantic and affective resource for opinion mining and sentiment analysis In: Proceedings of the Twenty-Fifth International Florida, Artificial Intelligence Research Society Conference Copyright c 2012, Association for the Advancement of Artificial Intelligence (2012)
18. Milos, I., Spalevic, P.: Mladen Veinovic Inverted Index Search in Data Mining, 22nd Telecommunications forum TELFOR 2014 978-1-4799-6191-7/14 ©2014 IEEE
20. Zhongwu, Z., et. al.: Product feature grouping for opinion mining, Published by the IEEE Computer Society 1541-1672/12/ © 2012 IEEE (2012)
21. Hamed, T., Javad, H.: Information mining on the web; E-business application, 2013 international conference on advanced computer science applications and technologies 978-1-4799-2758-6/13 © 2013 IEEE

Analyzing User Awareness on Security in Android Smartphone Devices

Aedunuri Sambaraju, Muralidhar Pantula, and K. S. Kuppusamy(✉)

Department of Computer Science, Pondicherry University, Pondicherry, India
sambaraju.aedunuri@gmail.com, vijayamuralisarma@gmail.com, kskuppu@gmail.com

Abstract. Today's Digital World is evolving rapidly and the smartphone usage has became mandatory. People use smartphones to get services like email, education, business, social communication, etc. For each service category, there are plenty of applications (Apps) available in the market. Along with Apps usage, it is obvious that a user need knowledge on securing devices and private data. We analyzed Naive Android Smartphone Users (ASUs) on different Security Areas where awareness is in need to secure the device as well as the data. The responses indicates that majority of the participants have a fear of Malicious Attacks on their private data, business information and financial transactions.

Keywords: Smartphone security · Android security features · Vulnerabilities · Security awareness

1 Introduction

Smartphones comes with features that are equivalent to a PC with high speed processing, large storage, HD screens, cameras, etc. The usage of smartphone growing rapidly as the number of smartphone users expected to increase to more than 2.8 billion in 2020 (Fig. 1). Smartphones provide services to user with built-in Apps such as browser, text messenger, Apps stores, e-mail termed as system apps. And it can run a variety of third party Apps installed from online markets for different services such as mailing, chatting, social networking, entertainment, etc. The expected number of Apps to be downloaded for the year 2022 is more than 250 billion (Fig. 2).

There are a few operating systems(OSs) available for Smartphones. The popular among them are Google's Android and Apple's iOS. As per the statsta around 1.5 billion smartphones with either Android OS or iOS were sold out. Among Android, iOS and other smartphone OSs Android leads the smartphone market with 74.45% of the share and iOS with 22.85% [3]. Popularity of Android attracted App developers to target Android Smartphones by developing malicious Apps, which makes the device vulnerable to attacks such as hacking, hijacking, phishing, Malfunctioning, etc. It would be a serious problem if the ASUs unaware of these attacks and the counter measures.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 213–221, 2020.
https://doi.org/10.1007/978-3-030-37051-0_24

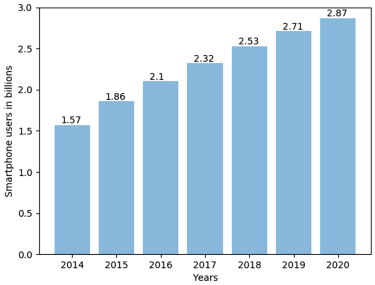


Fig. 1. Expected Smartphone Users Worldwide [5]

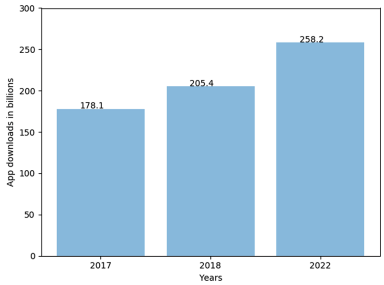


Fig. 2. Expected Apps download Worldwide [4]

ASUs must aware of security features which protect the device and the sensitive (private) data to reduce the risk of attacks. The inability of ASUs in recognizing vulnerable applications and malicious content is due to lack of awareness on types of vulnerabilities and precautions to take against them. So, it is important to the ASUs to possess the knowledge in security areas and confronting behavior with regard to information security. In this paper, we analyzed the ASUs of Pondicherry University who belong to different age groups.

2 Android Operating System

Every Smartphone needs an OS to control the functionalities of the hardware technologies (like Sensors, Camera, Fingerprint, NFC) [12]. OS is responsible in providing security, running other apps to fullfill user needs. As the Android leads the Smartphone market we presented introduction on its Architecture, App Structure and security features that Android OS provide to ASUs.

2.1 Android Platform Architecture

Android is an open source Operating System having a layered Architecture consisting of various components - Linux kernel, Hardware Abstraction Layer, Android Run Time, Android Libraries, Java API Framework, System Apps (Fig. 3).

- *Linux Kernel*: Linux Kernel make the device manufacturers easy to develop drivers for the device and allows to take advantage of key security features.
- *Hardware Abstraction Layer (HAL)*: HAL provides standard Android system interfaces (for hardware components such as Camera/Bluetooth) that allows developer to access the device hardware from Android OS feature-set [1].
- *Android Run Time (ART)*: Android RunTime (ART) used by Apps for system services that executes Dalvik executables and Dex bytecode specifications. It provides features like Ahead-of-time (AOT) compilation for tighter install time verification to improve app performance.

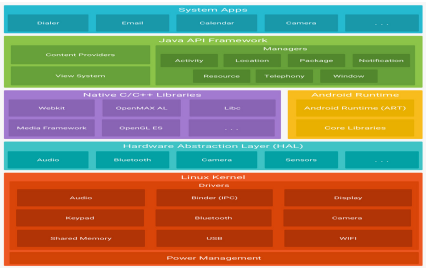


Fig. 3. Android Architecture [1]

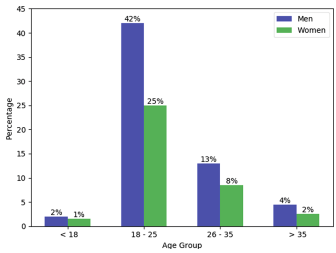


Fig. 4. Participants age groups

- *Android Libraries (AL)*: ALs consists of Android system components (ASCs) and services for ART and HAL. These are of two types: Core Libraries that support ART to write apps in Java and Native Libraries that allows Android Apps to get access to the Open Graphics Libraries (OpenGL)[6].
- *Java APIs framework Layer*: Java API Layer acts as an interface between Apps and the core of the Android Platform. It offers different services to the apps with different managers, System Views, and Content Providers [1].
- *System Apps Layer*: It consists of the basic apps that provide services such as Browsing, Calendar, mailing, SMS service, Keyboard, etc. There can be third party apps which replaces system apps for specific service.

2.2 Android App Structure

The developed Application contains the compiled code, with data and resource files archived as an Android Package (called as apk/APK) consists of the core framework components, a manifest file and resources applied to the device configurations [1].

- *App Components*: App components defines the life cycle of Android App. They are Activities, Services, Broadcast receivers, and Content providers [20].
- *The manifest file*: Components used by App can be declared in the manifest file. In Addition, it contain required permissions, the API level, features (hardware/software), and API libraries to be linked by the app.
- *App Resources*: These require to visually present App that define alternative images for different screen sizes, optimization of app for variety of device configurations, etc.

2.3 Security Features for Android Smartphone

To make Android as the safest Smartphone Platform, Google trying to develop different technologies that brace it's security and over 50 billion apps are checked daily to confirm their proper behavior [7].

- *Google Play Protect*: Google Play Protect acts as a built in malware protection with Google's machine learning algorithms as backbone to improve protection real-time [2].
- *Application Sandboxing*: Apps Sandboxing insulates and defends the installed Apps in Smartphone by stopping them to access ASU's sensitive information in between them [20].
- *Defending with designed Hardware*: For Android Platform, the hardware protects the access to device in the form of securing lock screen, verifying boot, encryption at device level [7].
- *Trusted Execution Environment (TEE)*: The TEE is a technique used for Android which provided by secure OS called Trusty. Trusty OS provides an isolated execution environment to secure App's sensitive information by executing them in TEE which is a highly secured area [8].
- *Security Updates*: For every layer in Android Platform Google reinforces security updates to all device manufacturers, in regular intervals [7].
- *User Access control*: Android Platform allows ASUs (as the Administrators) to customize App permissions in accessing App's data or hardware components [17].

3 Vulnerabilities in Android Smartphones

Android Smartphones vulnerable to attack when they are exposed to public networks to access services by always-on and always connected. There are different types of vulnerabilities with which Android Smartphones can be exploited [16] as follows.

- *Denial of Service (DoS)*: DoS vulnerability can effect the Android Smartphone by a malicious app installation or through a website. It makes the attackers service executed continuously even the malicious app is terminated [13].
- *Overflow*: This vulnerability in Android make the phone dead where ASUs can't make calls, and can't access screen [14].
- *Cross-site Scripting (XSS)*: XSS vulnerability steals credentials of the ASUs by injecting malicious scripts into trusted web pages loaded in browser.
- *Web view Vulnerability*: It is a customized web view of the web browser displaying the contents of the attacker by running customized functionalities. There are two web view vulnerabilities namely authorization and cross-zone scripting based on file [11].
- *Repackaging*: Android applications can be decompiled, modified and repacked with Attacker's code, finally published in official/unofficial market [14].
- *Android NFC*: Attacker can take full control of NFC (Near Field Communication) in Android Smartphone by using another hardware or device within distance to attack any operation can be done [9].
- *Social/Sharing Authentication Flaws*: The social Apps saving authentication details in unencrypted form can be vulnerable to that Smartphone device [14].

4 Awareness for ASUs to Secure Android Smartphones

The ASUs must focus on distinct areas relevant to information security in Android Smartphones. It is obvious that ASUs must have knowledge over security areas, and confronting behavior with regard to information security. From [19], the main security areas broadly categorized as Applications, Browsing and Accounts, Connecting Mediums, and Device. These security areas elaborated in the following sections.

4.1 Security Areas

- Application: The careless behavior of ASUs with rooted or jailbroken devices permits Apps to bypass the application sandboxing mechanism. With respect to Apps the two sub areas that ASUs must aware of are App installations and handling, discussed below.
  - Installation: In this, ASUs make sure of the App's source of installation, and permissions required by it before installing.
  - Handling: After installation, While handling the app, ASUs asked for granting required permissions, changing privacy settings and access control, and updating the app.
- Browsing and Accounts: ASUs communicate each other by surfing the Internet which in turn expose ASUs to different attacks like phishing, spam links, account hijacking, etc [13]. This area related to the browsing and device/social accounts management.
  - Browsing: While browsing, ASUs must take safety actions like avoiding unsecured websites, blocking pop-ups and spam, validating site certificates, and avoid giving personal details to distrusted web services.
  - Device/Social Accounts: Smartphones contain accounts which include customized privacy and security settings which can be hijacked by attackers to access the multimedia data, payment details and other business corresponding information. ASUs can avoid this by using strong passwords, service specific passwords, updating passwords in a regular interval, and securing those passwords appropriately [10].
- Connecting Mediums/Channels: Smartphones have connectivity technologies for information sharing through connecting Mediums (such as Wi-Fi, Bluetooth, etc) with distinct properties. Some of them have limited or no security/privacy features. To avoid ASUs falling in to these distrusted channels they can use VPNs, external security tools, and predefined settings.
  - Physical channels: Smartphones can connect to physical channels such as Wired headphones, PCs, memory cards, USB charging ports, different gadgets and accessories. These are also prone to attacks (like malicious chargers, replacement screens, etc.) [19]. So, ASUs must aware of risk in connecting to the physical channels and distrusted components.
- Device: To protect Smartphone device ASUs must have security concerns on Device OS, Data privacy, and Security systems.

- Device OS: ASUs must be careful in 'rooting' or 'jailbreaking' the smartphone to get the super user privileges. It may leads to the unofficial or unsupported OS updation used by malicious entities [18].
- Data privacy: The sensitive information abides in Android Smartphone need to be protected with privacy settings provided by the device. ASUs should use SIM card lock, setting Location on or off, encryption of data and account credentials to avoid privacy related issues [15].
- Security systems: Using security systems (system or user defined) on top of Android OS helps in scanning malware and preventing attacks in Android Smartphones [15].

5 User Awareness Survey

Participants were asked to answer the Questionnaire to analyze the knowledge on Security of Android Smartphone. The details of their responses are illustrated in this section.

1. Demographic data of the Participants: Majority of the participants (of different age groups) are 18 to 25 years of age having education as either graduation or post graduation (Fig. 4).
2. Different category of apps that participants using frequently: Majority of the participants are using Chat/Instant Messaging apps (with 92%) and Social Networking (76.5%), Browser (71%), Education (63.5%), and Entertainment (56.5%) Apps falls next in the most used apps categories (Fig. 5).

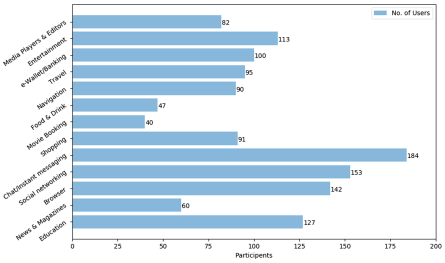


Fig. 5. Category of Apps frequently used

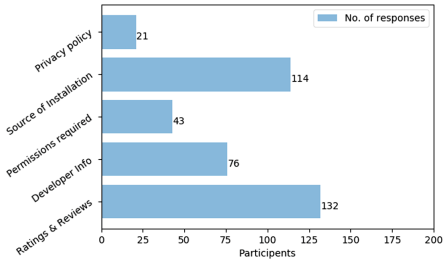


Fig. 6. Awareness on App installation

3. App Installation Concerns by ASUs: Related to App installations, from given options (Ratings & Reviews, Developer information, permission required, source of installation, and privacy policies), participants ignoring the privacy policies and permissions required (Fig. 6).
4. App Updation Awareness by ASUs: Regarding App/OS updations, the participants (51%) are thinking its only for the Feature Updation. Most of them are unaware of the fact that the updations meant for security patches and boosting efficiency (Fig. 7).

5. Type of data User thinks private: The responses reveal that multimedia data (like pics, videos, and voice notes) and chat history are considered as more private to them (Fig. 8).

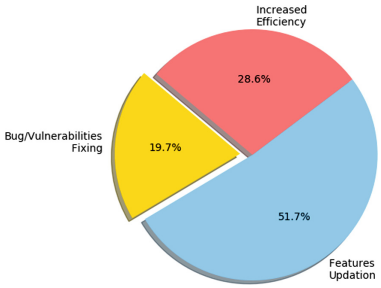


Fig. 7. Awareness on App updations

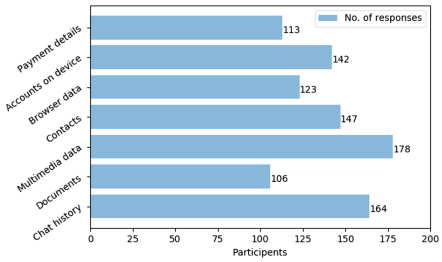


Fig. 8. Type of data considered Private

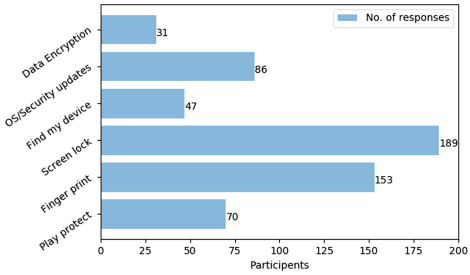


Fig. 9. Awareness on Android Security Features

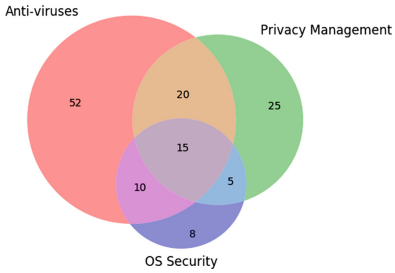


Fig. 10. Awareness on different security systems

6. Android Security Features awareness: Majority of the participants are unaware of the major security and privacy protection features (like Find my device, and Data Encryption) provided by the Android OS (Fig. 9).
7. Awareness on Security Systems Usage: Participants aware of additional security systems and Android OS Security usage. But, majority of respondents are aware of Antivirus systems (52) and Privacy Management Applications (25) and few (15) are using combination of all (Fig. 10).

6 Conclusion

Android has become a prominent smartphone OS used by more than 70% of the users. Android architecture eases the use of Apps and its openness allows attackers to target the Android devices for ASU's sensitive information by developing malicious Apps. We've surveyed the vulnerabilities (affects ASU's information)

and counter measures (exploits vulnerabilities). In this article we imposed set of questionnaire on ASUs targeting awareness of security in Android Smartphones. The analysis revealed that ASUs lack of knowledge on Android OS security features and usage of security systems. In this regard we are about to develop an Android App which provide knowledge on various security aspects and gives count that indicates the Freshness score of Android Smartphone.

7 Compliance with Ethical Standards:

All author states that there is no conflict of interest. We used our own data. Humans/aniamls are not involved in this research work. We used our university students and got approval from the university.

References

1. Android, platform architecture. https://developer.android.com/guide. Accessed 15 Feb 2019
2. Google play protect. https://www.android.com/intl/en_in/play-protect/. Accessed 11 Feb 2019
3. Mobile operating system market share worldwide. https://gs.statcounter.com/os-market-share/mobile/worldwide/2019. Accessed 10 Feb 2019
4. Number of mobile app downloads worldwide in 2017, 2018 and 2022. https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/. Accessed 10 Feb 2019
5. Number of smartphone users worldwide from 2014 to 2020. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. Accessed 10 Feb 2019
6. OpenGL ES. https://developer.android.com/guide/topics/graphics/opengl.html. Accessed 12 Feb 2019
7. Protect every android user,hardware designed to defend and regular security updates keep things in order. https://www.android.com/security-center/. Accessed 15 Feb 2019
8. Tee in android development by varun malhotra. https://dzone.com/articles/overview-tee-in-android. Accessed 09 Feb 2019 (published on 10 Jan 2018)
9. Top mobile vulnerabilities and exploits of 2012, darkreading. https://www.darkreading.com/top-mobile-vulnerabilities-and-exploits-of-2012/d/d-id/1138833. Accessed on 18 Feb 2019 (Published on 12 Dec 2012)
10. Adams, A., Sasse, M.A., Lone, P.: Making passwords secure and usable. In: People and Computers XII, p. 15. Springer (1997)
11. Chin, E., Wagner, D.: Bifocals: analyzing webview vulnerabilities in android applications. In: International Workshop on Information Security Applications, pp. 138–159. Springer (2013)
12. Divya, K., Kumar, S.K.V.: Comparative analysis of smart phone operating systems android, apple ios and windows. Int J Sci Eng Appl Sci (IJSEAS) **2**, 432–438 (2016)
13. Goel, D., Jain, A.K.: Mobile phishing attacks and defence mechanisms: State of art and open research challenges. Comput. Secur. **73**, 519–544 (2018). (Elsevier)
14. Hur, J.B., Shamsi, J.A.: A survey on security issues, vulnerabilities and attacks in android based smartphone. pp. 40–46 (2017). (IEEE 978-1-5386-2186-8/17)

15. Park, J.H., Yi, K.J., Jeong, Y.S.: An enhanced smartphone security model based on information security management system (ISMS). Electron. Commer. Res. **14**, 321–348 (2014). https://doi.org/10.1007/s10660-014-9146-3 (Springer Science and Business Media)
16. Joshi, J., Parekh, C.: Android smartphone vulnerabilities: A survey. 5 (2016). (IEEE 978-1-5090-0673-1/16)
17. Ahvanooey, M.T., Li, Q., Rabban, M., Rajput, A.R.: A survey on smartphones security: software vulnerabilities, malware, and attacks. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **8**(10), 16 (2017)
18. Miller, C.: Mobile attacks and defense. Secur. Priv. IEEE **9**(4), 68–70 (2011)
19. Bitton, R., Finkelshtein, A., et al.: Taxonomy of mobile users' security awareness. Comput. Secur. **73**, 266–293 (2018). (Elsevier Publication)
20. Yadav, S., Apurva, P.R., et al.: Android vulnerabilities and security. In: International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), pp. 204–208 (2017). (IEEE 978-1-5386-0627-8/17)

A Systematic Review of Different Data Compression Technique of Cloud Big Sensing Data

I. Sandhya Rani[1,2(✉)] and Bondu Venkateswarlu[1]

[1] DayanandaSagar University, Bangalore, India
isandhya.85@gmail.com, bonduvenkat-cse@dsu.edu.in
[2] BCET, Bangalore, India

Abstract. Sensing devices like camera, satellite, earthquake monitoring, video etc., are producing large number of data. Big data techniques paves the way for the handling the more number of data along with streaming data. Cloud computing technology make it easy to store, access and manage the data with low cost. The data compression techniques helps to minimize the data in the cloud and store the data effectively. The aims of the study is to provide a systematic review of the data compression on big sensing processing. The image compression is used to minimize the size effectively and useful for the cloud environment. The deduplication technique is another method is used to compress the data in the cloud and helps in minimize the size. The clustering based compression technique process the cluster for similar data. The three kinds of compression technique in the cloud are investigated in this study. The investigation of this methods shows that the compression technique is still need to be increased in the manner of scalability and flexibility.

Keywords: Big data · Big sensing processing · Cloud computing · Clustering based compression · Data compression · And scalability

1 Introduction

The email, blogs, RSS feeds, social networks, Internet of Things (IoT) etc., are producing large number of data and are stored in cloud. This increases the challenges for the batch learning system such as expensive retraining to process the streaming of data. The development of the IoT in the various fields involves in creating large volume of sensing data. For examples, the amount of sensor data by sensor based management system is huge that makes the storage and management inconvenient. Processing and analyzing of data is also challenging and time consuming function due to abundant data available from the scientific workflows technological advances in sensors, detectors etc. [1–3]. Such kinds of data requires large storage space and more time for execution. So, the compression techniques are necessary for Big data to represent small subset of them. Since the presence of contemporary user data compression technique is common and these methods are efficient due to the available of GPU system.

Cloud computing has the many advantages to store the big data and process them with the considerable performance. In many real world applications like social

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 222–228, 2020.
https://doi.org/10.1007/978-3-030-37051-0_25

networks, big sensing process, scientific analysis of protein interaction etc., it is negligible to deal with the big graph data streams and big graph data [4]. The challenge is to adapt the method for the streaming of data and processing the large data for processing. The data compression technique consume more power and data compression take time that delay data transmission. To solve this issue, a theoretical model of data gathering networks with data compression techniques has been recently formulated by some researchers [5]. The main aim of this review is to analyze the recent research in the data compression of big data on cloud in the data sensing processing. The latest research on the data compression are investigated with advantages and limitations.

This paper is organized as analysis of various data compression on cloud is provided in the Sect. 2 and comparison of several methods of data compression with advantages and limitations are given in the Sect. 3.

2 Data Compression of Big Sensing Processing

More number of data is generated every data and this is the big data era, that creates new scientific challenges for big sensing data processing. The data from the sensing system like camera, video, satellite etc., is having more size. The cloud computing provides the way to store the more number of data and make it simple to handle. The general architecture of the data compression of big sensing processing is shown in the Fig. 1.

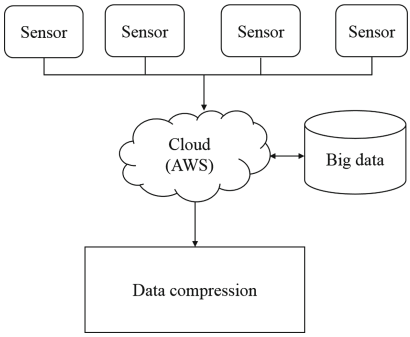


Fig. 1. The general block diagram of data compression in big data processing

2.1 Big Data

BIG DATA is the new scientific trend. Driven by the data analysis in the high dimension data, Big data find the correlation between the data to insight to the inherent process. The problem is not all the data are relevant and one of the difficulties is that the obtained information can be noisy, biased, incorrect, misleading, outdated, and thus unreliable. Hybrid storage provides the promising solution for managing the large data at low cost that provides large storage capacity and at high speed. Hybrid storage method distribute the data on the different devices based on the data's performance benefit.

2.2 Cloud Computing

Cloud computing has the many advantages to process the Big data and much helpful for the academic students and professionals. The tech giants like Amazon, Microsoft, Google etc., are provide their cloud services. This provide new way to store the data in the remote storage at the low cost with high reliability IoT embedded that generates the Big data.

2.3 Big Sensing Processing

The connected objects and mobile devices develop the IoT and this technology is utilized by the various professionals. The data has been chucked to transmit to the cloud storage and the data can be processed in the cloud for the effective performance. The cloud computing provides the effective solution for the IoT big data processing task.

2.4 Review on Compression of Big Streaming Data on Cloud

The data compression in single modality and multiple modality method based on deep learning approach, which involves in acquires data characteristics and dynamic networks. An energy efficient model has been developed for the data compression technique and each user can able to collect the data and transmit to the health care system. The investigation of this method shows that the single modality compression technique.

The photo album compression approach based on feature is given in the research [6] and this is based on the local features rather than pixel value in analyzing. As the pseudo sequence is much more complicated than natural video, further proposes the three step process to decrease redundancy of inter-image based on the local features. The evaluation of the feature based compression technique shows that this local features are 10 times more efficient than the JPEG compression.

Parikh et al. [7] proposes the High Efficiency Video Coding (HEVC) technique for the medical image compression to increase the compression efficiency than the conventional JPEG 2000. The lossy compression in medical image compression are analyzed in this research. The testing of proposed HEVC method in the compression shows that this method has the compression performance of 54% over JPEG 2000.

Hua et al. [8] proposed a remote communication service named as Neptune to increase the efficiency. Neptune effectively transmit the large data between the distance data center based on a cost-effective filtration method. The filtration method is interpreted to minimize the redundancy and compress the similar files. Usually, these are processed individually in the existing methods. The chunk level compression is followed in the Neptune to eliminate the duplicate files and uses approximate delta compression technique to compress the similar files. Neptune make use of locality aware hashing method to group the similar file and proposed the short distance for the data recovery that helps to reduce the computation overhead and complexity. Delta encoding method highly reduce the redundancy. The unique deltas collections are considerably more space efficient than their non-encoding equivalents. Encoding deltas

need to compress the difference between target and source file as a delta. The data flow of the research in compressing big spatial data [9] is shown in the Fig. 2.

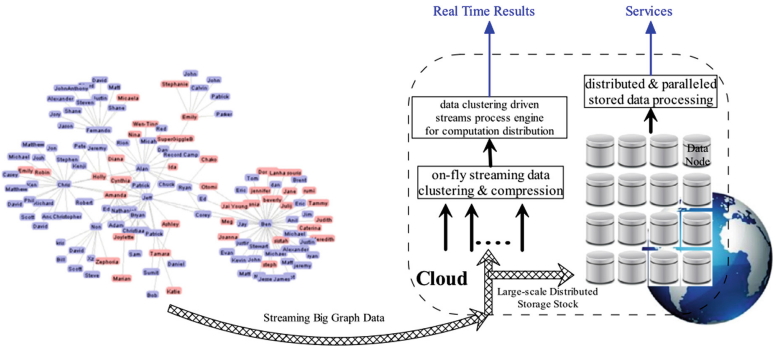


Fig. 2. The framework of the compression of big data in the cloud [9]

3 Comparative Analysis

The process big sensing data involves in the costly in terms of space and time on the cloud platform. Many methods are proposed and developed to decrease the cost and improve the performance. The recent method of compression technique for the cloud data are investigated in the Table 1.

Table 1. Quantitative comparative analysis

Author	Methodology	Advantages	Limitations	Performance evaluation	Data and platform
Yang et al. [9]	The scheduling algorithm is developed for the optimization of data process	The data size is reduced effectively and low fidelity loss is achieved	The more correlation is need to be analyzed for the effective performance on big data and scheduling techniques is not flexible	The accuracy is achieved around 95% and error bound is less than 2%	U-Cloud platform Sound and vibrational data stream from 500 nodes
Deng et al. [10]	Proposed an online Direction Preserving Trajectory Simplification (DPTS) and Bound Quadrant System (BQS) to minimize the compression time	The compression time and construction of graph is highly reduced by GPU aided method	The efficiency of the method are need to be increased	The compression time is reduced up to 21% and compression time for this method is 3.95 times faster than DPTS	GeoLife dataset and T-drive dataset

(*continued*)

Table 1. (*continued*)

Author	Methodology	Advantages	Limitations	Performance evaluation	Data and platform
Hou et al. [11]	There are two designs are made to compress the Motion capture data with low latency The first method involves in process the data in the frame by frame manner and this is efficient in mocap data	This method has the higher compression performance with low latency and low cost This method can be applicable to various mocap data	The efficiency is need to be increased and error value is high	The computational cost is low, the implementation is easy and compression performance is high	Motion Capture database
Hsu [12]	This research proposed a method based on the three-dimensional histogram Competitive Hopfield Neural Network (CHNN) clustering The Block Truncation Coding (BTC) and regularization are processed in this method The cluster region is analyzed by the modified BTC with various compression rates depend on its importance	The proposed method has the high flexibility and has better performance than several existing method This method is convenient for the telemedicine and long term care	The scalability of the method are need to be improved	The PSNR for three dataset is 34.378, 32.064, and 31.222	Medical datasets

The MapReduce algorithm is tested for this review to analyze the performance and this algorithm has been implemented using 1 master and 2 slaves. The dataset size is set as 1.4 KB and analyze the 2 commonly used text compression method. The achieved compression rate is 724 Bytes by this MapReduce algorithm.

4 Conclusion

The IoT devices like camera, satellite, earthquake monitor etc., generates the more number of data in the cloud. The Big data technique helps to handle these data and store them effectively. The data compression technique in the cloud helps to manage the data and decrease data size. Many research are presented to provide the data compression in the cloud to increase the efficiency and scalability. The data compression of streaming data are important for cloud stores the sensing device data. The three kinds of data compression technique like cluster based data compression, image compression and deduplication are briefly analyzed in this review. The research of [9] shows the effective compression, where data compression is carried out in the data chunks. The cluster based compression shows the effective compression compared to the other methods. Although, most of the study shows the effective compression and some research provides scalability, there is still need to improve the flexibility and effectiveness.

References

1. Nguyen, T.T., Nguyen, T.T.T., Quoc, A.V.L., Nguyen, V.H., Liew, A.W.C., Stantic, B.: Multi-label classification via label correlation and first order feature dependance in a data stream. Pattern Recogn. **90**, 35–51 (2019)
2. Yu, Y.U., Guo, Z.W.: Sensor data compression based on MapReduce. J. China Univ. Posts Telecommun. **21**, 60–66 (2014)
3. Jung, E.S., Kettimuthu, R., Vishwanath, V.: Cluster-to-cluster data transfer with data compression over wide-area networks. J. Parallel Distrib. Comput. **79**, 90–103 (2015)
4. Tabata, K., Sato, M., Kudo, M.: Data compression by volume prototypes for streaming data. Pattern Recogn. **43**, 3162–3176 (2010)
5. Chłopkowski, M., Walkowiak, R.: A general purpose lossless data compression method for GPU. J. Parallel Distrib. Comput. **75**, 40–52 (2015)
6. Shi, Z., Sun, X., Wu, F.: Photo album compression for cloud storage using local features. IEEE J. Emerg. Sel. Top. Circuits Syst. **4**, 17–28 (2014)
7. Parikh, S.S., Ruiz, D., Kalva, H., Fernández-Escribano, G., Adzic, V.: High bit-depth medical image compression with HEVC. IEEE J. Biomed. Health Inform. **22**, 552–560 (2018)
8. Hua, Y., Liu, X., Feng, D.: Cost-efficient remote backup services for enterprise clouds. IEEE Trans. Ind. Inform. **12**, 1650–1657 (2016)
9. Yang, C., Zhang, X., Zhong, C., Liu, C., Pei, J., Ramamohanarao, K., Chen, J.: A spatiotemporal compression based approach for efficient big data processing on cloud. J. Comput. Syst. Sci. **80**, 1563–1583 (2014)

10. Deng, Z., Han, W., Wang, L., Ranjan, R., Zomaya, A.Y., Jie, W.: An efficient online direction-preserving compression approach for trajectory streaming data. Futur. Gener. Comput. Syst. **68**, 150–162 (2017)
11. Hou, J., Chau, L.P., Magnenat-Thalmann, N., He, Y.: Low-latency compression of mocap data using learned spatial decorrelation transform. Comput. Aided Geom. Des. **43**, 211–225 (2016)
12. Hsu, W.Y.: Clustering-based compression connected to cloud databases in telemedicine and long-term care applications. Telemat. Inform. **34**, 299–310 (2017)

A Survey on Big Data Solution for Complex Bio-medical Information

Meena Moharana(✉), Siddharth Swarup Rautaray, and Manjusha Pandey

School of Computer Engineering, KIIT University, Bhubaneswar, Orissa, India
meenamoharanall@gmail.com, manjushapandey82@gmail.com, siddharthfcs@kiit.ac.in

Abstract. Today's healthcare system deals with a huge data that needs a larger storage space and proper updating phenomenon. It is so obvious that big data is a buzz word in the field of healthcare. Not only specific to engineering field it ranges from institutional to organizational domain. Also its techniques not only helpful for doing research also in storing, manipulating with the observational or stored data. Many online based companies adopt big data analytical techniques for developing assets or medical equipment, so that respective domain can be benefited while providing treatment to patients. There are such companies' deals with genomic data and helps in finding the specific reason to particular disease. Applying the big data techniques in medical data helps in finding best result and provide proper treatment to patients. Now it is possible to avoid such difficulties found in past time on giving treatment to patients through traditional methods.

Keywords: Healthcare and big data · Big data in medical research · Examples to complex biomedical information · Personalized medicines

1 Introduction

Exponential growth of huge amount of data in healthcare, which have an onset theory of doing the manipulation with the information of patients regarding various health issues and required well maintained database. Laboratory observations to doctor prescription maintained a well formatted database. Study reveals, observational and experimental data require more synchronised system so that patient records have been well maintained. Insufficient data storage facilities, lack of proper knowledge and experience are the major hurdle to manage medical data, laboratory experiment and observations. Medical information kept, processed and diagnosis of any disease particular to any patients through computerization. It is important to every patients that the data regarding medical issues, pathological observations should be well maintained and managed for getting error freed diagnosis of disease, as well for concerned physiology. It is quite difficult to manage and absorb such DNA pattern, protein sequences, any changes in human cell or any disorders found in human body that are present in higher dimension. Somehow difficulties arise with such complex pattern and higher dimension while analysing and diagnosing disease which is that a normal eye could do with more perfection.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 229–237, 2020.
https://doi.org/10.1007/978-3-030-37051-0_26

Dermatological changes to human body, disorder to nervous system, any fatal disease, cardio vascular or any infectious disease to human, the researcher subsequently analyses and mapped various learning techniques with the high dimensional data. One of the bigger problems is that the communication and proper interaction between patients and physician somehow leads to miss interpretation or wrong diagnosis of disease. Some time it leads to serious and un-filled mistake. Medical analysis or any diagnosis of disease requires the linkage between other recourses. Data extraction may be in terms of text mining or data mining, needs the linkage to other resources, and demands to have huge data or information. Any sequence of genomic expression or any oral or sound records and integer data needs proper repository where both therapist and disease carrier be help full, most important researcher be more beneficiary to data extraction for their worthy research and also for developing latest technology relate to medical science. It needs hundreds and hundreds of data repository linkage having number of intra and inters connected data bases. However largely developed databases are independent as well they are inter-connected naturally and offers a vast of knowledge and hence give the information about interrelated biomedical entities such as specified drugs, particular diseases to particular patients, genomes and its structure, patients, clinical trials and observations, researchers and agencies [1]. It is very common in exploiting the linkage between intra and inters connected medical recourses which are very specific to particular medical issues.

It is often observed that many of the symptoms are the cause of some of the disease and somehow very common to more than one disease i.e. some of the cause are common to more than one disease. Many disease categorised or belongs to one categories like fever, diarrhea, cold and cough, other such type of disease are categorized under infectious disease, blood pressure, diabetes, cancer or cardiovascular disease all are categorized to chronic disease and also all heart related disease like asthma and chronic obstructive pulmonary disease (COPD) or failure of heart are sub categorized under cardiovascular disease. Likewise there are several other health issues that need proper maintain of database. One database has more than one linkage between other databases which would be helpful in finding solution to more complex medical issues. Rather searching one database it will search whole data storage system to any health issues. Hence it can't be possible of handling this huge data or any medical observation through traditional database management system, hence needs some more storage space as well some latest technology to store huge amount of data in well maintained format. More often, the medical data or clinically recorded data, may be structured or unstructured are thus collected and stored electronically. As on demand, of a good system, it is necessary that the data collected must be sufficient or as enough as one can develop a carrier between patient and healthcare structure. Because more the information and have the fare history of patient record, best will be the treatment procedure. Maintaining the fare history record regarding patient health condition, leads to develop or it will beneficiary to deal with a good medical system. Either through EMR or EHR medical data has been collected. EMR i.e. electronic medical records is a way of keeping the data in a digital way rather keeping and maintaining the data through traditional way for each and individual patient [2]. The EHR technology is what exactly the EMR, of keeping the health issues electronically. Not only observed integer data but medical images i.e. MRI, vocal recorded data all can be managed through big data.

It is very necessary that data should be managed in a synchronized through interconnected dataset to each other. Such data are very much use full in terms of diagnosis as well for any kind of medical research because now-a-days one field is not limited to only that field. Researchers from other background show much interest in medical domain for which updated data is needed. In recent trends so many web base companies are showing interest in storing medical or health regarding dataset like PubMed, Medicare/Kaggle, and MEDLINE. Also there are so many such web based companies which put in interest to provide various healthcare solutions to different issues.

2 Healthcare and Big Data

MRI data signal processing data or any numerically observed data are all along need proper synchronized database. Big data help in storing, manipulating or processing with meta data which are kept in different inter connected dataset. It is necessary that patient current pathological observation along with history of patient should be well maintained and it will be with different technology like EHR i.e. electronic health record or EMR i.e. electronic medical record and it is very obvious that all are regularized and practised through big data analytics. EMR under goes various steps to keep and processed the electronically observed data. The given Fig. 1 shows how EMR going through different steps to store and manipulate with data whether it is sound signal or processed image or any observation through pathological or clinical data along with concerned chemist, druggist or doctors. EHR/EMR [3], before a couple of year, it was touted or consider as a key for increasing the quality of care. In recent trends, providers use the recorded patient data for increasing the quality of outcomes through care management programs.

2.1 EHR

EHR technique helps in finding any queries regarding health issues to any patient. The technique kept all the information related to patient's lab observation, physician report with unique patients ID. So that when diagnosis of disease takes place, it will help in retrieving the patient details that give the summary of exactly the patient suffering from which disease. On the basis of EHR when after storing data, the data can properly be classified as well indexing of stored data could be possible. But when large data required classification or indexing, or storing and multiplication of patients, this is become very easy while applying Big Data technique.

2.2 Big Data and Medical Research

Big data spurt most of the healthcare data that are consists of unstructured information which is difficult to analyze and develop a well defined methodology for any domain specific like healthcare, or for any organization. Real fact behind big data it is not confined to a certain facilities, due to its properties like variety, velocity and veracity [6] it is much more than it is and apogee a new challenge, opportunities & provision in the area of medical domain in the coming years. It needs a convey in computational

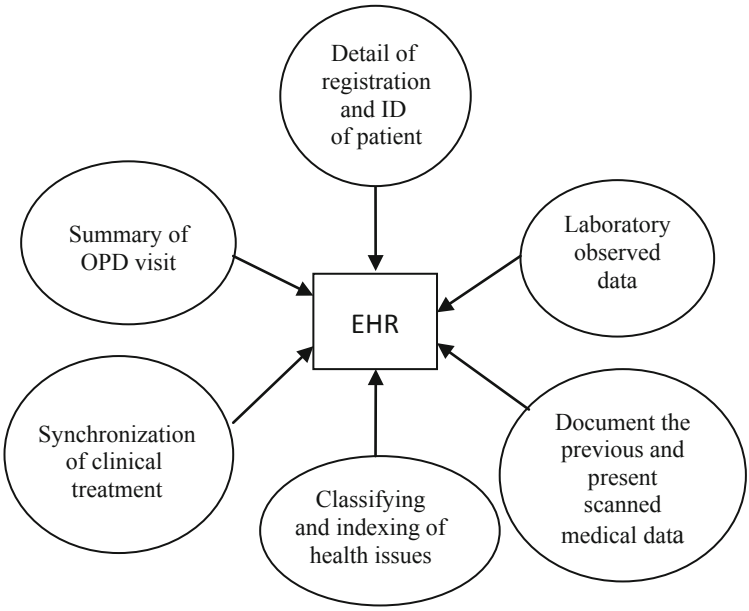


Fig. 1. Schematic representation of EHR

intelligence so that researchers or developers could able to handle and process over data easily.

Knowledge and insights gathered with the help of the tools that need to from huge accretion of unstructured data available through different source like web search that are improving at this task. There are number of institutions like NIH [8] and companies which they provide solution to generates, decipher, analyze and visualize combined clinical and omics data [2]. There are number of companies provide clinical data set which would be helpful for researcher as well clinicians. Some of them sited below with the respective web browsing sites [2, 5] (Table 1).

2.3 Examples to Complex Biomedical Information

There are the some of the companies who provides the solution to various healthcare issues for academic researchers, software developers and mostly pharmaceutical and medical researchers.

2.3.1 DELL Healthcare Solutions

It gives the solution regarding any healthcare issues. The DELL Healthcare company provide the proper techniques and technology with which the researchers do their research to monitories the total healthcare system be a information driven healthcare system that will accelerate the innovations towards research in new area or sub area of medical data science. The respective company give a move on through number of innovations in life cycle with medical records stored electronically.

Table 1. Different type database repository and web site

Web based company	Web search address
Nextbio	http://www.nextbio.com
DNAnexus	http://www.dnanexus.com
Genome International Corporation	http://www.genome.com
GNS Healthcare	http://www.gnshealthcare.com
Pathfinder	http://www.pathfindersoftware.com
Context Matters	http://www.contextmattersinc.com
Appistry	http://www.appistry.com
Beijing Genome Institute	http://www.genomics.cn/en
CLC Bio	http://www.clcbio.com
Pathway Genomics	http://www.pathway.com
Foundation Medicine	http://www.foundationmedicine.com
Knome	http://www.knome.com
23andme	http://www.23andme.com
Counsyl	http://www.counsyl.com
Personalise	http://www.personalis.com

Example: http://www.dell.com/Learn/us/en/70/healthcaresolutions?c=us&l=en&s=hea.

2.3.2 IBM Healthcare and Life Sciences

IBM Healthcare and Life Science Company provide latest analytical techniques and solutions related to the different healthcare issues and enable the particular health organization to retain greater efficiency along with different operations of health issues of patient by merging structured and unstructured data. Thus collaborating the information gathered, the IBM healthcare company provide more improved results and merge the respective in a new way of developing the more tenable, patient-centric system with more personalized databases.

Example: http://www-935.ibm.com/industries/healthcare.

2.3.3 Intel Healthcare

Intel healthcare helps in making the frame work for IT tools for health issues. The respective company also provides the services to the governments sector, various healthcare organizations different technology innovators worldwide. The company combines the various data regarding health issues and provide best solution to different issues.

Example: http://aws.amazon.com.

2.3.4 Amazon Web Services

Amazon Web Service is a web based company that provides necessary computing to reserve solution to the different healthcare organization. The company thus create the environment that includes CPUs, storage place like RAM, ROM, networking, operating system for the sake of hardware infrastructure. This provides the necessary

service in the field of healthcare and scientific research area, and also in scientific field in case of biomedical fields.

Example: http://aws.amazon.com.

2.3.5 GE Healthcare Life Science

It furnishes the expatiation and tools for the wide range application. It includes research like drug discovery research, research about cells and proteins as well provides tool for supporting large-scale manufacturing companies of bio-pharmaceuticals.

Example: http://www3.gehealthcare.com/en/Global_Gateway.

2.3.6 Oracle Life Sciences

Key functionalities that has been delivered in making of pharmaceutical, medical device companies and also for biotechnology. Market products that will help in treating specific diseases which increases the chances of discovering and bringing the more possibilities through Oracle life science.

Example: http://www.oracle.com/us/industries/life-sciences/overview/index.html.

2.3.7 Cisco Healthcare Solutions

Cisco Healthcare Solutions offers numbers of various solution to the life science, that have includes cloud computing and specified assets. In includes more secure and highly reliable data has been communicated and shared across the healthcare community.

Example: http://www.cisco.com/web/strategy/healthcare/index.html.

3 Personalized Medicines

Day-to-day huge amount of omics data needs proper treatment as storing, analyzing, visualization of data, re-arrangement of stored data [9, 12, 14]. Big data provide its advanced analytic techniques to fulfil the needs of data to resolve medical issues. Omics data has been used to produce ‘short’ reports on stored data for researcher and clinicians for their further research oriented work. Short reports are valuable in terms of finding new solution or treatment method to healthcare problem. The new genomic industry required the transformation techniques to deal with huge omics data for solving conventional health care issues [17]. Somehow cloud computing is the cause of evolution of genomic industry and providing the solution that has been transplanted in the medicines and life science world. There is also another solution to deal with genomic data that changes the path that has been adopted for the transformation and utilization of genomic data. Graphics processing unit (GPUs) is the technique to big data which improves in computational power as well, brings the improvement in conventional approaches to medical science (Table 2).

Table 2. Different companies for personalized medicines and omic solution

Company	Websites	Services
Personalis	http://www.personalis.com	It is a genomic-scale diagnostic service centre provides accurate genetic sequence data
Foundation	http://www.foundationmedicine.com	It is a molecular information company provide routine clinical care to cancer patient
Pathway Genomics	http://www.pathway.com	Address a variety of medical issues, incorporates customized and scientifically validation of data
Knome	http://www.knome.com	Analyze data through software based test for gene network as well genomes
23andme	http://www.23andme.com	Provides educational tool and information to each and every individual to learn and for their research on DNA analysis
Counsyl	http://www.counsyl.com	Provide the test for genome mutation and validation

3.1 Counsyl

Counsyl is the genetic based testing companies that help in finding afterbirth disease in offspring of a couple. It screens upon genes of both the partner for 100+ genetic diseases that could be passed on to their child. Since 2008 it give the service to genetic test and claims that the genomic test could help in giving the practical applications in so many life changing decision.

Web address: http://www.counsyl.com.

3.2 Foundation

Foundation, a world-leading molecular insights company that connects physicians and patients with lab observations for the latest cancer treatment approaches and making exactitude medicine to reality for thousands.

Web address: http://www.foundationmedicine.com.

3.3 Knome

Knome is one of the genome interpretation company that helps in analyzing the human gene structure for improving the human living style. It apply the scientific insights to the human genome for identifying the specific variant, genes & its set of genes which are very specific to particular disease or particular disease is responsible for which particular gene or gene set [16]. The company helps many academic, pharmaceutical and medical researchers providing services and products on human genomes [3].

Web address: http://www.knome.com.

4 Conclusion

Medical data and big data both are dealing with a huge data collections and from the study we found that the requirement of day-to-day medical or healthcare domain, that should be well managed and should be updated the patient's health records of pathological with physician observations. And big data analytics provides a vast technical support to deal with omic data. For which complications to critical issues of any patients can now easily diagnosis on applying big data techniques. So many company come to front with idea of big data analytic techniques and apply in the medical domain for solving many problems what both the academic and medical researcher faces problems while dong their researchers.

We found, the strategies of big data analytic techniques have provide numerous facilities in terms of methodology or techniques while dealing the pathological observations, gene and its set for genomic problem and also many company deployed the ideas of same for developing many medical equipments or accessories to avoid or overcome the difficulties that were faced in past time while diagnosing the disease. The study is a further step that might be helpful in getting the knowledge of how big data analytics is required while handling omic data of medical or healthcare data or information [15–17].

References

1. Anupindi, T.R., Srinivasan, P.: Disease comorbidity linkages between MEDLINE and Patient Data. In: 2017 IEEE International Conference on Healthcare Informatics (ICHI), pp. 403–408. IEEE (2017)
2. Costa, F.F.: Big data in biomedicine. Drug Discov. Today **19**(4), 433–440 (2014)
3. Wikipedia providing information about EHR. https://en.wikipedia.org/wiki/Electronic_health_record
4. Howe, D., Costanzo, M., Fey, P., Gojobori, T., Hannick, L., Hide, W., Hill, D.P., et al.: Big data: the future of biocuration. Nature **455**(7209), 47 (2008)
5. Luo, J., Wu, M., Gopukumar, D., Zhao, Y.: Big data application in biomedical research and health care: a literature review. Biomed. Inform. Insights **8**, BII-S31559 (2016)
6. Bellazzi, R.: Big data and biomedical informatics: a challenging opportunity. Yearb. Med. Inform. **23**(01), 08–13 (2014)
7. Raghupathi, W., Raghupathi, V.: Big data analytics in healthcare: promise and potential. Health Inf. Sci. Syst. **2**(1), 3 (2014)
8. Margolis, R., Derr, L., Dunn, M., Huerta, M., Larkin, J., Sheehan, J., Guyer, M., Green, E. D.: The National Institutes of Health's Big Data to Knowledge (BD2K) initiative: capitalizing on biomedical big data. J. Am. Med. Inform. Assoc. **21**(6), 957–958 (2014)
9. Elsebakhi, E., Lee, F., Schendel, E., Haque, A., Kathireason, N., Pathare, T., Syed, N., Al-Ali, R.: Large-scale machine learning based on functional networks for biomedical big data with high performance computing platforms. J. Comput. Sci. **11**, 69–81 (2015)
10. Mittelstadt, B.D., Floridi, L.: The ethics of big data: current and foreseeable issues in biomedical contexts. Sci. Eng. Ethics **22**(2), 303–341 (2016)
11. Weber, G.M., Mandl, K.D., Kohane, I.S.: Finding the missing link for big biomedical data. Jama **311**(24), 2479–2480 (2014)

12. Luo, P., Tian, L.P., Ruan, J., Wu, F.X.: Disease gene prediction by integrating PPI networks, clinical RNA-Seq data and OMIM data. IEEE/ACM Trans. Comput. Biol. Bioinform. (TCBB) **16**(1), 222–232 (2019)
13. Chrimes, D., Moa, B., Zamani, H., Kuo, M.H.: Interactive healthcare big data analytics platform under simulated performance. In: 2016 IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, 14th International Conference on Pervasive Intelligence and Computing, 2nd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 811–818. IEEE (2016)
14. Buczak, A.L., Moniz, L.J., Feighner, B.H., Lombardo, J.S.: Mining electronic medical records for patient care patterns. In: 2009 IEEE Symposium on Computational Intelligence and Data Mining, pp. 146–153. IEEE (2009)
15. Khalaf, M., Hussain, A.J., Al-Jumeily, D., Keenan, R., Fergus, P., Idowu, I.O.: Robust approach for medical data classification and deploying self-care management system for sickle cell disease. In: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 575–580. IEEE (2015)
16. Raghu, V.K., Ge, X., Chrysanthis, P.K., Benos, P.V.: Integrated theory-and data-driven feature selection in gene expression data analysis. In: 2017 IEEE 33rd International Conference on Data Engineering (ICDE), pp. 1525–1532. IEEE (2017)
17. Kovatch, P., Costa, A., Giles, Z., Fluder, E., Cho, H.M., Mazurkova, S.: Big omics data experience. In: Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis, p. 39. ACM (2015)
18. Xu, X., Zhang, W., Li, L.: The impact of technology type and life cycle on IT productivity variance: a contingency theoretical perspective. Int. J. Inf. Manage. **36**(6), 1193–1204 (2016)
19. Brennan, P.F., Bakken, S.: Nursing needs big data and big data needs nursing. J. Nurs. Scholarsh. **47**(5), 477–484 (2015)

Optimized Real Time Drowsy Driver Warning System Using Raspberry Pi

A. Almah Roshni(✉), J. Balaji, D. Kaushik, and K. R. Sarath Chandran

Department of Computer Science Engineering, SSN College of Engineering, Chennai, India
{almahroshnil5006, balajil5015, kaushikl5045}@cse.ssn.edu.in, sarathchandran@ssn.edu.in

Abstract. Accidents are undesirable, incidental and unexpected events that can be prevented if they are recognized and acted upon, prior to their occurrence. Driver drowsiness is one of the major causes of road accidents. A solution to this problem is inclusion of a drowsiness warning system in vehicles to warn the driver of drowsiness. The main objective of this paper is to develop a non-intrusive real-time drowsiness warning system by monitoring eye state of the driver. The proposed system uses eye-aspect-ratio and is implemented in Raspberry Pi. This system is optimized using three techniques, by re-sizing the frame to be processed, using a single eye for drowsy detection and by not processing every frame. The selection of frames is based on analyzing the redundancy nature of video frames. This system is designed by considering several factors to minimize frame processing latency to match with Raspberry Pi's processing speed.

Keywords: Drowsy driver · Driver state · Haar cascade classifier · Facial landmark detection · Eye aspect ratio · Raspberry Pi

1 Introduction

Safe driving is a major concern of all societies around the world as transport systems have become an essential part of human activities. The sensation of sleep reduces the driver's level of vigilance, alertness and concentration, thereby increasing the probability of occurrence of accidents. The early hours of the morning, middle of the afternoon and late nights are the peak times for a driver to fall asleep. A new technology called "Drowsy Driver Detection System" has been developed by major vehicles including Ford [1], Mercedes-Benz, Volvo, Toyota [2], Nissan [3], Renault [4] and Hyundai. These studies have limitations in terms of usage of expensive hardware (e.g., sensors and infrared cameras).

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 238–245, 2020.
https://doi.org/10.1007/978-3-030-37051-0_27

2 Existing Approaches

Methods to detect drowsy driving can be classified as the following four: monitoring vehicle's speed and movements, measuring driver's biological signals, monitoring driver's state and hybrid methods. Among all the above methods, monitoring of driver's state by using a camera is considered to be the most promising due to its accuracy, reliability and non-intrusiveness. Table 1 lists the parameters, advantages and limitation of the different drowsy driver detection techniques.

Table 1. A comparison of various drowsy driver detection techniques.

Technique	Parameters	Advantages	Limitations
Vehicle response [5]	Change in shift lever, deviation from lane position, speed of the vehicle, steering wheel movements, pressure from gas and brake pedal	Non-intrusive	Unreliable, doesn't fully differentiate between normal and drowsy driving because it depends on nature of the road, traffic and the driver's lack of experience
Physiological technique [6]	Brain waves (EEG), Eye movements (EOG), Heart rate (ECG), Signals from muscle cells (EMG)	Accurate, determines decrease in level of alertness ahead of time before actual drowsiness starts	Intrusive, hardware cost is high, Physiological signals are easily contaminated by muscle movements of different parts of the body
Behavioral technique [7]	Change in facial expressions, head movements, yawning, blinking	Non-intrusive, reliable	Performance may decrease in limited lighting conditions
Hybrid technique [8]	Steering wheel movements and pupil diameter	Non-intrusive, reliability is significantly higher than other techniques	Complex, needs proper analysis for better accuracy

3 Overview of the Proposed System

This section presents the architectural design, overall flowchart and methodology of the proposed system. Figure 1 refers to the architectural design of the proposed system.

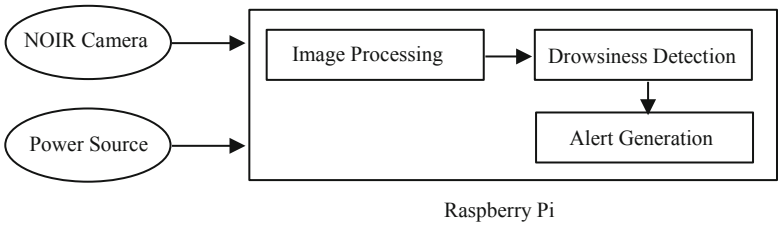


Fig. 1. Architecture design of the system

3.1 Image Pre-processing

The proposed system has a camera fixed inside the car, right in front of the driver to monitor the driver's state. The live video feed from the camera is sent to the Raspberry Pi which splits the video into frames and is later pre-processed. When the frame to be processed is large in size, the area to be scanned increases, thereby slowing the rate of detection. Instead, re-sizing of the frame to a smaller size without the loss of any information, enhances the speed of detection. Moreover, the proposed system doesn't need color information of the image for processing. Hence, converting the image to gray scale eliminates noise in the image up to an extent, and increases the speed of computation by removing the color information. The flow diagram for the proposed system is shown in Fig. 2 where Thr refers to the fixed threshold value for Eye Aspect Ratio.

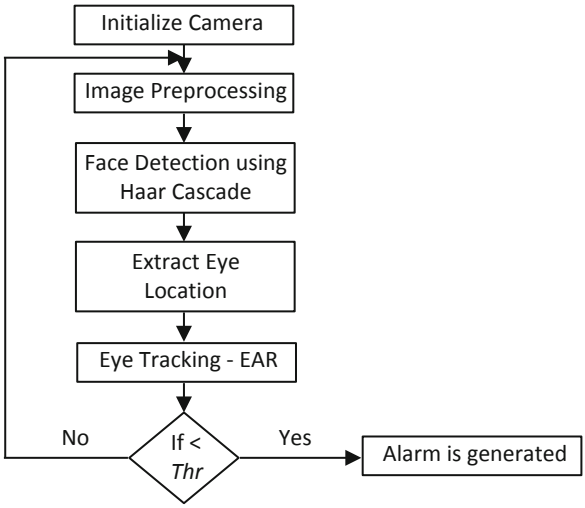


Fig. 2. Flow diagram of the proposed system

3.2 Drowsiness Detection

Since the eyes are always in a defined area in the face, a shape predictor can be used to detect the region of eyes. This system uses the facial landmark detector of dlib library [9, 10] in eye localization. This facial landmark detector produces 68 (x, y) coordinates that map to specific facial structures. Dlib library has functions to recognize eye, nose, mouth and ear and these coordinates can be stored in a numpy array.

To monitor the state of the driver's eye, Eye aspect ratio [11] provides an elegant solution involving simple calculation based on the ratio of distances of the width and height of the eye as shown in Fig. 3.

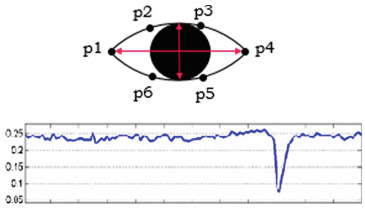


Fig. 3. Eye aspect ratio

An eye is characterized by 6 (x, y) coordinates, starting from the left corner and then moving in a clockwise direction for the remaining regions.

It is observed that eye aspect ratio is approximately constant when the eye is open, but falls down rapidly when an eye blink occurs, but is ever zero. The average of EAR values of both the eyes is considered as to detect an eye blink.

3.2.1 Comparison and Assigning of Threshold Values

By comparing various values for thresholds, it can be observed from Table 2 that, an EAR threshold of 0.25 and 10 consecutive frames prove to be optimal conditions for drowsiness detection.

Table 2. Comparison and assigning of threshold values

EAR threshold	Consecutive frames	Time to detect drowsiness	Observations
0.1	–	–	Unable to detect eye blink, EAR too low
0.15	5	1.56	Eye needs to be closed very tightly
0.15	10	2.026	Head position should be very straight
0.2	5	1.178	Very low detection time
0.2	10	1.932	Late detection of drowsiness

(*continued*)

Table 2. (*continued*)

EAR threshold	Consecutive frames	Time to detect drowsiness	Observations
0.2	16	3.058	Very late detection of drowsiness
0.25	5	1.232	Too fast detection
0.25	**10**	**1.736**	**Optimal value**
0.25	16	2.936	Too late detection of drowsiness
0.3	5	0.870	Early detection of drowsiness
0.3	10	1.802	Approximately stable detection
0.3	16	2.64	Late Detection of drowsiness
0.35	–	–	Unable to detect eye blink, high EAR

3.3 Alert Generation

An alert is generated to awaken the drowsy driver using mp3 files which is better than the alternative .wav files because of smaller size. Threads are used to synchronize and handle multiple processes.

4 Optimization Techniques

Executing a code in computer differs from running the same code in Raspberry Pi due to the limitation of 1 GB of RAM in Raspberry Pi. That too, real time applications should not have any delay, as a delay of even a fraction of second in alerting the driver of drowsiness, may lead a serious accident. We have come up with certain optimizations for the current system.

4.1 Single Eye Optimization

A person usually closes both of his eyes when he falls asleep. So, when a single eye is considered for EAR calculation instead of average of both the eyes, the time reduced in computation per frame is negligible, but when real time processing for long duration is considered, there is a significant reduce in processing time, hence making the process efficient as depicted in Table 3.

Table 3. Single eye optimization technique.

Number of frames considered	Time taken for processing when both the eyes are used (s)	Time taken for processing when a single eye is used (s)	Time saved in processing (s)
100	4.0	3.845	0.15
500	15.83	13.86	1.97
1000	26.085	23.6	2.485

4.2 Optimization by Frame Skip

Processing every frame gives perfect accuracy, but overloads the Raspberry Pi. A Raspberry Pi board processes around 50 frames per second. When this is done for over a long period of time, like an hour, thousands of frames need to be processed out of which some frames wouldn't bring much change in the face of the driver. A solution for this problem is by processing every n^{th} frame, instead of every frame. Too high values for n leads to lower accuracy but faster processing while lower values for n maintains the accuracy but doesn't improve the processing. By observing certain values for n from Table 4, it can be observed that when every 7^{th} frame is considered for processing, the accuracy is maintained and the performance of the system is improved.

Table 4. Optimization by frame skip

Frame Processed	Time taken to process 500 frames (s)	Percentage of time saved in processing	Delay observed in detection
All frames	87.82	0%	No
Every 2^{nd} frame	41.568	53%	No
Every 3^{rd} frame	29.16	67%	No
Every 4^{th} frame	22.469	72%	No
Every 5^{th} frame	17.77	79%	No
Every 6^{th} frame	15.108	82%	No
Every 7^{th} frame	**12.34**	**85%**	**Acceptable**
Every 8^{th} frame	11.212	87%	Slight delay
Every 9^{th} frame	11.1	87%	Yes
Every 10^{th} frame	9.363	89%	Yes

5 Results and Analysis

Various orientations of the face and eye were tested on the designed system and the following results were obtained.

(a) **(b)**

Fig. 4. (a) Drowsiness alert. (b) Danger alert

A drowsiness alert is generated when the driver's eye remains close for 10 consecutive frames as shown in Fig. 4(a). When the driver doesn't react to the continuous drowsiness alert given by the system, a danger alert is sounded as in Fig. 4(b), denoting that the driver's life is at serious risk and that the driver should stop the vehicle immediately to avoid any accidents.

When the driver looks at the side mirror or keeps talking to the adjacent person by facing them, the system sounds an alert to warn the driver to focus on the road as shown in Fig. 5. Similarly, when the driver has fallen asleep with his head bent down or when the driver is looking down instead of the road, the system sounds an alert for the driver to look at the road as shown in Fig. 5.

Fig. 5. Alert when driver isn't looking at the road

6 Conclusion and Future Work

In this paper, Eye-tracking and Image Processing are used in developing a non-intrusive drowsiness detection system. The problems caused by changes in illumination that influence the eye detection was reduced by using a NOIR Camera and an IR light source which doesn't disturb the driver. Efficiency of the system is improved by using a single eye for eye closure duration calculation, by re-sizing the frame to be processed and by processing every 7^{th} frame. Various values for threshold of EAR were observed and an optimal value is used in designing this system.

The proposed system detects drowsiness using eye closure duration and an alert is generated to awaken the driver. But in some cases, generating an alert wouldn't be enough to awaken the driver. In such cases, a future enhancement to the current system can be made by slowing down the vehicle and halting it when the driver doesn't respond to the continuous alerts.

Similarly, in some cases, driver may fall asleep due to tiredness during long and tiresome journeys. In such cases, a future enhancement can be made such that the system interacts with the driver to keep him awake. The interaction may be in the form of reading a joke, or playing a song based on the preference of the driver.

Acknowledgement. All author states that there is conflict of interest.

We used author photo in the Figs. 1 and 2.

We used our own data.

References

1. Teyeb, I., Jemai, O., Zaied, M., Amar, C.B.: Towards a smart car seat design for drowsiness detection based on pressure distribution of the driver's body. In: 11th International Conference on Software Engineering Advances, pp. 217–222 (2018)
2. Li, X., Han, G., Ma, G., Chen, Y.: A new method for detecting fatigue with camera based on OpenCV. In: International Conference on Wireless Communications and Signal Processing (WCSP 2011), Nanjing, pp. 1–5 (2011). https://doi.org/10.1109/WCSP.2011.6096867
3. Yabuta, K., Iizuka, H., Yanagishima, T., Kataoka, Y., Seno, T.: The development of drowsiness warning devices. In: 10th International Proceedings on Technical Conference on Experimental Safety Vehicles, Washington, USA (1985)
4. Artaud, P., Planque, S., Lavergne, C., Cara, H., De lepine, P., Tarriere, C., Gueguen, B.: An on-board system for detecting lapses of alertness in car driving. In 14th International Technical Conference on the Enhanced Safety of Vehicles, Munich, Germany, pp. 350–359 (1995)
5. Mortazavi, A., Eskandarian, A., Sayed, A.: Effect of drowsiness on driving performance variables of commercial vehicle drivers. Int. J. Automot. Technol. **10**(3), 391–404 (2009). https://doi.org/10.1007/s12239-009-0045-x
6. Lin, F., Ko, L., Chuang, C., Su, T., Lin, C.: Generalized EEG-based drowsiness prediction system by using a self-organized neural fuzzy system. IEEE Trans. Proc. Circuits Syst. I Regul. Pap. **59**(9), 2044–2055 (2012). https://doi.org/10.1109/TCSI.2012.2185290
7. Tianyi, H., Huabiao, Q., Qianshu, S.: An improved real time eye state identification system in driver drowsiness detection. In: Proceedings of the IEEE International Conference on Control and Automation, Guangzhou, China, pp. 1449–1453 (2007). https://doi.org/10.1109/ICCA.2007.4376601
8. Viola, P., Jones, M.: Rapid object detection using a boosted cascade of simple features. In: Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR 2001, Kauai, HI, USA (2001). https://doi.org/10.1109/CVPR.2001.990517
9. Cheng, B., Zhang, W., Lin, Y., Feng, R., Zhang, X.: Driver drowsiness detection based on multisource information. Hum. Factors Ergon. Manuf. Serv. Ind. **22**(5), 450–467 (2012). https://doi.org/10.1002/hfm.20395
10. King, D.E.: Dlib-ml: a machine learning toolkit. J. Mach. Learn. **10**, 1755–1758 (2009). https://doi.org/10.1145/1577069.1755843
11. Soukupova, T., Cech, J.: Real-time eye blink detection using facial landmarks. In: 21st Computer Vision Winter Workshop, Slovenia (2016)

Blockchain Based Efficient and Accurate Property Title Retrieval and Secured Storage System

Saee M. Joshi(✉), Jayant Umale, and K. Rajeswari(✉)

Computer Department, Pimpri Chinchwad College of Engineering, Pune, India
saee.joshi46@gmail.com, {jayant.umale,kannan.rajeswari}@pccoepune.org

Abstract. A future-oriented, blockchain real estate market could help with making new plans of action of allying potential buyers and sellers. It is difficult to assume how properties of numerous sorts could be liquified, tokenized and exchanged. This blockchain paper will considerately influence transaction times as property sellers find entrusted buyers and the other way around, instead of hunting down a certifiable buyer and seller. It is more than likely that the entire real estate industry will gain advantage by this move, by bringing down the obstacle of real estate speculation and likewise eradication of center men. New meanings of property ownership and rental agreement will emerge from this move in the real estate business. The ownership of property need to be clearly stated and historically defined by documentation. There are many conflicts in ownership which is challenged in judicial/legal systems. The provision of maintaining the clarity of ownership is the responsibility of identified advocates and provided as Certificate of Title. There is no system taking care systematically of the overall transactions. The proposed will provide the secured transaction maintenance system for land/property transactions to support the timely verification of titles of said property. Also the implementation would be based on Blockchain Technology making the system transfer proof in storage of transactions.

Keywords: Blockchain · Ethereum · Smart contracts · Solidity

1 Introduction

Blockchain is a hotly debated issue right now and it's essential to really understand it. In conventional money related transactions, there is a "trusted" (brought together) outsider who is in charge of confirming the transaction. For instance, on the off chance that we send cash to another person it will be confirmed by a bank and the bank will charge an expense for doing this [1]. In any case, blockchain is open-source innovation that evacuates the requirement for a go-between or "middleman" when making transactions. Rather, information on each transaction is put away in "blocks" which are time- stepped and connected together to frame a "chain [7]." The majority of the information put away in the chain can't be changed or expelled, which implies that it is secure and permanent until the end of time [4]. It is a record of transactions that, rather

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 246–255, 2020.
https://doi.org/10.1007/978-3-030-37051-0_28

than being put away in one explicit (incorporated) area, is put away and encoded on thousands of PCs around the globe. This trusted advanced record is unmistakable to all members and it demonstrates each component of the transaction. This evacuates the need to depend on a middleman to make secure transactions [12]. There's no compelling reason to confide in a bank. For whatever length of time that the transaction is recorded, everybody can see it and go to an agreement to check it.

Ethereum, an open programming stage that enables designers to fabricate and convey blockchain applications (called DApps, in type of smart contracts). It makes building blockchain applications increasingly effective. In October 2017, Michael Arrington TechCrunch) has made blockchain history when he utilized an Ethereum smart contract to buy a loft in the Ukraine. It was viewed as one of the principal times ever a real resource other than a cryptographic money was exchanged on the blockchain [5]. This was a critical initial phase in mechanizing the procedure of real estate buys and disposing of the requirement for one single amazing element that controls the whole framework. In the event that a smart contract can dispose of the requirement for an outsider when sending cash, it can likewise disturb a scope of different ventures where mediators are as of now required to give trust [15]. This has a tremendous measure of potential for the real estate industry. The primary advantages of blockchain speed, trust and expelling a focal authority can all apply to the real estate showcase.

Right now real estate is the biggest resource class on the planet and it is worth around $217 Trillion consistently. Notwithstanding, the market is divided, which makes it troublesome for financial specialists to buy a bit of a real estate property [11]. Real estate possession has recently been very elitist [9]. Most common individuals can scarcely stand to buy one home, not to mention put resources into numerous properties. So as to meet all requirements to purchase a home, buyers must have fantastic credit and have the capacity to exhibit their strong budgetary standing as a great job and a hold of advantages.

Tokenization of real estate property dispenses with the issue of illiquidity. It is conceivable to change over real estate esteem into "tokens" that speak to a benefit, (for example, an individual real estate offer) and exchange and move those tokens rather, at any minute in time [13]. Tokenization is when delicate information is supplanted with a special image to distinguish it, which has the majority of the fundamental data without trading off security. In this way, basically resource sponsored tokenization implies changing over the rights to an advantage into a computerized token [10]. When a property is tokenized, a token is produced on a smart contract and then an incentive is connected with that Token which compares to the real resource [8].

2 Literature Survey

Snall et al. [1], attempted to separate the hype from the hyperbole of blockchains and how they might relate to land administration. There is no doubt that in countries embarking on a mission to embed the notion of title and have it attached to identified individuals may do worse than consider the advantages that the blockchain concept may potentially offer. With a largely blank canvas from which to work, the blockchain might well, to borrow a visual image, stack up against other central forms of land

registries once some of the uncertainties in terms of its application are ironed out. By operating without any need for long, ongoing central involvement (if this is possible), the effect on the public purse is greatly diminished, and with the increased flexibility offered by a distributed ledger and the ability to have a true peer-to-peer verification and validation service, greater financial flexibility is achieved. Such advantages may be significant in countries where there is no central enforceable evidence that one has a secured and legally binding title to land.

Chandra and Rangaraju [3], describes that two-third of civil cases pending in Indian courts deal with land related disputes, most of which revolve around establishing ownership. The existing legal framework, based on the system of presumptive ownership, lends itself to litigation as land and property undergo several mutations over generations that are not always captured on public records. Moreover, data related to a specific parcel of land is stored in siloed government departments, and in formats that vary substantially from one state to another. Access to these records is time- and cost-intensive, as they involve frequent visits and bribes to government agents. For some time now, there have been suggestions to improve this abysmal state of land records by introducing blockchain technology. The popularity of cryptocurrencies has brought forth this new concept of storing and sharing of information between participants.

Gap Analysis: For verifying the documents of both buyer and owner in Real Estate transactions Government Authority or Real Estate Broker act as third party. Often Real Estate Brokers or any other third party involved in the transactions perform some fraudulent activities such as selling properties of Multiple owners predicting himself as single owner, selling property to Multiple Buyer's, Encroachments, Dubious Agreements etc. Also SSL (Secured Socket Layer) certificate used in existing system could only secure the requests that pass through network, but data when stored in database after passing through network was not secured. Moreover there are conflicts in identifying the detailed Ownership of Property as well as there is delay in providing the Title clear documentation by the manual system.

3 Proposed Work

The undesired manipulation of sensitive data in real estate property transactions and storage is to be provided security so the system aims towards preventing the data by putting it on Blockchain to stop its manipulation, because it is almost impossible to tamper the data on blockchain.

A Proof-of-Concept (PoC) is a transaction based framework which is made for a completely distributed and decentralized application where there is no central expert and the transaction is acknowledged in the form of an agreement on a shared system [2]. A duplicate of the ledger is present on every hub of the P2P and every transaction is included onto the ledger if dominant part of the P2P acknowledges the transaction through the accord. The major focus is on the fraudulent exercises in the real- estate advertises for this application. The clients can undoubtedly buy and sell their property without stressing over fraud and also pay the mediators for a transaction that excludes anybody other than the sellers and the buyers through the PoC.

The real Estate transactions are secured using Blockchain Technology because there is no central point of failure. A hacker would need to attack simultaneously at least 51% of network in order to alter one record fraudulently because the ledger (collection of financial accounts) is distributed among many computers [3]. Various proofs like PoC (Proof of Concept), PoS (Proof of Stake), PoW (Proof of Work) etc. which are known as Blockchain Consensus can be used to secure records.

A. Architecture:

See Fig. 1.

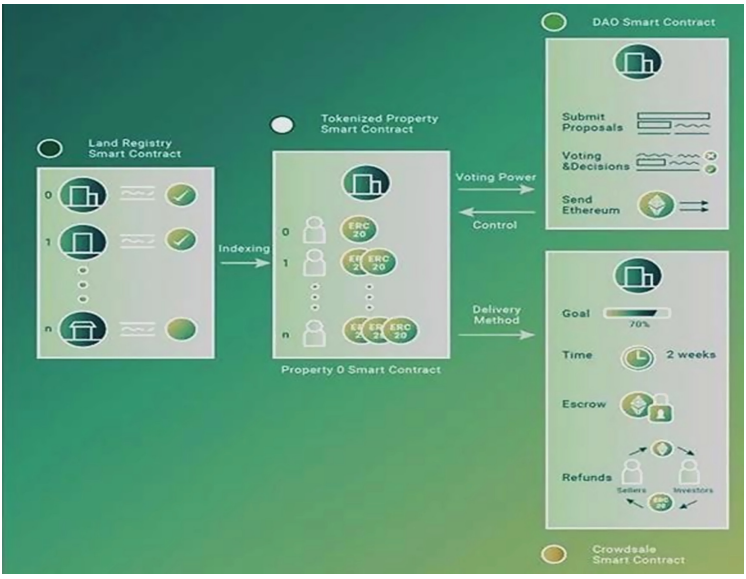


Fig. 1. System architecture

B. Mathematical Model:

Let S = { X, Y, Fi } be the user's perspective of a successful deal.
Let X be the input document such that X= { X1, X2,X3, }
Such that there exists function fx_1 : X1 {0,1}

X2 is hash code accepted for the document Let X2 = HC(Hash Code) where HC Є X1
There exists a function f_{X2} : X2 {Hash function }

X3 is the element which checks document Let X3 = documents of various formats , where X3 Є .jpg , .pdf There exists a function f_{1X3}: X3

Let Y is the buyer
Let Y= F2Y1:Y1{0,1}
Y { Fake Buyer, Genuine Buyer} Let Fi = { F1 ,F2 }
Where F1 = checks the uniqueness F2 = checks the buyer credibility.

C. Algorithm:

The below code snippet is of whether a seller wants to sell his/her property to the buyer and the functions associated with it forms the core of our working.

```
(RealEstateOwner,price,originalNumber,status)=m.g etRealEstateInfoByIndex(_index);

require(msg.sender==RealEstateOwner);          //Only owner of this realEstate can make contract!

require(status==1); //Status of realEstate should be 1 which means it is FOR SALE MODE;

addressnewContract=newRealEstateSingleContract(_ index,msg.sender,price,originalNumber,status,_type
OfContract);

New Contracts.push(newContract); numberOfContracts++;

emit

LOG_NewContractAddress(newContract,msg.sender
,price,originalNumber);//This is for interacting with web3 later.
```

D. The Advantages of the system are as follows:

1. Property Documents once stored on Blockchain cannot be tampered compared to existing scenario.
2. The system will try to efficiently retrieve Property Titles as compared to manual system.
3. The framework is permanent. Nobody can make changes to the information.
4. It is difficult to degenerate the framework. The system depends on accord, which makes it difficult to mess with.
5. The framework is secure, as the system ensures it against hacking assaults. There is likewise no danger of downtime.

4 Result and Discussion

DAO (Decentralized Autonomous Organisation) and Ethereum were chosen concerning the choice of systems to integrate for the implementation. Reasons are threefold:

1. Opt for Ethereum over hyperledger because of its consensus mechanism with lower inclusion time, resulting in higher throughput and thus it's better suited to match DAO's performance;
2. Ethereum provides certificate authority service that all system components can use to ensure trust across complete system; and
3. Good natural mapping between DAO and ethereum components allow for efficient deployment.

This DAPP submits transactions directly from within the app, uses an ERC-20 token to authorize seller and buyer data, and stores data decentrally. Further, it uses smart contracts to reward miners processing the successful transactions. For retrieval of data it uses a decentralized app accessing a local Ethereum node.

A. System Specification Requirements:

1. Ethereum Framework
2. Truffle
3. Remix IDE
4. Solidity 4.23
5. Docker
6. Postgres SQL
7. HTML, CSS
8. Javascript
9. JSON
10. Web3
11. Node JS 11.4.0
12. Ropsten
13. Metamask.

B. Realestate Dapp Performance and transaction status:

By the time of compiling, the smart contract is deployed on Ganache which is known as a Blockchain server and only front end web app remains to perform the transaction in actual. Smart Contract is written in solidity language version 4.23 and it contains various code snippets which checks the uniqueness of Real Estate buyer and seller. It also checks whether a successful deal can be done. Ganache server contains 10 different blocks having different private keys and hashes and a successful transaction between the blocks using smart contract have been tested. Firstly compile solidity smart contract which is the basis of transaction between two accounts. Metamask is used to choose Ropsten test network and show the interaction between accounts. The Fig. 2 shows the contract deployment status.

Contract is deployed from 0x7f1be5223136751111167d1b57c67eccd08976ba account address to 0xbfe668de3d8dadf0150b98d956bb69df89267233 and the whole transaction summary i.e. the transaction is successful is seen in Fig. 3.

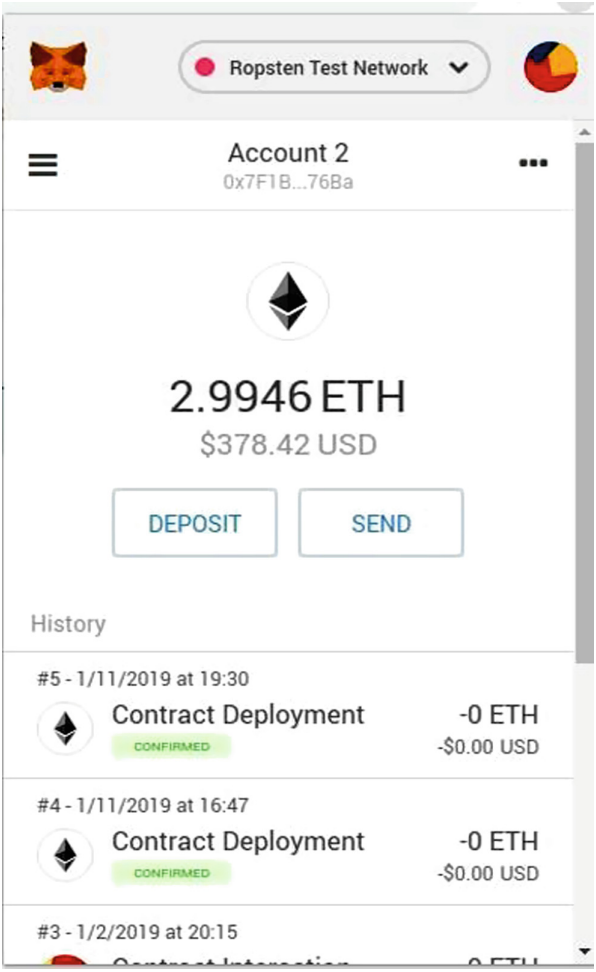


Fig. 2. Contract deployment on metamask

C. Statistics:
Our block status gas price and other statistics can be seen in below ether scan window (Fig. 4).

5 Conclusion

Blockchain as a distributed ledger can help conduct Property Title Retrieval in a transparent manner, which can also be validated. Secure Storage on blockchain can form the basis for strengthening the good governance principles of ethical conduct, fairness and efficiency. Thus Blockchain Technology can be used to reduce reliance on trusted third parties, reduce costs and reduce number fraud and errors. This technology

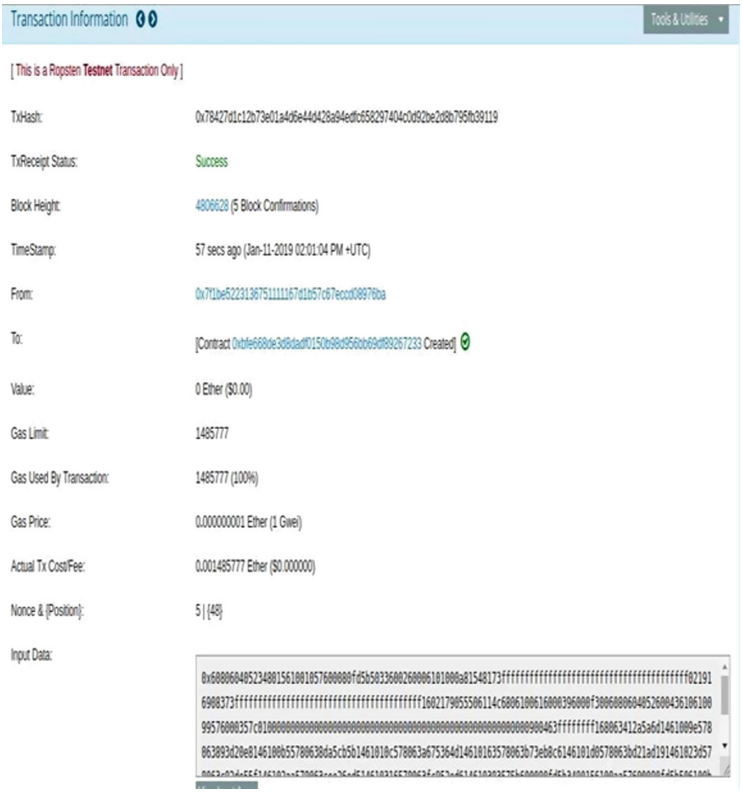


Fig. 3. Transaction summary

Fig. 4. Statistics

brings Security to Real Estate transactions because there is no central point of failure. From Security point of view the ledger is distributed among many computers so attacker needs to attack 51% of network which will be next to impossible. This paper presents that Real Estate development to assess whether and when Blockchain can be used as a technology in their organization. Hence this project work eliminates the third party like Real Estate Broker in the proposed system, which totally relies on the Blockchain Node Implementation.

6 Future Work

In our research attempt, We have focused on how Blockchain technology brings security to Real Estate transactions because of it's transparency and no central involvement. Thus, our future work would be to extend the use of Blockchain technology to facilitate an accessible, streamlined Indian Real Estate Market making it more efficient and effective by employing faster or simpler working methods.

References

1. Snall, M., Sannagard, J., Lundberg, S.F.T.: The Land Registry in the Blockchain. Testbed (2017)
2. Mizrahi, A.: A Blockchain Based Property Ownership Recording System. ChromaWay (2017)
3. Chandra, V., Rangaraju, B.: Blockchain for Property A Roll Out Road Map for India. Copyright 2017 India Institute
4. Bach, L.M., Mihaljevic, B., Zagar, M.: Comparative analysis of blockchain consensus algorithms. In: MIPRO 2018 (2018)
5. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C.: A Review on Consensus Algorithm of Blockchain. IEEE (2017)
6. Krishnan, A.: Blockchain Projects that Will Change the Real Estate Industry. Invest in Blockchain (2018)
7. Crosby, M., Nachiappan, Pattanayak, P., Verma, S., Kalyanaraman, V.: BlockChain Technology Beyond Bitcoin. Fairchild, University of California (2015)
8. Updating the Land Registration Act 2002. @ Crown Copyright 2016
9. Registering property the paths of digitization. Doing Business (2016)
10. Lian, H., Yu, Y.: Reference of land registration system from countries in Asia Pacific Region: comparison of the United States, Canada, Russia, South Korea, Japan and Australia. IOSR J. Bus. Manag. (2016)
11. Akingbade, A.O.: Improvement of Availability of Land Registration and Cadasrel Information in Ondo State Nigeria (2005)
12. Porat, A., Pratap, A., Shah, P., Adkar, V.: Blockchain Consensus: An Analysis of Proof-of-Work and its Applications
13. Nichols, S.: Land Registration: Managing Information for Land Administration. University of New Brunswick

14. Mulholland, G., Pontes, L.: The technology behind the integrated cadastre/land registry solutions in the canadian provinces of new brunswick and Nova Scotia. In: Symposium on Innovative Technologies for Land Administration Madison WI, June 2005
15. USAID: Land Titling and Credit Access Understanding the Reality. (United States Agency International Development)

Multi Keyword Search on Encrypted Text Without Decryption

Vemula Sridhar[1(✉)] and K. Ram-Mohan Rao[2]

[1] CSED, MVSR Engineering College, Hyderabad, India
sridhar_cse@mvsrec.edu.in
[2] ITD, Vasavi Engineering College, Hyderabad, India
kmrao@staff.vce.ac.in

Abstract. Various organizations use plain text to store data related to day-to-day computations. Data is stored in the form of plain text documents without any structure and specifications. Retrieval and searching from structured data will be easier with various existing database systems. Querying and searching on unstructured content is difficult. In general, searching on unstructured content can be implemented using a similarity between input keywords and documents. Organizations are moving towards cloud to store the data because of high availability, lower maintenance cost, reliability, and portability. In a cloud system, sensitive data like personal records are to be protected to avoid malicious access from intruders. But searching data from encrypted content is difficult. In this paper, we are proposing a scheme called Multi Keyword Search on Encrypted text (MKSE) which enables searching on encrypted unstructured text without decryption in the cloud using Cosine Similarity. To store the documents, we are using CryptDB database where documents are stored in encrypted form. Thus the multi-keyword search is done on encrypted data in the cloud using cryptDB for providing data security.

Keywords: Querying · Cloud encryption · Cloud security · Information retrieval · Cosine similarity

1 Introduction

Latest computing trends involve maintaining various forms of data in the form of tables, record, files documents, etc. Among these, some of the data is in a structured format, and some are in unstructured format. Structured data can be stored in the form of tables, databases, namespaces, etc. Querying from structured data does not require developing a new application. Existing database software provides efficient and faster retrieval of data from structured content [1]. For retrieving and querying data from unstructured content, various methods can be used, which includes searching for a keyword, ranking the results, feature extraction, discovering knowledge, etc. [2]. In the latest computing model, huge amount of unstructured content is going to be processed. It is difficult to maintain such a huge amount of data due to the various risks involved in providing availability, security, integrity, etc. Due to this customers are moving towards a cloud computing model.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 256–263, 2020.
https://doi.org/10.1007/978-3-030-37051-0_29

With the help of cloud computing, business customers can enjoy on- demand applications and services provided by cloud providers. There are various benefits by using the cloud computing model which includes universal data access, high availability, avoidance of maintenance, storage management, etc. With the advantages of cloud, large amount of sensitive data are being moved towards cloud such as medical records, account information, private information, company financial data, etc. Maintaining the security of this sensitive information is a big challenge. Most of the cloud service providers offer encryption methods to store documents so that sensitive information can be secured [3]. But there is a chance of data theft by the curious cloud administrator. Because of this, documents need to be encrypted at the administrator side and transferred to cloud providers.

When the data is stored in encrypted format, searching, querying and other processing of data is not possible. Various special encryption methods are proposed like order-preserving encryption, homomorphic encryption, symmetric searchable encryption, etc. so that the retrieval of information is possible from encrypted content. Order-preserving encryption [4, 5] enables to perform comparisons between number data values on the encrypted text. Homomorphic encryption [6] allows performing addition and subtraction on data values stored in encrypted form. But these encryption algorithms work efficiently on numeric values only, and it is difficult to get efficient results if data is stored in unstructured text format. In this paper, we discuss a simple process of implementing Multi Keyword-based search on Encrypted text (MKSE).

The rest of the paper is organized as follows. Section 2 explains preliminaries and the basic searching using cosine similarity, in Sect. 3 we provide system model and the design, in Sect. 4, we provide the algorithm steps of the proposed method, Sect. 5 specifies experimental support needed for the work, in Sect. 6 gives the security analysis and performance evaluation respectively. Finally Sect. 7 gives the conclusion of the paper.

2 Preliminaries

In this section we will discuss preliminaries required. In this proposed system we use CryptDB database to store the text files, and we use Apache Lucene API for creating the index and finding similarity using Cosine Similarity. The details about these are described below.

2.1 CryptDB

CryptDB [7] provides a design for securing large databases involved in various applications. CryptDB protects the database system from an unauthorized user who tries to access confidential information. CryptDB works by sending queries on encrypted data through Database proxy. The proxy encrypts and decrypts data and changes query operators for security. CryptDB uses SQL aware encryption strategy. According to this strategy, SQL consists of several operators like equality checks, joins, comparisons operators, etc. By using known encryption methods for joins,

CryptDB encrypts the data so that DBMS executes the transformed queries. Figure 1 represents the architecture of CryptDB.

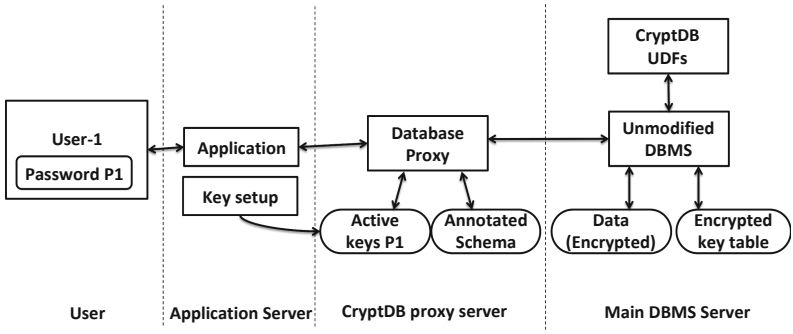


Fig. 1. The architecture of CryptDB

CryptDB architect ture includes three levels of functionality.

1. Application server
2. CryptDB proxy server
3. Database Server.

Application server

- The user interacts with an application server to send queries and collect the results.
- This application server issues DBMS queries to the CryptDB proxy for one or more users
- The application server can be altered for providing encryption keys to the database proxy.

Database server

- Maintains data which is encrypted by CryptDB which includes table and column names
- It Processes encrypted data stored in tables like normal data as if it were unencrypted data
- It provides user-defined functions (UDFs) which are used in cipher text operations
- It has some auxiliary tables (ex. Encrypted keys) used by CryptDB proxy server.

Database proxy

- It is the main component of CryptDB, and it acts as an interface between the application and actual database.

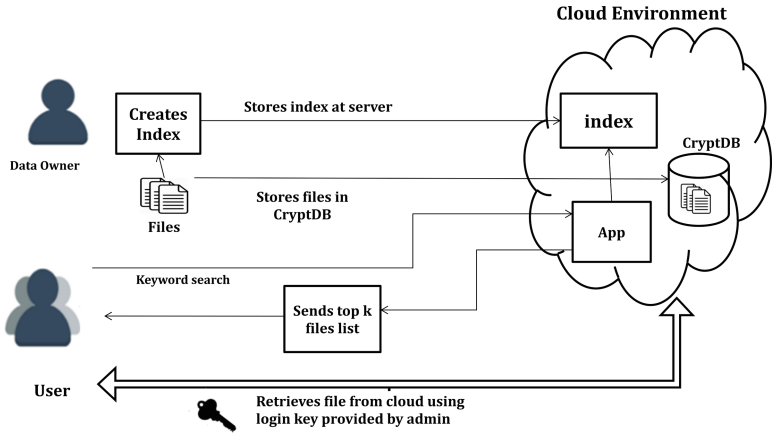
- It receives the queries from the application, encrypts and sends them to DBMS.
- While maintaining the query's semantics, some query operations can be modified if required.
- It decrypts results generated by DBMS Server and sends them to the application server.

2.2 Cosine Similarity

Cosine Similarity [10] plays an important role in keyword searching applications. Using cosine similarity, we can find the difference measure, given two vectors. In text processing applications, TF*IDF values are calculated on text keywords and, then they are represented in the form of vectors. Here cosine similarity helps to find the documents which contain key words by finding similarity between TF*IDF vector values between input documents and query.

3 System Model

The system model of MKSE contains three entities: A data owner, User and Cloud Server application. Data owner maintains plain text documents to be uploaded to the cloud. Cloud server application is running in the cloud and interacts with user and CryptDB. The User is the end user who interacts with the cloud server application to extract search results.



The system model of MKSE is shown in Fig. 1.

The architecture system model is shown in Fig. 1. It contains three entities: The data owner, User and Cloud Server application.

Data owner uploads plain text documents in encrypted form to cloud database. Before uploading, data owner creates an index using Apache Lucene API [9] Library. After creating index data owner uploads plain text data in cryptDB table in the form of BLOB type. CryptDB stores the data in encrypted format and allows processing on it

without decryption. Storing plain text file into cryptDB database enables the data owner to add any additional parameters and properties along with files into the table. When new data needs to be added, data owner recalculates index and updates index and files at the server.

In addition, data owner also transfers the created index to a cloud server. Now cloud server contains text data files stored in encrypted form by cryptDB and index entries which are created at data owner. Because the files are stored in encrypted format, a curious cloud administrator cannot view the data.

Cloud server is the application running in the cloud machine along with cryptDB database at its backend. Cloud server receives index entries from the data owner.

Cloud Server is the application which interacts with the user to implement the searching of text. User or client initially sends the keyword(s) to be searched to cloud server. After receiving the keyword(s) from user, cloud server finds out the cosine similarity between keyword from query and which are available in files also. Using cosine similarity, the cloud server returns top k documents which contain the given keyword(s). The User is an entity which can be a client or customer of business organization.

4 MKSE Algorithm

The steps of our proposed keyword searching algorithm are:

Step-1: Administrator collects text documents from customers which are be stored at cloud and uses it for searching in the future.

Step-2: Administrator creates an index on these documents using Apache Lucene Library. Now the Administrator is having collection of documents and index created on it.

Index is created on the documents using apache Lucene API.

Step-3: Administrator uploads documents into CryptDB database as BLOB type which is running on cloud instance.

He also uploads generated Lucene index to cloud instance so that the application running on cloud machine uses this index for processing. Now, server is ready to accept keyword searching.

Step-4: CryptDB user login credentials are given to all users. Users initiate keyword(s) search by sending them to the application running on cloud server.

Step-5: Cloud server generated top n documents names which contain given keyword (s) sent by the user using Cosine similarity. This top n documents list is sent to user.

Step-6: Upon receiving top n documents list from cloud server, user logs into CryptDB and retrieves the respective file from it based on the result.

4.1 Finding Cosine Similarity

The processing of finding Cosine Similarity between documents and given query keywords includes three steps [11].

Step 1: Calculating Term Frequency (TF)

Term Frequency also known as TF measures the number of times a term (word) occurs in a document. The formula for finding Term Frequency is shown in Eq. 1.

$$TF = (no.\ of\ times\ word\ occurs)/total\ words \tag{1}$$

Step 2: Inverse Document Frequency (IDF)

The main purpose here is to search out relevant documents matching the keyword. Generally few keywords occur too ofttimes have in numerous documents. Thus these keywords have very little power in looking effectiveness. We want how to plague the results of too ofttimes occurring terms. Additionally the terms that occur less within the document are often a lot of relevant. We need a way to weigh up the effects of less frequently occurring terms. Using IDF we can do this. The formula for IDF is shown in Eq. 2.

$$IDF(term) = 1 + log(Total\ Number\ Of\ Documents/Number\ Of\ Documents\ with\ term\ in\ it) \tag{2}$$

Step 3: Finding TF*IDF vector

For each term in the query multiply its normalized term frequency with its IDF on each document. Now we are having TF*IDF vector of input docs/words.

Step 4: Vector Space Model – Cosine Similarity

Cosine Similarity of query and each document is computed and results are sorted in descending order to retrieve top n document names which contain given keyword(s).

Based on search result user can request and retrieve the contents of any document using view credentials of CryptDB which are provided to the user by admin.

5 Experimental Setup

For implementing our proposed work MKSE, we used Amazon Cloud Service. The requirement of proposed work is:

- A platform where CryptDB database needs to be run
- An instance where the server application needs to be run.

The above mentioned two requirements are handled by creating an Instance with Google Cloud.

The Operating System requirement of running CryptDB database is Ubuntu 12.04 LTS. So we created an Instance with Ubuntu 12.04 LTS OS on Google Cloud Platform in Asia (Mumbai) region. After creating Ubuntu cloud machine, CryptDB is installed

by connecting to it by SSH. Our proposed work is developed using JAVA and to be deployed on Apache Tomcat web server. To run our application on cloud server, JAVA and Apache Tomcat are installed on Ubuntu Cloud Instance.

Now, our cloud machine is ready with CryptDB database to store documents and application to accepts keyword(s) then returns top k relevant documents list.

We also created another instance of Ubuntu on Google Cloud in same region and installed unencrypted database MySQL to compare the retrieval performance with an encrypted database.

6 Results and Discussion

The proposed work MKSE is tested with set of text files. Initially an index is created on text files and they are uploaded to Google cloud machine along with index. Inside Google cloud machine, CryptDB is the destination for text files where they are stored in encrypted form. Hence any malicious administrator is unable to view the data.

Our algorithm is implemented as web application which is running on Google cloud machine. The uploaded index is stored with web application which is running and it can be used for keyword searching.

To compare the performance of keyword search in encrypted text files, we stored same files on unencrypted database MySQL and implemented same keyword searching.

Comparison of searching on encrypted files and unencrypted files shows that CryptDB consumes only up to 10% to 15% extra time for processing. It can be compromised in the view of data security. Table 1 shows the processing times between these two methods.

Table 1. Performance comparison of searching using secure database-CryptDB and plain database

File name	Word count	Processing time to read file (in Milli seconds)		%ge of excess time for cryptDB
		Using encrypted database CryptDB	Using plain database MySQL	
file1	8135	2546	2240	13%
file2	1548	800	712	12%
file3	1448	516	465	10%
file4	1328	418	362	15%
file5	1005	290	262	10%

7 Conclusion and Future Work

In this paper, we proposed a methodology MKSE for single or multi-keyword search on encrypted text data without decryption. Our approach provides data security by encrypting data at cloud server, makes data always available to retrieve at cloud instance and avoids the risk of data maintenance. With our proposed approach, it is

proven that as the word count increases, the performance of the algorithms may not increase beyond five percent. This work can be extended for multi-cloud environment that leads to high availability of data and fault tolerance of database system.

Acknowledgement. All Author states that there is no conflict of interest.
We used crypt Database from http://css.csail.mit.edu/cryptdb/.

References

1. Florescu, D.: Kossmann, D: Storing and querying XML data using an RDBMS. IEEE Data Eng. Bull. **22**, 3 (1999)
2. Bao, Z., et al.: Effective XML keyword search with relevance oriented ranking. In: 2009 IEEE 25th International Conference on Data Engineering. IEEE (2009)
3. Hingwe, K.K., Bhanu, S.M.S.: Two layered protection for sensitive data in cloud. In: International Conference on Advances in Computing, Communications and Informatics (ICACCI, 2014), 24–27 Sept 2014, pp. 1265–1272 (2014)
4. Agrawal, R., et al.: Order-preserving encryption for numeric data. In: Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data. ACM (2004)
5. Boldyreva, N.C., Lee, Y.: Order-preserving symmetric encryption. In: Advances in Cryptology-EUROCRYPT, 2009, pp. 224–241. Springer, Berlin (2009)
6. Gentry, C.: A fully homomorphic encryption scheme. Ph.D. dissertation, Stanford, CA, USA (2009)
7. Popa, R.A., Redfield, C.M.S., Zeldovich, N., Balakrishnan, H.: CryptDB: protecting confidentiality with encrypted query processing. In: Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles (SOSP 2011). ACM, New York, NY, USA, pp. 85–100 (2011). https://doi.org/10.1145/2043556.2043566
8. McCandless, M., Hatcher, E., Gospodnetic, O.: Lucene in action: covers Apache Lucene 3.0. Manning Publications Co. (2010)
9. Apache Lucene API. https://lucene.apache.org/core/
10. Tata, S., Patel, J.M.: Estimating the selectivity of tf-idf based cosine similarity predicates. SIGMOD Rec. **36**(2), 7–12 (2007)
11. Finding Similarity of documents using TF*IDF vectors. https://guendouz.wordpress.com/2015/02/17/implementation-of-tf-idf-in-java/

An Efficient Approach for Traffic Monitoring System Using Image Processing

Minal Pinto(✉), Sharan Lional Pais, Nisha, Swarna Gowri, and Vishwath Puthi

Department of ISE, Alva's Institute of Engineering and Technology, Mangalore, India
minalpinto21@gmail.com, lionalpais@gmail.com, nishakotian18@gmail.com, rsswarna8396@gmail.com, puthivishwath@gmail.com

Abstract. Traffic congestion has become a major problem in the world wide. So we need efficient system which monitors the traffic and updates the time setting in traffic signal. The cameras installed in the road junction will be used to capture the real time traffic and these images will be processed to count the number of vehicles in each lane. MATLAB Platform is used where it develops the various object detection algorithms for the combination of many image processing algorithms. The real time object detection and tracking will be generated by control signals where Arduino programming will provide an interfacing hardware prototype. The centroid value will be calculated in each lane. Based on the centroid values obtained from the system, the signals will be sent for the traffic pole as the output.

Keywords: Zigbee communication · Arduino · MATLAB

1 Introduction

The increase in population in the world has created increase in number of vehicles in day today life, which leads to the traffic congestion problem that occurs in different countries. Due to traffic congestion people are not able to reach their destination on time and it also makes people to wait for longer time. Because of traffic, people are violating the traffic rules and also we can come across some accidents that happen due to the traffic. Traffic congestion also harms the environment by creating pollution which would also influence the health of the people. To overcome traffic congestion problem, one of the method that is proposed is RFID-based on smart traffic control context for emergency vehicles [1]. Based on RFID technology it controls and manages the traffic signal at the junction and make an easy way for an emergency vehicle to travel from the traffic jam. RFID technology helps in computing the density of vehicle to control the traffic.

In common traffic jam is associated with many more problems like mismanagement of traffic signals which leads to the loss of time, loss of fuel as well as loss of money. People nowadays are very busy, so that they don't want to waste the time. It is very necessary to develop fast, economical and efficient traffic monitoring system. To avoid such problems there are a many techniques available. But no technique is perfect as the

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 264–270, 2020.
https://doi.org/10.1007/978-3-030-37051-0_30

real time situations keeps on changing. But we have made an attempt to reduce the traffic congestion problem by monitoring the traffic signal with the help of image processing technique, where the camera is present at the centre of the four lanes and capture the images of the vehicles.

The images which are captured are sent to the MATLAB, where the images are processed and centroid values are calculated. If the centroid value is more, then for that particular lane green signal is provided with the help of Arduino. The information from the MATLAB is transferred to Arduino through Zigbee communication link. Thus the traffic signal is change accordingly. The cycles are repeated after every thirty seconds which is the pause time that has been provided. In general, when the count of vehicles in one particular lane is more, traffic monitoring technique will help in resolving the traffic problem.

2 Literature Survey

In 2018, Mousa et al. [2], Lah et al. [6] proposed a system where the possible solution includes an IoT Cloud system for traffic monitoring and quick warning. Geo-location and speed data are collected by a GSM/GPRS/GPS TK103 tracker based on the system installed in vehicles and the data is sent through OpenGTS servers which are stored in a SQL database, presenting instantly OpenStreetMap visualization of traffic outline. The disadvantage is that it fails to plan to inspect the impression of the reliability in system which not used in future.

In 2018 Celesti et al. [3], Nagmode and Rajbhoj [5] proposed a system where the implementation is done which senses the existence of such gases and uploads the data to the website and sends the information to the concerned people. The next part of this work is vehicle monitoring unit, which can be static in vehicles. The system will track the location of the vehicle, detect the accidents that cause to the vehicle, monitors its engine temperature and presence of poisonous gases. This system also contains the feature where it locates the vehicle and avoid it from moving till the message is sent by the owner. The further part of the system is that vehicle which do signal jumping are detected and punished. This system is used in the countries where the traffic is more violated. The drawback of this system is that it is not used for future.

Recently in 2017, Soleh et al. [4], Nagmode and Rajbhoj [7] proposed a system where vehicle traffic flow is monitored by vehicle detection, tracking, counting. Here the vehicle detection is done by background detection algorithm and morphology operation. The detected vehicle is tracked by adaptive measurements. The vehicles are counted by the counting lines when the vehicles pass after it. This system efficiently counts the vehicle by adaptive tracking; yet it is recommended to use the method which combines the calculation with distribution state estimation method like kalman filter.

Recently in 2017, Ye et al. [8], Dubey and Rane [9], Talukder et al. [10] proposed a system in which real time vehicle traffic is monitored by using IOT including Sensing Technology. In real time application ultrasonic sensor are used to distinguish the traffic at different tracks. Then the managed and identified data is moved to server through WIFI. However the disadvantage of the system is, it makes use of sensors which need to be placed on each lane of road.

In 2016, Gao et al. [11], Tian et al. [12] planned a system where innovative method is used to detect the traffic thickness and user attention jointly which uses the wireless private communication system which is real and consistent. The proposed method will detect the records and estimate the traffic data using the real time and ancient traffic data. But the system is designed for the prediction of traffic not for proficiently monitoring a traffic.

In the literature to summarize the traffic congestion is controlled by various methods using sensors like ultrasonic sensor which is used to detect the vehicle traffic level. The existing systems also make use of RFID, camera, Vehicle Ad-hoc Network, Image processing algorithm, such as Haar-cascade and Background subtraction and also make use of traffic dataset. But the existing system is not so efficient in solving the traffic congestion problem. In order to overcome, the proposed framework an image processing technique is used to monitor the traffic which would not led in traffic congestion.

3 Methodology

Figure 1 portrays the detailed diagram of the proposed framework.

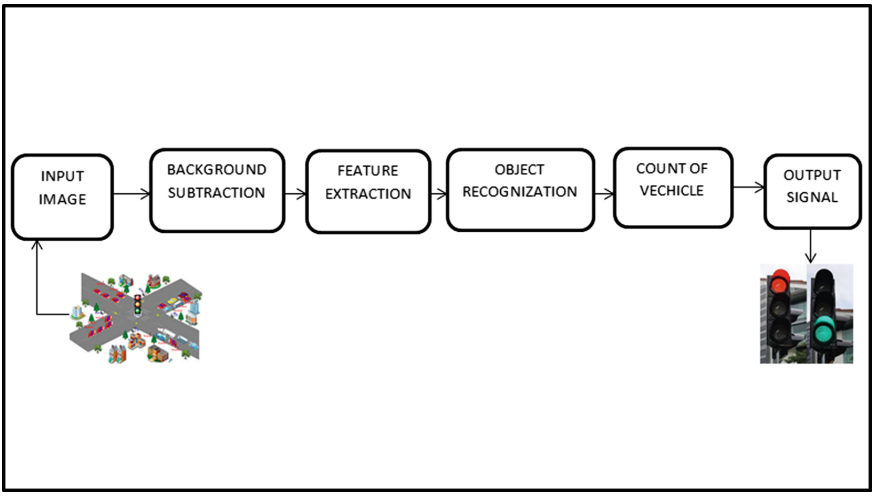


Fig. 1. Block Diagram

The proposed system consists of following stages:

Stage 1: The images are captured from the camera which is located at the centre of the traffic lane and the captured images are processed.
Stage 2: The background subtraction method take place where the objects are tracked and the foreground elements are extracted from background models.

Stage 3: The feature extraction. Where the images are extracted as given input so that the extracted images can be used as the relevant data.
Stage 4: The object recognition is done. The vehicles present in the traffic lane are recognized and density is calculated.
Stage 5: Counting the number of vehicles present in the particular lane. Each traffic lane vehicles are counted and estimated.
Stage 6: When once counting of vehicles is done then the centroid value of each lane is estimated. If the centroid value is more than the particular lane consist of high centroid value that traffic signal is made green. Thus the signals are outputted to traffic lane.

4 Experimental Setup

Figure 2 appearances the several segments of the proposed system which embraces Arduino Uno microcontroller, Zigbee segment, LED lights and power supply. These segments are unified for proficient traffic control. The results of the processed images are transmitted to Zigbee module. Arduino Uno accepts the data since the Zigbee segment. According to the data received by the Arduino Uno the traffic signal are given.

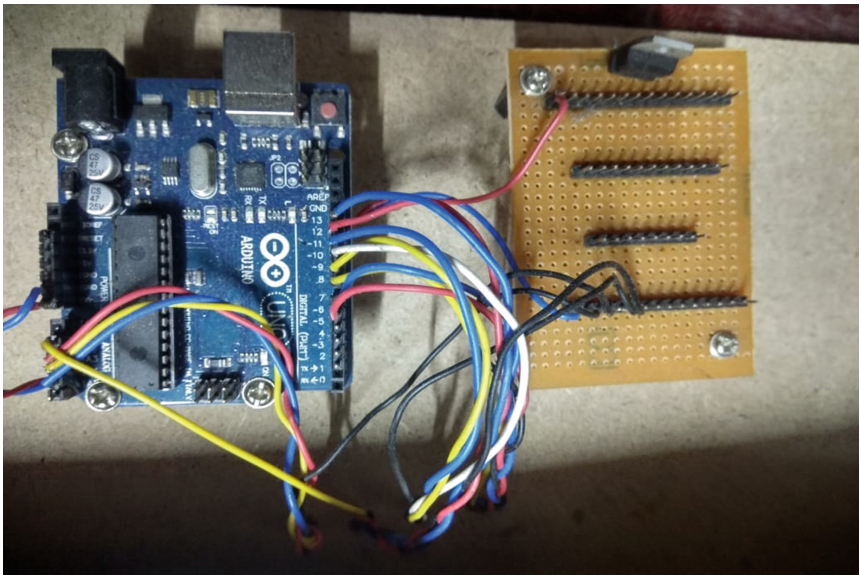


Fig. 2. The Hardware experimental arrangement

Figure 3 demonstrate the experimental arrangement of the proposed framework. Small toy cars are used to pretend a traffic consequence on the traffic junction.

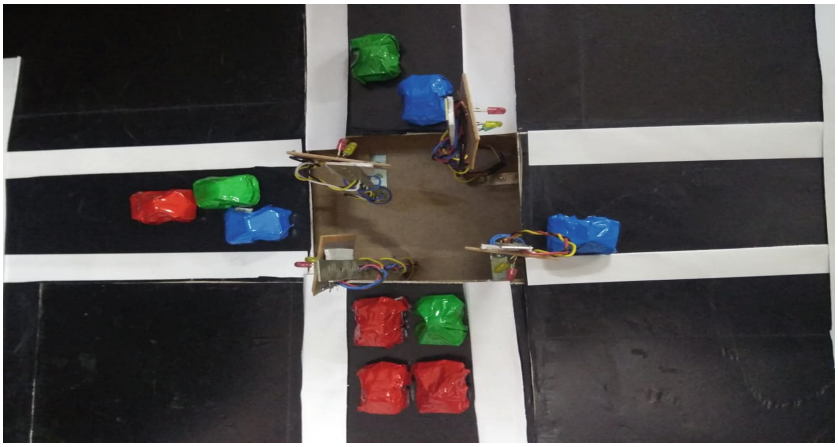


Fig. 3. The implementation of vehicle traffic monitoring system

Video recording of each lane is done by the camera which is installed in the traffic junction. Images are captured from the video for every 5 s. The captured images are processed and the objects are identified. The total vehicle count in each of the four lanes is calculated. The calculated count of the vehicle is transmitted to Arduino Uno through Zigbee module. The Control signal is sent for the traffic light by Arduino. So the green signal is activated to the lane with maximum vehicles.

5 Results and Discussion

The Table 1 shows the number of vehicles present in the lane_1, lane_2, lane_3 and lane_4. The first row in the table shows that lane_1 has more number of vehicles present than other lanes, so the lane_1 will be provided with green signal and rest other lanes are provided with red light. In second row, lane_1 has more number of vehicles so the green signal will be updated and other lanes are provided with red signal. The third rows represents that lane_2 has got more number of vehicles so green signal is updated to lane_2 and rest lanes are updated with red signal. The fourth row represents that lane_5 and lane_4 will be having same number of vehicles and lane_2 and lane_4 are having 0 numbers of vehicles. Now the preference given to the lane that is calculated first, so lane_1 will be provided with green signal rest lanes are provided with red signal.In the fifth row the lane_4 has more number of vehicles compare other lanes so the lane_3 will be provided with green signal and rest lanes are provided with red signal. To avoid the accidents in real time we introduced a minimum of 5 s delay between switching the lights from green to yellow then red. In this way the vehicles are calculated in the lanes and based on the more number of vehicles present in the lanes the green signal will be updated to the lane.

Table 1. Represents testcases with number of vehicles in the traffic junction.

Test case	Lane_1	Lane_2	Lane_3	Lane_4	Green signal
1	5	4	3	2	Lane_1
2	4	3	3	1	Lane_1
3	1	5	4	3	Lane_2
4	5	0	0	5	Lane_1
5	2	3	4	1	Lane_3

The results are processed in the MATLAB by calculating the centroid values of the object in the images. These calculated values are sent to Arduino using Zigbee wireless connection. The traffic signals are altered according to the results received by the Arduino. The lane with highest vehicle density gets the green signal.

6 Conclusion

To address the difficulties in Traffic management, an efficient traffic monitoring system is introduced, which monitors the traffic in real time. The snapshots will be processed to extract the details of the vehicle density at intersection of each side and the time slots for the traffic signal will be computed. As the development is object-driven, the system has a scope for modification. In future, if anyone wants to build a complex system for handling complicated roads, they can easily develop complex systems over our proposed system or use our system as a module in it. Experimental results show that this system has good performance and robustness, which can satisfy the need of time monitoring. Certain intelligent traffic monitoring system successfully implemented on some particular region will not be successful on some other regions.

References

1. Naik, T., Roopalakshmi, R., Ravi, N.D., Jain, P., Sowmya, B.H.: RFID-based smart traffic control framework for emergency vehicles. In: 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018) (2018)
2. Mousa, M., Abdulaal, M., Boyles, S., Claudel, C.: Wireless sensor network-based urban traffic monitoring using inertial reference data. IEEE. 978-1-4799-8856-3/15 $31.00 © 2015
3. Celesti, A., Galletta, A., Carnevale, L., Fazio, M., Lay-Ekuakille, A., Villari, M.: An IoT cloud system for traffic monitoring and vehicular accidents prevention based on mobile sensor data processing. IEEE Sens. J. **18**(12), 4795–4802 (2018)
4. Soleh, M., Jati, G., Sasongko, A.T., Jatmiko, W., Hilman, M.H.: A real time vehicle counts based on adaptive tracking approach for highway video. IEEE. 978-1-5386-2038-0/17/ $31.00 c 2017
5. Nagmode, V.S., Rajbhoj, S.M.: An IoT platform for vehicle traffic monitoring system and controlling system based on priority. In: 3rd International Conference on Computing, Communication, Control and Automation (ICCUBEA) (2017)

6. Lah, A.A.A., Latiff, L.A., Dziyauddin, R.A., Kaidi, H.M., Ahmad, N.: Smart traffic monitoring and control architecture and design. In: IEEE 15th Student Conference on Research and Development (SCOReD) (2017)
7. Nagmode, V.S., Rajbhoj, S.M.: An intelligent framework for vehicle traffic monitoring system using IoT. In: International Conference on Intelligent Computing and Control (I2C2) (2017)
8. Ye, D., Liu, X., Liu, G., He, B., Lin, H.: Self-organization traffic flow methods based on traffic intelligent control systems. In: 29th Chinese Control And Decision Conference (CCDC) (2017)
9. Dubey, A., Rane, S.: Implementation of an intelligent traffic control system and real time traffic statistics broadcasting. In: International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017 (2017)
10. Talukder, M.Z., Towqir, S.S., Remon, A.R., Zaman, H.U.: An IoT based automated traffic control system with real-time update capability. In: IEEE-2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (2017)
11. Gao, Y., Hong, A., Zhou, Q., Li, X., Liu, S., Shao, B.: Prediction of traffic density and interest using real time mobile traffic data. In: International Conference on Identification, Information and Knowledge in the Internet of Things (2016)
12. Tian, S., Shi, S., Gu, X.: Framework design of monitoring system for traffic based on embedded and RFID technology. IEEE. 978-1-4799-5344-8/15/$31.00 ©2015

Analysis of Breast Cancer Dataset Using Big Data Algorithms for Accuracy of Diseases Prediction

Ankita Sinha(✉), Bhaswati Sahoo, Siddharth Swarup Rautaray, and Manjusha Pandey

KIIT Deemed University, Bhuneshwar, India
ethosankita@gmail.com, {bhaswati.sahoofcs, siddharthfcs,manjushafcs}@kiit.ac.in

Abstract. Data Mining Techniques easily handle and solve the problem of handling the massive amount of data due to heterogeneous data, missing data, inconsistent data. HealthCare is one of the most important applications of Big Data. Diagnosis of diseases like cancer at an early stage is also very crucial. This paper focuses on the prediction model analysis for the breast cancer diagnosis either benign or malignant at an early stage as it increases the chances for successful treatment So predicting breast cancer at benign increases the survival rate of women. Data mining classification algorithm like SVM, Naive Bayes, k-NN, Decision Tree compares a variety of statistical techniques like accuracy, sensitivity, specification, positive prediction value, negative predictive value, area under curve and plotted ROC curve in R analytical tool which is promising independent tool for handling huge datasets is proven better in a prediction of the breast cancer diagnosis.

Keywords: Big data · Cancer · Breast cancer · Data mining classification algorithm · R analytical tool · Prediction

1 Introduction

Breast cancer mostly endows in women usually sustain in women breast's duct or glands. Breast cancer diagnosis is of two types Benign and Malignant. In benign the cancerous cell spread slowly throughout the other body parts and malignant is the dangerous one as it spread very rapidly throughout the other body parts and effects lungs, kidney, brain, skin, etc. So the diagnosis of breast cancer at preliminary increases the chances of overcomes from the cancerous cells. For the analysis and extraction of information from the large massive amount of datasets is quite challenging for analyst and also faces the problem regarding the prediction analysis of diseases because of noisy data, inconsistent data, missing values in large datasets. So the Data Mining techniques with Big Data Analytical tool come into the pictures. Data Mining Classification Algorithm always play a vital role in Prediction analysis, which compares a variety of statistical techniques for different Data Mining Classification

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 271–277, 2020.
https://doi.org/10.1007/978-3-030-37051-0_31

Algorithm that analyzes the current and historical facts to make predictions about the unknown events (either benign or malignant).

This paper is organized into section as follows. Section 2 summarizes the background followed by a brief discussion of breast cancer-related research work. The experimental setup steps are discussed in Sect. 3. Section 4 is all about the brief introduction of the classification algorithms like naive bayes, decision tree, SVM, k-NN. Problem definition for Predictive analysis of breast cancer followed by dataset collection attributes information, comparative analysis is discussed in Sect. 5. Section 6 is the conclusion, summarizes a brief overview of the proposal followed by and future work.

2 Background

Breast cancer is very different and complicated disease occur in one's breast's ducts and gland with multiple symptoms like pain in breast part or may be a pain in nipples, rosiness or decrease in the density of breast or nipple, irritation in nipples and many more. It can be easily analyzes in blood tests, MRI test, mammogram test or in CT scan. Result gives the details of effective biopsy tissues and that area of breast goes for advanced treatment like surgery, chemotherapy, radiation, hormone therapies. When the breast cancer is diagnosed in benign stage it can be easily cure within 5 years but if it is diagnoses as malignant it is very different to recurred it. Since to focus on the breast cancer related research, some related work on breast cancer is provided. Sakri et al. [1], evaluated the naive bayes, k-NN and fast decision learner in order to increase the accuracy of breast cancer recurrences prediction model by using feature selection i.e. Particle swarm optimization with an objective to reduce the number of attributes and the naive bayes generates the best output among all the other classifier with PSO and without PSO. Alwidian et al. [2], proposed a new prediction technique with new pruning methodology i.e. WCBA for weighting and pruning with an objective to produces more accurate association rule based on a statistical measure in order to enhance the accuracy level of association classifier. Asri et al. [3], compares the Wisconsin breast cancer datasets performances on different classifiers like the random forest, naive bayes, idk on WEKA which gives best and high accuracy results for naive Bayes. Tripathy et al. [4], introduces a new technique i.e. Parallel SVM for risk analysis with an objective to generate best and an efficient way to work on large datasets based on map reduce. Bhardwaj and Tiwari [5], introduces a new genetically optimized neural network algorithm to classify breast tumor benign or malignant with an objective to deal with classification issues and compares the performances like accuracy, sensitivity, specificity, confusion matrix, ROC curve, area under curve. Gupta et al. [6], presented the overview of all the latest research on breast cancer using a data mining algorithm to upgrade the breast cancer detection and prediction.

3 Experimental Setup

The systematic diagram of the proposed prediction analysis model as shown in Fig. 1, sketched after studying number of papers. Initially, breast cancer data are collected from Kaggle and then datasets are subjected to data pre-processing in order to remove noise, inconsistent, outliers and missing values. Then data mining classification algorithms is applied and obtain the output as performances statistical results, we compared the all statistical measures like accuracy, sensitivity, specificity, auc, ROC cure, ppv, npv for different data mining classification algorithms. And in the final step, we will do a prediction based on result analysis.

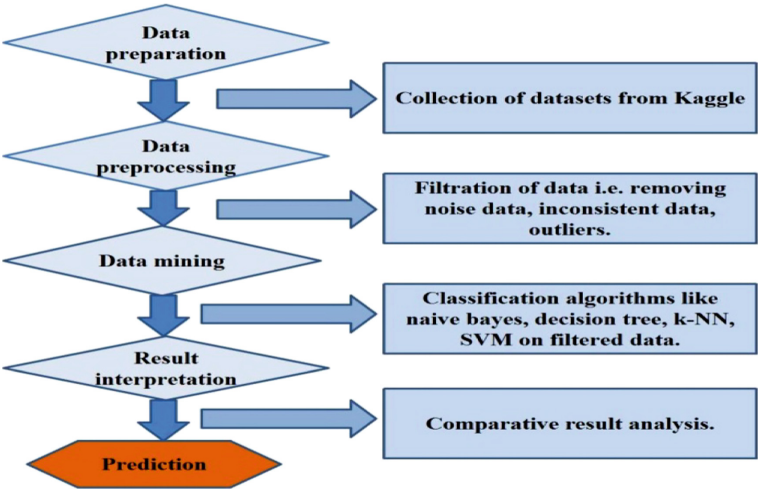


Fig. 1. Schematic diagram for prediction analysis [1–5]

4 Classification Algorithm

In the research area, data mining has appealed a lot of consideration because of the excessive amount of data and for extracting the new information and insight pattern for unknown events. Data mining is also known as Knowledge Discovery Databases (KDD), used for exploring new and appropriate information from a massive amount of datasets [7].

4.1 Decision Tree

It is a very simple classifier represent in the form of a tree diagram that exhibits the range of possible outcomes and after the initial decision, the subsequent decision comes into the picture (Tables 1, 2 and 3).

Table 1. Advantages and disadvantages of decision tree

Advantages	Disadvantages
Easy to understand and generates rules	Training cost is high, over fitting
Reduces problem complexity	Document connected to one branch

Table 2. Advantages and disadvantages of naive bayes

Advantages	Disadvantages
Fast in train and classify the data	Assume independence of features
Handle discrete, streaming data, missing value	Outcome is very biased results

Table 3. Advantages and disadvantages of support vector machine

Advantages	Disadvantages
High accuracy & less over-fitting	Training time is high for large data
Uses small and clean datasets	Less effective for noisy data

4.2 Naive Bayes Classifier

Naive Bayes classifier is the collection of classifier family where all the pair of feature shares the common principle but independent to each other based on Bayes Theorem.

4.3 Support Vector Machine

SVM is used for text classification like assignment, detecting spam and sentiment analysis. It is mainly used for image reorganization as well as in aspect-based classification and also in colour based classification [8–10].

4.4 k-Nearest Neighbour

k-Nearest Neighbour is also known as the lazy learning algorithm which classifies the datasets based on their similarity measures with a neighbour and k stands for the number of datasets items that are considered for classification [9] (Table 4).

Table 4. Advantages and disadvantages of k-NN

Advantage	Disadvantage
Non-parametric & best performing text classifier	Difficult for similarity measure
Handle large amount of predictors	Computationally expensive

5 Problem Definition of Predictive Analysis of Breast Cancer

5.1 Data Source

To classify all the classification algorithm, we have used Kaggle Wisconsin Breast Cancer datasets. The datasets consists of 31 attributes and one class attribute i.e. diagnosis with 699 instances. Figure 2 presents the attribute specification of datasets of breast cancer.

Sl.no	Attribute	Description
1	id	ID number
2	radius_mean	mean of distances from center to points on the perimeter
3	texture_mean	standard deviation of gray-scale values
4	perimeter_mean	mean size of the core tumor
5	area_mean	mean area inside the boundary of core tumor
6	smoothness_mean	mean of local variation in radius lengths
7	compactness_mean	mean of perimeter^2 / area - 1.0
8	concavity_mean	mean of severity of concave portions of the contour
9	concave points_mean	mean for number of concave portions of the contour
10	symmetry_mean	mean of similar area of tumor parts that matches
11	fractal_dimension_mean	mean for "coastline approximation" – 1
12	radius_se	standard error for the mean of distances from center to points on the perimeter
13	texture_se	standard error for standard deviation of gray-scale values
14	perimeter_se	standard error for mean size of the core tumor
15	area_se	standard error for mean area inside the boundary of core tumor
16	smoothness_se	standard error for local variation in radius lengths
16	smoothness_se	standard error for local variation in radius lengths
17	compactness_se	standard error for perimeter^2 / area - 1.0
18	concavity_se	standard error for severity of concave portions of the contour
19	concave points_se	standard error for number of concave portions of the contour
20	symmetry_se	standard error for mean of similar area of tumor parts that matches
21	fractal_dimension_se	standard error for "coastline approximation" – 1
22	radius_worst	"worst" or largest mean value for mean of distances from center to points on the perimeter
23	texture_worst	"worst" or largest mean value for standard deviation of gray-scale values
24	perimeter_worst	"worst" or largest mean value for mean size of the core tumor
25	area_worst	"worst" or largest mean value for mean area inside the boundary of core tumor
26	smoothness_worst	"worst" or largest mean value for local variation in radius lengths
27	compactness_worst	"worst" or largest mean value for perimeter^2 / area - 1.0
28	concavity_worst	"worst" or largest mean value for severity of concave portions of the contour
29	concave points_worst	"worst" or largest mean value for number of concave portions of the contour
30	symmetry_worst	"worst" or largest mean value for similar area of tumor parts that matches
31	fractal_dimension_worst	"worst" or largest mean value for "coastline approximation" – 1
32	diagnosis	The diagnosis of breast tissues (M = malignant, B = benign)

Fig. 2. Detail description of dataset [11]

5.2 Comparative Analysis

A Confusion Matrix helps in finding the comparison between classifier by computing Accuracy, Sensitivity, Specificity, Area under curve and ROC curve [12]. Confusion Matrix table for breast cancer diagnosis is shown in Table 5.

Table 5. Confusion matrix for breast cancer

Diagnosis	Classified as benign	Classified as malignant
Benign	TP	FN
Malignant	FP	TN

Table 6 gives the performance result of classifier algorithms. According to performance table the SVM gives the highest accuracy i.e. 97% as compared to other classification algorithms.

Table 6. Performance table of classifier algorithms

Classifier	Acc (%)	Sen (%)	Spec (%)	PPV (%)	NPV (%)	AUC
Decision tree	91.15	93.85	87.50	91.04	91.30	0.9516
Naive bayes	95.33	97.49	66.51	83.06	94.00	0.9649
SVM	97.35	61.07	41.99	63.93	39.04	0.9888
k-NN (Roc)	85.94	97.48	66.51	83.05	94.00	0.8572
k-NN (Acc)	74.99	81.23	22.16	63.73	41.22	0.8147

True Positive: Probability of (+) given the individual has the Benign stage.
False Negative: Probability of a Benign stage tests negative (-).
True Negative: Probability of (-) given the individual does not have the benign stage, have Malignant stage;
False Positive: P(+|M) = Probability of a Malignant stage tests positive (+).

Figure 3 represents the ROC curve for the different classification classifiers and SVM classification techniques is the superior algorithm as compared to other classifier. SVM gives higher accuracy and higher area under curve.

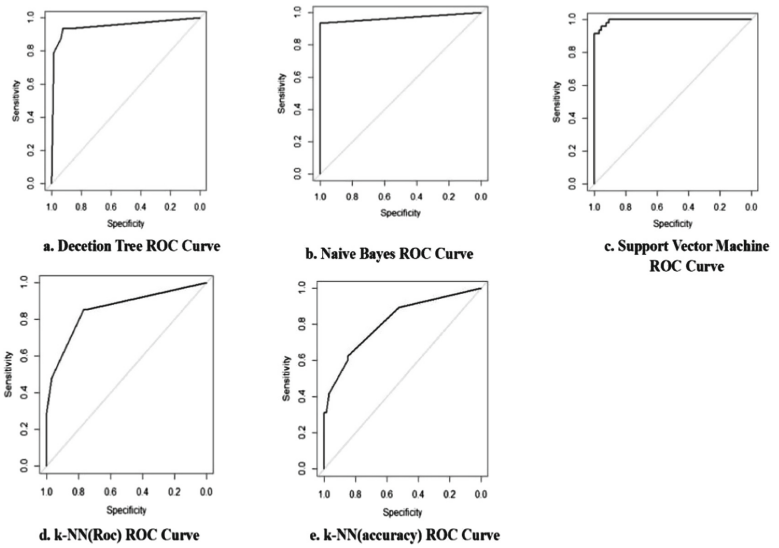


Fig. 3. Roc curve of different classifier

6 Conclusion and Future Work

Data mining classification algorithm enhances the work of predictive analysis we have presented the results of our experiments on popular classifying algorithms, NB, DT, SVM and k-NN and SVM generates better output in both field accuracy and ROC curve as it produces highest area under curve as compared to other classification techniques. In future work we will try to implement model, in association rule mining techniques on Breast Cancer Wisconsin-datasets.

References

1. Sakri, S.B., Rashid, N.B.A., Zain, Z.M.: Particle swarm optimization feature selection for breast cancer recurrence prediction. IEEE Access **6**, 29 (2018)
2. Alwidian, J., Hammo, B.H., Obeid, N.: WCBA: weighted classification based on association rules algorithm for breast cancer disease. Appl. Soft Comput. **62**, 536–549 (2018)
3. Asri, H., Mousannif, H., Al Moatassime, H., Noel, T.: Using machine learning algorithms for breast cancer risk prediction and diagnosis. Procedia Comput. Sci. **83**, 1064–1069 (2016)
4. Tripathy, P., Rautaray, S.S., Pandey, M.: Parallel support vector machine used in map-reduce for risk analysis. In: 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1–4. IEEE (2017)
5. Bhardwaj, A., Tiwari, A.: Breast cancer diagnosis using genetically optimized neural network model. Expert Syst. Appl. **42**(10), 4611–4620 (2015)
6. Gupta, S., Kumar, D., Sharma, A.: Data mining classification techniques applied for breast cancer diagnosis and prognosis. Indian J. Comput. Sci. Eng. (IJCSE) **2**(2), 188–195 (2011)
7. Witten, I.H., Frank, E.: Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann, San Francisco (2005)
8. Zaki, M.J., Meira Jr., W.: Data mining and analysis: fundamental concepts and algorithms. Cambridge University Press, New York (2014)
9. Jonsdottir, T., Hvannberg, E.T., Sigurdsson, H., Sigurdsson, S.: The feasibility of constructing a Predictive outcome model for breast cancer using the tools of data mining. Expert Syst. Appl. **34**(1), 108–118 (2008)
10. Han, J., Pei, J., Kamber, M.: Data mining: concepts and techniques. Elsevier, New York (2011)
11. Database. http://archive.ics.uci.edu/ml/datasets/breast+cancer+wisconsin+(diagnostic)
12. Shah, C., Jivani, A.G.: Comparison of data mining classification algorithms for breast cancer prediction. In: 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1–4. IEEE (2013)

CPW Fed Antenna with Beveled Radiating Strip and Ground Plane for Ultra Wide Band Applications

K. A. Ansal, Divya Susan Jose(✉), and Riboy Cherian

Department of Electronics and Communication Engineering, Saintgits College of Engineering, Kottayam, India
divya.sjl7l9@saintgits.org

Abstract. The design and analysis of Coplanar waveguide fed antenna for ultra-wideband application is proposed in this paper. The designed antenna has a compact size of 28 mm × 32 mm and provides impedance matching over a bandwidth of 3.07–11.58 GHz. The characteristic parameters such as return loss, voltage standing wave ratio, current distribution and gain are simulated and these parameters compliance with existing UWB standards. The results are simulated and analyzed using Ansys HFSS Electromagnetic Solver Version-16.2.

Keywords: Coplanar waveguide · Defected ground structure · Ultra-wideband · Beveled radiating strip

1 Introduction

The term ultra-wideband (UWB) was introduced by US Department of Defence (DoD) around 1989. It refers to signals having relatively large bandwidth. It is this large bandwidth that distinguishes UWB signals from conventional signals/systems. Generally signal bandwidth refers to the range of frequencies containing certain energy content or a certain power level of a signal. Federal Communication Commision (FCC) officially released regulations for UWB technology in 2002. The UWB covers a bandwidth of 7.5 GHz (3.1–10.6 GHz). Recently UWB system achieves a lot of attention because of its properties such as high data rate, low power consumption, reliability, immunity to interference and its applications in areas such as radar, data communication, location and tracking, image sensing etc. [1, 2].

Now a days most of the wireless portable devices require antenna operated at different frequencies for various wireless transmission functions. This may result in challenges in antenna design such as antenna space limitation, multi antenna interference etc. Inorder to solve this problem we need to have ultra wideband antenna. One UWB antenna can be used to replace multiple narrow band antenna there by effectively reducing the antenna number. In the last decade various omni directional UWB antennas have been developed along with wireless system miniaturization and increased operation bandwidth. It mainly consist of two types, planar monopole antenna and printed monopole antenna. Planar monopole antenna can be realized by simply replacing conventional wire monopole with planar monopole which is located above the ground. Various geometries of planar monopole such

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 278–284, 2020.
https://doi.org/10.1007/978-3-030-37051-0_32

as circular, elliptical, trapezoidal etc. provides wider bandwidth. But the planar monopole needs a perpendicular ground plane which may result in increased antenna volume. So for most wireless portable devices prefer printed monopole antennas. Printed monopole antennas have a monopole patch and groundplane. CPW or microstrip line is used to excite the monopole. Compared to omnidirectional UWB antenna directional UWB antenna has higher gain. Most popular among them is the printed wide slot antenna. It consist of wide slot tuning stub fed using CPW or microstrip line. Here the slot shape plays an important role in improving the bandwidth compared to the shape of tuning stub. The slot shape includes rectangular, circular, tapered, hexagonal etc. The simplest among them is rectangular slot. In addition to the regular slot or tuning stub several irregular shapes are also introduced for UWB application. Sharma et al. [3] proposed a CPW fed antenna for UWB application. Here the slotted rectangular patch is used to obtain a wide bandwidth. The antenna proposed by [4] consists of two symmetrical strips having two steps and CPW feeding. This design provides good impedance matching and low dispersion. A number of techniques have been introduced to make better the bandwidth of the antenna. These techniques include the use of beveling plate, double feed or an asymmetrical feed arrangement, trident- shaped feeding strip, etc. [5–12].

In this paper, a miniaturized CPW fed antenna with an area of 28 × 32 mm^2 is proposed. The design and simulation of the antenna are done using high-frequency structure simulator which is based on the finite element method. The antenna provides an impedance bandwidth of 3.07–11.58 GHz with VSWR < 2. Appropriate gain and radiation pattern are also obtained.

2 Design of Proposed Antenna

The theoretical values of Wand L are obtained from Eq. (1) for the centre frequency f_0 = 6.85 GHz. The parametric optimized values of W and L are obtained using high frequency structure simulator (HFSS). These values are shown in the Fig. 1.

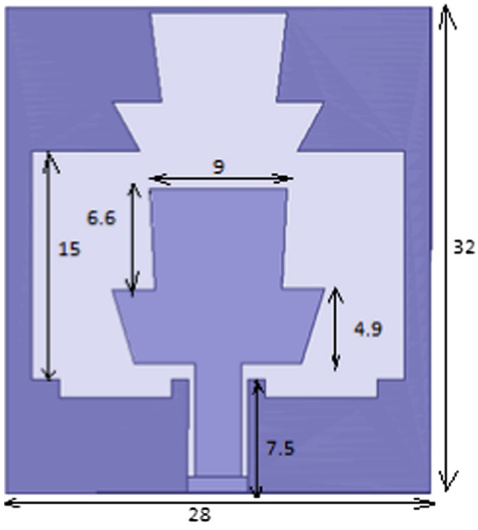


Fig. 1. The proposed antenna geometry

The antenna is printed on FR-4 epoxy substrate with a size of 28 × 32 mm^2 and a height of 0.8 mm with dielectric constant 4.4 and loss tangent 0.001. CPW means coplanar waveguide. That is the radiating strip and ground plane are on the same side of the substrate. So it is easy to integrate with MMICs. The CPW feed has a characteristic impedance of 50 Ω. 50 Ω is used as a standard characteristic impedance value since the characteristic impedance for maximum power transfer is 30 Ω and for minimum attenuation is 70 Ω. CPW fed Antenna with Bevelled Radiating Strip and Ground Plane is a good candidate for ultra-wideband application. Introduction of beveled radiating strip can increase the upper frequency band. Inorder to obtain the desired range, the beveling angle should be adjusted. The antenna has irregular wide slot. In the upper part of the ground a slot similar to the shape of beveled radiating strip is created to obtain the desired bandwidth.

$$W = L = \frac{c}{2f_l\sqrt{\varepsilon_{eff}}} \tag{1}$$

3 Simulation and Results

The antenna performance is evaluated using HFSS software. For this antenna, the basic parameters are simulated.

3.1 Return Loss (RL)

Refection coefficient is the amount of signal that get reflected back to the source while it is transmitting through a line. The amount of signal that is lost when it is reflected back is the return loss. For an efficient antenna the 'RL' should be more negative. RL of the antenna is given in Fig. 2.

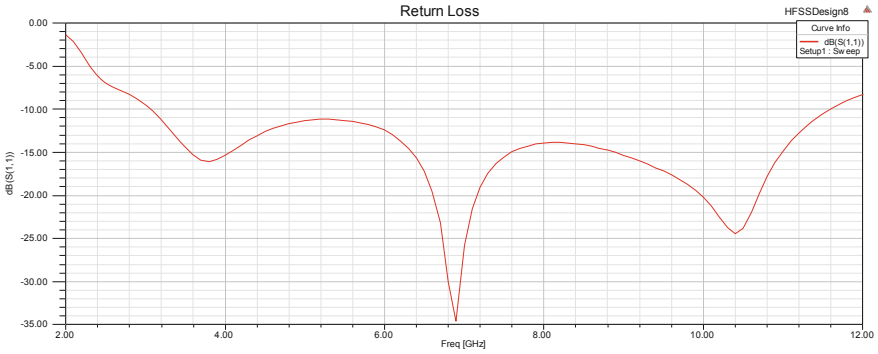


Fig. 2. The RL characteristics of the presented antenna

A bandwidth of 8.5 GHz is obtained and return loss values of −16.07 dB, −37.08 dB and −24.46 dB are obtained at 3.74 GHz, 6.89 GHz, and 10.4 GHz respectively.

3.2 VSWR

VSWR is Voltage Standing Wave Ratio. It is the amount or degree of mismatch between antenna and line. The simulated VSWR results of the antenna are shown in the Fig. 3. From the graph, we can find that antennas impedance bandwidth extends from 3.07–11.58 GHz with VSWR less than 2. For an efficient antenna the value of VSWR should be closer to 1.

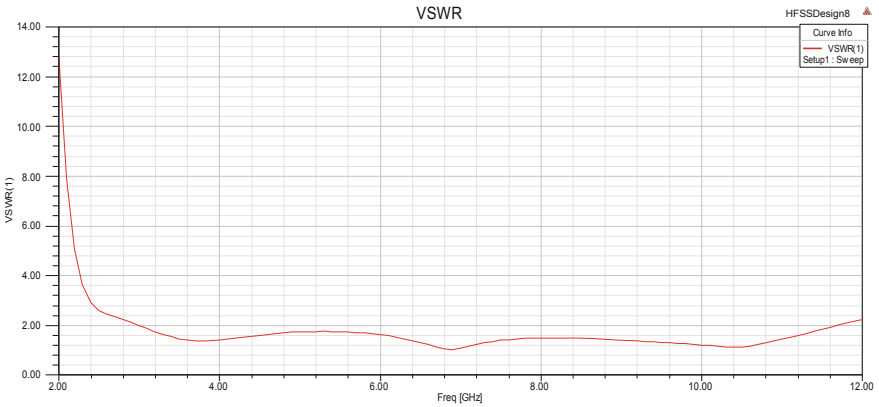


Fig. 3. VSWR of the presented antenna

The values of VSWR are 1.37, 1.03 and 1.12 at 3.74 GHz, 6.89 GHz and 10.4 GHz. This antenna shows good performance for UWB applications since it covers the spectrum defined by FCC for UWB.

3.3 Gain (G)

The simulated 'g' of the proposed antenna is illustrated in Fig. 4.

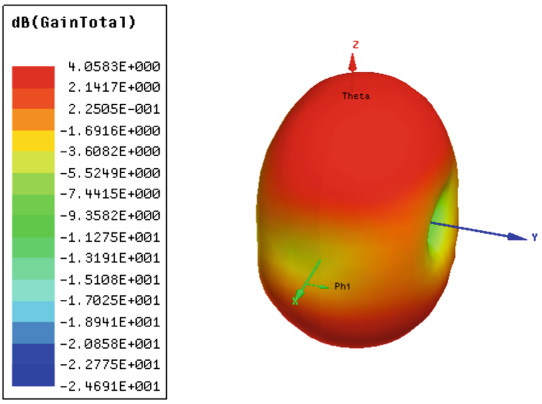


Fig. 4. 'g' of the presented antenna

A stable gain with an average of 4.05 dB is obtained over the entire UWB operating band.

3.4 Radiation Pattern (R)

The 'R' of the proposed antenna is shown in Fig. 5.

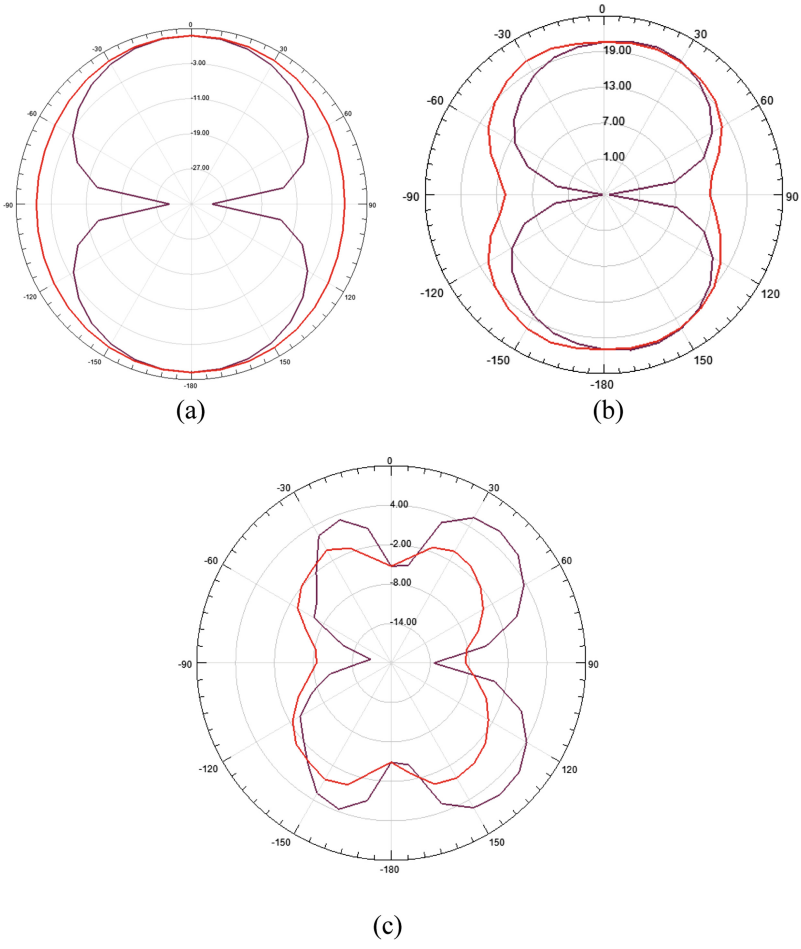


Fig. 5. 'R' of proposed antenna at (a) 3.74 GHz (b) 6.89 GHz (c) 10.4 GHz

In order to plot the radiation pattern of the presented antenna, we use two planes. The x–y plane plots the E plane while y–z plane plots the H plane. The antenna has good omnidirectional radiation pattern at 3.74 GHz frequency. At 6.89 GHz the radiation pattern has deviated from omidirectional pattern. At 10.4 GHz the radiation pattern gets more deviated from the omnidirectional pattern.

3.5 Current Distribution

Figure 6 shows the surface current distribution of various peak frequencies.

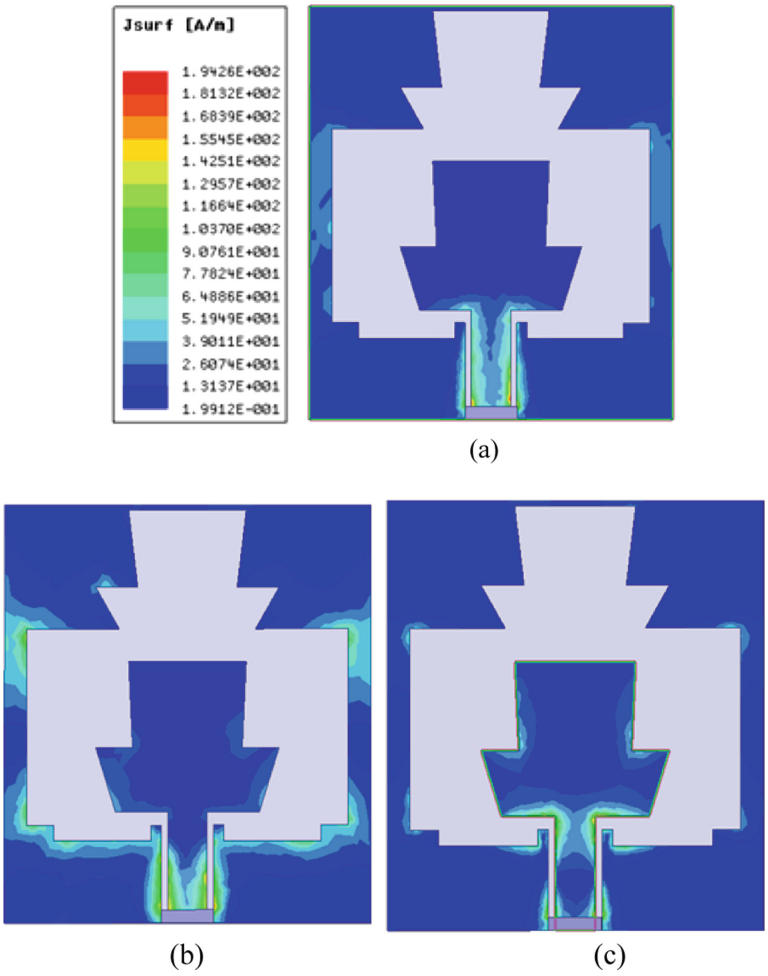


Fig. 6. Surface current distribution of antenna at **a** 3.74 GHz, **b** 6.89 GHz, **c** 10.4 GHz

At 3.74 GHz the electric current density is concentrated at the sides of the ground, feed and lower portion of the patch. At 6.89 GHz the electric current density is concentrated at sides, the upper and lower portion of ground, feed, and sides of the patch. At 10.4 GHz the electric current density is concentrated at sides and lower portion of ground, feed, the upper and side portion of the patch.

4 Conclusion

A compact novel coplanar waveguide fed UWB antenna is presented. The antenna shows a bandwidth ranging from 3.07–11.58. UWB band is achieved by beveled radiating strip and ground plane. The miniature size and simple structure of the antenna makes it a good candidate for UWB applications. In the future, this work is going to integrate with transreceiver system for wide range of coverage. Ansys HFSS electromagnetic solver is used to simulate various antenna parameters.

Acknowledgment. Authors are greatly acknowledged Centre for Engineering Research and Development (CERD) for the financial support given for doing the project.

References

1. Siwiak, K., McKeown, D.: Ultra Wideband Radio Technology. Wiley, Hoboken (2004)
2. Liang, J.: Antenna study and design for ultra wideband communication applications, Ph.D. Thesis, (2006)
3. Sharma, P., Kumar Jha, S., Pratim Bhattacharya, P.: A new CPW-fed patch antenna for UWB applications. J. Telecommun. Inf. Technol. 75–78 (2017). https://doi.org/10.26636/jtit.2017.112017
4. Park, S.Y., Oh, S.-J., Park, J.-K.: A simple CPW Fed UWB antenna design. J. Koren Inst. Electromag. Eng. Soc. **10**(1), 1317 (2010)
5. Ammann, M.J., Ning Chen, Z.: A wideband shorted planar monopole with bevel. IEEE Trans. Antenna Propag. **51**, 901–903 (2003)
6. Ammann, M.J.: A wideband monopole for reconfigurable multiband radio terminal. IEEE Trans. Antenna Propag. **1**, 170–173 (2001)
7. Antonino-Daviu, E., Cabedo Fabres, M., Ferrando Bataller, M., Valero-Nogueira, A.: Wideband double-fed planar monopole antennas. Electron. Lett. **39**, 1635–1636 (2003)
8. Ammann, M.J., Ning Chen, Z.: An asymmetrical feed arrangement for improved impedance bandwidth of planar monopole antenna. IEEE Trans. Antenna Propag. **40**(2), 156–158 (2004)
9. Subbarao, A., Raghavan, S.: Compact coplanar waveguide-fed planar antenna for ultra wideband and WLAN applications. Wirel. Pers. Commun. **71**(4), 2849–2862 (2013)
10. Kumar, A., Shanmuganantham, T.: A CPW fed octagonal patch UWB antenna with WiMAX band notched characteristics. In: International Conference on Information, Communication and Embedded Systems (ICICES 2014) (2014)
11. Chandelkar, A., Shanmuganantham, T.: Compact CPW Fed U shaped antenna with defected ground plane for WiMAX/UWB applications. In: 2014 International Conference on Computer Communication and Informatics (2014)
12. Lu, G., von der Mark, S., Korisch, I., Greenstein, L.J., Spasojevic, P.: Diamond and rounded diamond antenna for ultra wideband communications. IEEE Antennas and Wirel. Propag. Lett. **3**(1), 249-252 (2004)

Two-Level Text Summarization with Natural Language Processing

Rupali Hande(✉), Avinash Sidhwani, Deepesh Sidhwani, Monil Shiv, and Divesh Kewalramani

Vivekanand Education Society's Institute of Technology, Mumbai, India
{rupali.hande, 2015avinash.sidhwani, 2015deepesh.sidhwani, 2015shiv.monil, 2015divesh.kewalramani}@ves.ac.in

Abstract. Text summarization is the process of shortening a text document in order to create a summary covering important points, aspects of the original document. Text summarization methods are based on extractive model and abstractive model. Two-level text summarization is used to form summary of different news articles. In the first level, multiple news articles are read and first level summary is generated. These multiple summaries are then analyzed and a single summary concerning the news topic is generated in second-level. TextRank with TF-IDF algorithm is used which is an extractive summarization technique to create news summary. The performance of the summary is evaluated using ROUGE matrix.

Keywords: Text summarization · Extractive-based summarization · Abstractive-based summarization · TextRank algorithm · TF-IDF algorithm · ROUGE matrix

1 Introduction

There is surfeit of textual material available on the internet, and it is growing every single day. This data is very large and the best we can do is to navigate it through search and skim the results. Due to immense amount of text data available on the internet, it has become difficult to find information which is relevant to user's requirements. To obtain such relevant information from the internet, user needs to jostle through entire article which causes a glut of information. Also, it leads to wastage of time and efforts. To overcome this problem, text summarization will help people to get relevant data from much condense form of a document. Text summarization curtails length of source document into significant content without adulterating main thought of document. With this, user can understand the idea of the document within short period of time.

There are two different approaches for text summarization which are abstractive and extractive.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 285–291, 2020.
https://doi.org/10.1007/978-3-030-37051-0_33

1.1 Extractive Text Summarization

In extractive based summarization, predominant sentences are selected and merged to generate concise summary without altering the sentences from source text. The major task of extractive summarization is to determine which sentences from source document are notable and credible to be included in the final summary. To select the sentences from source document we assign a score to each sentence based on its characteristics. After assigning score, sentences which rank highest are likely to be included in the final summary [1]. There are various methods used for extractive text summarization such as term frequency-Inverse document frequency method, Cluster based method and Graph based method, etc. [2] proposed the use of TextRank algorithm—a graph-based ranking model for text processing. The model is used in various natural language processing applications.

1.2 Abstractive Text Summarization

In abstractive based summarization, first we need to understand the source text and then generate summary which are not copied from source text and the result text may contain new text phrases. To generate abstractive summary we need to use natural language processing techniques. Abstractive summary contains new sentences that aren't the part of original source text [1]. Structured based approach and semantic based approach are different types of approaches for abstractive text summarization.

Shouzhong and Minlie [3] proposes the use of TextRank model with TF-IDF factor for extracting user interests keyword in microblog texts. Our proposed system presents similar concept in creating the news summary. We are referring multiple articles to summarize the broader picture of the news. The generation of summary is divided in two levels. At first level, TextRank algorithm is applied on each news article to create first level summary. At the second level, these summaries are referred and TextRank algorithm with TF-IDF factor is applied to create the final summary. In addition to this, we are using sentiment analysis in the second level to understand if any sentence is biased and if that sentence is included in the final summary, then that sentence is highlighted. ROUGE matrix is used for evaluating the performance of the summary.

2 Related Work

2.1 Two-Level Text Summarization

Two-level summarization helps to extract relevant information from different sources in the first level and generate a concise single summary in the second level. Mirani et al. implemented Two-level Text Summarization from online news sources, they used extractive based technique to form the summary [4]. In the first level, the news article URLs are fetched and provided as input. Two/Three summaries were generated by assigning scores to sentences based on frequency of words. They performed sentiment analysis to show whether news channels have any different views. The second level summary is generated by extracting important sentences from two/three first level

summaries, using the same algorithm. ROUGE matrix is used to evaluate the performance of the summary.

2.2 TextRank Algorithm

TextRank algorithm is a graph-based unsupervised model which helps in understanding the relations among the sentences. The algorithm ranks the sentences and the higher ranked sentences are selected for final summary. Mihalcea et al. proposed the TextRank algorithm, which is based on Google's PageRank algorithm [2]. The algorithm creates graphs from the texts written in natural language. The graph is used for ranking the sentences. They evaluate the application of TextRank to two language processing tasks consisting of unsupervised keyword and sentence extraction. For sentence extraction, each graph vertex represents a sentence to be ranked. The similarity between vertices(sentences) is measured depending on their content overlap. The two vertices are connected if they are similar. The algorithm analyzes the information from the source text, and thereby identifies the most important sentences in the text. Another important aspect of this algorithm is that it can be adapted to extracting very short summaries.

2.3 TextRank with TF-IDF Factor

TextRank algorithm with TF-IDF factor can be used in multi-document text summarization. Shouzhong et al. presented a framework for mining and analyzing personal interests from microblog text, with an algorithm which integrates term frequency-inverse document frequency (TF-IDF) with TextRank [3]. Their system preprocessed the posts, comments and reposts in various categories to select the keyword. The keyword appears in both category system and microblogs. Later, weight is assigned to each category to calculate the weight of each keyword to get TF-IDF factors. This helps in obtaining the keyword of interest. An improved model was proposed (named as $\text{TextRank}_{\text{TFIDF}}$) by introducing the TF-IDF factor in the iterative calculation of the TextRank algorithm. This model blends the advantages of both TextRank model and TF-IDF model and gives better results.

2.4 Sentiment Analysis

Sentiment analysis give the overall sentiment of a piece of text, i.e. it judges the positivity and subjectivity of a sentence. Bhelande et al. presented their work on sentiment analysis which identifies controversial news [5]. The core idea is that controversial news is the one that contains mixed sentiments in it. Once the sentiment is found, then based on several outputs, controversial news can be identified. They collected news from Twitter, as controversial news in social media affects the accuracy of online content. Finally, they displayed the controversial news via a user interface.

3 Architecture and Methodology

Different documents will be passed as input to our system. The content of the document will be related to each other. We will carry the summarization process in two steps. In the first level, we generate summaries of related documents using extractive method. After this, we perform sentiment analysis to identify potentially biased statements and finally, generate second level summary using the TF-IDF approach. The block diagram of our architecture is shown in Fig. 1.

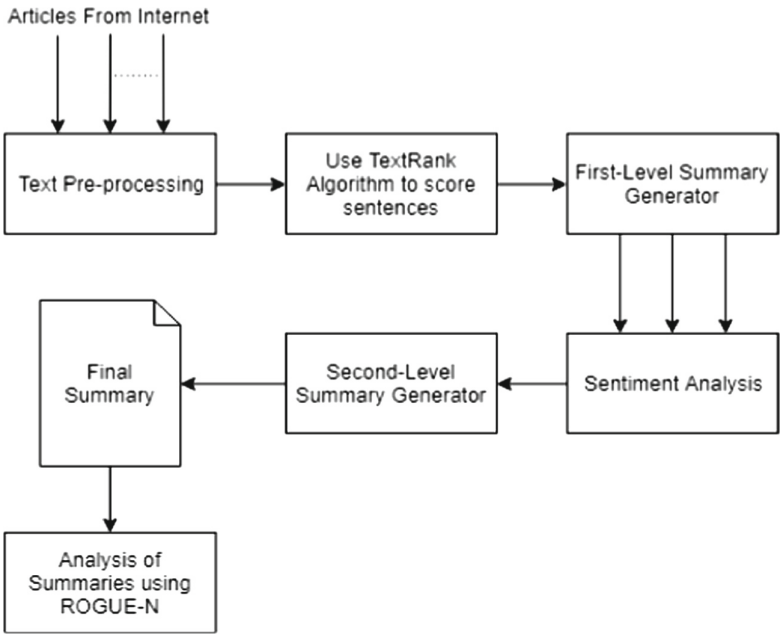


Fig. 1. Block diagram

3.1 First-Level Summary

As our system will summarize online news articles, links of news articles will be provided as input. These articles are generally raw data, so it will be noisy. To remove noise we have to do some pre-processing (methods for preprocessing). The system will web scrape the whole page and will remove HTML tags from the documents. After this, the article will be converted into lower case and all the punctuation characters are removed. To remove stop words from our documents, each sentences in the document is splitted and then sentences are splitted into words. Stop words are then removed by comparing each word with dictionary. After this we store clean sentences in vectors.

Now we will use extractive summarization to generate summaries for each article. First, we fetch vectors (with the help of the GloVe word vectors) for each word in a sentence and then take mean of those sentences to obtain a vector for the sentence. Thus, we find the vector for each sentence in the article. Next, we find similarities

between sentences using the cosine similarity approach and generate a graph where, each node represents a sentence and each edge represents the similarity score between two sentences. Now, we apply the TextRank formula to obtain the sentence rankings and select the top N sentences (based on rankings) to generate the summary.

3.2 Sentiment Analysis and Second-Level Summary

Here, we will have different summaries of related documents. First, we perform sentiment analysis on each sentence. This gives us the subjectivity and polarity of each sentence. If there is a subjective sentence, which has a polarity different from other sentences, it means that it has the potential to represent biased views. More work needs to be done on this part to detect biased statements more accurately.

While generating second-level summary, task will not be as tough as it was to generate first-level summary. Here the data will contain less noise which will help to generate much more concise summary. We provided article links as input in the first-level. Here, in the second-level, different first-level summaries will be provided as input.

The process to generate the summary will be modified a bit, by introducing TF-IDF factor in the formula. TF-IDF factor helps in understanding how common or rare is a particular word. The higher the TF-IDF factor, the rarer the word and the smaller the TF-IDF factor the more common is the word.

The TF-IDF factor for a particular word is calculated as follows:

1. We first calculate the Term-Frequency (TF) of the word in the entire article.

$$\text{TF} = \frac{\text{no.of times the word appears in the document}}{\text{no.of words in the document}} \quad [3]$$

2. We then calculate the Inverse Document Frequency (IDF) of the word

$$\text{IDF} = \log\left(\frac{\text{total no. of documents}}{\text{no. of documents containing that word}}\right) \quad [3]$$

3. Multiply TF*IDF and the resultant value is called as TF-IDF factor.

The TF-IDF factor is introduced in the formula to increase the probability of jumping to vertices with higher correlation. Finally, the modified TextRank algorithm (i.e. $\text{TextRank}_{\text{TFIDF}}$) is used to generate second level summary.

4 Evaluation of Summaries

The summaries are evaluated using ROUGE Matrix, which stands for Recall-Oriented Understudy for Gisting Evaluation [4]. ROUGE is a human-based evaluation of summaries. In this the summary generated by computer is compared with human summary on the same topic. There are two values computed for evaluation, these are

Recall and Precision, Recall tells us how much of the source reference summary (human summary) is the computer generated summary covering. It is calculated as

$$\frac{\text{number\_of\_overlapping\_words}}{\text{total\_words\_in\_reference\_summary}}$$

Precision tells us how much of the system generated summary was required or needed. It is calculated as

$$\frac{\text{number\_of\_overlapping\_words}}{\text{total\_words\_in\_system\_summary}}$$

These values are evaluated for different n-grams (unigrams, bigrams, etc.), these n-grams refer to the number of words the summaries (both system and reference summary) are considered. For instance, in unigram the source summaries are divided into single word and then it's precision and recall are generated. ROUGE-1 refers to overlap of unigrams between reference summary and system summary. ROUGE-2 refers to the overlap of bigrams between reference summary and system summary. The reason higher level ROUGE-N are computed is to evaluate the fluency of the system generated summary. If the words are in same order as the reference summary then that means the system summary is fluent. ROUGE-N technique is used after the second level summary is generated. It helps in evaluating the key points present in the final summary.

5 Conclusion

The intent of two-level text summarization is to ensure that the user is provided with a factual and verified summary. The technical approach in the form of extractive summarization establishes the purpose. The summarization system possesses tacit knowledge of the content and vocabulary to generate precise judgement for intelligible summaries. Multiple articles are referred to ensure the broad coverage of a news [2]. The accuracy achieved by TextRank algorithm is competitive with the previously proposed state-of-the-art algorithms [3]. We have improved the TextRank algorithm by integrating TF-IDF factors. The algorithm aggregates the benefits offered by both the models and outperforms other methods in terms of average Rouge scores (precision, accuracy and recall). In the future, the research can be extended to studying the effect of neural network in text summarization. As the news articles have certain important words, we can assign different weights to that particular word, which will change the weights of statements in the news article. These sentences can be inputted through axon to a suitable activation function which can summarize the article much more accurately. The important thing that neural network can bring is that the synaptic strengths (the weights) are learnable and so we can control the strengths of sentences influence in summary.

References

1. Andhale, N., Bewoor, L.A.: An overview on text summarization techniques. In: 2016 International Conference on Computing Communication Control and Automation (ICCUBEA). https://doi.org/10.1109/iccubea.2016.7860024, 12–13 Aug 2016, Pune, India (2016)
2. Mihalcea, R., Tarau, P.: TextRank: bringing order into texts. https://web.eecs.umich.edu/~mihalcea/papers/mihalcea.emnlp04.pdf
3. Shouzhong, T., Minlie, H.: Mining microblog user interests based on TextRank with TF-IDF factor. ScienceDirect **23**(5), 40–46 (2016). https://www.sciencedirect.com/science/article/abs/pii/S1005888516600560
4. Mirani, T.B., Sasi, S.: Two-level text summarization from online news sources with sentiment analysis. In: 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), 20–22 July 2017, Trivandrum (2017)
5. Bhelande, M., Sanadhya, A., Purao, M., Waldia, A., Yadav, V.: Identifying controversial news using sentiment analysis. Imper. J. Interdisc. Res. (IJIR) **3**(2) (2017). ISSN 2454-1362
6. See, A., Liu, P.J., Manning, C.D.: Get to the point: summarization with pointer-generator networks. Cornell University (2017)

Visual Cryptography and Image Processing Based Approach for Bank Security Applications

Bageshree Pathak, Darshana Pondkule(✉), Rasika Shaha, and Apurva Surve

Department of Electronics and Telecommunication, Cummins College of Engineering for Women, Pune, India
{bageshree.pathak, rasika.shaha}@cumminscollege.in, {darshanapondkules, apurvasurvel}@gmail.com

Abstract. Authentication is a critical step in initializing a bank transaction. Core banking and net banking systems use ID cards, passwords/PIN, OTP, etc. for authentication. However, these methods are still prone to forgery and hacking, due to which unauthorized person could gain access to user's account. We propose a methodology which uses an image share as authentication key. This has been created using visual cryptography and other image processing techniques to encrypt authentication parameters. It is encrypted such that the share becomes incomprehensible to human eyes and non-decryptable by hacker, thus protecting the data from forgery or hacking. This paper proposes a double authentication system where user is identified by decrypted image and PSNR value. Hence this system provides a very high level of security.

Keywords: Authentication · Cryptography · Decryption · Encryption · Extended visual cryptography · PSNR · Watermark security

1 Introduction

Authentication is validating user's identity. It is used in banks to determine whether the given user is the rightful owner of concerned account, to decide whether to allow or deny access to user. We propose a system where a unique image known as 'Encrypted share' is given to each user by the bank, which is used for authentication. Core banking uses signature, photograph, or ID card details like pan-card/UID number for authentication. Since public knows what details are used for verification, forgery of the same is possible. If authentication parameter is undisclosed, forgery is avoided. Hence, our image share is designed to hide verification parameters. Net Banking uses OTP to authenticate transaction. OTP can be accessed if device is cloned. Our encrypted share designed is incomprehensible to recreate. It is made accessible only via linked devices. The hackers cannot provide the same image as input to bank application from their side. Decryption of images is harder than decryption of string of alphanumeric data as it is multidimensional entity; hence generation of image key is preferred.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 292–298, 2020.
https://doi.org/10.1007/978-3-030-37051-0_34

Visual Cryptography is a method to generate multiple noisy shares of an image which are encrypted such that combining these shares reveals the hidden image. We combine our authentication parameter as a secret image with a color image, for generating encryption share using a variation of visual cryptography approach. Unlike other cryptography techniques, we do not hide the secret image in encrypted share, rather form a different image altogether that can be mapped to secret image if keys i.e. color image and passkey are known.

2 Literature Survey

In [1], secret sharing is used to encrypt secret image into some specified cover image. This paper uses symmetric secret key for encryption of image and secret shares are generated from this image. It produces meaningful shares. Secret key ensures security of scheme.

In [2], a complex algorithm divides image into some parts for encryption process. k–n secret sharing scheme is special type of visual cryptographic scheme. Encryption of the image is done using random integer generator.

In [3], multiple images can be hidden in all image types using image rotation in various angles. Direct binary search using halftone had good quality shares resulting in good recovered image with good contrast and less pixel expansions.

In [4] the secret image shares are watermarked with different cover images and are transmitted. At the receiving side, the cover images are extracted from the shares and stacked one by one which reveals the secret image progressively.

3 Methodology

In the proposed algorithm bank decides the identification parameters to be used for each user to form his/her information available to bank. It is saved as a secret image in a secured database created for authentication. A color image is taken as an encryption key, this image would be known to bank authentication database only. After using password decided by user, an encrypted share is generated by these three elements and given to the user. User should have both, password and encrypted share for verification. In net banking, password and share are generated like OTP and sent to device linked to the concerned account. Our system performs decryption on encrypted share, and compares decrypted share with secret image in authentication database using PSNR. The PSNR value is stored in that authentication database for every user. On every authentication request, if the encrypted share is correct and password is exact, then decrypted value of PSNR will match the value stored in database. Change in any one of these parameters will give a different PSNR value resulting in denial of access (Refer Fig. 1).

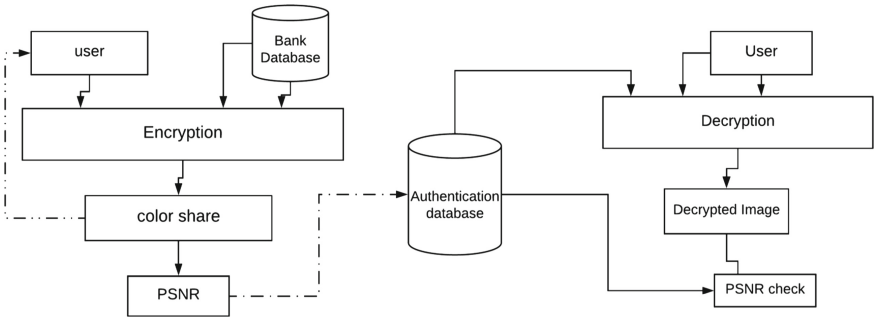


Fig. 1. Methodology

4 Implementation

Implementation is done in 2 parts. 1. Encryption 2. Decryption.

- Encryption
  Database is created in banks for every user. Steps used in the encryption algorithm to create the cryptographic image are as follows:

A. **Creation of watermark shares**

Step 1 The unique secret image that is provided to user is converted into binary.
Step 2 Generate random matrix same as size of the image.
Step 3 Generate three different matrix by shuffling the pixels from original image randomly. Watermark shares are shown in Fig. 2.

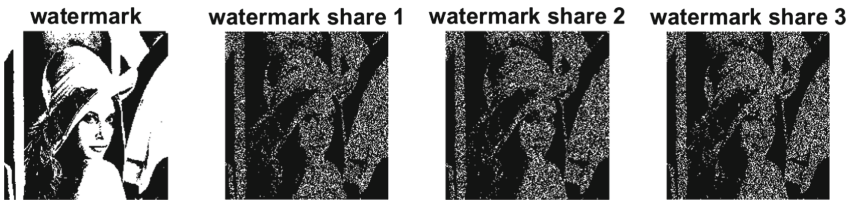


Fig. 2. Watermark shares

B. **Split color image into its R-G-B planes**
As shown in Fig. 3.

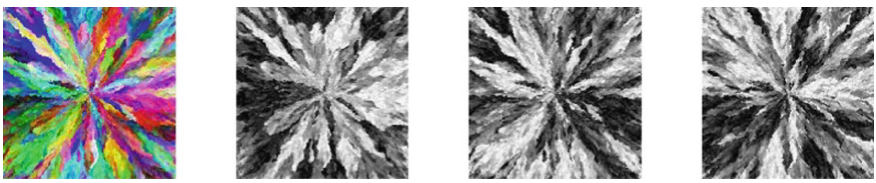


Fig. 3. RGB planes

C. **Creation of encrypted image**

- One watermark share with one plane of color image is taken as input every time.
- Passkey controls generation of verification matrix which becomes our encryption key.
- Map each element of random matrix to a pixel position in color image plane, this is known as mapping pixel.
- Determine conditions using properties of mapping pixel and its neighbors.
- According result of conditions given above and pixel value of watermark share assign two bit value to the mapped pixels in encrypted image.
- We obtain three different encrypted images for each combination of color image plane and a watermark share.
- Combine these three shares to form an encrypted share which will be present with the user for authentication.

Encrypted share seen in Fig. 4 will be given by bank to the user.

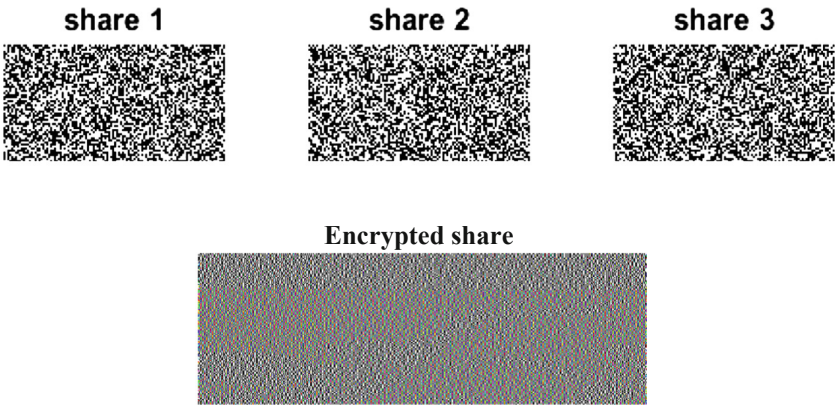


Fig. 4. Enrypted share

- Decryption

Inverse operation is performed in decryption to extract the secret image from the encrypted image. Function asks user to enter encrypted image and the passkey, and accesses color image stored in its database. Figure 5 shows flowchart for decryption of image.

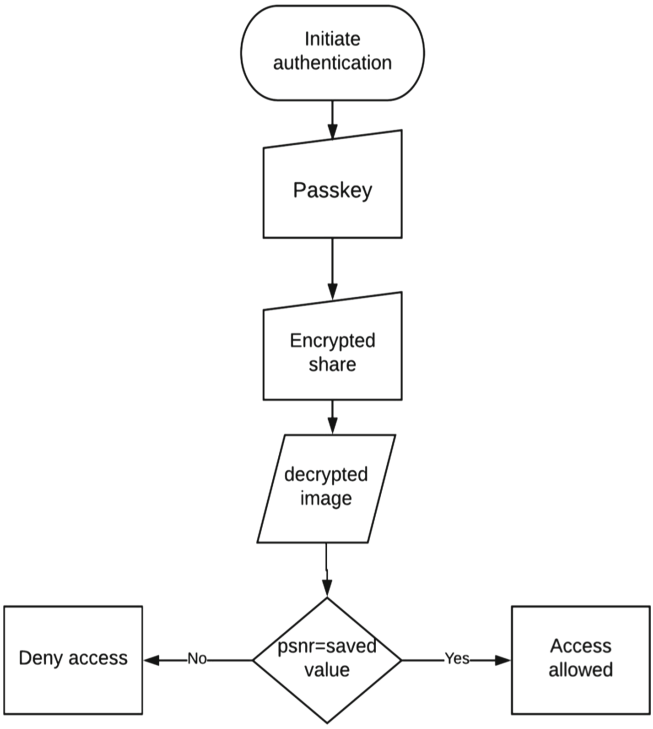


Fig. 5. Flowchart for decryption

PSNR is used to find the correlation between secret and decrypted image. PSNR is given by:

$$\mathrm{PSNR} = 10 * \log\left(255^2/\mathrm{MSE}\right) \tag{1}$$

$$\mathrm{MSE} = 1/(\mathrm{M} * \mathrm{N}) \sum \sum [\mathrm{I}(\mathrm{i},\mathrm{j}) - \mathrm{I}'(\mathrm{i},\mathrm{j})]^2 \tag{2}$$

The decrypted image after following the reverse procedure is as shown in Fig. 6.

Fig. 6. Decrypted image

5 Results

Decrypted image gives high and constant PSNR value if share and password both are correct, if different password or share is used, PSNR value drops drastically. PSNR value varies for different users. Figure 7 shows two cases of result of image with correct password and decrypted image with wrong password (Refer Table 1).

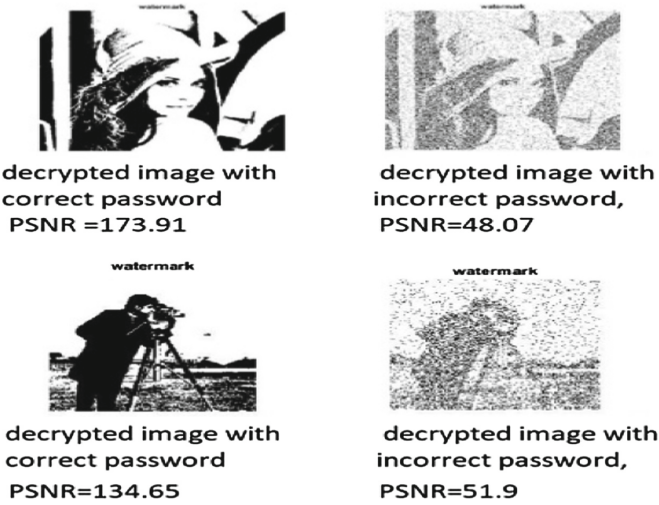


Fig. 7. Results

Table 1. Testing results

Secret image	Encryption passkey	Decryption passkey	PSNR
LENA	1234	1234	173.91
	1234	1264	48.5
	768	768	173.91
	768	76	48.5
ELIZA	234	234	153.61
	234	281	43.4
	896	896	153.61
	896	348	43.4

6 Conclusion

We have implemented a system where a user will be given a unique encrypted image which can be used for authentication in banks to handle core or net banking applications instead of sign/cards which are presently used. This system will avoid forgery by

hackers where the OTP or password can be hacked. Every share is randomly created in this system which increases its efficiency. The hacker is not able to extract the hidden image due to randomness which is otherwise possible in visual cryptographic systems. The drawback of the other systems being, revealing the information of the secret image is eliminated in our algorithm. This system has multi layer symmetric key encryption. Every user has specific PSNR value for his/her image. User does not have access to the database contents hence decrypted image and PSNR value is not known to the user as well as the hacker. The system may result in loss of data due to noise. The future scope for expansion can be achieved by combining biometric authentication along with our project. It can also be integrated into cloud for a more secure option with OTP.

References

1. Bidgar, P., Shahare, N.: Key based visual cryptography scheme using novel secret sharing technique with steganography. IOSR J. E &TC
2. Kandar, S., Maiti, A., Chandra Dhara, B.: K–N secret sharing visual cryptography scheme for color image using random number. IJCSI Int. J.
3. Liu, F., Wu, C.K., Lin, X.J.: Colour visual cryptography schemes. IET Inf. Secur. **2**(4), 151–165 (2008)
4. Saturwar, J., Chaudhari, D.N.: Secure visual secret sharing scheme for color images using visual cryptography and digital watermarking

Data Streaming Framework on Cloud Platform for Surveillance of Unmanned Sensors

G. Manjushree[1(✉)], A. Kalpana[2], N. H. Rajashekhar[2], and B. R. Shivakumar[1]

[1] CNE-Department of ISE, Bangalore Institute of Technology, Bangalore, India
manjushreegl4l2@gmail.com, shivakumarrajanna@gmail.com
[2] Central Research Laboratory-BEL, Bangalore, India
{kalpanaa, rajashekharnh}@bel.co.in

Abstract. By integrating various unmanned vehicles with ground station on a cloud infrastructure for data streaming, monitoring and visualization processes in real-time has been considered as a challenging task. In a traditional approach, data collection method for unmanned sensors is not flexible and it has various limitations when it is dealt with the humongous volume of data. To address this, we propose a cloud data framework for sensing, securing and maintaining the sensors from cloud for surveillance and take quick decision based on the input. The another main intention of this framework is to enhance the system throughput, reduce the man power and cost by leveraging unmanned sensors and all integrated sensors. In order to meet the above, we create a platform to support in all levels, such as infrastructure, network and software to simplify the processes and services. In addition, all integrated sensors tend to have multiple roles, all should be monitored, data should be captured and captured data will be analyzed and visualized.

Keywords: Data acquisition · Cloud computing · Microservices · Kafka · Containers · Elasticsearch · Kibana

1 Introduction

Data acquisitions from the sensors generate a large volume of data, which is also known as big data. We are in the era of big data, which is characterized by the fastest collection of ubiquitous information and which incorporates the endless information. The actual challenge is about collecting data and managing it as well. Earlier data acquisition system with Graphical User Interface (GUI) is providing valuable information about speed, altitude and GPS. Here altimeter and airspeed modules are interfaced with aurdino Uno microcontroller which is used to gather all real time data and reading of UAVs location and altitude. The data acquisition system is transmitted wirelessly via the XBee radio model to GUI. The disadvantage is the structure of an aurdino Uno model not support to build project with large data. Other approaches for the data acquisition system is by using proprietary data loggers and one is by building

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 299–307, 2020.
https://doi.org/10.1007/978-3-030-37051-0_35

the own system. The disadvantages of both the approaches are lined with more cost and the person should have the full knowledge of platform for controller [1]. The coordination of the data acqusition system with Graphical user Interface is developed [2]. This provides valuable information about speed, and altitude.

UAV resources are developed as a web services and provide their resources and services using the uniform interface through the Restful HTTP architecture. This concept is developed based on the internet of the things where the smart objects are connected to the internet for a unique identification. It provides smart objects with interfaces to be accessed through the World Wide Web. In our proposed method, using Restful HTTP architecture, integrating all unmanned sensors into Cloud paradigm where the unmanned sensors become part of the cloud infrastructure and can be accessed ubiquitously [3].

Existing System

On existing technology, integration of UAV helps to achieve a specific task. Currently, to control and monitor, the UAV's are required man power and resources in huge numbers. This is due to, minimal utilization of resources and lack of knowledge in technologies. To utilize the UAV's resources and services efficiently, UAV's are integrated with cloud computing to ubiquitous access of their services. Resource Oriented Architecture (ROA) model is proposed to utilize by UAV to access the service and send request through Application Programming Interface (API).

Client-server architecture uses a Representational State Architecture as a broker to efficiently utilize the resources. UAV register their services on broker, and requester can request a service from the broker. This approach has implemented by Cloud Computing technology. UAV and other devices on the network has connected using Internet of Things (IoT) and accessed and monitored the services through the concept of Web of Things (WoT). Cloud Computing is a shared pool of service provider and enabled ubiquitous, convenient, on-demand network and provisioned usage of resources. So this approach can be efficiently used by collaborative UAVs. This paper is proposed to design and develop a system to automate surveillance, which is capable for streaming the data from sensors and transfer the data to cloud for analysing and visualization [4].

2 Proposed Method

2.1 Background Cloud Architecture

Open Stack Cloud Infrastructure

Cloud computing is a tending to be a future of computing for resource utilization and services with reliability and security. Its providing a broad network access, flexible resource allocation, flexible capacity and application can deploy quicker than traditional methods. Data store on cloud ensuring data backup thus offering access to previous log data even when the unmanned sensors out of service and it increase the reliability. Sensors required continuous connectivity to the cloud and they can access the service and resource through standard API. Openstack is used to deploy the services

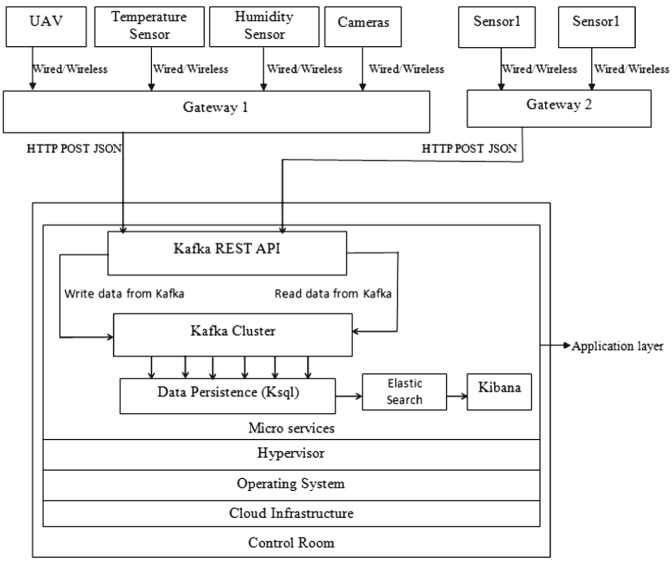


Fig. 1. System architecture

into cloud, the hadoop cluster is created for the purpose of integration and this is done for ubiquitous access and secure storage [5].

Microservices

Microservices are software architecture and that delivers functionality by composing small runtime services. This functionality is discrete, lightweight services with a well-defined API and it greatly improves the reliability and scalability. Functionality exposed through a browser UI and each service in the microservices is independent.

Docker Container

Docker is a computer software that is used for virtualization in order to have multiple os running on same host [6]. It is a client server type of application where clients relay to the server so called docker daemon. Docker images are source code for containers which helps to build containers. Containers are instances of Docker Image.

Applications like data acquisition, data persistence, and data visualizations are running as single microservices, hence each application run as single microservices, each microservices are further broke down into the processes which is running as a Docker container. Docker container can be indicated by Docker file and Docker composes.

2.2 Event/Data Streaming

Data streaming is the process of sending data continuously rather in batches. One of the popular tools used for streaming data is the Apache Kafka.

Kafka
It uses distributed publish-subscribe messaging system and a queue that can handle a large amount of data and enables message passing from one point to another point [7]. The data which is acquired from the sensor is the large volume of the data. Kafka is a distributed messaging system that collecting the high volume of data from the sensors with low latency. Once the messages are published, the consumer subscribed to the particular topics and read the messages from consumer [8]. The Kafka REST API provides a Restful interface to a Kafka cluster. Where can produce and consume messages by using the API.

2.3 Data Storage

It is the process of storing the data in the storage medium. KSQL is the streaming the SQL engine and powerful interactive SQL interface that enables real-time data processing using apache Kafka. In this project KSQL database is used as a storage medium since the data from Kafka is stored to the KSQL database.

2.4 Data Visualization

Visualization
To presenting huge amount of information, visualization is an art which can be accessible in a form of graph. Acquiring the data is not enough to understand about the data; hence to visualize it for better understanding of the data. In this project to visualize the different data we are using the Kibana tool.

Elastic Search
It is a search engine based on the real time search platform. To make search faster, it uses concept of indexing and it is a big data technology and schema less. The document will be indexed and representative fields are mapped the document stored in the form of index. It is also known as a database to store enormous amount of the data. Elastic search is used as the inter process communication between the Kafka and Kibana.

Kibana
Kibana ease the analysis and visualization. It queries with the elastic search engine which acts as both data store and visualization engine. In Kibana, the various types of graphs can be plotted depend upon the data which is used to visualize.

3 Implementation

The proposed project is to design a framework of data acquisition from different types of sensors and integration same to the cloud paradigm. The real time streaming data acquired from various integrated sensors and saved as CSV, JSON or XML format in offline mode for further data processing. Once huge volume of data is collected, it has to publish and subscribe as streams of records using Kafka under different topics. For implementation Apache Kafka has used for distributed streaming to replicate data on

multiple servers with low latency and high throughput. The major keystones of Kafka are the producers, brokers and consumers, and a key concept is the topic. The producer API which is reading the data from CSV, JSON or XML file and writes messages to a topic as a log in the order they arrive. Each message has an offset number which makes it possible to get the specific message's position in the log. The offset number starts at 0 and is increased for each message. Likewise distributed multiple streaming API writes data to Kafka topics which is managed by Kafka brokers. Multiple Kafka brokers form a Kafka cluster and it manages the data between the producers and consumers. And consumers can subscribe the data by topic and messages can be processed by using Kafka Streams. Producer and Consumer Kafka API's developed by Java.

The Fig. 2 shows how the producer and consumer read the record data using topics in the Kafka cluster.

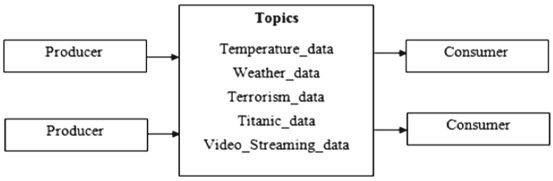


Fig. 2. Kafka producer and consumer

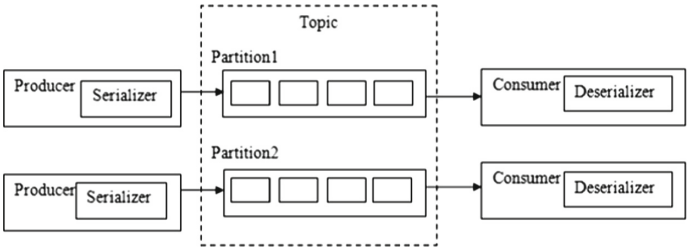


Fig. 3. Creation of Kafka producer and consumer

The Kafka producer will send the data where Consumer will consume that data. The overall creation of Kafka producer and consumer is shown in Fig. 3. To create a Kafka producer, we need to pass a list of bootstrap servers (a list of Kafka brokers). Which also specify a client id that uniquely identifies this Producer client. The message body is a string, so we need a record value serializer as records value field. The message id will be passed through a Kafka's records key.

Here we need to specify a Key serializer and a value serializer. To create a Kafka consumer, define properties which pass through the constructor of a Kafka consumer. The bootstrap server's configuration is to define the list of broker and its value, that is a list of host/port pairs that used by consumer to establish an initial connection to the Kafka cluster. The group id configuration identifies the consumer group of this consumer. The key deserializer class configuration is a Kafka deserializer class for Kafka record keys that implements the Kafka deserializer interface. The next process is data persistence and the data is stored into Ksql database. Spring Boot is a structure that

made easy development of web applications. It contains a many pre-configured modules which help to eliminate the manual addition of dependencies which is needed for developing an application with spring. The steps are explained below [9].

Steps:

- Create a java Maven application using spring starter libraries.
- With dependencies, create Artifact Group and Name for maven web project using spring boot and java, which will generate ZIP file to import as a maven project.
- In a workspace, spring boot application has created. After API has tested using REST controller. Output can be viewed while running and accessing the end point of API.
- To run the application as a Docker container, create a Dockerfile that will contain the steps to be executed by Docker to create an image of this application with all dependencies and run that image from Docker.
- JAR file create by Maven commands should be added in the pom.XML file.
- To do this process, clean up the target folder using maven clean and maven install. This procedure will create a jar file.
- These are the steps included in the dockerfile to create docker image.
  FROM JAVA
  EXPOSE 8080
  ADD/target/kafkadrive.jar kafkadrive.jar
  ENTRYPOINT [“java”, “-jar”, “kafkadrive.jar”]
- Docker image is created and create the container by execute the docker image.
- Now the Spring Boot application is running as a docker container on local system with port 8080.

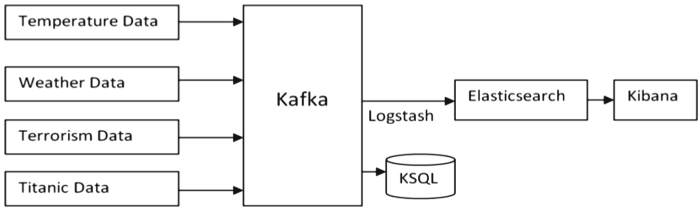


Fig. 4. Loading of data from Kafka to Kibana using elasticsearch

To data visualization module is done using the elasticsearch and the kibana. The data can be loaded to the elastic search using logstash from Kafka. Elastic search is a way to categorize data and make it easily available [10]. It is a highly scalable, distributed and full-text search engine. Elastic search is developed in Java. Elastic search is a standalone database server, which is written in Java and using HTTP/JSON protocol, it’s takes data and optimized the data according to language based searches and stores it in a primitive format. Logstash is a plug-in based data collection engine. Logstash input plug-in is used to collect the data from where it is placed as a queue. Filter plug-in which is to read the data and the input and output filter can be termed as codec plug-in. The configuration file is written by using the I/O plug-ins to read the data from the Kafka and stored into the elastic search [11]. The configuration file as shown below.

```
Input {
Kafka {
    Bootstrap_server = "localhost: 9092"
     Topic = ["datastream"]
        }
      }
Output {
Elasticsearch {
              Host = ["local host: 9200"]
              Index = "sensordata"
              }
          }
```

The configuration file is written by using the logstash plug-ins to read the data from the Kafka and stored into the elastic search. Once the data is stored into the elastic search using logstash and the data loaded into kibana and discover the data using discover tab. This can be done by creating an index pattern, Using similarity from the SQL world, indexing is similar to a database. And the data is visualized by using different types of the graphs as shown in Fig. 4. For an example the data which contains latitude and longitude can be visualized as a co-ordinate graph etc. Finally, microservices are integrated with cloud using Openstack.

4 Results

Surveillance system is used for analysis and exploration of object behaviour, monitoring and track the movement for take quick decision. Figure 5 shows the results obtained after data Visualisation, here the dashboard is created for various data like temperature data, weather data, terrorism data and titanic data.

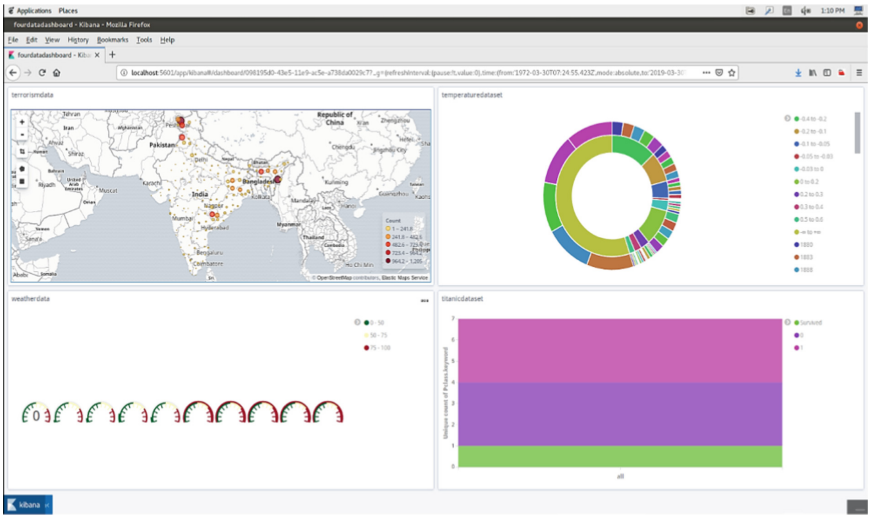


Fig. 5. Data visualisation dashboard

5 Conclusion and Future Work

Finally we conclude that this survey on data acquisition and data streaming with effective frameworks, works successfully with limited bandwidth and low latency. While acquiring and processing the data, it also requires ubiquitous access and security by handled cloud environment. In this paper, we discussed a Data Streaming Framework on Cloud Platform for Surveillance of Unmanned Sensors, which acquire the data from the integrated sensors efficiently and the data is used for further process like data visualisation and data persistence. Data has read in the form of messaging queues by using the Kafka, the data visualisation is done using elastic search and Kibana, the data persistence is by Ksql database, these applications as microservices that are integrated to cloud platform by using container on open stack cloud platform for ubiquitous access for surveillance.

For future research, data preprocessing of real-time streaming data should be considered rather than reading data as a batch. For realtime streaming, apache spark preprocessing model can be used and machine leaning algorithm can be apply on spark for scalable and integration with other tools. When data is increases in large size, data inspecting on dashboard is becoming complex and impractical. To inspect data on kibana dashboard, machine leaning algorithm can be used for better predictions and analyzation.

References

1. Masic, A.: Unmanned aerial vehicle as a data acquisition system. J. Trends Develop. Mach. **19**(1), 181–184 (2015)
2. Chavan, S., Patil, A., Kumar, N.: Data acquisition system for an unmanned aerial vehicle. Int. J. Sci. Technol. **1**(1), 333–337 (2015)
3. Mahmoud, S., Mohamed, N., Al-Jaroodi, J.: Integrating UAVs into the cloud using the concept of the web of things. J. Robot. **2015**, 1–10 (2015)
4. Mahmoud, S.Y.M.: UAV-Cloud: a platform for UAV resources and services on the cloud. M. Tech thesis, pp. 1–105, May 2015
5. Jadhav, B., Patnakar, A.B.: A framework for integrating cloud computing and big data analytics into e-governance using Openstack Sahara. In: Proceedings of ICTIS, vol. 2 (2018)
6. Rad, B.B., Bhatti, H.J., Ahmadi, M.: An introduction to docker and analysis of its performance. IJCSNS Int. J. Comput. Sci. Netw. Secur. **17**(3), 228–235 (2017)
7. Hiraman, B.R., Chapte Viresh, M., Karve Abhijeet, C.: A study of Apache Kafka in big data stream processing. In: International Conference on Information, Communication, Engineering and Technology (ICICET) (2018)
8. Narkhede, N., Shapira, G., Palino, T.: Kafka: the definitive guide real-time data and stream processing at scale. Textbbook
9. https://dzone.com/articles/micro-components-architecture-1
10. Gupta, P., Nair, S.: A survey paper on Elasticserach. Int. J. Sci. Res. 333–336 (2014)
11. Dharur, S., Swaminathan, K.: Efficient surveillance and monitoring using the ELK stack for IOT powered smart buildings. In: Proceedings of Second International Conference on Inventive Systems and Control, pp. 700–705 (2018)

12. Mohamed, N., Al-Jaroodi, J., Jawhar, I., Lazarova-Molnar, S.: Middleware requirements for collaborative unmanned aerial vehicles. In: International Conference in Unmanned Aircraft Systems (ICUAS), pp. 1051–1060 (2013)
13. Sridhar, S., Smys, S.: A hybrid multilevel authentication scheme for private cloud environment. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1–5. IEEE (2016)

High-Speed Big Data Streams: A Literature Review

R. Patil Sneha(✉) and V. Dharwadkar Nagaraj

Rajarambapu Institute of Technology Rajaramnagar, Sangli, Islampur 415414, Maharashtra, India
Snehal4688@gmail.com, nagaraj.dharwadkar@ritindia.edu

Abstract. In today's word, high-speed data streams are continuously generated via a variety of sources like social media and organizational business related data. We have listed the basic characteristics of big data and challenges in handling big data and data streams. This paper shows present work on processing and analyzing big data and data streams, real-time data analytics, decision making, and business intelligence. Our aim is to research different trends in distributed data analysis, a study on security of big data, applications of big data and processing of data streams. Even though there is vast research happening in the field of big data across the globe, still there is a scope of improvement in this field.

Keywords: Big data · Data streams · Nearest neighbor · Support vector machine

1 Introduction

1.1 Big Data and High Speed Data Streams

Data collection is the collection of data values and variables which are correlated to each other in some aspect and are different from one another in some another aspect. The size of data warehouses is growing massively. This leads to the development of the tools which are capable of extracting knowledge from the data. The information is created which is suitable for making decisions from the collected and analyzed data [1]. So, the data provides a resource for knowledge extraction and support of the decision. This database is the collection of organized data so that it can be accessed, managed and updated easily. Data mining can be defined as the process of discovering relevant knowledge such as associations, modifications, important structures from huge data stored in databases. This definition of data mining is widely accepted.

Based on this definition, data mining is an extremely complex extraction of previously unknown and useful information about the data required. It presents the hidden information patterns and relationships of a large amount of raw data. Big data is one of the newly postulated terms which are used to detect datasets with large size and having more complex data. So, this complex data cannot be stored, studied and analyzed with the currently available technologies of data mining software. The big data is a collection of heterogeneous structured as well as unstructured data. This has the capability

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 308–316, 2020.
https://doi.org/10.1007/978-3-030-37051-0_36

for extracting relevant information from the large sets of databases or the data streams which are currently impossible its volume and variety.

Big data is the collection of structured and unstructured data. The main reasons for the appearance and the growth of data big are the speed of processing, availability of data, increased storage capacity. It refers to the use of large data sets that handles the collection of data that serves the business and other industries in their decision making process. The data project on general, public or private aspects. This is featured with three respective V's i.e. Volume, Velocity, and Variety.

These are explained below:

Volume: refers to the size of data which is larger than terabytes and petabytes. The large size and increment of size make the storage and analysis of data very difficult.

Velocity: tells that the data should be used in a large amount in pre-defined time. The already existed method requires a huge time to control such a volume of data.

Variety: this big data originates from the different sources in which both structured as well as unstructured data is involved. The traditional systems were created to address a small volume of structured and reliable data. This big data is the geospatial data, 3D data, audio and visual, unstructured [2] text involving log and social media files.

Later, as the research advanced, below dimensions have been identified:

Veracity: according to IBM, it is defined as the unreliability of data with data sources. For e.g. sentimental analysis is using social networking websites like facebook, twitter, etc. to subjects their uncertainty. The reliable data is distinguished from the uncertain data which further is helpful to manage the unnecessary data.

Variability: variability and complexity are the two additional dimensions. The inconsistency in the big data analysis leads to a variable flow of data, which is called variability. Data are formed from several resources and the complexity is increasing which disturbs the data management. Data generated from different resources have different scenarios.

Low-value density: Data which is present in its original format is not much effective and remains unused. Data is used to discover high value for e.g. logs are taken from the websites which cannot be used in their original form to get desired business values. It should be analyzed to check the user's behavior.

1.2 Challenges in Big Data

Even though extensive studies are being carried out across the globe in the field of big data mining, there is still a huge scope of development and research. Some limitations and challenges in existing are listed below:

Scalability and Storage Issues: The data has grown much faster than the existing mining and processing systems. The system is not able to store this amount of data all its sudden. There is a need to introduce such a system that can and store a huge volume of data.

Timeliness of Analysis: The data is increased with time. Many applications like fraud detection, insurance, banking need real-time or likely to be the real-time analysis of the transmitted data.

Representation of Heterogeneous Data: With the development of cloud architectures, data is collected from a variety of resources. This combined data is not necessarily in the same structure or format. Thus, the need to handle such heterogeneous data is growing. Data formats like images, audio, visuals, social media are difficult to be stored and processed using tools like SQL. The data like images, video, music, word files, etc. are now able to be stored and shared with the help of smartphones. The use of smartphones is interestingly increasing and forcing our brains to work more. The process of representation of data like images, video, audio lacks efficient storage capacity.

Data Analytics System: Traditional methods like RDBMS are appropriate for storing structured data, however, they lack in scalability and expandability characteristics. As, non-relational databases are required for processing homogeneous data in an unstructured format, but there are still performance-related problems. The tradeoff should be achieved between traditional relational models and new non-relational models to maintain flexibility and get better performance.

Lack of talent pool: With this advancing technology, the need of expert developers and data architects is also growing. According to the report of the research, approximately 140,000–190,000 skilled people are required to handle big data analysis.

Privacy and Security: Cloud computing is a new methodology that provides a gateway to access and the storage of information for the study. The IT architectures are at huge risks due to its data security and intellectual infrastructures. Privacy related concerns are increasing due to direct access to the personal data file, buying preferences and [3] call records. Researchers are proposing new infrastructures just to have access to the data from any resources including social networking sites. These infrastructures can be used for future purposes also, however, the users are not aware of the potential of knowledge that can be extracted from data warehouses and data streams.

Not always better data: Researchers are highly influenced by the potential of knowledge obtained by social media mining. Twitter is one of the most common and popular social media sites. The users are not globally represented. Big data is not always complete data. The tweets today contain references to pornography and other spam, which should be properly checked and removed. This kind of spam references leads to inaccurate topic frequency.

Out of Context: Current mathematical models and data mining computations are complex and computationally expensive. Thus, wasting resources on meaningless data or noisy data is not desirable. Thus, more research work is needed for data reduction techniques. The addition of data during data abstraction is [4] very difficult to perform. Data that is out of content loses its meaning and values.

Data errors: The large datasets which are extracted from the internet have more risks of errors and losses. The data should be properly understood by the source in order to minimize the errors caused by multiple datasets. To fit incoming data streams into existing models, errors from data need to be removed. Data relationships should be free from ambiguity.

2 Literature Review

2.1 Distributed Data Analysis and Topology Based Analysis

Hu and Zhang obtaining quality data [5] from social media is difficult. This paper explains an efficient selection method based on important attributes like space or time. The selected or filtered data is later ready for effective clustering and mining. The filtered dataset has a small volume. However, it has qualities of efficient classification with high precision. The paper proposes an effective selection method for clustering mining and space data analysis. The proposed method divides a large amount of data from the space-time dimension and quality. Various experiments were conducted and show the result that the proposed method can quickly and effectively extract data from the Weibo data set and shows the distribution of the Wuhan business circle. These extracted data sets have different features and applications of high clustering and high precision. Therefore, the research draws some conclusions from the experiments that obtaining a reliable dataset is possible by removing redundancy and uncertainty that can be used in the crowd sourcing process of geographical data.

HongJu et al. analyzed [6] the problems of data management in data analytics like huge data volume, heterogeneous data, highly rated data generation and more time requirement for data processing. The paper used data for a critical application like army data. The data was widely separated all over the network and fetched selectively. This respective paper provided army data analysis construction; especially the data management gave some basic idea for building and managing the important research. Therefore, the researcher highlighted key issues in traditional data management in critical applications in handling a variety of data types, time criticality, distributed data, data integration and proved that advanced scientific research techniques need to be adapted.

McHugh et al. presented [7] Semantics Toolkit (SemTK), a framework that was accessible through big data stores and provides the appearance to all captured data within the knowledge graph. The proposed method allowed storing data on multiple locations like Data stores such as Hadoop, graph databases, and semantic triple stores which gave the best-suited location for all of them. The best platform was provided to each data type and maintains a single interface and access points given to each user across the data. Therefore, the researcher concluded that the proposed technique was improved and maintained a good balance between the complex applications and exposed data to the user.

Moon et al. designed [8] a policy for public goods by studying the big data analysis throughout the world. The study showed that there are so many researches available on this topic of the big data analysis. The author found that the research performed on the big data analysis was very much active on social as well as on the public areas. There are nine methods available for big data analysis like; Hadoop, method, cloud, analysis, social, mobile, privacy, health and policy. The researcher tried to bridge the gap between technology developers and business developers and policymakers. Therefore, the result obtained from the research is that the respective paper analyzed the features

of each research method and their effect on public services and products. It is combined with three criteria: data structure, policy tool, and market regulation. This helped to build an ecosystem that can be managed legally and politically and used in organizing market-based services on big data technology and utilizing contents.

Yang et al. proposed [9] a model for the big data analysis enterprise decision-making management system. Due to high market competition; managers are more focused on the decision making aspect of big data like trend analysis. Big data analysis is one of the most important methods being used by many researchers and scientists and they are still working on it. Big data analysis has generated influential and relevant theories on the decision making management project. The paper focused on varies steps of decision-making processes like data acquisition, data analysis, data screening, and data application. It identified the gaps between current big data decision-making applications and actual requirements and optimization of current processes.

Sunghwan et al. proposed [10] ORANGE method based on Apache Hadoop methodology. As, there is no specific technique that can handle large data at the same time so, in order to overcome this issue the researchers had proposed this method. This technique entirely worked according to the Hadoop methodology. ORANGE loaded the vector and data based on the Hadoop Distributed File System. It managed the metadata and created an index for the data using this proposed technique. Therefore, the improvement made by this method made the platform to process faster on large scale data analysis. The researcher concluded that the introduced method was two times faster than the legacy based RDMS databases.

2.2 Study on Security and Privacy of Big Data

Strang et al. demonstrated [11] big data program commence in 2011 and the production increased exponentially from 2011 to 2012 which was approximately based on Weibull distribution which captured 82% variance. The paper recommended more work and study on this big data analysis privacy and security. Therefore, the researcher showed that there were 13 other topics capturing 49% of the big production of data in journals from 2011–16. However, security and privacy were the most concerning issues still faced by technology. Various experiments were conducted which showed various results that the proposed approach was effective and time-saving as compared to any other techniques (Fig. 1).

Rong et al. [12] focused on cloud-based data security in data mining. As the current trend is to outsource data mining operations, security plays a vital role more than before. The paper developed a kNN computation extended to preserve privacy in cloud-based distributed environments. The researcher had identified that due to frequent data transfer between client and server, traditional single key based security options are failing. They had proposed a collaborative kNN computation with safe building blocks and proved that the privacy improves and also the access patterns were hidden.

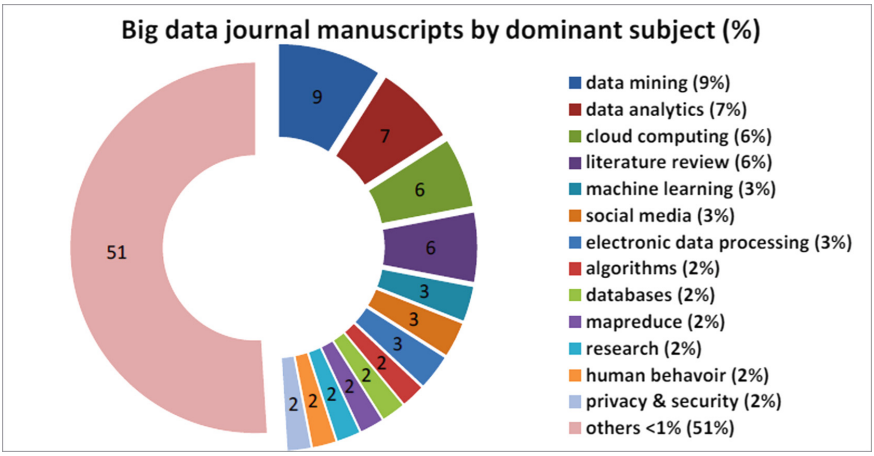


Fig. 1. Research topics and their relative percentages

2.3 Applications of Data Streams and Big Data

Zhang et al. studied [13] the impact of two bus fares adjustment policies in Beijing on the transport sharing rate. This method was designed and developed on big data analysis by application of SPSS and went through the respective suggestion of bus fares. The main objective of this paper was to introduce the changes in public transport and select the two typical public transport fare policies as a time node.

Balan et al. proposed [14] two techniques i.e. R and Tableau to analyze the tobacco smoking trends amongst the youngsters in the United States of America. Various results had put forward that the smoking trend is increasing rapidly in the USA in almost every age group. The paper also concluded that more than 51% of young smokers are interested in quitting smoking. The paper analyzed smoking trends in young male and female smokers. Therefore, the results focused on the different and more modernized techniques that can be used to control this smoking habit; proper health advice and counseling should be given to every individual the one who smokes and the one who wants to quit. This can be done by spreading awareness through different modes like open sessions, social media and so on.

Xianglan et al. proposed [15] big data-specific technical methods like data retrieval, storage, integration, processing, and visualization extended and applied to the coal mine industry. The paper also focused on managerial aspects like copyright protection, organization rules and standards, ad hoc scheduling and effective visualization. The model showed five layers which include resources, data collection, processing, protection, and data presentation. The architecture considered an innovative business model of coal mines and data preservation for a longer period than before. This model helped the sustainable development of coal mine enterprise.

Kang et al. compared three algorithms [16] to compare high speed and high volume data generated by an IoT market. The paper considered Support Vector Machine (SVM), Ridge Regression (RR) and Decision Tree (DT) algorithms. The researcher found the optimal algorithm which can efficiently manage the energy based on big data

by compromising the analyzed data using the proposed algorithms. Therefore, the researcher concluded that the accuracy was increased in DT > RR > SVM this order. However, if the processing speed was considered then this order can be modified as RR > SVM > DT. The author showed that the proposed method was much more effective than any other proposed techniques (Fig. 2).

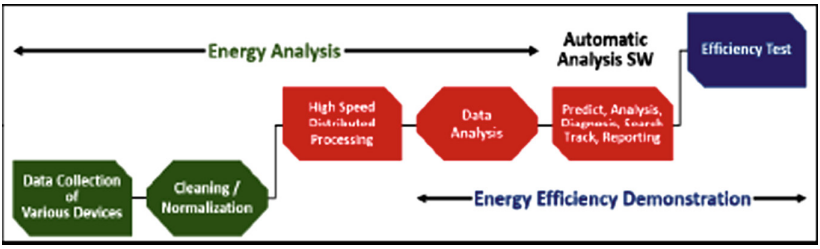


Fig. 2. Process of data capture, cleaning and knowledge extraction

2.4 Data Stream Processing and Clustering

Ramírez-Gallego et al. presented [17] the latest enhanced and widely spread method nearest neighbor method being accepted by the present scenario. It was discovered by Apache Spark which distributes the metric-space for faster research. Moreover, an interesting incremental method was proposed for the selection of massive data. The data which was selected using the proposed approach was continuously updated and the outdated data was removed from the base. The researcher has performed some experiments on the set of massive data and shows that the proposed algorithm was able to give a more efficient solution with great speed and data streaming. This research paper suggests distributed Relative Neighborhood Graph Edition (DS-RNGE) algorithm which is proved efficient for high-speed data streams.

Therefore, the researcher concluded that the cost obtained from the edition can be increased by removing the unnecessary data and also maintains the effectiveness of the original data. Also, DS-RNGE implementation develops a tree-based classification approach that can be executed in parallel in distributed environments. This algorithm requires lesser in memory storage.

Yang et al. [18] designed and implemented a data retrieval method based on elastic search. The data will be stored on the system and searches the big data policy more effectively and relies on index data for their real-time performances. The big data policy has its own applications like policy data having applications of time, category and source; hence the main objective of this paper was to propose multidimensional data analysis. The science and technology work together in different platform and solves the distributed problems of the data. But there are some policies which do not collaborate with each other and do not provide any solution.

The paper implements Long Short Term Memory Network. It is used to classify policies based on technology and other disciplines like science. The policies are

divided into 15 groups. The algorithm is based on real-time performance. Also, data visualization is implemented for knowledge extraction.

Therefore, the researcher concluded that the respective algorithm takes different categories of policy platforms, time, regions were considered as the analytic keywords from the comprehensive features and most importantly provides a reference to different departments.

Awaghad et al. proposed [19] a scheme that performs a very efficient retrieval of data from complex and high-speed streaming of data from the crowded place. The proposed system performs sufficient processing from the raw and non-uniformly distributed data from different locations so that processed data is distributed, the storage and analysis and knowledge extraction can be performed in less processing time with higher accurate degrees. The data accuracy is quite good than the existing approaches. Therefore, the researcher was able to investigate and include more complex data and forward the performances in a more efficient and sophisticated manner.

Chen et al. presented [20] a data analysis technique that is based on traditional cause and effect relationships. Microscopic analysis was formed according to the quality and quantity of trend estimation analysis. This helped to decide if current trends will keep occurring or not. This big data has a basic effect on the previously defined data. This approach worked according to the current correlation analysis and the latest trends in the analysis. Casual traditional analysis to interdependence analysis, the extraction of knowledge from data mining to model fitting, from logical reasoning to associated rules and regulations are some correlation analysis outcomes. The research proposed major differences between traditional data analysis and big data analysis considering how data objects and analysis results are created and operated. The research suggested that traditional data analysis is non-real time, based on cause and effect analysis and also prone to multiple errors. On the other hand, big data analysis handles real-time data, works on correlation analysis and prone to fewer errors. The result concluded that big data analysis requires rebuilding traditional data analysis models to handle distributed data sources, huge data processing capabilities for complex services, distribution and utilization.

3 Conclusion

Big data is giving great power to decision makers to extract hidden facts and knowledge. However, handling big data streams is an immensely challenging task. Researchers all over the globe are putting their efforts to make this information effective to store and analyze. This paper gives an insight into current research trends in big data streams operations.

References

1. Zicari, R.V.: Big data: challenges and opportunities. Big Data Comput. **564**, 104–110 (2014)
2. Blumberg, R., Atre, S.: The problem with unstructured data, pp. 42–46 (2013). http://soquelgroup.com/Articles/dmreview_0203_problem.pdf. Accessed 1 July 2012

3. Li, M., et al.: Conditional random field for text segmentation from images with complex background. Pattern Recognit. Lett. **31**(14), 2295–2308 (2010)
4. Jaseena, K.U., David, J.M.: Issues, challenges, and solutions: big data mining. CS & IT-CSCP **4**(13), 131–140 (2014)
5. Hu, Q., Zhang, Y.: An effective selecting approach for social media big data analysis—taking commercial hotspot exploration with Weibo check-in data as an example. In: 2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA), pp. 28–32. IEEE (2018)
6. HongJu, X., et al.: Some key problems of data management in army data engineering based on big data. In: 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA), pp. 149–152. IEEE (2017)
7. McHugh, J., et al.: Integrated access to big data polystores through a knowledge-driven framework. In: 2017 IEEE International Conference on Big Data (Big Data), pp. 1494–1503. IEEE (2017)
8. Moon, H., et al.: Ecosystem design of big data through previous study analysis in the world: policy design for big data as public goods. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 525–528 IEEE (2017)
9. Yang, L., Zhang, J.-J.: Realistic plight of enterprise decision-making management under big data background and coping strategies. In: 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA), pp 402–405. IEEE (2017)
10. Cho, S., Hong, S., Lee, C.: ORANGE: spatial big data analysis platform. In: 2016 IEEE International Conference on Big Data (Big Data), pp. 3963–3965. IEEE (2016)
11. Strang, K.D., Sun, Z.: Meta-analysis of big data security and privacy: scholarly literature gaps. In: 2016 IEEE International Conference on Big Data (Big Data), pp. 4035–4037. IEEE (2016)
12. Rong, H., et al.: Privacy-preserving k-nearest neighbor computation in multiple cloud environments. IEEE Access **4**, 9589–9603 (2016)
13. Zhang, S., et al.: Impacts of public transportation fare reduction policy on urban public transport sharing rate based on big data analysis. In: 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), pp. 280–284. IEEE (2018)
14. Balan, S., et al.: Big data analysis of youth tobacco smoking trends in the United States. In: 2017 IEEE International Conference on Big Data (Big Data), pp. 4727–4729. IEEE (2017)
15. Xianglan, L.: Digital construction of coal mine big data for different platforms based on life cycle. In: 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA), pp. 456–459. IEEE (2017)
16. Kang, D., et al.: Energy information analysis using data algorithms based on big data platform. In: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1530–1531. IEEE (2016)
17. Ramírez-Gallego, S., et al.: Nearest neighbor classification for high-speed big data streams using spark. IEEE Trans. Syst. Man Cybern.: Syst. **47**(10), 2727–2739 (2017)
18. Yang, A., et al.: The research of policy big data retrieval and analysis based on elastic search. In: 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD), pp. 43–46. IEEE (2018)
19. Awaghad, S.: SCEM: smart & effective crowd management with a novel scheme of big data analytics. In: 2016 IEEE International Conference on Big Data (Big Data), pp. 2000–2003. IEEE (2016)
20. Chen, J., et al.: Study of data analysis model based on big data technology. In: 2016 IEEE International Conference on Big Data Analysis (ICBDA), pp. 3–6. IEEE (2016)

Towards Power Aware Data Transmission in Sensor Cloud: A Survey

Mohammad Farhan Khan(✉), Rajendra Kumar Dwivedi, and Rakesh Kumar

Department of Computer Science and Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur, India
farhank082@gmail.com,
rajendra.gkp, rkiitr@gmail.com

Abstract. Sensor cloud is the integration of cloud computing and wireless sensor networks (WSN). This integration is beneficial for both WSN providers and cloud service providers. WSN data can be kept over cloud which can be efficiently used by several applications and cloud provider can provide sensor-as a- service through this integration. In sensor cloud, there are multiple physical sensor networks which are mapped with the virtual sensor networks using a cloud to provide services to the users. End users are facilitated to execute multiple applications of WSNs through such VSNs. Some applications can also demand more than one WSN at a time. Virtualization supports to achieve this goal in sensor cloud. Although sensor cloud has several advantages, still it has many research issues like energy efficiency, security, data transmission, QoS, etc. This paper presents a survey on energy efficient data transmission in sensor cloud that discusses and compares the existing techniques of this field.

Keywords: Sensor cloud · Cloud computing · Wireless sensor networks (WSN) · Virtual sensor networks (VSN) · Energy efficiency · Virtualization

1 Introduction

Sensor networks are widely used in various applications these days. Sensor cloud merges sensor network with the cloud computing to provide shared processing resources to the end users. It is a technique that focuses on physical sensors to assemble the data and transmit it into the cloud to serve multiple applications of end users [11, 15, 25]. Sensor cloud provides scalable and efficient computing infrastructure for real-time applications.

This combined infrastructure can be treated as an extension of cloud computing that can manage the physical sensors of WSN in order to meet the enhancing need for large scale wireless network applications. Figure 1 shows the basic architecture of the sensor cloud. The architecture of sensor cloud uses virtualization to create virtual sensor networks.

Sensor cloud infrastructure merges WSN and cloud computing in such a way that it provides on demand services for real time data processing and storage of sensor data. This integration has a lot of advantages but it has some research issues and challenges too. Energy efficiency [12, 18, 21, 22] and security issues [16, 19, 20, 23] are few of

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 317–325, 2020.
https://doi.org/10.1007/978-3-030-37051-0_37

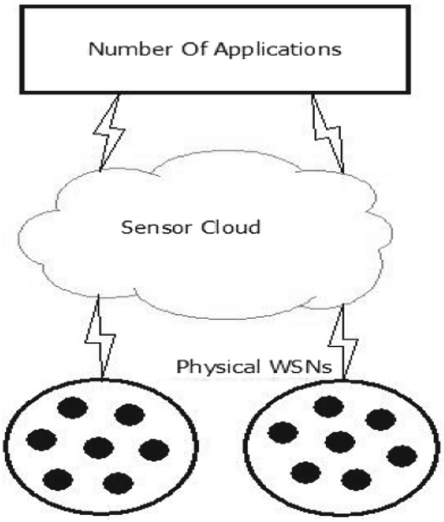


Fig. 1. Sensor cloud

them. Data transmission is one of the important issues in sensor cloud. During data transmission, sometimes data compression is also essential. Data compression is implemented in sensor networks if execution of the compression algorithms does not require much energy for each transmission otherwise the compression process is done at the gateway. Gateway is a platform that provides management of sensor nodes and also acts as an interface to the real world [17]. This paper provides a brief survey on energy aware data transmission in sensor cloud.

Rest of the paper is organized as follows. Section 2 describes the basic terminologies and preliminaries of sensor cloud. Section 3 presents a brief survey on power aware transmission of data in sensor cloud. At last Sect. 4 concludes the paper with some future research directions.

2 Background

Some basic terminologies and preliminaries of sensor cloud are discussed in this section as below.

2.1 Wireless Sensor Network

A WSN also termed as a collection of spatially distributed self-directed sensors. These sensors generally have the low processing power and storage accessibility. Few controlling and monitoring application accept and evaluate information from the environment and then transmit the data to the user. It can be categorized into two types i.e., structured and unstructured. For the unstructured wireless sensor network, its physical sensor can be deployed in an ad-hoc manner whereas structured network must be a pre-

plan for deploying either one or more of the sensor nodes. Based on the operation done by the entire system, it can be described into two sub-systems: data analysis and data acquisition.

Figure 2 shows the architecture of WSN. Wireless sensor networks are often used for many reasons unexpected Environmental Monitoring. There is also low battery power consumption in WSN [13, 14, 16], so various plans have been developed to minimize the consumption of energy at the time of processing the data.

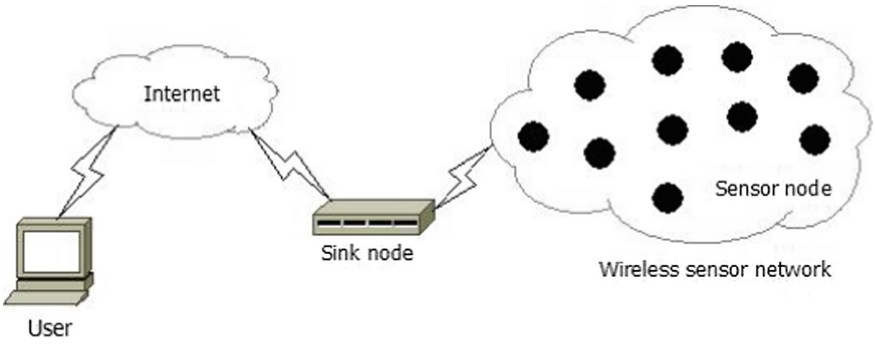


Fig. 2. Wireless sensor network

2.2 Cloud Computing

loud computing is defined as process of computing, which gives general concept for delivery of services over the internet. It provides basically three services namely SaaS, PaaS and IaaS [24]. All of the cloud services (e.g. software, platform, infrastructure etc.) are delivered to the user through the internet. Cloud computing can be thought as a model of network computing which is based on pay per use technique. It is also known as the virtual storage of data because it uses the concept of virtualization. Figure 3 describes the cloud computing and its services.

2.3 Sensor Cloud: Major Applications, Advantages and Issues

The architecture of the sensor cloud is capable of providing an open, extensible, intelligent and interoperable sensor network. Whenever a request is made, the services are automatically provisioned. Sensors are made free when the requested tasks are completed. The owner of the sensor can track the physical sensor usage. End users do not have to think about the precise places of sensors and extended description of the sensors and they can independently control services. There are various applications of sensor cloud. Some of them are mentioned as below:

(i) Transport monitoring
(ii) Military use
(iii) Weather forecasting
(iv) Health care.

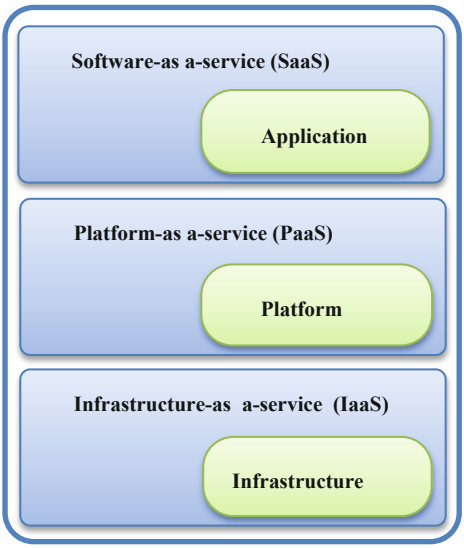


Fig. 3. Cloud computing and its services [24]

Cloud computing is integrated with WSN to provide the promising solution in many ways such as agility, flexibility, reliability, portability etc. Advantages of this integration are as follows:

(i) Scalability
(ii) Visualization
(iii) Multi-tenancy
(iv) Resource optimization
(v) Quick response time.

There are many issues such as designing issues, continuous data flow, engineering issues, reliable connections, issues of electricity etc. In the different real scenario such as the health care industry, hospital etc. Different problems are encounter while structuring a system for them.

(i) Energy efficiency
(ii) Bandwidth limitation
(iii) Network access management
(iv) Pricing
(v) Interface standardization.

2.4 Data Transmission in Sensor Cloud

Data Transmission or Data communication is the branch of telecommunication related to the transmission of information which is performed, on the basis of Protocol, represented by symbol or analog signals. The term "data transmission" is also apply to the actual process of transmitting the information. Such information is called data. Data

transmission can be done in two ways: Parallel and Serial. Serial communication is of two types. First is Synchronous and second is Asynchronous. Figure 4 explains the transmission of data in sensor cloud. The intermediate node, is a built-in real node of sensor for VSN, which transmits information in the cloud via a set of bridge nodes. This task basically focuses on finding a best rule to work with bridge node with concern of a Virtual Sensor Network. This work improves the energy efficiency of VSN completely.

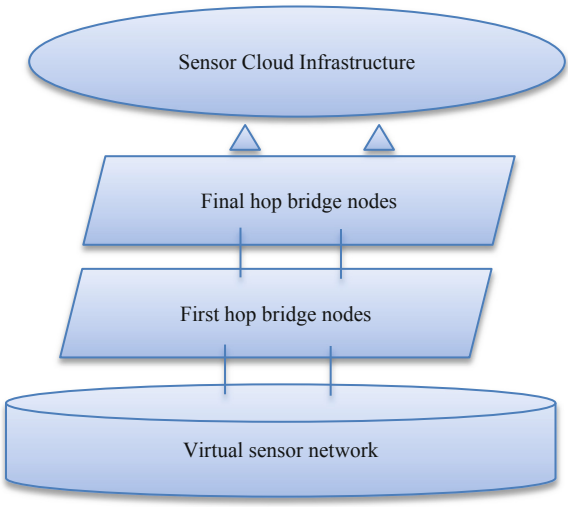


Fig. 4. Data transmission in sensor cloud

A WSN can be made up of network of devices that can communicate information accepted through a monitoring area through a wireless link. Data is distributed over more than one node, and with gateway, the data is connected to other networks, such as wireless Ethernet. The wireless storage system, which is part of the wireless network, has not been used in large-scale.

3 Literature Survey

In this section, a survey on various energy- efficient data transmission approaches is presented. This survey focuses on the energy-efficient methods for the sensor cloud which are categorized on basis of six categories such as sensing techniques, data transmission techniques, scheduling techniques, data processing.

Chatterjee [1] described that built-in real sensor nodes transmit the information to the cloud via a set of bridge nodes.

Dinh [2] proposed an interactive model of energy efficient sensor-cloud for latency. On-demand integration supplies more than one application at time with various delay requirements. In this model, they prepared the aggregation system for total application

requests for sensor-cloud so that the workload required for the forced sensor nodes could be reduced to save energy. Interactive model guarantees the latency demands of many applications.

The energy-efficient techniques are classified for different categories of sensor cloud and also been analysed using each technique for different standards is proposed by Das [3]. Several applications such as environmental monitoring, smart homes, health care services, designing of the vehicular network and complex event monitoring need optimization of energy as well as QoS parameters. From their analysis, they found that most energy-efficient technique ignores the parameters, quality of service, network lifespan and scalability.

Rahman [4] proposed an efficient sensor-cloud communication approach that minimizes the enormous bandwidth and time requirement by using statistical classification based on machine learning as well as compression using deflate algorithm with a minimal loss of information.

Napolean et al. [5] presented an innovative technique to improve energy saving. For each cluster head, sink data calculates several paths for transmission.

Ghai and Yan [6] presented a power aware model to reduce the power consumption of routes. It sets a sleep mode for sensor node.

Grace [7] had proposed a model which is based on energy-efficient at middleware also known as Sense Controller, a collection of both cloud gateway as well as sensor gateway. This is helpful in dealing in different environment in case of long and continuous term tracking of data. (SCA) Senud reduces compression algorithm Suitable for data replication and numerical data Compression. It is structured for numerical value sensor data that exhibits with large data.

Sheng [8] proposed a approach to reduce the energy consumption of an application processing in for MWSN in order to minimize the consumption of energy so as to meet the requirements. Their solution give significant saving in terms energy.

Nguyen [9] had given design and its implementation for water quality monitoring system which uses a reliable wireless sensor network. The cellular protocol is used for data transmission to the cloud in order to reduce power consumption. Data in the cloud is mined so the warning notification in real time can be transferred to the users.

Yan [10] proposed energy saving approach. In this approaches both node level and network level energy savings methodologies is presented and their test have been proven successful.

The comparison of related work is given in Table 1:

Table 1. Comparative study of the related work

Authors	Contribution	Technique
Chatterjee [1]	Power-efficient transmission of data in sensor-cloud	Optimal decision rule and Bayesian classifier
Dinh [2]	Interactive model of an efficient sensor-cloud for latency on-demand	Interactive model

(*continued*)

Table 1. (*continued*)

Authors	Contribution	Technique
Das [3]	A review of energy efficient sensor cloud	Optimal decision rule, wireless energy transfer, customizable sensor information system, compression algorithm and Pull-push communication
Rahman [4]	Efficient sensor cloud communication	Lossless data compression algorithm
Napolean [5]	Power efficient design of sensor node in WSN	Periodic sleep awake scheme and multipath selection
Ghai and Yan [6]	Design of energy efficient WSN and its applications	Adaptive transmission power settings
Grace [7]	An energy efficient transmission in sensor cloud is presented	Senud compression algorithm (SCA)
Sheng [8]	Power efficient cooperative computing in mobile WSN	Minimize energy consumption
Nguyen [9]	An efficient and reliable WSN of water quality monitoring	Lightweight ACK mechanism
Yan [10]	Power efficient design of sensor node of WSN	Periodic sleep/wake-up scheme

4 Conclusion and Future Directions

This paper presents model for data transmission very efficiently in case of sensor cloud. Several types of research are carried out nowadays in this direction. Various architectures are provided to minimize the energy for data transmissions in sensor cloud. Some frameworks can reduce the strong bandwidth demand of sensor cloud communication where the loss of data will be negligible and the demand time for the transaction has also reduced to some extent. This results in efficient data transmission.

There might be some future directions to protect the transmission of data in the sensor cloud.

References

1. Chatterjee, S.: Energy-Efficient Data Transmission in Sensor-Cloud. International Conference on Applications and Innovations in Mobile Computing. School of Information Technology, pp. 45–51 (2015)
2. Dinh, T.: An efficient sensor-cloud interactive model for on-demand latency requirement guarantee. In: IEEE Symposium on Internet of Things, pp. 92–98 (2017)
3. Das, K.: Survey of energy-efficient techniques for the cloud-integrated sensor network. J. Sens. Hindawi 110–116 (2018)
4. Rahman, T.M.: Efficient sensor-cloud communication using data classification and compression. Int. J. Inf. Technol. Comput. Sci. 9–17 (2017)

5. Napolean, A.: Energy efficient sensor node design in wireless sensor networks. IJCSMC **3** (4), 1356–1363 (2014)
6. Ghai, S., Yan, R.: Energy-aware sensor node design with its application in wireless sensor. Networks **1**(4), 136–142 (2015)
7. Grace, S.S.: SCA–an energy efficient transmission in sensor cloud. In: International Conference on Recent Trends in Information Technology, pp. 1–5 (2014)
8. Sheng. Z.: Energy efficient cooperative computing in mobile wireless sensor networks. IEEE Trans. Cloud Comput. 1–13 (2015). https://doi.org/10.1109/tcc.2015.2458272
9. Nguyen. D.: A reliable and efficient wireless sensor network system for water quality monitoring. In: 13th International Conference on Intelligent Environments, pp. 84–91 (2017)
10. Yan. R.: Energy-aware sensor node design with its application in wireless sensor networks. IEEE Trans. Instrum. Meas. **62**(5) (2013)
11. Dwivedi, R.K., Singh, S., Kumar, R.: Integration of wireless sensor networks with cloud: a review. In: 9th IEEE International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2019, pp. 115–120 (2019)
12. Naik, A.K., Dwivedi, R.K.: A review on use of data mining methods in wireless sensor network. Int. J. Curr. Eng. Sci. Res. IJCESR **3**(12), 13–20 (2016)
13. Agarwal, A., Maddhesiya, S., Singh, P., Dwivedi, R.K.: A Long Endurance Policy (LEP): an improved swap aware garbage collection for NAND flash memory used as a swap space in electronic devices. Int. J. Sci. Eng. Res. IJSER **3**(6), 412–417 (2012)
14. Chaudhary, M.K., Kumar, M., Rai, M., Dwivedi, R.K.: A modified algorithm for buffer cache management. Int. J. Comput. Appl. IJCA **12**(12), 47–49 (2011)
15. Dwivedi, R.K., Kumar, R.: Sensor cloud: integrating wireless sensor networks with cloud computing. In: 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gorakhpur, India, pp. 820–825(2018)
16. Dwivedi, R.K., Sharma, P., Kumar, R.: A scheme for detection of high transmission power based wormhole attack in WSN. In: 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gorakhpur, India, 2018, pp. 826–831(2018)
17. Kumar, P., Kumar, R., Kumar, S., Dwivedi, R.K.: Improved modified reverse AODV protocol. Int. J. Comput. Appl. IJCA **12**(4), 22–26 (2010)
18. Dwivedi, R.K., Tiwari, R., Rani, D., Shadab, S.: Modified reliable energy aware routing protocol for wireless sensor network. Int. J. Comput. Sci. Eng. Technol. IJCSET **3**(4), 114–118 (2012)
19. Dwivedi, R.K., Sharma, P., Kumar, R.: Detection and prevention analysis of wormhole attack in wireless sensor network. In: 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, pp. 727–732 (2018)
20. Dwivedi, R.K., Pandey, S., Kumar, R.: A study on machine learning approaches for outlier detection in wireless sensor network, In: 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, pp. 189–192 (2018)
21. Verma, K., Dwivedi, R.K.: A review on energy efficient protocols in wireless sensor networks. Int. J. Curr. Eng. Sci. Res. IJCESR **3**(12), 28–34 (2016)
22. Verma, K., Dwivedi, R.K.: AREDDP: advance reliable and efficient data dissemination protocol in wireless sensor networks. In: 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, pp. 1–4 (2017)
23. Sharma, P., Dwivedi, R.K.: Detection of high transmission power based wormhole attack using received signal strength indicator (RSSI). In: Communication, Networks and Computing. CNC 2018. Communications in Computer and Information Science, vol. 839, pp. 142–152. Springer, Singapore (2019)

24. Dwivedi, R.K.: From grid computing to cloud computing & security issues in cloud computing. Technia Int. J. Comput. Sci. Commun. Technol. IJCSCT **5**(1), 805–809 (2012)
25. Dwivedi, R.K., Saran, M., Kumar, R.: A survey on security over sensor-cloud. In: 9th IEEE International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, pp. 31–37 (2019)

Real-Time Environment Description Application for Visually Challenged People

Amey Arvind Bhile(✉) and Varsha Hole

Information Technology, Sardar Patel Institute of Technology, Mumbai, India
ameybhile7@gmail.com, Varsha_hole@spit.ac.in

Abstract. In real world, visually challenged people face the great challenge of understanding nearby objects and movements going on in their vicinity. They mainly depend upon their auditory or physical abilities of touch to recognize things that are happening around them. Being able to describe the surrounding environment and objects that are present around them using properly formed sentences could only be done if a normal person is present and can describe it to them. We plan on creating an application that can solve this very challenging task by generating description of a real-time video captured from a mobile phone camera, which will aid the visually challenged in their day to day activities. In this paper, we are using concepts of Object detection and Caption generation and present our approach for the same, this which will enable us to run the model on smart phone devices in real time. The description pertaining to the objects, as seen in real time video generated will be converted to audio as the output. We train our proposed model on various datasets so that the generated descriptions are correct and up to the mark. Using the combinations of Convolutional Neural-Network and Recurrent Neural-Network and our own modifications, we tend to create a new model. We also are implementing an Android application for the visually challenged people to show the real-life applicability and usefulness of the Neural Network.

Keywords: Image captioning · Object detection · Neural network

1 Introduction

The concept of creating a language description of a video which is also called Video Captioning is new trend going in Artificial Intelligence. Extending this concept further, where the caption of only a static image is generated, we need to implement a method which generates the caption pertaining to a dynamic real-time video. As we all know that the sense of vision is not available to visually impaired people, a unique method is implemented in this paper to convert caption of the video generated to an audio format so that it will help visually impaired people to hear about objects in their surroundings using the application on their smartphone. This application will be so designed that it will help people who are visually challenged to gain more independence by giving real-time auditory cues about objects, text, and people around them. We will be able to provide a real-time update to the person in audio format about the objects around them which will also provide safety while moving around in the open environment. This

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 326–332, 2020.
https://doi.org/10.1007/978-3-030-37051-0_38

system will focus not only on the real-time description but also will help the user to differentiate between similar objects present in the environment. The system will mainly focus on the indoor and semi-open environment like parks, malls, airports etc. The C.N.N detects the features pertaining to the image and the R.N.N generates a description pertaining to image provided as the input. In this paper, we propose a new approach that combines the techniques of C.N.N and R.N.N to generate a description of a real-time video and convert it to audible format as the output for the visually challenged.

2 Overview

Our model tends to create a descriptions of real-time video captured from the user's phone and convert it to audio format. The below images are the actual output of the mobile application that converts the video in front of the camera to audio output. The captions generated below the screenshots taken from the actual output is the same that is heard by the user in audio format. The main aim of this application is that it would eventually help visually impaired people to identify various objects and scenario in their surroundings. We have used Flickr30k and MS-COCO datasets [4] for training our model. At first we created a model that corresponds the objects to the description of the objects of the model. We train this model on training data Set so that it can identify the objects when sampled. Successively, we convert the caption generated in the video to audio format and produce it as output.

Following is the implementation methods block diagram of Real-Time Video to Audio Conversion (Fig. 1).

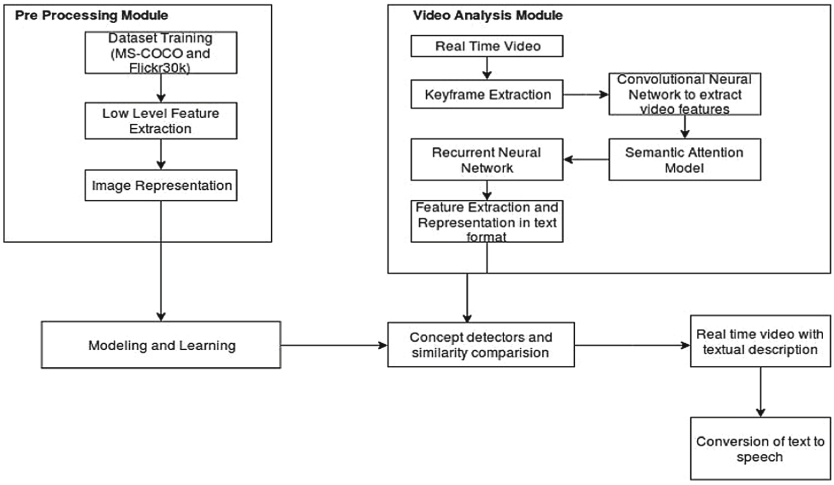


Fig. 1. Block diagram for representation of our model.

The first step of conversion of audio to video conversion is the pre-processing module which mainly consists of dataset training on MS-COCO and Flickr30k dataset. Then all the low-level objects are detected from the image and then the initial module is set for training. The adjacent module to the pre-processing module is the video analysis module. The real-time video is captured on an application, and the algorithms of C.N.N and R.N.N are used to obtain objects from the video. The features from the earlier step and the current features extracted from the video are compared and then the caption pertaining to real-time video is generated. Finally, the caption generated is converted to speech in audio format.

3 The Proposed Model

The model takes a input of a instance of the video and is trained to max the probability of P (S|I) where S is the sequence of words generated from the model and each word is generated from a dictionary built from the training dataset.

The input image I is fed into a deep vision C.N.N which helps in detecting the objects. The image encodings are passed on to the Language Generating R.N.N which helps in generating a meaningful description for the given image as shown in the figure. An analogy to the model can be given with a language translation RNN model where we try to maximize the p(T|S) where T is the translation to the sentence S. However, in our model the encoder RNN which helps in transforming an input sentence to a fixed length vector is replaced by a C.N.N encoder [3].

A L.S.T.M network follows the pre-trained VGG16. The L.S.T.M network is used for language generation. LSTM differs from traditional Neural Networks as a current token is dependent on the previous tokens for a sentence to be meaningful and LSTM networks take this factor into account. C.N.N are a category of Artificial intelligence which has proven to be much effective in the field of objects reorganization and classification. They have been used extensively for the task of object detection, self-driving cars, image captions etc. The first convnet was discovered in the year 1990 by Karpathy and Fei-Fei [1] and the architecture of the model was called the LeNet architecture (Fig. 2).

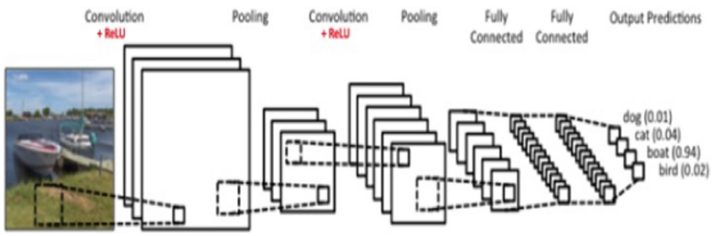


Fig. 2. Steps in a convolutional neural network.

The entire architecture of a convnet can be explained using four main operations namely:

1. Convolution Operation
2. Non- Linearity (ReLU)
3. Spatial-Pooling
4. Image Classification.

3.1 The Convolution Operator

We consider filters of the size smaller than the dimensions of the image. The entire operation of convolution can be understood with the example below. Consider a small 2-dimensional 5 × 5 image with binary pixel values. We slide the 3 × 3 matrix over the real image by 1 pixel and calculate element-wise multiplication of the 3 × 3 matrix with the sub-matrix of the original image and add multiplied output to get a final integer that will form the elements of the output matrix.

3.2 Introducing Non-linearity

An additional operation is applied after every convolution operation. The most commonly used Non-Linear function for images is ReLU.

The Re LU operation is a pixel by pixel operation which changes the -ve pixels in the image to zero. Since most of the operations in real-life relate to non-linear data but the output of convolution operation is linear because the operation applied is element-wise multiplication and addition.

3.3 Spatial Pooling

The pooling operation reduces the dimensionality of the image but preserves the important features in the image. The most common type of pooling technique used is max pooling. In max pooling, you slide a window of (N × N) where N is less than side of the image and determine the maximum in that window and then shift the window with the given stride length.

3.4 Fully-Connected Layer

The convolution and pooling operation generate features of an image. The task of the fully Connected layer is, Map these feature vectors to the classes in the training data. The advantage of using a ReLU layer over sigmoid and tanh is that it accelerates the process (Fig. 3).

Also unlike the extensive operations (exponential etc.), the ReLU operation can be easily implemented by activating the zero matrices. For our purpose, however, we need not classify the image and hence we remove the last 1 × 1 × 1000 classification layer. The output of our CNN encoder would thus be a 1 × 1 × 4096 encoded which is then passed to the language generating R.N.N. There have been more successful CNN frameworks like ResNet [7] but they are computationally very expensive since the number of layers in ResNet was 152 as compared to VGG16 which is only a 16-layered network.

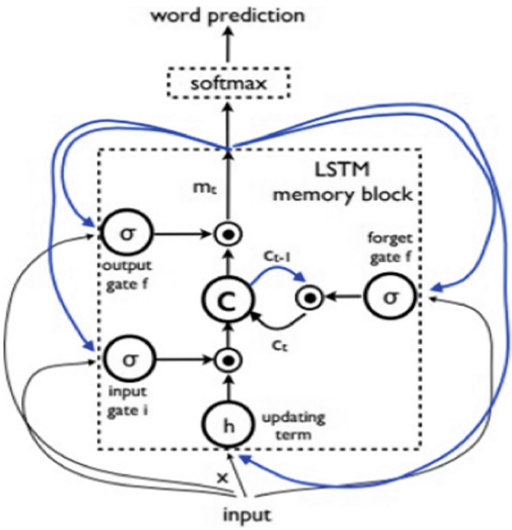


Fig. 3. Representation of a fully connected network.

R.N.N are a type of artificial neural network in which connection between units forms a directed cycle. The advantage of using R.N.N over conventional feed forward net is that the RNN can process an arbitrary set of inputs using its memory. Recurrent neural nets in simple terms can be considered as networks with loops which allows the information to persist in the network.

For the Android implementation of our real-time model [13], we used the interface provided by "Tensorflow Android Camera Demo" [7]. In the initial step, the CNN model is trained and a proto buffer file is generated. We need to hold and save the values obtained to save our CNN graph.

Then by using Android tool, our Application can load model with values and read output values. The application that we have designed streams the live video from users phone, and ones instance of the video is used for object detection. And then the detected results are captioned in real time.

4 Conclusion

We have implemented an effective real-time synchronized video to audio description system to help visually challenged people that can be run with low-end hardware and processing Devices. We have created a application on the phone that can easily be used by the visually challenged people in their day to day activities. Our model can detect and locate objects such trees, people, bench, etc. using various object detection algorithms like CNN and RNN as explained earlier.

We have improved the pre-existing algorithms so that we can produce results in real time even for devices with low processing power. Finally, We are able to prove an application that will help Visually Challenged people in real life situations. The

application can be further extended to various environments and complex scenarios and improving the camera quality and adding new sensor application to the system can definitely increase the accuracy of the system.

5 Result

Tested our application on real-life scenarios and these are some of the results.

References

1. Karpathy, A., Fei-Fei, L.: Deep visual-semantic alignments for generating image descriptions. IEEE Trans. Pattern Anal. Mach. Intell. **39**(4) (2017)
2. Sutskever, I., Vinyals, O., Le, Q.V.: Sequence to Sequence Learning with Neural Networks. Department of Computer Science, University of Cornell. arXiv:1409.3215
3. You, Q., Jin, H., Wang, Z., Fang, C., Luo, J.: Image Captioning with Semantic Attention. Department of Computer Science, University of Rochester, Rochester NY 14627, USA
4. Vinyals, O., Toshev, A., Bengio, S., Erhan, D.: Show and tell: lessons learned from the 2015 MS-COCO image captioning challenge. IEEE Trans. Pattern Anal. Mach. Intell. **39**(4) (2017)
5. Hori, C., Hori, T., Marks, T.K., Hershey, J.R.: Early and Late Integration of Audio Features for Automatic Video Description. Mitsubishi Electric Research Laboratories. TR2017-183 Dec 2017
6. Wang, J., Yang, Y., Mao, J., Huang, Z., Huang, C., Xu1, W.: CNN-RNN: a unified framework for multi-label image classification. The University of California at Los Angles. TR2017-183 Dec 2016
7. Hori, C., Hori, T., Lee, T.-Y., Sumi, K., Hershey, J.R., Marks, T.K.: Attention-based multimodal fusion for video description (2017). arXiv:1701.03126
8. Aytar, Y., Vondrick, C., Torralba, A.: Soundnet: Learning sound representations from the unlabeled video. In: Advances in Neural Information Processing Systems, pp. 892–900 (2016)
9. Chorowski, J.K., Bahdanau, D., Serdyuk, D., Cho, K., Bengio, Y.: Attention-based models for speech recognition. In: Cortes, C., Lawrence, N.D., Lee, D.D., Sugiyama, M., Garnett, R. (eds.) Advances in Neural Information Processing Systems, vol. 28, pp. 577–585. Curran Associates, Inc. (2015)
10. Bahdanau, D., Cho, K., Bengio, Y.: Neural machine translation by jointly learning to align and translate. In: CoRR (2014). arXiv:1409.0473
11. Lin, M., Chen, Q., Yan, S.: Network in the network. In: CoRR (2013). arXiv:1312.4400
12. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. In: CoRR (2014). arXiv:1409.1556
13. Li, Z., Rao, Z.: Object Detection and its Implementation on Android Devices (2015)
14. Tran, D., Bourdev, L.D., Fergus, R., Torresani, L., Paluri, M.: Learning spatiotemporal features with 3D convolutional networks. In: 2015 IEEE International Conference on Computer Vision, ICCV 2015, Santiago, Chile, pp. 4489–4497 (7–13 Dec 2015)
15. Fiscus, J.G.: A post-processing system to yield reduced word error rates: Recognizer output voting error reduction (rover). In: IEEE Workshop on Automatic Speech Recognition and Understanding, 1997. Proceedings. IEEE, pp. 347–354 (1997)

A Survey on Internet of Things (IoT): Layer Specific vs. Domain Specific Architecture

Sharad Pratap Singh[1(✉)], Vinesh Kumar[1], Akhilesh Kumar Singh[1], and Shalini Singh[2]

[1] GLAU, Mathura, UP, India
{sharad.singh, vinesh.kumar, akhileshkr.singh}@gla.ac.in
[2] RVIT, Bijnor, UP, India

Abstract. "The next Industrial Revolution", Internet of Things (IoT) is the technology giant which is rapidly gaining ground in the scenario of modern Wireless Sensor Networks (WSNs) where physical objects (or "Things") are connected through the common platform i.e. Internet. The Internet of Things paradigm is paving the way towards success, providing services in different domains. Single architecture is not enough to provide essential services in all domains. The Reference model can be made to provide a starting point for developers looking further for developing strong IoT solutions. In order to facilitate future research and to help the product builder to choose from the different architectures, This paper does an analysis of Layer-Specific, Do-main-Specific and Industry defined IoT architectures. Intel, IBM, and CISCO have also made a push towards developing new models that aims to standardize the complex and fragmented IoT Industry by releasing IoT platform reference architectures. This paper contributes the IoT, basic elements of IoT, systematic classification of different IoT architectures and comparison of industry-defined architectures.

Keywords: Internet of things · IoT-architecture layers · Domain-specific architecture · Industry-defined architecture · CISCO architecture · IBM Architecture · Intel architecture

1 Introduction

INTERNET OF THINGS (IoT) term was introduced for the first time in the year 1999 by Kevin Ashton, which is an intelligent network infrastructure that allows numerous individually identifiable objects (sensors, actuators, wireless devices etc.) to inter-connect with each other to perform intricate tasks in a supportive manner [1]. According to 2020 conceptual framework, the term Internet of Things (IoT) can be represented using the following general statement:

IoT = Sensors + Data (or information) + Network + Services [2].

The International Telecommunication Union (ITU) described about IoT in a report in 2005 that: "IoT will interconnect objects from the world together in an intelligent and

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 333–341, 2020.
https://doi.org/10.1007/978-3-030-37051-0_39

sensory manner" [3]. In the IoT foresight, the term "things" is a pervasive term that embraces various physical objects, moveable personal items such as smart phones, digital cameras, and tablets [4]. As the Internet-connected devices are rapidly growing in number, the traffic generated by them is likely to augment considerably. For instance, Cisco guesstimates about the generation of internet traffic by IoT devices will climb to 70% in year 2019 from 40% in 2014 [5]. One more anticipation made by Cisco is that the number of Device-to-Device (D2D) connections will augment from 24% (in year 2014) to 43% (in year 2019) of all connected IoT devices [6].

IoT is a parasol term that comprises of diverse categories [7]: Wireless sensors or actuators, RFID tags, wearables connected to internet, devices with Internet connectivity facility, Bluetooth-enabled smart phones, smart homes and connected cars etc. So single architecture is not enough that go well with all these applications of IoT for their diverse needs. Vendors like CISCO, INTEL and IBM have come up with their own reference architectures. When the enthusiasts and the researchers are developing any IoT product, the scarcity of comprehensive knowledge regarding these IoT architectures put a ceiling on them to prefer any one particular architecture [8].

The rest of the paper is arranged as: Sect. 2 presents the basic elements of internet of things in tabular form, In Sect. 3, architectural considerations are summarized. Section 3.3 demonstrates the comparisons of different IoT based Industry-defined architectures. Section 4 describes the conclusion of the paper that shows the usefulness of the work presented in this paper.

2 Basic Elements of IoT

To better understand the concept of the emerging technology- Internet Of Things, one should have the general knowledge of the basic building blocks of this technology. IoT implementation includes the following basic elements as shown in Table 1 [9].

Table 1. Basic elements of IoT

Elements of IOT	Description
Sensors	Sensors perceives information from the environment
Actuators	Actuators performs the actions
Things	Responsible for communication and gathering the data without any human involvement
Gateways	Acts as a middleware between the devices and network enables connectivity among devices and other infrastructures and during the information flow, it provides security and management facilities
Network infrastructure (NI)	NI IoT devices includes: Routers, Aggregators, Gateways, Repeaters, It provides data flow control from services or things to the cloud infrastructure and during flow of data, it also enables security
Cloud infrastructure (CI)	CI IoT devices are: Virtualized Server (VS) and Data Storage Unit (DSU), It allows advanced computing functionalities and the storage facilities
RFID Tags	Physical objects are equipped with Radio Frequency Identification (RFID) tags or other identification bar-codes. Smart sensor devices can sense these codes [28]

3 Architectures of IoT

There are numerous architectures that have been proposed by various researchers in the recent years of emergence of IoT technology. They can be classified in 3 different ways:

i. Layer-specific architectures
ii. Domain-specific architectures
iii. Industry defined architectures

These are further classified as shown in Figs. 1 and 2.

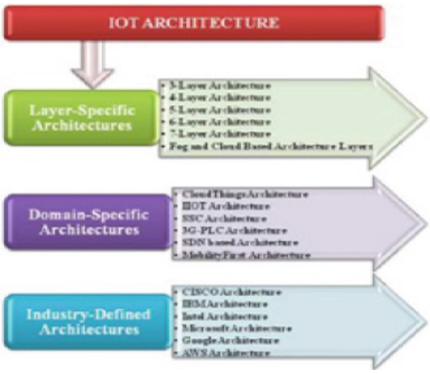


Fig. 1. Classification of IoT architecture

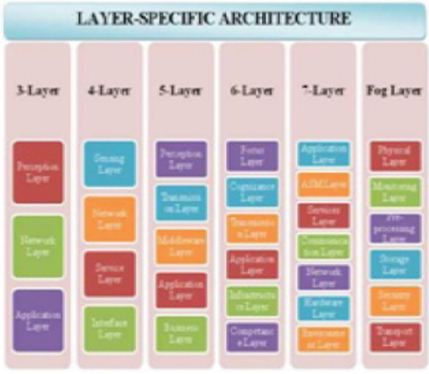


Fig. 2. Classification of layer-specific architecture [8, 10, 16, 18, 9, 20–22]

3.1 Layer-Specific Architectures

On the basis of number of layers, IoT Architectures can be classified as shown in Fig. 2.

3-Layer Architecture: According to the work performed in paper [10], it comprises of three layers: (1) Perception Layer (or sensor layer/recognition layer) [11], is the lower most layer that interrelates the physical things and components via smart devices (sensors, actuators, RFID tags etc.) (2) Network Layer, well-known as gateway layer or transmission layer, is imposed as the central layer of IoT architecture [12]. It allows the integration of various devices (switches, hub, gateway etc.) and various communication technologies (like- LTE, Bluetooth, WiFi, etc.) (3) Application Layer, or business layer, is the upmost layer in IoT architecture [13]. It receives the information transmitted from the network layer and use this information to allocate required services [10]. Advantages: simplicity, effortless problem identification and flexibility. Limitations: absence of application layer security [14].

4-Layer Architecture: P.P. Ray, in his work [16], describes a service layer, that acts as a middleware between network and interface (or application) layer, that is responsible for providing the data services in IoT. Following this concept, a Service-oriented Architecture (SoA) have recently been introduced by the researchers to sustain IoT [13,

15]. Its main functions are: the SOA based IoT helps in reduction of time of product development, it helps in designing the workflow in simple way and it makes the process of marketing the commercial products easier.

5-Layer Architecture: Rafiullah Khan in [18] illustrates the IoT architecture as arrangement of 5 layers as shown in Fig. 2. Main functions of layers of 5-Layer model are: (1) Perception layer perceives and gathers the information about physical objects and pass it to the next layer (2) Transmission layer, helps in secure transmission of data to the next layer. It encompasses wireless networks like LTE, Wifi, Wi-Max, Zigbee etc. (3) Middleware layer, is associated with data storage (4) Application layer, performs the function of application management (5) Business layer, the up-most layer, helps in data analytics and based on that, it takes the further decisions [19].

6-Layer Architecture: In paper [20], the author introduced a 6-Layer architecture in which 2 new layers are augmented into the previous IoT model. These are: (1) MAC layer, that helps to monitor and control the devices (2) Processing and Storage layer, that helps to process the queries, analyze and store the data [19]. In paper [21], 6-layer architecture was proposed for IoT as shown in Fig. 2. The different functions of these layers are: (1) Focus layer, is mainly concerned with identification of devices (2) Cognizance layer, determines the sensing adequacy (3) Transmission layer, allows transmission of data (4) Application layer, determines the collection and categorization of information according to the necessity in the application region (5) Infrastructure layer, provides facilities that are concerned with SOA (6) Competence business layer, allows to analyse the business networks of the IoT systems.

7-Layer Architecture: Researchers proposed a 7-layer architecture [9], which consists of 7-layers as shown in Fig. 2: (1) Application layer, gathers data about a particular task according to client's needs (2) Application support and management layer, determines the security and is responsible for management of IoT devices and their operations (3) Services layer, determines various activities performed by the developers in order to provide essential services to the customers (4) Communication layer, provides a connection between the sensing layer and service layer to transmit the data (5) Network layer, helps devices in transmission and processing of data through internet (6) Hardware layer, allows the integration of hardware components that are needed for deploying the IoT system [21].

Fog and cloud based Architecture Layers: In paper [8], a Fog layered architecture [22] is presented which comprises of 6 layers as demonstrated in Fig. 2: (1) Physical Layer, is concerned with the analysis of things. (2) Monitoring layer, monitors the factors like resources and services by the customers and diverse responses. (3) Preprocessing layer performs the functions like processing, filtering and analyzing the data. (4) Storage Layer performs the function of storing the information and distributing the data when needed. (5) Security layer, ensures the security and privacy of the data. (6) Transport Layer, is the uppermost layer that allows transmission of data.

3.2 Domain-Specific Architectures

CloudThings Architecture: In his work [23], J. Zhou described smart home based scenario for IoT. In this perspective, a CloudThings architecture was introduced that is a cloud-centric IoT platform which with Cloud presents a feasible approach that smooth the progress of development of an application [14].

Industrial IoT Architecture: The architecture for green Industrial IoT is demon-strated in Fig. 3. It comprises of: (1) Sense entities domain that involves Sense nodes (SNs), Gateway nodes (GNs), Control nodes (CNs). (2) Constrained RESTful Network (3) Cloud Server (4) User applications [24].

Smart and Connected Communities (SCC) IoT Architecture: In their work [26], the authors introduced an IoT based SSC architecture for smart cities that comprises of 4 different layers, as illustrated in Fig. 4: (1) Responding layer (or Sensing Layer) is the outer most layer which contains smart devices that interact with the IoT system (2) Interconnecting layer allows information exchange and data transfer among different devices and different domains (3) Data layer performs the tasks like storing huge amount of heterogeneous and trivial data, extracting necessary knowledge from perceived data (4) Service layer provides the interface between IoT system and users in the town.

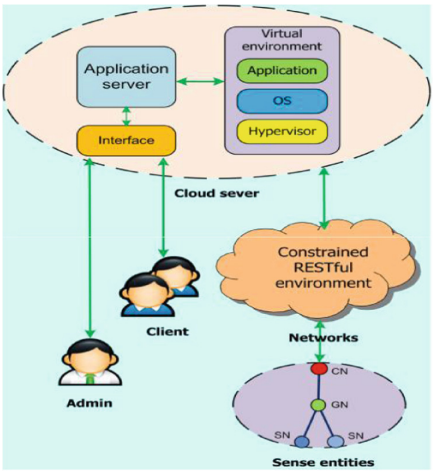


Fig. 3. Energy efficient IIoT architecture[25]

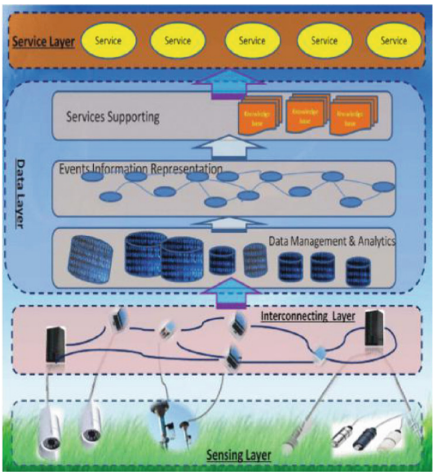


Fig. 4. IoT architecture for smart and connected communities [26]

3G-PLC (Power Line Communication) Architecture: In paper [27], the authors described 3G-PLC based IoT architecture, which collaborates 2 complex communication networks: Third generation (3G) network and Power Line Communication (PLC) network. Scalability factor is the main motive after using the 3G and PLC networks. The IoT framework layers such as perception layer, network layer, aggregation layer, and application layer are integrated with the purpose of discovering a new

3G PLC IoT based architecture. Advantages: Enhanced services as compared to backhaul network opponents, Reduced cost of network construction. Limitation: Deficiency of incorporation of network heterogeneity factor [14].

MobilityFirst Architecture: In paper [29], the authors introduced a name-specific Future Internet Architecture (FIA) termed as MobilityFirst that helps in addressing various challenges related to mobile phones when they act as spontaneous gateways of WSNs in IoT systems. The capacity of the system is analyzed and compared to the sensor data rate at a given hotspot. Advantages: Ad hoc services, high security. Limitation: lack of incentive mechanisms for mobile contributors [14].

3.3 Industry-Defined Architectures

- CISCO Architecture: It follows an Edge model, the processing layer of five-layer model is divided into 3 layers, where data aggregation like collecting data from group of devices is done by data abstraction layer, storage is done by data communication layer and real processing is done by edge computing layer [8, 30, 31].
- IBM Architecture: IBM's cloud computing architecture has been converted to model suitable for IoT with some modifications like device handling and device management [31]. Most of the IBM architecture for IoT deals with middleware rather than the complete architecture. Bringing the power of IBM's Watsons IoT [35] with CISCO's Edge computing, the architecture components revolve around the four major components: Connect, Information Management, Analytics and Risk management [8].
- INTEL Architecture: The INTEL System Architecture Specification (SAS) architecture comprises of 8-layers: the business layer, application layer, control layer, management layer, data layer, communications and connectivity layer, Security layer and developer enabling layer [32].
- Google Architecture: Google reference architecture for IoT introduced by Google Cloud platform comprises of three basic components: (1) Device: includes hardware/software that have direct contact with the world and establish connection to a network for communication among each other, (2) Gateway: helps devices to connect to the cloud services, (3) Cloud: device data is sent to the cloud for processing and combining it with the data generated from other devices [31].
- AWS IoT Architecture: Amazon Web Services (AWS) Reference Architecture for IoT released in 2015, is a managed cloud platform within Amazon IoT solutions. It comprises of- device gateway, message broker, rules engine, security and identity service, thing registry, device shadows, and device shadow service [32].

Comparison of industry-defined architectures for IoT

K.L. Lueth, 2015 [42] performed a survey to know about the top most internet of things companies. The author collected the data from different sources like- Google, LinkedIn, Company Websites, Twitter, and IoT Analytics as described in Fig. 5.

Company	Searches on Google	Tweets on Twitter	Newspaper & Blogs	LinkedIn survey
Intel	1K	2.6K	4K	616
Microsoft	480	1.6K	26K	545
Cisco	1K	1.4K	5K	719
Google	390	3.1K	21K	99
IBM	720	1.5K	7K	504

Fig. 5. Analysis of Top 5 IoT Companies on the basis of survey performed in 2015 [32]

Fig. 6. Top 5 IoT companies ranking [31]

Based on the scores gathered from different resources, it was clear that the Intel company has overtaken Google in 2015 in terms of searches on Google and LinkedIn survey of the number of employees that carry "Internet of Things" as their tag. Therefore on this basis the growth of the companies can be represented in terms of a bar chart as shown in Fig. 6 which represents the top 5 IoT company's rankings.

4 Conclusion

As IoT is rapidly gaining popularity in the technological environment, there is also a need of specific standard architecture. However there is no one particular architecture standardization. Therefore in order to gain knowledge about the IoT architectures, This paper summarized the current state-of-art of Internet of Things architectures that are classified on three different basis i.e. Layer-Specific Architectures, Domain-Specific Architectures and Industry-Defined Architectures along with the comparison of the industry-defined architectures. However, IoT architecture in some application domains like in agriculture, in noise detection systems etc. still need to be explored.

References

1. Nguyen, T.D., Khan, J.Y., Ngo, D.T.: Energy harvested roadside IEEE 802.15.4 wireless sensor networks for IoT applications. Ad Hoc Netw. (2016). http://dx.doi.org/10.1016/j.adhoc.2016.12.003
2. Bilal, M.: A review of internet of things architecture, technologies and analysis smartphone-based attacks against 3D printers (2017). arXiv:1708.04560
3. International Telecommunications Union, ITU Internet Reports 2005: The Internet of Things. Executive Summary. ITU, Geneva (2005)
4. Ungurean, I., Gaitan, N., Gaitan, V.G.: An IoT architecture for things from industrial environment. In: 2014 10th International Conference on Communications (COMM), Bucharest, pp. 1–4 (2014)
5. Cisco Visual Networking Index: Forecast and Methodology, 2014-2019. Cisco, 27 May 2015

6. Rose, K., Eldridge, S., Chapin, L.: The internet of things: an overview-understanding the issues and challenges of a more connected world. The Internet Society (ISOC), (Oct 2015)
7. Swan, M.: Sensor Mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. J. Sens. Actuator Netw. (2012). https://doi.org/10.3390/jsan1030217
8. Masoodhu Banu, N.M., Sujatha, C.: IoT architecture a comparative study. Int. J. Pure Appl. Math. **117**(8), 45–49 (2017). https://doi.org/10.12732/ijpam.v117i8.10
9. Kumar, N.M., Mallick, P.K.: The internet of things: insights into the building blocks, component interactions, and architecture layers. In: International Conference on Computational Intelligence and Data Science (ICCIDS) (2018)
10. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. **4**(5), 1125–1142 (2017)
11. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the internet of things: a review. In: International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012, pp. 648–651 (2012)
12. Leo, M., Battisti, F., Carli, M., Neri, A.: A federated architecture approach for internet of things security. In: Proceedings of 2014 Euro Med Telco Conference (EMTC) (Nov 2014)
13. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. **17**(4), 2347–2376 (2015)
14. Yaqoob, I. et al.: Internet of things architecture: recent advances, taxonomy, requirements, and open challenges. IEEE Wirel. Commun. **24**(3), 10–16 (2017)
15. Xu, L.D., He, W., Li, S.: Internet of things in industries: a survey. IEEE Trans. Ind. Inf. **10** (4), 2233–2243 (2014)
16. Ray, P.P.: A survey on internet of things architectures. J. King Saud Univ. Comput. Inf. Sci. (2016). http://dx.doi.org/10.1016/j.jksuci.2016.10.003
17. Digital Service Innovation and Smart Technologies: Developing Digital Strategies based on Industry 4.0 and Product Service Systems for the Renewal Energy Sector
18. Scientific Figure on ResearchGate. https://www.researchgate.net/Service-oriented-architecture-for-IoT-adapted-from-Li-et-al-2015_fig5_309807447. Accessed 23 Sep 2018
19. Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future internet: the internet of things architecture, possible applications and key challenges. In: 10th International Conference on Frontiers of Information Technology (2012)
20. Ara, T., Shah, P.G., Prabhakar, M.: Internet of things architecture and applications: a survey. Indian J. Sci. Technol. **9**(45), 0974–5645 (2016). https://doi.org/10.17485/ijst/2016/v9i45/106507
21. Thingom, I.B.: Internet of things: design of a new layered architecture and study of some existing issues. IOSR J. Comput. Eng. (IOSR-JCE) (2015)
22. Darwish, D.: Improved layered architecture for internet of things. Int. J. Comput. Acad. Res. (IJCAR) **4**, 214–223 (2015)
23. Sethi, P., Sarangi, S.R.: Internet of things: architectures, protocols, and applications. J. Electr. Comput. Eng. https://doi.org/10.1155/2017/9324035
24. Zhou, J., et al.: Cloudthings: a common architecture for integrating the internet of things with cloud computing. In: IEEE 17th International Conference Computer Supported Cooperative Work in Design, pp. 651–657 (2013)
25. Wang, K., Wang, Y., Sun, Y., Guo, S., Wu, J.: Green industrial internet of things architecture: an energy-efficient perspective. IEEE Commun. Mag. **54**(12), 48–54 (2016). https://doi.org/10.1109/MCOM.2016.1600399CM
26. Green Industrial Internet of Things Architecture: An Energy-Efficient Perspective Scientific Figure on ResearchGate

27. Sun, Y., Song, H., Jara, A.J., Bie, R.: Internet of things and big data analytics for smart and connected communities. IEEE Access **4**, 766–773 (2016). https://doi.org/10.1109/ACCESS.2016.2529723
28. Hsieh, H.-C., Lai, C.-H.: Internet of things architecture based on integrated PLC and 3G communication networks. In: IEEE 17th International Conference on Parallel and Distributed Systems, pp. 853–856 (2011)
29. Qin, Z., et al.: A software defined networking architecture for the internet-of-things. In: 2014 IEEE Network Operations and Management Symposium, pp. 1–9 (May 2014)
30. Li, J., et al.: A mobile phone based WSN infrastructure for iot over future internet architecture. In: Green Computing and Communications, IEEE and Internet of Things, and IEEE International Conference Cyber, Physical and Social Computing, pp. 426–433 (2013)
31. Javeed, Z.: Edge Analytics, the pros and cons of immediate, local insight (May 2018)
32. Development of an Architecture for a Tele-Medicine-Based Longterm Monitoring System-Scientific Figure on ResearchGate

RETRACTED CHAPTER: A Study on Email Security Through Cryptographic Techniques

Akhilesh Kumar Singh(✉), Vinesh Kumar, and Sharad Pratap Singh

GLAU, Mathura, UP, India
{akhileshkr.singh,vinesh.kumar,
sharad.singh}@gla.ac.in

RETRACTED CHPATER

The original version of this chapter was retracted: This chapter has been retracted by the Editors because it reports research undertaken by Shafiya Afzal Sheikh and M Tariq Banday. The retraction note to this chapter is available at https://doi.org/10.1007/978-3-030-37051-0_108

© Springer Nature Switzerland AG 2020, corrected publication 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 342–348, 2020.
https://doi.org/10.1007/978-3-030-37051-0_40

Page Locked GPGPU Rotational Visual Secret Sharing

M. Raviraja Holla[1(✉)] and D. Suma[2]

[1] Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education (MAHE), Manipal, Karnataka, India
raviraj.holla@manipal.edu

[2] Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education (MAHE), Manipal, Karnataka, India
suma.d@manipal.edu

Abstract. Visual Secret Sharing (VSS) schemes address the security concerns of digital images. Rotational VSS schemes are unique in that the shares stacked with the specific rotated shares reveal the secret images. However, these schemes iteratively process huge pixels in sequence. We propose a GPGPU based rotational (2, 3) VSS scheme which leverages concurrency inherent in the traditional rotational schemes. The proposed scheme also makes use of contemporary hardware resources efficiently. The reduction in the memory band-width demand and increased data transfer speed further accelerates the speedup of this scheme. A significant improvement in performance with an efficient resource utilization is observed.

Keywords: Gpgpu · Transparencies · Cuda · Pixel

1 Introduction

Visual Secret Sharing (VSS) schemes address one or more of the security concerns of digital images. The commonality in most of the VSS schemes is that each scheme encrypts the secret image into a number of shares. Individual shares are not sufficient to restore the secret image. This enables safe communication of these shares over the public Internet channel. The combination of the prescribed number of shares can construct an image approximate to the secret image. This technique is different from the traditional cryptography schemes mainly in that the encryption is less-computational and decryption is computation-less. This difference is obvious owing to the size of the secret images to be encrypted and decrypted in the VSS schemes. The assumption here is that the shares are photocopied on to a number of transparencies. When these transparencies are stacked on each other in a certain manner, human visual system perceives the sufficient secret image. It is in this context, the shares are also called as

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 349–359, 2020.
https://doi.org/10.1007/978-3-030-37051-0_41

transparencies. Most of the VSS schemes allow randomness to certain extent so that restored image is approximately equal to the original secret image. The rotational VSS schemes differ from the traditional VSS schemes mainly in that the secret image is restored after stacking the subset of shares with the predefined rotation. However, these schemes suffer from the problem of pixel expansion in the generated shares.

Images over the Internet can be considered the mid-size massive data. Image in the computer is basically a 2-dimensional discrete values. Visual secret shares are also the encrypted images and hence they are the 2-dimensional data. The techniques of creating visual shares intuitively amenable to huge data parallelism. On the other hand the emerging General Purpose Graphic Processing Unit (GPGPU) technologies intend data parallel tasks. They are throughput efficient devices rather than Central Processing Unit (CPU) like latency efficient devices. The GPGPU technologies are evolving faster, and they are part of almost all "things" of Internet of Things (IoTs). Hence the speed at which the security concerns are met, is also an added important security concern therein. The use of GPGPUs in rotational VSS schemes is a significant solution to reduce the increased time needed to generate the expanded shares. This use enables rotational VSS schemes for real-time applications. The cost concerns of such rotational GPGPU VSS schemes are also met as they are scalable. The speedup of such schemes is considerably significant when the image size and the number of transparencies are more. These rotational GPGPU schemes require parallel designs and implementations to make use of the GPGPUs.

The Compute Unified Device Architecture (CUDA) is NVIDIA's heterogeneous data parallel platform. The CUDA provides Application Program Interfaces (APIs) to manage the operations of GPGPU. There are many wrappers of these APIs. PyCUDA keeps python features and facilities accessing CUDA APIs to program the GPGPUs. The CUDA is also evolving to facilitate the advanced features of evolving GPGPU technology available to the programmer. As a result, there exists many speed accelerators available in CUDA. The judicious choice of these catalysts in the parallel design can bring better speedup. For the GPGPUs to perform data parallel tasks, the data need to be transferred from CPU memory to the GPGPU memory. For the rotational VSS schemes, these data are the original image and the expanded share images. Like traditional VSS schemes, the rotational schemes are also less-computational in generating encrypted shares. Introducing concurrency to perform this task certainly improves the speed at which these shares are generated. This gain is due to the volume of data to be processed in the images. Moreover, reducing the speed of large data transfer between CPU memory and the GPU memory considerably reduces the time required to generate the shares. The page locking is such a technique to boost the performance of GPGPU implementation of the rotational VSS scheme. The paper contributes the parallel design and implementation of the page locked GPGPU based rotational VSS scheme. The speedup over the conventional rotational speedup is analyzed. We achieved a better performance gain due to the improved data transfer speed between the CPU and the GPGPU.

2 Related Works

2.1 The VSS Schemes

The title Visual Cryptography (VC) was coined by Allusse et al. [1]. They proposed an image encryption mechanism that avoids computation for its decryption. Assume that there are two participants and hence two transparencies or shares need to generated, say $S0$ and $S1$, out of a single binary secret image I. This scheme generates two (2×2) basis matrices M^0 and M^1 as shown in the Table 1:

Table 1. The basis matrices for $n = 2$.

$M^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$	$M^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

M^0 and M^1 can be considered the reference matrices for the transparent and opaque pixels in I respectively. For a given transparent pixel of I, any one row of M^0 is encoded in corresponding two sub-pixels of $S0$ and $S1$. Similarly for the opaque pixel in I, randomly one row of M^1 is encoded in $S0$ and $S1$. This scheme suffers from pixel multiplicity or expansion problem. In this example width of the transparencies are doubled. In general, this scheme can be extended to yield shares of any size larger than the original image. The secret image can be deciphered only when two shares are overlapped. This scheme can be extended to yield a threshold k out of n or (k, n) scheme. In this scheme, n shares containing concealed image information are generated. Then superposing of minimum k shares properly aligned, decrypt the secret image [12]. This scheme costs additional storage overhead for the basis matrices and the larger shares. While maintaining confidentiality aspect in secured transactions, shares need to be communicated. Hence, they consume additional traffic bandwidth. Moreover, this scheme requires additional cumbersome effort in designing appropriate code books or basis matrices [3].

However, the image encryption proposed in [8] dates back to the Visual Cryptography(VC) [3]. There are many traditional VSS schemes in the literature. Most of the VSS schemes evolved later are refinements of the schemes proposed in [8,12]. Hence, these schemes can be considered belonging to two classes of VC models namely, deterministic models and random grid models [6]. However, the proof in [5] showed that these two classes are closely related and they are the variants of different thresholds. The main issues in all these VSS schemes are the visual quality, the pixel multiplicity and the randomness [6]. The visual quality and pixel multiplicity are closely related in deterministic models of VC [6]. The main objective in the scheme proposed in [18] is to improve the visual quality of the recovered image of a random-grid model. The technique proposed in [7] tries to minimize the randomness in generating transparencies.

The rotational VSS scheme proposed in [14] is a $(2, 3)$ scheme which makes use of technique of the $(2, 2)$ scheme. The used $(2, 2)$ scheme generates two complementary pair of pixels in one share and the same pair in another share, for the corresponding white pixel in the secret image. For the given black pixel in the secret image, it also generates two complementary pair of pixels in one share and a pair of pixels in another share that is complementary to the earlier pair. Obviously it results in 50% contrast degradation of the recovered image for the white pixels. The width of these transparencies is doubled due to the pixel multiplicity ratio of 1:2, with respect to every pixel of the secret image and each transparency.

The $(2, 3)$ scheme in [8] uses three secret images to generate three transparencies. The $(2, 3)$ means that among three transparencies generated, when specific two transparencies properly aligned and superposed can construct one concealed image. This proper alignment is done by appropriate rotation of one transparency relative to the other. Similarly other concealed images can also be deciphered.

2.2 Parallel Rotational VSS Scheme

The scheme in [10] proposed a parallel design for the technique in [14] using NVIDIA GPU and CUDA. The three input secret images and the allocated three share images are copied to the GPU memory, Then a GPU kernel function is invoked. The number of threads created is equal to the height of the image. Each thread executes the kernel, processing distinct pixels according to the technique in [14]. The integer thread block index ($blockIdx.x$), each thread index within a block ($threadIdx.x$), and the total number of threads per block ($blockDim.x$) determines which element of the inputs the thread supposed to process. Each thread is thus responsible for generating the encrypted pixels in all columns corresponding to its row. The encrypted shares are then transferred back to the CPU memory.

2.3 Trends in Heterogeneous Computing and CUDA

The collaboration of both Central Processing Unit (CPU) and the GPGPU or in short GPU in computing is called heterogeneous computing. The term accelerator also refers to GPU with regard to its purpose in computation. In this collaboration, the work needs to be divided for CPU and GPU. The CPU also gains performance in this work distillation A. There are two types of architectures supporting heterogeneous computing. They are fused architecture where CPU-GPU are integrated in the same chip [19] and discrete architecture in which CPU and GPU are separate chips connected by Peripheral Component Interconnect Express (PCIe). In the context of HC, CPU is the host and GPU is called the device. There is a rapid evolution that has already taken place in the architectural features of both CPU and GPU. Table 2 reflects these trends. This evolution will continue further in future. This is indeed a motivation to explore possibilities of exploiting performance through this heterogeneous computing.

Algorithm 1. To set the pixel values in a single row of the three shares using three input images with their corresponding white pixel values.

Input: Three images $I1, I2, I3$. Assume their widths (w) and heights (h) are equal.

Output: Three shares $S1, S2, S3$ of size $(2 \times w) \times h$ with their first row pixels values corresponding to the $WHITE\_PIXELs$ in the first row of the input images

Allocate memory for three output shares of size $(2 \times w) \times h$;
Set $p = 0$; $q = 2 \times w - 1$; $n = w - 1$;
For $j \in [0, ..., w/2]$ do:
if$(random == 1)$:
  if $(I1[i][j] == WHITE\_PIXEL)$: Check I1 —Left
    $S1[i][p] = WHITE\_PIXEL; S1[i][p+1] = BLACK\_PIXEL;$ Set S1 —Left
    $S2[i][q] = WHITE\_PIXEL; S2[i][q-1] = BLACK\_PIXEL;$ Set S2 —Right
  if$(I2[i][n] == WHITE_PIXEL)$: Check I2 —Right
    $S3[i][p] = WHITE\_PIXEL; S3[i][p+1] = BLACK\_PIXEL;$ Set S3 —Left
  if $(I3[i][j] == WHITE\_PIXEL)$: Check I3 —Left
    $S1[i][q] = WHITE\_PIXEL; S1[i][q-1] = BLACK\_PIXEL;$ Set S1 —Right
  if $(I1[i][n] == WHITE\_PIXEL)$: Check I1 —Right
    $S2[i][p] = WHITE\_PIXEL; S2[i][p+1] = BLACK\_PIXEL;$ Set S2 —Left
  if $(I2[i][j] == WHITE\_PIXEL)$: Check I2 —Left
    $S3[i][q] = WHITE\_PIXEL; S3[i][q-1] = BLACK\_PIXEL;$ Set S3 —Right
  $n = n - 1$; $p = p + 2$; $q = q - 2$;
End

The CUDA GPGPU framework by NVIDIA is a matured framework with which a sequential program can be easily reformulated to a parallel program to utilize GPGPU capability [17]. This reformulation of the sequential programs to fit on GPGPU can be considered as novel approaches in research [17]. The algorithms that can utilize GPGPU fits to their use in real time applications [4]. The CUDA platform is the best choice for image processing applications as it offers good performance with an affordable cost [2]. The GpuCV framework for parallel implementation is useful in computer vision [1]. This framework integrates OpenGL-GLSL (OpenGL Shading Language) and NVIDIA CUDA API and contributes best from each. There are many application case studies discussed in [9] that are conducive for the GPU computing. The CPU parallelism and the GPU parallelism with their salient differences are mentioned in [15]. The PyCUDA python library augments CUDA [16] with its programming convenience. Parallel processing is the viable alternative to such applications [13].

Table 2. Trends in features of processing units [11].

Features	CPU	GPU
1. Transistor count	>10 Billion	8 Billion
2. Core count	>60 in near future	3072
3. LLC size	96 MB	2048 KB
4. 3D stacking	Available	Available
5. Interconnect-Bandwidth	NVLink promises to offer 5× to 12× bandwidth compared to PCIe-Gen3	

All these reviews cue that the use of GPGPU enables VSS schemes apt for the real-time applications with an affordable cost and efficient resource utilization.

3 The Proposed Page Locked GPGPU Streaming Rotational VSS

The scheme proposed in [10] uses GPGPU for generating transparencies. In this scheme, the inputs to the kernel are the three secret images and also the allocated three transparency images for the output. These transparency images are double in width than their input images. The memory allocation to all these images is done by the host or the CPU in host or the CPU memory. However, this memory is a paged memory. Many virtual pages maps to the same CPU memory page. Hence, the allocated pages of the images may have to be frequently removed and reloaded by the operating system before those pages get transferred to the GPGPU memory. Moreover these data transfers are done in large chunks using a technique called Direct Memory Access (DMA) for efficiency considerations. In addition to this, theses massive data need to be transferred from host memory to the GPGPU memory or the device memory. The CUDA driver makes this data transfer in small chunks through a memory called page locked memory or a pinned memory. It means that chunks of input images gets copied to pinned memory and then to the destination. Figure 1 depicts the paged data transfer.

This double data transfer can be reduced to one, if the allocations are done directly in the pinned memory. On the other hand, there is a considerable disparity in bandwidths offered by the host memory and the device memory. The bandwidth of the host memory is less than the bandwidth of the device memory. This disparity in the bandwidths results in resource underutilization and also poor performance. Also, the Compute to Global Memory Access (CGMA) ratio is significantly less in this scheme. It means that the amount of data transfer is much more than the GPGPU computation. It allows room for the better performance if data transfer is optimized. The CUDA provides an advanced feature called page locked memory [9] with which the allocation can be done directly in the page locked memory. These allocated pages in the page locked memory instead of the paged memory cannot be paged out by the operating system. This

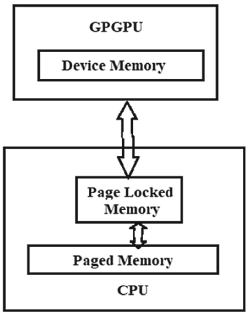


Fig. 1. The paged data transfer.

reduces the data transfer or the communication overhead between the host and the device. This also improves bandwidth. With the advancements in the CPU memory technology, judicious utilization of pinned memory is viable solution to improve the performance. Figure 2 depicts the page locked data transfer.

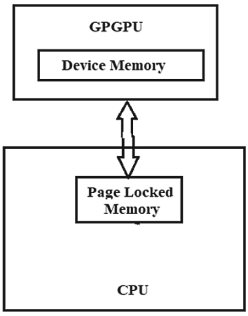


Fig. 2. The page locked data transfer.

The $cudaHostAlloc()$ function is used to allocate page locked memory to the input images. The $cudaFreeHost()$ frees the page locked memory.

The Algorithms 2, 3, and 4 show the procedure involved in the proposed scheme.

4 Experimental Results

The PyCUDA with OpenCV is used to implement the scheme proposed in this paper. The execution is done on a high-end system namely, PARAM Shavak super computer. This super computer has Intel(R) Xeon(R) -E5-2670 CPU interfaced to an NVIDIA Tesla K40c GPGPU through PCIe. The hardware configuration is shown in Table 3. We observe from Table 3 that the GPGPU has massive number of streaming processors compared to the number of CPU cores.

Algorithm 2. To allocate memory, invoke kernel and reconstruct the secret images **(Host module)**

Input: Three secret images $I1, I2, I3$. Assume their widths (w) and heights (h) are equal.

Output: Three recovered images $R1, R2, R3$ of size $(2 \times w) \times h$.

1 Convert $I1, I2, I3$ to their corresponding binary images, I_{b1}, I_{b2}, I_{b3}.
2 Allocate three $(w \times h)$ page locked memory and copy I_{b1}, I_{b2}, I_{b3} images to the allocated memory using $cudaHostAlloc()$ function.
3 Allocate $(2 \times w) \times h$ page locked memory using $cudaHostAlloc()$ function for the three $outShare1, outShare2, outShare3$.
4 Copy I_{b1}, I_{b2}, I_{b3} to device global memory (GPU memory).
5 Invoke GPGPU Encryption Kernel(I_{b1}, I_{b2}, I_{b3},$outShare1, outShare2, outShare3$)
6 Copy the $outShare1, outShare2, outShare3$ available in device global memory to host pinned memory.
7 Invoke Image Reconstruct($outShare1, outShare2, outShare3$,$R1, R2, R3$)
8 Output $R1, R2, R3$.
9 Free the page locked memory with $cudaFreeHost()$ function.
10 End

Algorithm 3. GPGPU Encryption Kernel: To generate shares in device memory **(Device module)**

Input: Three secret binary images I_{b1}, I_{b2}, I_{b3} with allocated $outShare1, outShare2, outShare3$.

Output: Three shares $outShare1, outShare2, outShare3$ of size $(2 \times w) \times h$.

1 $j = 0$
2 For $m \in [0, ..., width]$ and $n \in [width, ..., 0]$ do:
3 Let each thread compare the pixels of I_{b1}, I_{b2}, I_{b3} row-wise, according to algorithm in [14] and generate j and $(j + 1)^{th}$ pixels of $outShare1, outShare2, outShare3$.
4 $j = j + 2$
5 Return $outShare1, outShare2, outShare3$ device global memory.
6 End

Algorithm 4. Image Reconstruct: To reveal the secret images **(Host module)**

Input: Three shares $outShare1, outShare2, outShare3$ with allocated recovered images $R1, R2, R3$.

Output: Three recovered images $R1, R2, R3$.

1 $R1$ = Overlay $outShare1$ with the 180° anticlockwise rotated $outShare2$.
2 $R2$ = Overlay $outShare2$ with the 180° anticlockwise rotated $outShare3$.
3 $R3$ = Overlay $outShare3$ with the 180° anticlockwise rotated $outShare1$.

Table 3. Super compuer PARAM Shavak specifications.

Features	CPU	GPU
	Intel(R) Xeon(R)- E5-2670	Tesla K40c
Clock	2.30 GHz	745 MHz
Cache memory	30720 KB	64KB(L1), 1.5 MB(L2)
RAM	8 TB	12 GB VRAM
Number of cores	2 with 12 cores each	2880
Memory bandwidth	68 GB/s	288 GB/s

Many images of varying features are used as test cases. A sample secret image with the respective generated share and the reconstructed image upon stacking is shown in Figs. 3, 4 and 5 respectively.

Fig. 3. A sample input secret image for the proposed scheme.

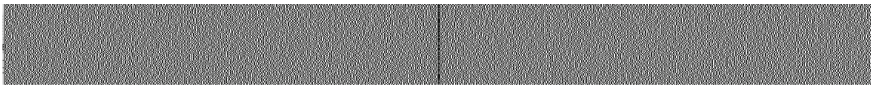


Fig. 4. The encrypted transparency generated by the proposed scheme.

Execution time of the proposed scheme is compared with the execution time of the PRVC, and the corresponding values are shown in Table 4. Figure 6 plots the execution of times of the PRVC and the proposed schemes. There is significant decrease in the execution time of the proposed scheme com-pared to the PRVC. The speedup of the proposed scheme over the PRVC decreases as the image size increases because the speedup is taken over the parallel counterpart rather than the sequential traditional rotational scheme.

Fig. 5. The recovered secret image by the proposed scheme.

Table 4. The speedup of the proposed scheme over Parallel Rotational VC (PRVC) scheme.

Sl.no	Image Resolution	Execution time in milliseconds		Speedup of the proposed scheme
		PRVC	Proposed scheme	
1	256 × 256	0.565	0.278	2.03
2	400 × 400	0.578	0.321	1.8
3	760 × 570	0.618	0.345	1.79
4	2048 × 1536	0.721	0.452	1.6

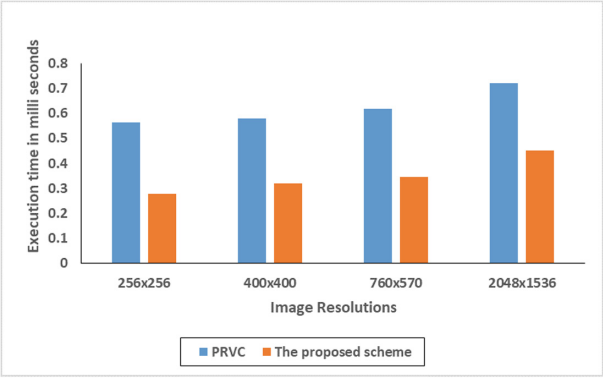


Fig. 6. The execution of times of PRVC and the proposed scheme with different Image resolutions.

5 Conclusion

We propose a page locked GPGPU rotational VSS scheme for the gray scale images in this paper. Most of the VSS sharing schemes are intuitively less computational but more data intensive. The proposed scheme makes use of GPGPU for this data intensive share generating process. Moreover the scheme proposes a data transfer optimization thereby reducing communication overhead. We achieved a significant performance gain of 1.8× due to the improved bandwidth. Reformulating a sequential design to a GPGPU design itself being a novel approach, the use of advanced features of a matured platform like CUDA enables the VSS schemes to meet the matured demands like speed. But the GPGPU capacity constraints and the mutually conflicting features must be taken into consideration while exercising with those advanced features. For example the pinned memory is a limited resource. This memory can not be oversubscribed. A single application consuming more pinned memory can have very serious consequences as it degrades the performance of virtual memory.

In future we refine the proposed scheme using other design alternatives to overcome this limitation. There are many VSS schemes which can be reformulated to leverage the advanced features of GPGPUs.

References

1. Allusse, Y., Horain, P., Agarwal, A., Saipriyadarshan, C.: Gpucv: a gpu-accelerated framework for image processing and computer vision. In: International Symposium on Visual Computing. pp. 430–439. Springer (2008)
2. Asaduzzaman, A., Martinez, A., Sepehri, A.: A time-efficient image processing algorithm for multicore/manycore parallel computing. In: SoutheastCon 2015, pp. 1–5. IEEE (2015)
3. Chen, T.H., Tsao, K.H.: Threshold visual secret sharing by random grids. J. Syst. Softw. **84**(7), 1197–1208 (2011)
4. Daga, B., Bhute, A., Ghatol, A.: Implementation of parallel image processing using nvidia gpu framework. In: Advances in Computing, Communication and Control, pp. 457–464. Springer (2011)
5. De Prisco, R., De Santis, A.: On the relation of random grid and deterministic visual cryptography. IEEE Trans. Inf. Forensics Secur. **9**(4), 653–665 (2014)
6. D'Arco, P., De Prisco, R.: Visual cryptography. In: International Conference for Information Technology and Communications, pp. 20–39. Springer (2016)
7. D'Arco, P., De Prisco, R., Desmedt, Y.: Private visual share-homomorphic computation and randomness reduction in visual cryptography. In: International Conference on Information Theoretic Security, pp. 95–113. Springer (2016)
8. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Opt. Lett. **12**(6), 377–379 (1987)
9. Kirk, D.B., Wen-Mei, W.H.: Programming massively parallel processors: a hands-on approach. Morgan Kaufmann (2016)
10. Mayya, V., Nayak, A.: Parallel implementation of rotation visual cryptography on gpu using cuda. In: Proceedings of the International Conference on Advances in Image Processing, pp. 62–65. ACM (2017)
11. Mittal, S., Vetter, J.S.: A survey of cpu-gpu heterogeneous computing techniques. ACM Comput. Surv. (CSUR) **47**(4), 69 (2015)
12. Naor, M., Shamir, A.: Visual cryptography. In: Workshop on the Theory and Application of Cryptographic Techniques, pp. 1–12. Springer (1994)
13. Pitas, I.: Parallel algorithms for digital image processing, computer vision and neural networks. Wiley (1993)
14. Reddy, B.D., Kumari, V.V., Raju, Y.P.: Rotation visual cryptography using basic (2, 2) scheme. Int. J. Comput. Sci. Commun. Technol. Citeseer (1984)
15. Soyata, T.: GPU parallel program development using CUDA. Chapman and Hall/CRC (2018)
16. Vaidya, B.: Hands-On GPU-Accelerated Computer Vision with OpenCV and CUDA: Effective techniques for processing complex image data in real time using GPUs. Packt Publishing (2018)
17. Wang, H., Peng, H., Chang, Y., Liang, D.: A survey of gpu-based acceleration techniques in mri reconstructions. Quant. Imaging Med. Surg. **8**(2), 196 (2018)
18. Yan, X., Liu, X., Yang, C.N.: An enhanced threshold visual secret sharing based on random grids. J. Real-Time Image Process. **14**(1), 61–73 (2018)
19. Yang, Y., Xiang, P., Mantor, M., Zhou, H.: Cpu-assisted gpgpu on fused cpu-gpu architectures. In: IEEE International Symposium on High-Performance Comp Architecture, pp. 1–12. IEEE (2012)

Opinion Mining Based on People's Feedback About Engineering Degree

M. Karpagam, S. Kanthimathi, S. Akila, and S. Kanimozhi Suguna(✉)

School of Computing, SASTRA Deemed University, Thanjavur, India
kanimozhi.suguna@gmail.com

Abstract. Support Vector Machine (SVM) is a learning model which can be used as data analyzer for classification by its associated algorithms. SVM classifies the data by finding the hyper-plane that maximizes the gap between two classes. The structure of decision tree consists of root, branches and leaf nodes and the tests performed on an attribute and leaf nodes were represented by internal nodes which denote the result of the test. In this paper, a model to classify data using an ensemble of decision tree and support vector machine is proposed on a dataset collected on the topic of 'Engineering Degree'. Combining the decision tree and support vector machine can be an effective method for classifying the data as it reduces the testing and training time of the data collected. The analysis of the result has been performed on a sample set of data taken from a large collection stored in the cloud using Hadoop.

Keywords: Support vector machine (SVM) · Decision tree algorithm · Classification · Hadoop hive · Engineering degree

1 Introduction

A classification is a form of data analysis that extracts models describing important data classes. A well-designed data classification technique allows essential data to be found and retrieved easily. Classification can help an organization to meet legal and regulatory requirements for retrieving specific information in a given timeframe, and this is often the motivation behind implementing data classification technology.

Data mining is an ever updating and an important topic in the current technological world. There have been many ensembles of classifiers created and experimented upon. A number of papers are presented based on data mining and machine learning and out of which a few are listed below.

- In [1] an approach using a combination of SVM and decision tree has been proposed. The aim is to reduce the number of data points that require SVMs' help in getting classified.
- Somvanshi and Chavan [2] proposed a brief summary of data mining classification by using the machine learning technique in their paper. Machine learning is used to get a machine to learn by observing recurring patterns or by observing which pattern leads to which outcome.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 360–372, 2020.
https://doi.org/10.1007/978-3-030-37051-0_42

- Zhao et al. [7] presented a paper on classification techniques by combining support vector machines and decision tree into one multi-class classifier to solve multi-class classification problems in their paper.
- Pachghare and ParagKulkarni presented a paper where a comparative study of the decision tree algorithm is done. An investigation of SVM models and the choice of which can be used for implementation and evaluation is found out in their paper [4].
- In the paper by Sangita et al. [3] the authors proposed a method for classifying the speed of wind in an area by using a decision tree, support vector machines, and Naive Bayesian classification.
- Yasodha and Prakash proposed a classification method for managing the organizational talents using Support Vector Machines.
- In one of the recent papers by Thamilselvan and Sathiaseelan, the authors proposed a method for classifying images using a hybrid of the data mining algorithms like GA-SVM, EKM-EELM, Decision tree- Naive Bayes [7].
- [9, 10] are papers wherein Hadoop has been used in for effective data analysis and make time efficient predictions.

2 Basic Principles of the Decision Tree

The structure of decision tree consists of root, branches and leaf nodes and the tests performed on an attribute and leaf nodes were represented by internal nodes which denotes the result of the test. The classification or regressions are built by decision tree in the form of tree structure. It breaks down a dataset into smaller subsets and an associated decision tree is incrementally developed at the same time. This working principle of the decision tree is represented in Fig. 1.

The splitting attribute can be selected based on a number of parameters. One such value is the Information Gain. The formula used is given in Eq. (1).

$$INFO(D) = -\sum_{i=1}^{c} p^i log_2 p^i \tag{1}$$

In Eq. (1), c represents the number of distinct classes.

$$INFO_A(D) = \sum_{j=1}^{k} \frac{|D_j|}{|D|} log_2 \frac{|D_j|}{|D|} \tag{2}$$

In Eq. (2), j represents the number of distinct values for attribute A in dataset D.

$$INFO\_GAIN(A) = INFO(D) - INFO_A(D) \tag{3}$$

Out of the list of attributes, the one with the maximum gain is selected as the splitting attribute. After which the dataset is split based on the selected attribute and checked if each one of the newly created datasets has a single or multiple labels. If single label then splitting for that data set is stopped else if there are attributes left out in

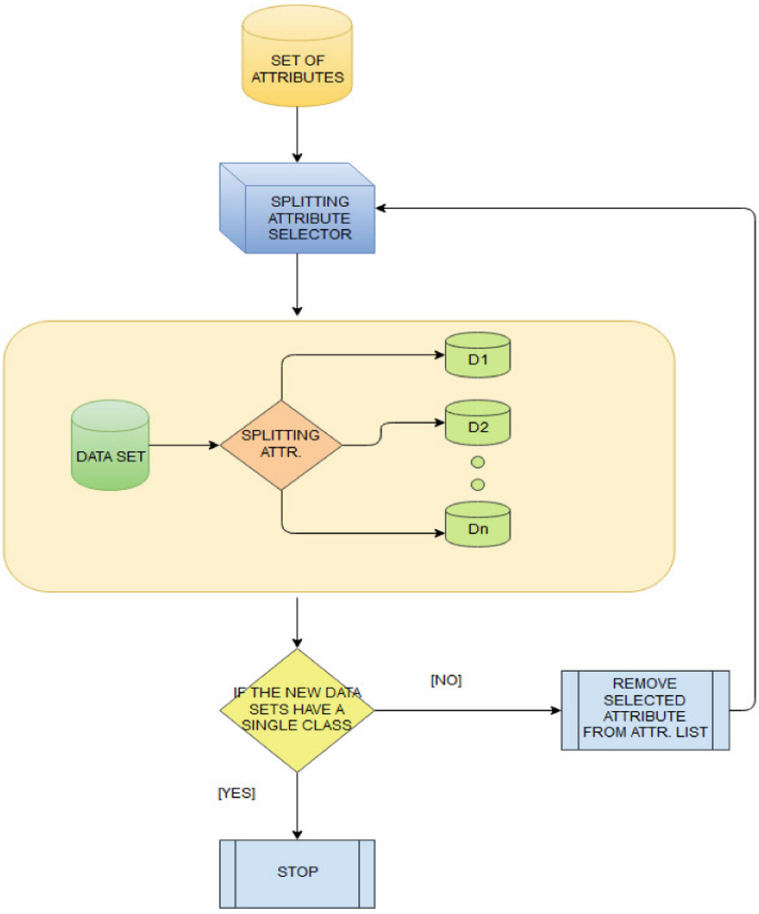


Fig. 1. Working principle of decision tree

the list still then the data set created is further split based on another attribute using information gain as attribute selection measure and then checked for a single label. If there are no attributes left and the obtained new data set is not containing a single label then the dataset is assigned the label with the maximum count.

3 Basic Principles of Support Vector Machine

SVM is a very powerful machine learning algorithm and a best-supervised classification technique. It can be used for regression and classification problems. It uses a technique called kernel trick to transform the data and finds an optimal boundary between the outputs based on the transformations obtained. It captures much more complex relationships between the data points without performing difficult transformations. An SVM classifies the data by finding the hyper-plane that differentiates the

classes of objects very well. Consider the given scatter plot in Fig. 2. The hyperplane required to differentiate the classes represented in Fig. 2 is as given in Fig. 3. The plane was found using SVM. The properties of the SVM include the degree of the plane polynomial have to differentiate the classes and the kernel is 'linear' and the decision function shape is 'one vs rest'. The planes were generated using the SVM classifier provided by the python's third-party module sklearn.

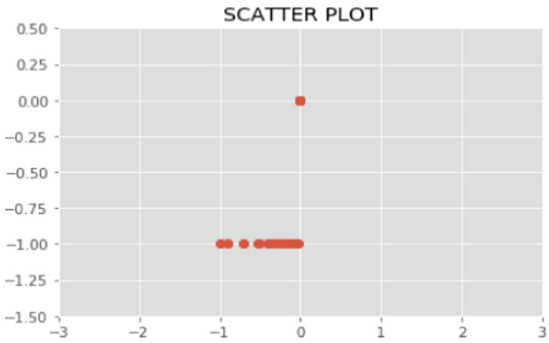


Fig. 2. Scatter plot for random sample with two classes

4 Engineering Dataset [8]

In this paper, an engineering dataset is considered. The dataset consists of a basic survey on the people's view about undergoing the undergraduate course in engineering degree. It consists of the timestamp as to when the record was created, gender of the person, age of the person, what do they prefer after UG course from parents point of view, the expected cost of the degree, the changes required to be made in the current engineering system, the quality of the engineers produced every year and the fate of the future engineering graduates. The dataset also collects the information about what effective steps can be taken to improve the education quality in the country. Basically, the age attribute in the data set is categorized into four types less than 21, 21–35, 35–50, above 50. Similarly, gender is classified into male and female, preference after undergraduate (U.G.) as work, studies, own wish etc. The following sample code represents the classification details of the collected data.

```
Out [4]: ['E:/Less than 21.csv', 'E:/More than 50.csv',
'E:/21-35.csv', 'E:/35-50.csv']
Out [6]: ['E:/Male.csv', 'E:/Female.csv']
```

The following Table 1 gives the list of attribute column in the dataset.

Furthermore, for the sake of classification purpose, the age, gender and preference after UG column have been considered. The preference after UG column contained many values most of which was either 'work' or 'higher studies'. So the entries in that column have been modified as to either 'work' or 'higher studies' or 'others'. This classification is represented in the Fig. 4.

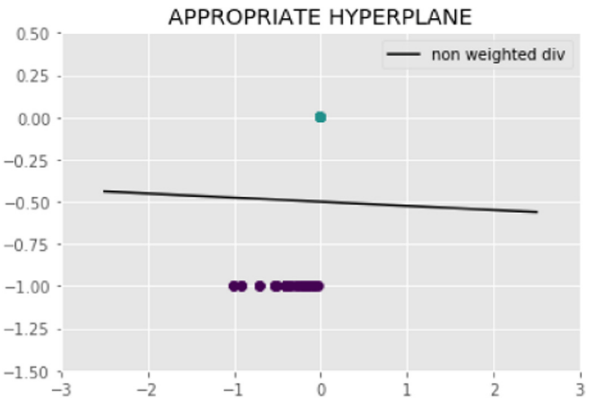


Fig. 3. Hyper-plane separating two classes

Table 1. Attribute column in the dataset

Timestamp	Gender	Age	What do you prefer after UG? (parents point of view)	Cost of engineering degree	Changes required on current engineering system	Quality of engineers produced	Fate of engineers and future graduates

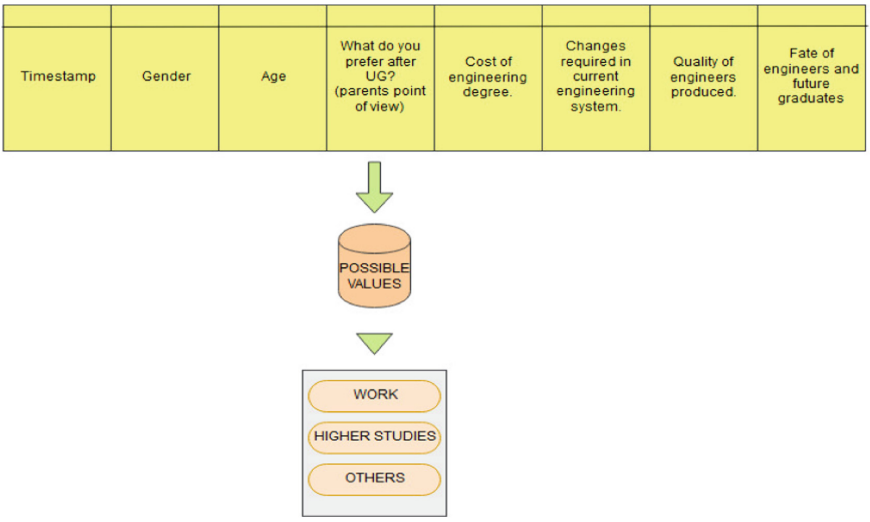


Fig. 4. Attribute values reassignment

5 Workflow of the Proposed System

The workflow for the suggested model involved first processing the dataset using the decision tree after which the results obtained were furthermore processed using the SVM classifier produced by the sklearn package in python. First, a sample of 100 entries is selected using querying in Hive software and 80% is taken as training data and 20% is taken as testing data. The dataset is classified using decision tree algorithm. The structure of decision tree consists of root, branches and leaf nodes and the tests performed on an attribute and leaf nodes were represented by internal nodes which denote the result of the test. Decision tree builds classification or regression models in the form of a tree structure. The initial class labels for the type of comment on the quality of engineers produced is generated by the Text blob package which computes the polarity of the comment and if polarity negative the comment is negative else if the polarity greater than zero then positive else if zero then neutral.

The work here consists of two phases. The first phase involves creating a model which makes use of 80 entries as training data. The model is created with the help of the decision tree. The splitting attribute is selected based on the information gain and is performed using the Eqs. (1), (2), and (3). The distinctions of three classes are represented using the variable c in Eq. (1). Using these initial conditions, the splitting of a dataset is based on 'Age' attribute into four datasets. Each of the datasets does not contain single class hence furthermore another attribute is selected using information gain for each of the new datasets separately until each newly created dataset contains a single class.

The next phase involves passing on the polarity values and the computed class labels using the decision tree into the SVM classifier specified by the skilearn package with the degree of the hyper-plane polynomial as 3 since we have three classes (POS, NEU, NEG) and the kernel s a linear one and the generated planes are represented by non-weighted. The workflow displayed in the following Fig. 5 is applied to the 80% of training data set and the results obtained are described in Fig. 6.

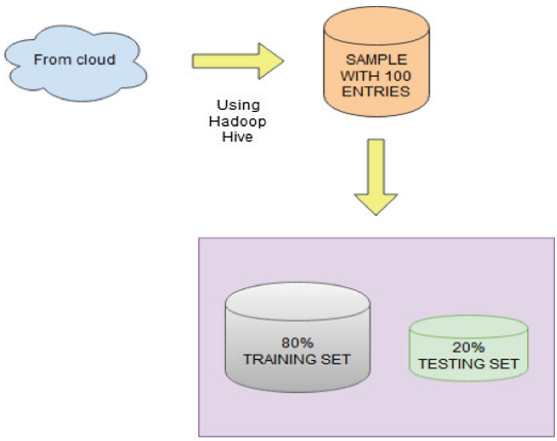


Fig. 5. Splitting of dataset into training and testing set

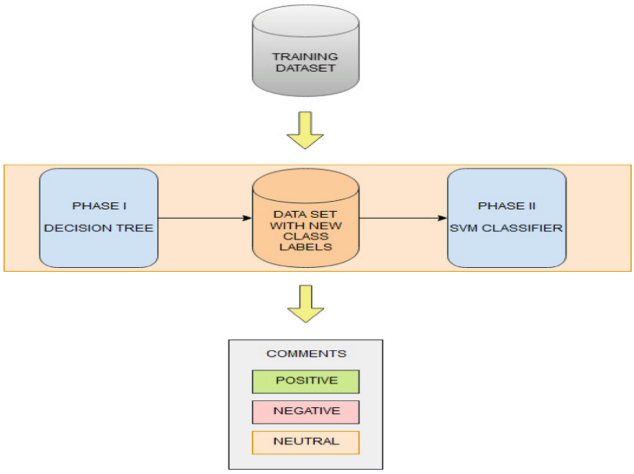


Fig. 6. Proposed workflow

6 Analysis and Result

The results after the initial split based on 'Age' attribute followed by split using 'Gender' attribute and 'Future' (i.e. preference after UG) is as in the below Table 2.

Table 2. Classification result using decision tree

Age	Preferences	Gender	Count		Total
Less than 21	Work	Male	POS	12	25
			NEU	4	
			NEG	7	
		Female	POS	0	
			NEU	1	
			NEG	1	
	Higher education	Male	POS	2	22
			NEU	10	
			NEG	4	
		Female	POS	2	
			NEU	1	
			NEG	3	
	Others	Male	POS	3	6
			NEU	1	
			NEG	1	
		Female	POS	0	
			NEU	0	
			NEG	1	

(*continued*)

Table 2. (*continued*)

Age	Preferences	Gender	Count		Total
21–35	Work	Male	POS	0	2
			NEU	0	
			NEG	2	
		Female	POS	0	
			NEU	0	
			NEG	0	
	Higher education	Male	POS	0	5
			NEU	1	
			NEG	3	
		Female	POS	0	
			NEU	0	
			NEG	1	
	Others	Male	POS	1	1
			NEU	0	
			NEG	0	
		Female	POS	0	
			NEU	0	
			NEG	0	
35–50	Male	Work	POS	0	7
			NEU	0	
			NEG	1	
		Higher education	POS	1	
			NEU	0	
			NEG	2	
		Others	POS	1	
			NEU	2	
			NEG	0	
	FEMALE	Work	POS	0	9
			NEU	1	
			NEG	2	
		Higher education	POS	2	
			NEU	2	
			NEG	2	
		Others	POS	0	
			NEU	0	
			NEG	0	
More than 50	Male	Work	POS	0	2
			NEU	0	
			NEG	1	

(*continued*)

Table 2. (*continued*)

Age	Preferences	Gender	Count		Total
		Higher education	POS	0	
			NEU	1	
			NEG	0	
		Others	POS	0	
			NEU	0	
			NEG	0	
	Female	Work	POS	0	1
			NEU	0	
			NEG	0	
		Higher education	POS	1	
			NEU	0	
			NEG	0	
		Others	POS	0	
			NEU	0	
			NEG	0	
					80

The gender attribute has two divisions such as male and female. The age attribute is classified as less than 21, 21–35, 35–50 and more than 50. The resultant decision tree is represented in the following Fig. 7.

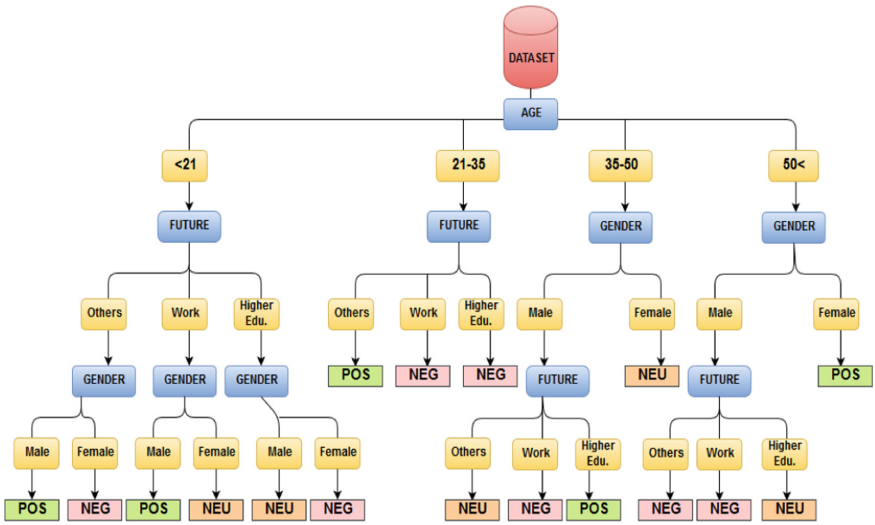


Fig. 7. Decision tree for the proposed dataset

The first splitting attribute is 'Age' which creates four datasets following which each one of the new datasets is split further either based on 'Gender' or 'Future'. The results from the phase II i.e. the SVM classifier is given in Fig. 8 (Fig. 9):

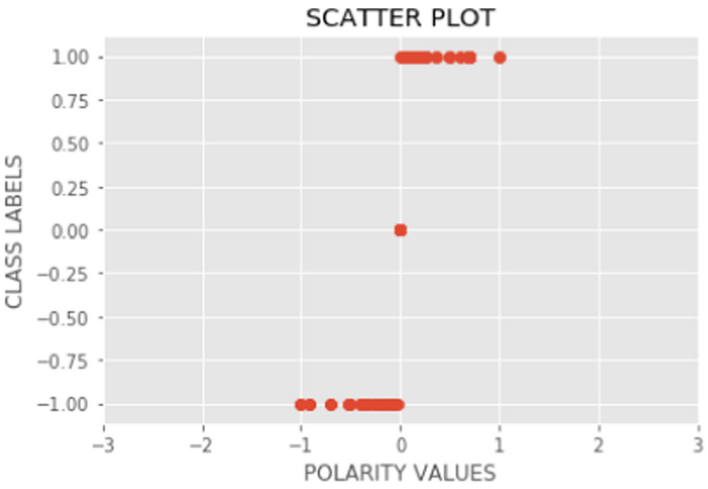


Fig. 8. Scatter plot for the given dataset with three classes

Fig. 9. Hyper-planes segregating the resultant classes

In order to evaluate the accuracy of the model proposed, the confusion matrix is employed. TP means both the predicted and the actual class label are the same and true. TN means both the predicted and the actual class label are same and negative. FP means the actual label is negative but the model has predicted it as positive. FN means

the actual label is positive but the model has predicted it as negative. The given Fig. 10 represents the confusion matrix for the proposed model using the 20% test data.

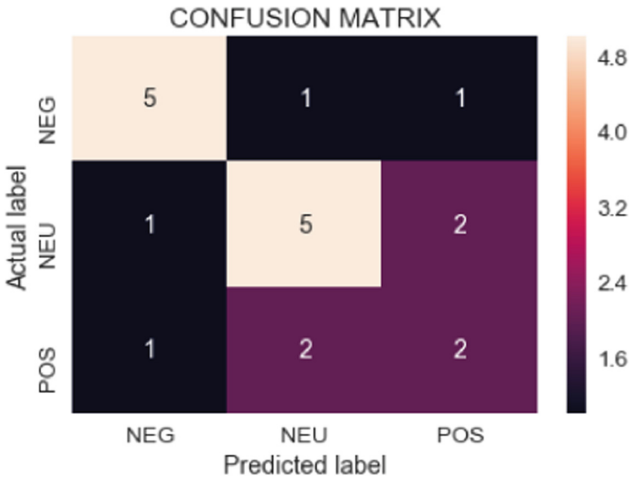


Fig. 10. Confusion matrix for the proposed system

The accuracy of the proposed model is calculated using the Eq. (4).

$$Accuracy = \frac{TP + TN}{P + N} \tag{4}$$

The values of TP, TN, P, and N can be obtained from the confusion matrix. For the proposed model the accuracy formula is slightly modified as it has 3 classes. It is calculated based on the Eq. (5). The accuracy rate is 60.00%.

$$Accuracy = \frac{T_{neg} + T_{neu} + T_{pos}}{neg + neu + pos} \tag{5}$$

The error rate of the proposed model is calculated using the Eq. (6).

$$Error\ rate = \frac{F_{neg} + F_{neu} + F_{pos}}{neg + neu + pos} \tag{6}$$

The values of F_{neg}, F_{neu}, and F_{pos} can be obtained from the confusion matrix. The error rate of the proposed model is around 40%. The confusion matrix for the test data using decision tree is as in the following Fig. 11.

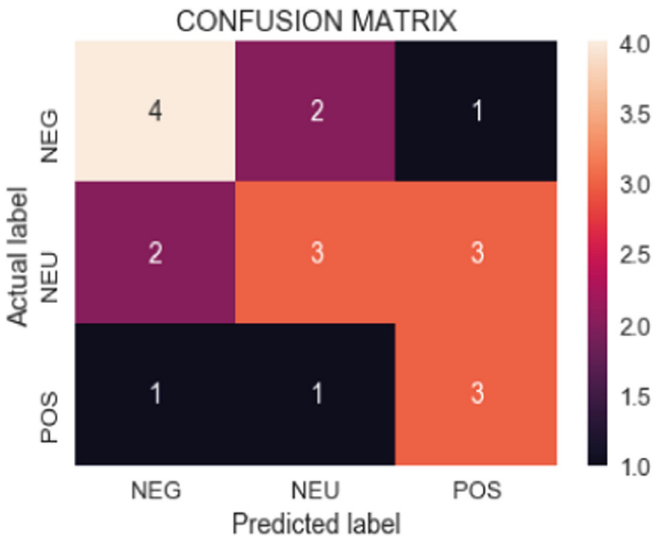


Fig. 11. Confusion matrix for the dataset using decision tree

The accuracy rate obtained using decision tree is obtained using the same formula as specified above. The accuracy rate is 50% for the test data. So it is pretty much obvious that the ensemble of two classifiers produces improved accuracy than a classifier used alone.

7 Conclusion

The result on the quality of engineers produced as of now is 'NEGATIVE'. Most of the people have provided a negative review on the quality of engineers produced. Also, a major portion of the people in the dataset has provided 'NEUTRAL' comments on the topic. There may be deviations due to various thought aspects of people. So maybe after all the engineers produced are not that bad. The combination of both the decision tree and the support vector machine (SVM) was used to obtain the overall result. Also, the accuracy of the model proposed is nearly 60% which is 10% more than the accuracy produced by using decision tree alone.

Also, these results represent a sample part of the entire population of data in the cloud. Constructing and executing this model in Hadoop environment provides improved results as well as efficient processing. This model can furthermore extend to larger datasets too.

Compliance with Ethical Standards. All author states that there is no conflict of interest. We used our own data. Humans/animals are not involved in this research work.

References

1. Arun Kumar, M., Gopal, M.: A hybrid SVM based decision tree. Pattern Recognit. **43**(12), 3977–3987 (2010)
2. Somvanshi, M., Chavan, P.: A review of machine learning techniques using decision tree and support vector machine. In: IEEE ICCUBEA 2016. IEEE (2016)
3. SangitaB, P., Deshmukh, S.R.: Use of Support Vector Machine, decision tree, and Naive Bayesian techniques for wind speed classification. In: IEEE International Conference on Power and Energy Systems (ICPS) 2011. IEEE (2011)
4. Ponni, J., Shunmuganathan, K.L.: Multi-agent System for data classification from data mining using SVM. In: IEEE International Conference on Green Computing, Communication, and Conservation of Energy (ICGCE). IEEE (2016)
5. Pachghare, V.K., KulKarni, P.: Pattern-based network security using decision trees and support vector machine. In: IEEE International Conference on Electronics Computer Technology (ICECT) 2011. IEEE (2011)
6. Yasodha, S., Prakash, P.S.: Data mining classification for talent management using SVM. In: IEEE International Conference on Computing, Electronics and Electrical Technologies (ICCEET) 2012. IEEE (2012)
7. Zhao, H., Yao, Y., Liu, Z.: A classification method based on non-linear SVM decision tree. In: IEEE Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD) 2007. IEEE (2007)
8. Thamilselvan, P., Sathiaseelan, J.G.R.: Image classification using hybrid data algorithms–a review. In: IEEE International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) 2015. IEEE (2015)
9. Song, J., Guo, C., Wang, Z., Zhang, Y., Yu, G., Pierson, J.-M.: HaoLap: a hadoop based OLAP system for big data. J. Syst. Softw. **102**, 167–181 (2015)
10. Agarwal, S., Yadav, L., Mehta, S.: Cricket team prediction with hadoop: statistical modeling approach. Proc. Comput. Sci. **122**, 525–532 (2017)

Design and Implementation of Steering Based Headlight Control System Using CAN Bus

M. Dhivya[1], K. Gayathri Devi[1], and S. Kanimozhi Suguna[2(✉)]

[1] Department of Electronics and Communication Engineering, Dr. N.G.P. Institute of Technology, Kalapatti, Coimbatore 641048, India
[2] School of Computing, SASTRA Deemed University, Thanjavur, India
kanimozhi.suguna@gmail.com

Abstract. The Controller Area Network is a simple, well designed, highly efficient and reliable in-vehicle bus standard widely used since its development in 1983. Controller Area Network is a serial communication protocol that supports distributed real-time control in Automotive Electronics. CAN is a thrust area for the past two decades in multi-disciplinary research, encompassing various tools and concepts for solving real-time problems. In this paper steering based headlight control system using CAN bus is implemented. The model consists of a steering control unit which determines the direction of the headlight according to the changes in the steering position. The Headlight control unit is varied from −16° to +16°. The proposed model is efficient in comparison with the conventional gaze controlled headlight system in terms of reduced transmission time, the speed of transmission and provides safety to the drivers during night time.

Keywords: Support controller area network · Headlight control system · CANalyser · Data transmission · MCP 2515 CAN controller

1 Introduction

The rate of accidents are increasingly higher at night time due to driving without seat belts, low beam/high beam headlights, distracted and drunk driving, speeding, reckless driving, poor weather and climatic conditions, design defects, tailgating, wrong-way driving, teenage drivers, drugs, potholes, tire blowout, animal crossing and construction sites [7]. A review by law offices of Michael pines statistics states that 40 percent of all fatal car accidents occur at night [8]. Among all the factors mentioned the condition of driver and car has a significant role in preventing accidents. The driver's perception is limited by the combination of headlight and road lights, darkness and curves in the roads. Jessica and Jermakian [5] stated that the average annual crashes relevant to adaptive headlight systems are 29,000 for Non-fatal crashes and 2,484 for fatal crashes. Hence, automotive and intelligent headlight systems are sought after to minimize accidents during night time. The concept of intelligent and automotive headlight systems is available in sophisticated cars like Mercedes-Benz Chevrolet, Audi, BMW, Nissan, etc.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 373–383, 2020.
https://doi.org/10.1007/978-3-030-37051-0_43

The Intelligent and Automotive Headlight Systems [IAHS] are aimed at improving safety in dim light and poor weather conditions [10]. The core of the IAHS is the Controller Area Network [CAN]. CAN be developed by Robert Bosch Cooperation limited in 1983 and its official release was in 1986 by the Society of Automotive Engineers [3]. CAN is a simple, reliable in-vehicle communication bus providing a high-performance solution for automotive and automation industries. CAN have a maximum signalling rate of one Megabit per second (Mbps) between nodes in the network. CAN is an event-oriented multi-master serial bus comprising of two standards ISO-11898-2 and ISO-11898-3 for high and low-speed applications among controllers, sensors and actuators [13]. This setup improves CAN FD which extends the length of the data section up to 64 bytes per frame. CAN protocol employs CAN transceivers to exchange data from one node to another. The applications of CAN in automation are Auto Start/Stop, Electric Park Brakes, Parking Assist, Collision Avoidance, Auto Brake Wiping, etc. [2]. Adaptive Headlight System is one of the essential applications implemented for collision avoidance during night time in roads.

CAN incorporate Adaptive Headlight system that provides an efficient control around the corner of roads with robustness and reliability. In the proposed model exact position of the Steering control unit is transferred to the Headlight control unit through the CAN bus. Three positions are considered in steering control unit viz balanced, left rotation and right rotation. Arduino UNO uses as the controller and MCP2515 for the CAN communication. Master Arduino will receive the data from steering control unit and transfer to the Receiver Arduino through CAN bus. The data from Slave Arduino controller is used to control the headlights. The angle of rotation of light varies from $-16°$ to $+16°$ by the steering position.

The organization of the paper is as follows: in Sect. 2 the related work in comparison with the conventional techniques is discussed. Part 3 gives a brief overview of the proposed architectural setup. The proposed steering based headlight control system is explained with necessary hardware in Sect. 3. In Sect. 4 experimental result and discussion are elaborated. In Sect. 5 the conclusions are stated.

2 Related Works

The progress in vehicular systems, technologies, and applications are always a significant scope of research as it accounts for safety and sophistication of people. The Current state-of-art vehicular technology employs several hundreds of high-end RISC Processors communicating over several networks to manage entertainment and navigation functions, central locking mechanisms, lighting, and other vehicle systems [14]. Controller Area Network is the defacto standard in a large variety of networked embedded control systems [6]. Researchers have contributed to the development of Controller Area Network as the most prominent technology in the automotive sector for the past three decades. Various projects and models on advancements in vehicular technology and communication have been devised. A detailed literature review is presented as follows.

Sunil Kumar Reddy Guram has implemented CAN Bus in an autonomous All-Terrain Vehicle (ATV) in [12]. The prototype employs CAN Protocol with the LIDAR,

GPS and IMU connected to the ECU. The author has designed the firmware with a compact design enabling the future insights of development. Control algorithms for adaptive front light systems were designed by Antony and Manoj [1]. The model features a leveling functionality which provides an intended positioning to the low beams according to the steering wheel angle, the vehicle speed and the direction of cornering. Giradhkar and Khanapurkar [9] have implemented the Adaptive Front Light System of Vehicle Using FPGA Based LIN Controller. The authors have simulated the model and controlled lateral roll angle of the vehicle body, and longitudinal irradiation distance of the vehicle's front light on curve roads by safe stopping distance of vehicles.

Cameras can also be incorporated with the adaptive headlight system which enhances the driving safety during night time. Captured images are processed, and details of road curvature are obtained. Then the processed images are given to the motor drive. PWM input from the LPC 2148 based on 16bit/32bit ARM7TDMI-S are provided to the motors for left-right rotation [11]. Adaptive headlights can be controlled using the necessary vehicle and road states obtained from the proposed algorithm. Stepper motor is interfaced with ATMEL 89S52 microcontrollers to control the headlight [4]. From the detailed analysis of literature, an efficient model is developed in this paper using CAN Protocol for the headlight control system.

3 Proposed Architecture

The proposed Steering Based Headlight Control System using CAN bus is shown in Fig. 1. It is categorized into three modules.

- Sensor Module – Steering Control Unit
- Controller Module – Arduino Controller, MCP2515 CAN controller
- Headlight Control Unit – Servomotor, Relay, LCD

The sensor modules consist of a steering control unit which is used to determine the position of the steering angle. The steering wheel angle is acquired using a potentiometer—measurement of Angles from the balanced position to the left and right direction. The message from the steering control unit is given to the ARDUINO control unit, and the corresponding steering angle is determined. If the steering is in a balanced position, no action will take place to the headlight. When the steering rotates to the right, the headlight also rotates in the same direction. Likewise movement of steering to the left side causes the headlight to turn in the left direction. There are two Arduino controllers: one for the control of the steering system, and another for the control of the headlight module. Communication between each module is through wireless technology through the CAN protocol. The algorithm used to implement steering based headlight control using CAN bus is given below.

ALGORITHM:

(1) Start of the function.
(2) Steering Control Unit detects the position.

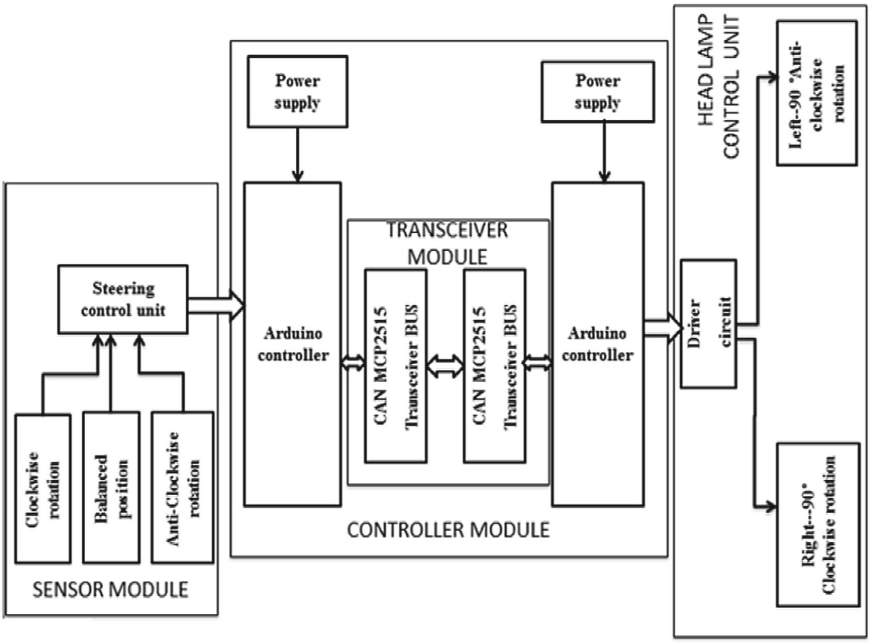


Fig. 1. Architecture of steering based headlight control system

(3) Master Arduino receives the data from sensor module.
(4) If the position is between 125 and 127 – Balanced Position
(5) If the position is between 127 and 255 – Right Rotation
(6) If the position is between 126 and 0 – Left Rotation
(7) Transmitter CAN receives the corresponding position
(8) If the Baud rate is equal to 100kbps data transmits to the Receiver CAN
(9) If the condition failed CAN module is not initialized
(10) Slave Arduino Receives the data and servomotor is controlled for headlight rotation.

3.1 Sensor Module

A 10 k potentiometer is used to measure the angle of rotation of the steering control unit. The range of steering angle varies from 0 to 255. Three Conditions are considered to identify the position of steering.

- The steering angle is between 125 and 127 – Balanced Position
- The steering angle is between 127 and 255 – Right Rotation
- The steering angle is between 126 and 0 – Left Rotation.

3.2 Controller Module

a. Arduino UNO

An Arduino UNO microcontroller is used to control the entire steering based headlight control system. The data from the Sensor module is given to the Master Arduino controller and transmits to the Slave Arduino controller through CAN bus. Slave Arduino controller is connected with LCD, Relay, and Servomotor.

b. CAN Controller

An MCP2515 CAN is used for the wireless transmission between Transmitter and Receiver unit. Standard and extended data and remote frames can be transmitted and received through the MCP2515 controller. CAN bus is used for the wireless communication between transmitter and receiver. It will enhance the speed of data transmission and hence reduces time delay in the system.

3.3 Headlight Control Module

Headlight control Unit consists of servomotor, Relay, and LCD. LCD display is used to display the steering position and CAN ID.

a. Servomotor

Automatic movement of the headlights are enabled by using SG-90 MINI; a position controlled servomotor. The rotation of servomotor ranges from 0 to 180 degree. Headlights are mounted above the servomotor. The headlights are controlled from −16° to +16° according to the steering position.

b. Relay

One channel relay board (JQC-3FC T73) is used to indicate the left and right rotation of the headlight mounted above the servomotor. When the steering position is between 125 to 127 Relay is in the off state. If the steering position is greater than 127 one of the LED blinks and if the position is less than 126 other LED blinks.

4 Results and Discussion

The proposed Steering based headlight control system has been simulated using LabVIEW. LabVIEW (Laboratory Virtual Instrumentation Engineering Workbench) is a platform and development environment for a visual programming language from National Instruments (Luo et al. 2013). A knob is used to determine the position of steering. The Arduino controllers and CAN module transmit data from the transmitter to the receiver to control the headlight. When the steering control is shifted to the right side the command is first transferred to the CAN controller unit. The output of the CAN controller unit is then given to the second Arduino controller is used to control the position of the headlight. According to the command from the controller, the headlight will also change its direction to the right side as shown in Fig. 2. When the steering

control is shifted to the left side Arduino controllers will control the entire action to perform the left side rotation of headlight as shown in Fig. 3.

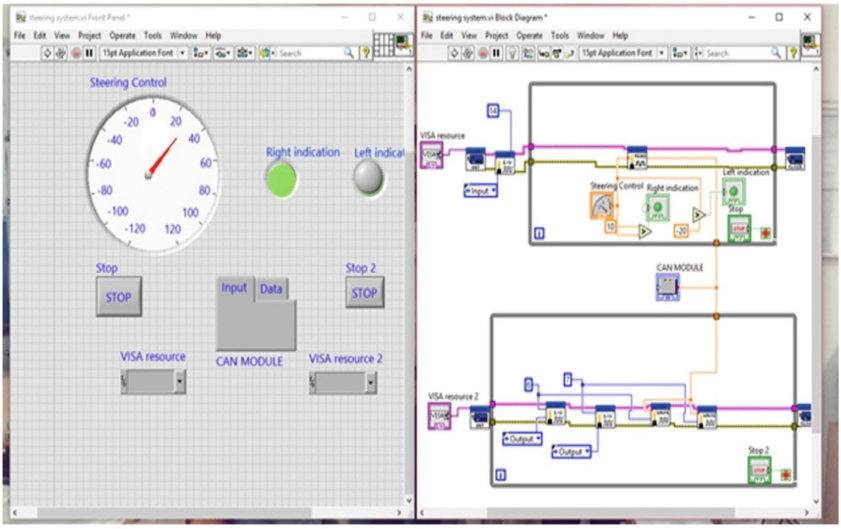


Fig. 2. Right-side rotation of headlight

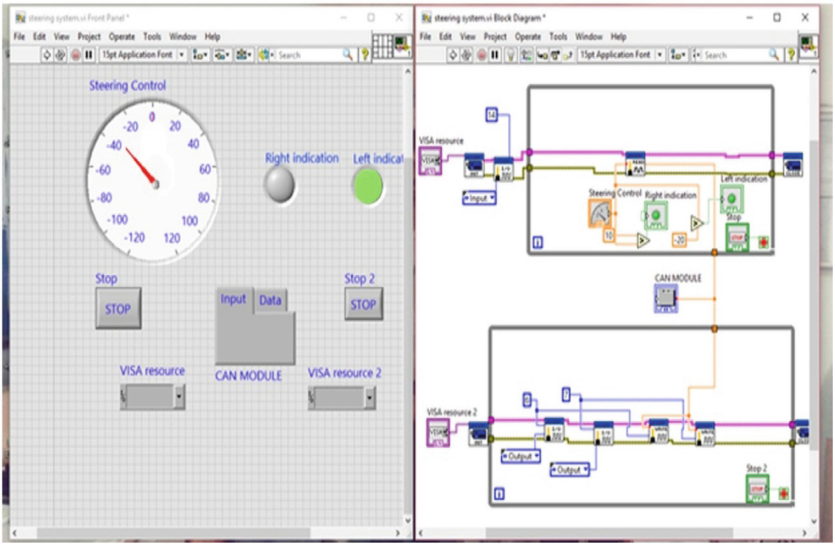


Fig. 3. Left side rotation of headlight

Further hardware setup of the proposed system is implemented. The signal transmitting through the system can be viewed using DSO. Table 1 shows the speed of data transmission through transmitter and receiver and the frequency obtained through Relay. The position of steering is varied from 0 to 255 to obtain various parameter values.

Table 1. Parameters obtained during data transmission

Steering angle (in degree)	Speed of data transmission in transmitter (in mV)	Speed of data transmission in receiver (in mV)	Frequency of signal through relay
0	36	15	5
29	64	20.8	5
61	80	35	5
93	120	41.33	0.9
126	144	55	3.33
159	160	64.6	0.5
191	216	81	1
223	224	93	1.1
255	231	119	1.25

Figure 4 shows the graphical representation of the speed of transmission through transmitter and receiver. Figure 5 shows the Frequency of Relay in Different Steering Position.

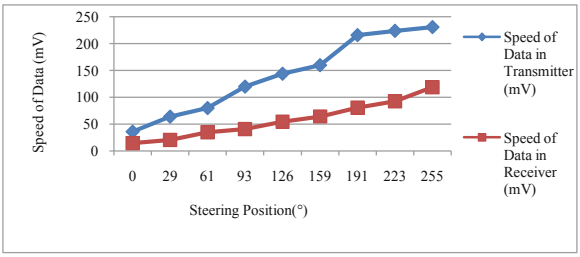


Fig. 4. Parameters during data transmission

Figure 4 shows the graphical representation of the speed of transmission through transmitter and receiver. Figure 5 depicts the frequency measured using the period of the signal while data is transmitting. Variation in steering position from left to right can be indicated using a relay.

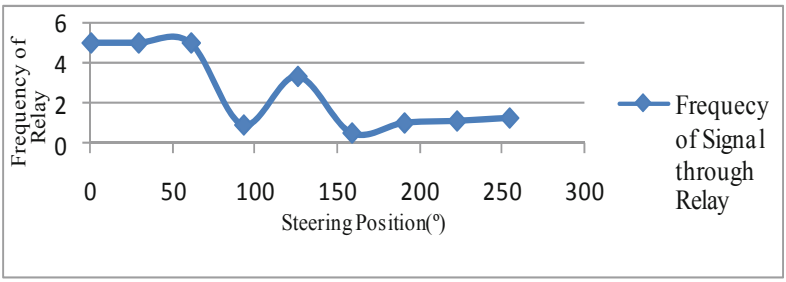


Fig. 5. Frequency of relay in different steering position

Figure 6 shows the controllers used for the transmission of data. Controllers used for the entire setup are Arduino UNO controller and MCP 2515 CAN controller. Figure 7 shows the hardware setup of the steering-based headlight control system. A DSO is interfaced with the system to represent the signal transmission.

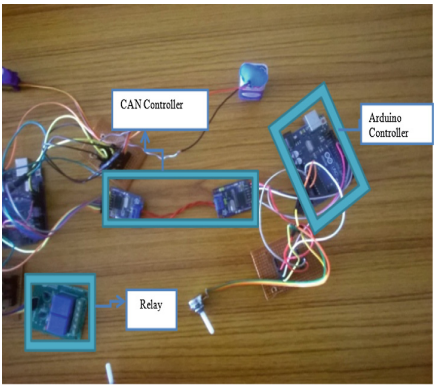


Fig. 6. Controllers used for data transmission

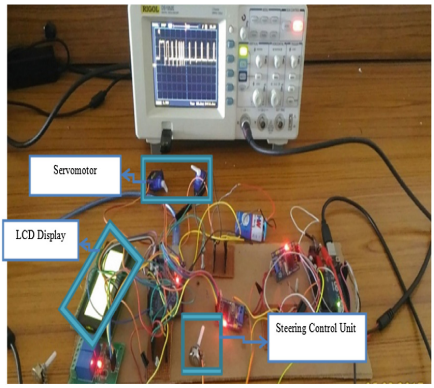


Fig. 7. Hardware setup of steering based headlight control using CAN bus

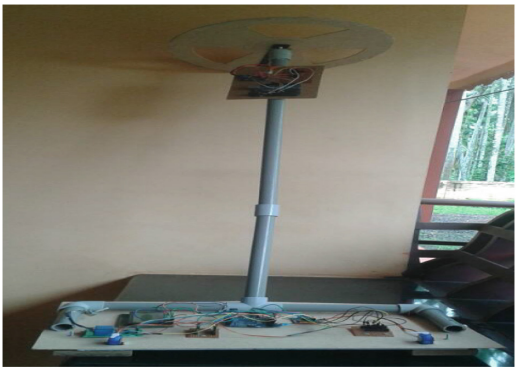


Fig. 8. Hardware with steering setup

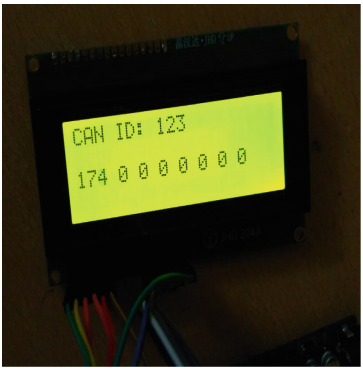


Fig. 9. Steering position and CAN ID in LCD display

The DSO is used to capture, process, display and store data of the signals according to the operations. An Arduino controller, MCP2515 CAN controller, Potentiometer, Relay and LCD are used to implement the hardware setup. LCD is used to indicate the position of the steering and CAN ID used for the MCP2515 controller. The entire hardware is mounded with a steering setup as shown in Fig. 8. Steering is attached with the potentiometer to control the servomotors.

Figure 9 shows the steering position and CAN ID in LCD. Table 2 shows the various input resistance reading of the potentiometer corresponding to the steering position. The input resistance is obtained in kilo-ohm, and the range increases at the initial state and decreases at the final states.

Table 2. Input resistance of different steering position

Steering position (in degree)	Input resistance (in KΩ)
0	0.0019
40	1.56
80	2.56
119	2.99
126	3.02
145	3.64
190	2.7
239	1.65
255	1.11

Table 3. Average voltage during different time period

Time period (in ns)	Vavg in transmitter (in mV)	Vavg in receiver (in mV)	Vavg in relay (in V)
5	80.9	352.0	12.0
10	70.0	373.0	14.3
20	68.8	416.0	11.8
50	68.4	310.0	11.3
100	69.0	195.0	12.1

Table 3 shows the average voltage obtained during the transmission of data from transmitter to receiver and also in the relay. Average voltage is observed from 5 to 100 ns. The Fig. 10 shows the graphical representation of average voltage of the waveforms during data transmission. Average Voltage of the waveform is obtained for different time period Table 3 shows the average voltage obtained during the transmission of data from the transmitter to the receiver and also in the relay. The average voltage is observed from 5 ns to 100 ns. The Fig. 10 shows the graphical representation of the average voltage of the waveforms during data transmission. Average Voltage of the waveform is obtained for a different period.

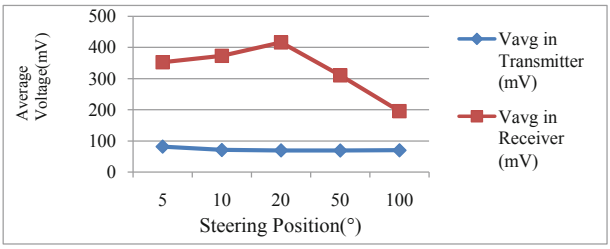


Fig. 10. Average voltage waveforms

5 Conclusion

The proposed system is an adaptive headlight which rotates to left and right according to the change in the steering control system. The maximum angle of rotation provided in this project is +16°, and the minimum degree of rotation is −16°. This design also improves the safety and comfort of the automobile driving and increases its reliability. The system is also in line with current automotive electronic safety, energy saving, environmental protection, intelligence, and information technology trends. In the future, the intelligence of the system can be increased by adding the function of headlights low beam and high beam automatic switching when two automobiles meet.

References

1. Antony, B., Manoj, M.: Control algorithm for adaptive front light systems. Int. J. Comput. Trends Technol. **9**(7), 339–343 (2014)
2. CAN bus [Online] https://en.wikipedia.org/wiki/CAN_bus. Accessed 28 April 2017
3. CAN in Automation Group [online] https://www.can-cia.org/can-knowledge/can/can-history/. Accessed 28 Feb 2017
4. Hacibekir, T., Karaman, S., Kurnal, E., Oztruk, E.S., Demirci, M., Aksun Guvenc, B.: Adaptive headlight system design using hardware-in-the-loop simulation. In: Proceedings of IEEE International Conference on Control Applications Munich, Germany, pp. 915–920 (2006)
5. Jermakian, J.S.: Crash avoidance potential of four passenger vehicle technologies. Accid. Anal. Prev. **43**(3), 732–740 (2011)
6. Johansson, K.H., Törngren, M., Nielsen, L.: Vehicle applications of controller area network. In: Dimitros Hristu-Varsakelis.et.al (eds.) Handbook of Networked and Embedded Control Systems, pp. 741–765. Birkhäuser Boston, Springer (2005)
7. Laiza King [Online] http://www.huffingtonpost.com/laiza-king-/top-15-causes-of-caraccidents_b_11722196.html. Accessed 31 Aug 2016
8. Micheal Pines [Online] https://seriousaccidents.com/legal-advice/top-causes-of-car-accidents/nighttime-driving/. Accessed 31 Mar 2017
9. Giradhkar, M., Khanapurkar, M.: Design and implementation of adaptive front light system of vehicle using FPGA based LIN controller. In: Proceedings of Emerging Trends in Engineering and Technology, Mauritius, pp. 258–261 (2014)

10. Tamburo, R., Nurvitadhi, E., Chung, A., Chen, M., Rowe, A., Kanade, T., Narasimhan, S. G.: Programmable automotive headlights. In: ECCV 2014: Proceedings of the European conference on Computer Vision, Zurich, Switzerland, pp. 750–765 (2014)
11. Shreyas, S., Raghuraman, K., Padhmavathy, A.P., Arun Prasad, S., Devaradjane, G.: Adaptive Headlight System for accident prevention. In: Proceedings of IEEE International Conference on Recent Trends in Information Technology, Chennai, Tamil Nadu, pp. 1–6 (2014)
12. Guram, S.K.R.: Implementation of controller area network (CAN) bus in an autonomous [sic] all-terrain vehicle. Published Ph.D. thesis, University of North Carolina, Charlotte (2011)
13. Singh, V.K., Archana, K.: Implementation of CAN protocol in automobiles using advance embedded system. Int. J. Eng. Trends Technol. **4**(10), 4422–4427 (2013)
14. Ng, W.L., Ng, C.K., Ali, B.M., Noordin, N.K., Rokhani, F.Z.: Review of researches in controller area networks evolution and applications. In: Proceedings of the Asia-Pacific Advanced Network, Hanoi, Vietnam, vol. 30, pp. 1–8 (2010)

RETRACTED CHAPTER: Enhanced Energy Efficient Bio-trusted Anonymous Authentication Routing Technique of Wireless Body Area Network

R. Sudha(✉)

Department of Computer Science, PSG College of Arts and Science, Coimbatore, India
sudha279@yahoo.com, sudha_r@psgcas.ac.in

Abstract. Wireless Sensor Networks (WSN) are rapidly developing technological platform with tremendous applications in several domains. Body Sensor Network (BSN) plays a major role in the fields of social welfare, medical treatment and sports. The major problems identified in health care based sensor networks are energy consumption and lifetime. These two factors directly depend on clustering and routing and hence this research resolves in enhanced uniform clustering of the sensor nodes. Initially, routing with better load balancing is determined by tree clustering technique. The K-Nearest Neighbor (K-NN) algorithm is used to enhance the uniform clustering of sensor nodes. Secondly, the biometric iris fusion based trusted anonymous secure routing protocol is proposed to preserve two factors namely anonymity and unlinkability of the wireless body area network. Finally, secure routing technique based on retina with DNA coding is made with the help of onion routing to avoid computational overheads.

Keywords: Sensor network · LEACH · Anonymous · Authentication · Energy efficiency · Clustering · Biometric security

1 Introduction

Wireless Body Sensor Network (WBSN) system plays a major role in health care services which is similar to that of normal wireless sensor network. It is a wireless network of wearable computing devices. Wireless Body Area Networks (WBANs) is promising paradigm to advance health care delivery, diagnostic monitoring, disease-tracking and related medical procedures. It comprises of various lightweight materials and smaller than expected sensors which could be put on the body as little part, coordinated into fabric or embedded under the skin or installed profoundly into the body tissues. The fundamental design is to empower specialists and restorative staffs to securely screen the status of patients. The framework is likewise used to permit consistent checking of patients signs and to screen their physiological signs.

The original version of this chapter was retracted. The retraction note to this chapter is found at https://doi.org/10.1007/978-3-030-37051-0_109

© Springer Nature Switzerland AG 2020, corrected publication 2024
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 384–391, 2020.
https://doi.org/10.1007/978-3-030-37051-0_44

RETRACTED CHAPTER

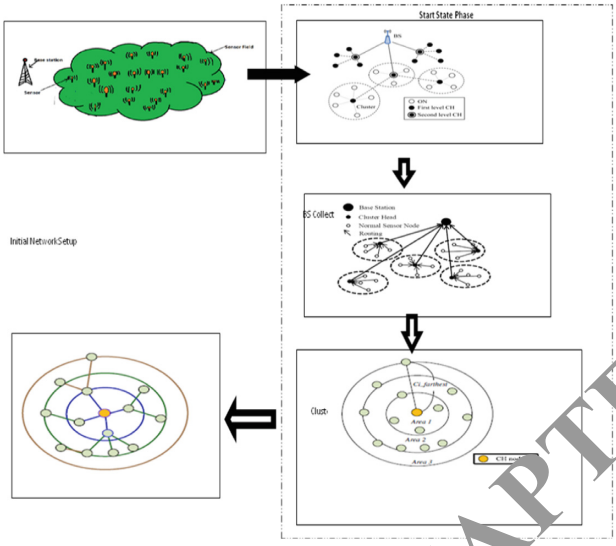


Fig. 1. Enhance saving energy cluster[illegible] architecture

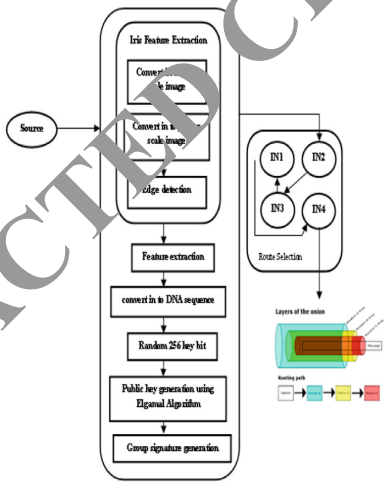


Fig. 2. BFTASR architecture

Energy saving is the main concern in enhancing the lifetime of sensor nodes. In the wireless body sensor network, battery is the main power supply of a sensor node which consumes most of the energy in sending and receiving packets. However, the battery energy must be stable in a sensor node and draining of energy could make the sensing area uncovered. In traditional research methodologies, the system is continuously monitoring the patients by bedside sensor nodes attached to the monitors. When upgrading this system to wireless sensors, then there is no relation between sensors and the bedside equipment [1].

RETRACTED CHAPTER

2 Literature Review

Recently several authors reported on body sensors in body area network. Milenković et al., discussed about issues presented in personal health care monitoring [2]. Amid the most recent couple of years there has been a noteworthy increment in the quantity of different wearable wellbeing checking gadgets going from basic heartbeat screens, action screens and versatile Holter screens to refined and costly implantable sensors. Customarily therapeutic observing frameworks like Holter screens have been utilized just to gather information. Various sensors, for example, physiological sensors can screen fundamental signs, ecological sensors (temperature, moistness, and light), and an area sensor can be incorporated into a Wearable Wireless Body/Personal Area Network. They have a Wearable Wireless Body/Personal Area Network model to check the issues in planning a wearable remote sensor organize. The WWBAN comprises of smaller than usual sensors that can take into account long haul wellbeing observing with quick input to the client about the present wellbeing status and ongoing updates of the patient medicinal records. Ragesh et al., built up a PC managed framework can be utilized for early identification of ailments [14]. For example, shrewd heart screens can caution the clients about ailments or give data to a specific administration. It portrays a WWBAN engineering just as model. WWBAN structured utilizing Telos bits and application explicit flag molding modules. The model comprises of a few movement sensors that can screen the client's general action and ECG sensor for checking heart action. WWBAN has equipment and programming stages for therapeutic observing, examines open issues, and presents answers for time-synchronization. It gives productivity on-sensor flag handling, and thus called vitality effective correspondence convention. Liu et al., have exhibited a framework on the scope of normal for WBAN with utilization of sensors, applications utilized, productivity of intensity, conventions utilized for correspondence, security necessities, realistic undertakings in WBANs and face met by remote body territory networks [10]. They set forth exchange on prerequisite of vitality, security and issues in various layers of WBAN. In light of correspondence conventions a few review are made by Cao and Chen et al. [3, 4]. Ehyaie et al., dissected productive vitality use in sensor nodes to give a long life time to the system [5]. They explored the impact of adding a transfer system to the system of body sensors to decrease vitality utilization of sensor nodes when transmitting information to the sink. Braem et al., introduced a vitality effective opened MAC system within the sight of a Wireless Autonomous Spanning tree Protocol (WASP) [6]. This convention has been utilized for on-body bundle steering. Ali et al., built up a security system utilizing Keyed Hashing Message Authentication Code (HMAC-MD5) to ensure the fighters and patient's close to home data, for example, beat oximeter information, pulse and heart yield [7]. Kim et al., announced an effective directing convention dependent on position data in portable remote body zone sensor systems [8]. Miao et al., exhibited a novel key dispersion arrangement which permits two sensors in a single body sensor system to concur on an alterable cryptographic key [9]. They have connected a fluffy vault to verify the arbitrary cryptographic key produced from Electrocardiographic (ECG) signals. Bao et al., proposed a novel answer for handle the issue of element validation in body zone sensor organize (BASN) for m-Health [11]. It was completed on 12 solid people, each with 2 channels of photoplethysmogram (PPG) caught all the while at various pieces of the body. Ramli et al., exhibited an outline of body region organize and their related

RETRACTED CHAPTER

issues accentuation in security issue [12]. Kumar et al., exhibited a rundown of body zone arrange and their associated issues worry in security drawback [13]. WBAN could be a little scale organize that incorporates short interchanges differ together with the correspondence in/on a person's body.

3 Proposed Work

The proposed methodology is more effective and provides better solution. This method uses a K-Nearest Neighbor (K-NN) uniform clustering to make a cluster-tree routing to reduce data transmission distances and improve the lifetime of total network. The authentication in routing is made by an iris and retina fused with DNA coding. The approaches are discussed in this research are explained briefly in the following sections.

A. K-Nearest Neighbor (K-NN) Based Clustering of Health Care Sensor Nodes

The health monitoring systems need to allow continuous monitoring for long period. During critical conditions, the failure of sensor nodes occurs due to the following reasons such as quick discharging of battery nodes and routing. In order to make effective routing, this work aims to develop a dynamic energy efficient protocol architecture with K-Nearest Neighbor (K-NN) based uniform clustering which finds the nodes on the basis of the uniform cluster location [15]. The K-Nearest Neighbors algorithm (K-NN) is a non-parametric method used for regression. It is a type of instance-based learning where the function is only approximated locally and all computation is delayed until the classification. The K-NN algorithm is one among the simplest algorithm of all machine learning algorithms. Enhanced Saving Energy Clustering Algorithm(ESECA) achieves reduction of energy consumption.

The data transmission distance between the sensor nodes can be reduced by employing an adaptive multi hop approach. A cluster-tree routing architecture is created for sensor nodes by using centralized and cluster based techniques. Finally, the overall power in wireless body sensor network is reduced and its lifetime is improved for applying in large scale detecting and sensing environments. The transmission distance between two nodes is also reduced considerably.

B. Authentication and Routing Using Iris Fused with DNA Coding

In recent body sensors networks, sensors are used to communicate to other control nodes of medical units through the control nodes like smart phones or medical sensors that can be interfaced with auxiliary types. This work aims to preserve two factors unidentifiably and unlinkabilty as essential characteristic of the wireless body area network. Traditional protocols are susceptible to the attacks of counterfeit routing packets, yet the node individualities are confined by pseudonyms. This research developed a new Biometric Fusion Based Trusted Anonymous Secured Routing Protocol (BFTASR) which assures prevention against such attacks [16].

Initially, the route request packets were authenticated by an iris fused with DNA coding to generate a dynamic complex group signature. Iris particular has exceptionally high acknowledgment precision in correlation with numerous other biometric highlights. In which edge location is performed both in vertical and level headings. The iris pictures

RETRACTED CHAPTER

in database have iris span 80 to 150 pixel and student range from 30 to 75 pixel. The yield of this strategy brings about putting away the range and x, y parameters of internal and external circles. In the event that the space is not exactly the limit it speaks to non impediment of eyelids.

The iris recognition process comprises of five noteworthy undertakings. The main assignment is the picture securing of an individual's eye at check time. The second assignment is to portion the iris out of the picture containing the eye and part of the face, which confines the iris design. The third assignment is the standardization in which the iris example will be separated and scaled to a predefined estimate. The fourth undertaking is the layout age here the iris data's are sifted, extricated and spoke to in a designed code. The last assignment is the coordinating stage, where two iris codes will be brought about and a likeness code is processed. After completing these processes it is necessary to secure beside possible active attacks exclusive of preventing the node identities. Finally, it also prevented revealing real destination to intermediate nodes by adapting key-encrypted pairing onion. From the observed experimental results, the efficiency of the projected BFTASR protocol is improved with enhanced performance.

C. Secure Routing Technique Based on Retina with DNA Coding

Secure routing is necessary because the medical reports give a detailed view for diagnosing. To make it effective there is a need to develop the secure routing technique that converts the extracted features in the form of binary data of retina to a DNA based representation string. The proposed Retina Biometric Fusion Based Trusted Anonymous Secured Routing Protocol (RBFTASR) provides highest protection of them all. There are numerous advances in this field to translate binary data to a DNA string and these are identified as DNA coding technology. Here, a new DNA coding technology is proposed to convert binary data to DNA strings.

To manage secure transmission by public key generation this method adapts Elgamal algorithm. The Elgamal algorithm is selected because the security of the elgamal depends on the difficulty of computing discrete logs into a large prime modulus. Another merit is that the same plaintext gives a different cipher text each time it is encrypted. For the whole process, it uses The Onion Routing (TOR), which helps in encryption for reliable and protected data transmission.

Onion routing is a layered communication technique over a computer network. In an onion network, messages are captured in layers of encryption. The encrypted data is transmitted through a series of network nodes called onion routers. Here each node "peels" away a single layer, uncovering the data's next destination. When the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediate nodes know only the location of the immediate preceding nodes and following nodes.

RETRACTED CHAPTER

4 Experimental Results

The simulation is done using Network Simulator (NS2) to simulate the proposed methodology. This proposed work undergoes two different kinds of simulation results. In the first simulation, the performance is analyzed based on the behavior beneath the packet

dropping, throughput and end to end delays in the presence of attacks with different levels. The second simulation is to evaluate the routing performances of proposed protocols after malicious attacks. Here assumed that 20% of the nodes are malicious nodes.

Table 1 shows the performance comparison of Packet Delivery Ratio (PDR), Throughput and End-to-End delay with increase in number of sensor nodes after Malicious attacks. When compared to the traditional protocols, the packet delivery ratio of RBFTASR is increased 17% tentatively under high density network (1000 nodes). Throughput also follows similar trend as PDR but end-to-end delay gets minimized.

Table 1. Comparative analysis of protocols before malicious attack.

Sensor nodes	Protocols	Packet delivery ratio (%)	Throughput (%)	End-to-end delay (ms)
1000	RBFTASR	87.3	82	31
	BFTASR	85	79.5	33
	ESECA	82.3	68.2	35
	LEACH	70	59.4	42

Table 2 shows the RBFTASR protocol using retina authentication requires less processing delays than the other protocol. If the protocol is under a heavy attack, it will initiate new route discovery for the broken routes, which cause more delays in usual.

Table 2. Comparative analysis of protocols after malicious attack.

Sensor nodes	Protocols	Packet delivery ratio (%)	Throughput (%)	End-to-end delay (ms)
1000	RBFTASR	96	78	23
	BFTASR	91	74.5	25
	ESECA	89	69.5	27
	LEACH	58.5	55.6	42

Compared to the attacked BFTASR, ESECA and LEACH the proposed RBFTASR reduces the need of re-routing, resulting in 23 ms less of delay in average. Experimental results show that the extremely highest Packet Delivery Ratio of 96% and Throughput of 78% in the presence of attacks with different levels are achieved by authorized node of WBAN.

5 Conclusion

In this research, a security framework is designed to secure the body sensor nodes communication with minimum overheads by using iris and retina information. To make an effective routing a K-Nearest Neighbor (KNN) based uniform clustering made a

RETRACTED CHAPTER

cluster-tree routing architecture. To authenticate the information, this exploration work proposed an iris combined with DNA coding approach that can display unmistakable biometric data and validate message marks among body sensors with high precision. BFTASR directing convention is fit for performing trusted steering practices as per the trust relationship among them. In BFTASR directing convention, every node can help commonly to accomplish a target supposition about another node's performances. Based on threshold limit, the nodes can adaptable select whether and how to perform cryptographic activities. Subsequently, the computational overheads are decreased in routing.

The results prove that onion routing has high throughput and packet delivery ratio, provided by authorized node of body sensor network and significantly decreased the average end to end delay and more secured.

RETRACTED CHAPTER

References

1. Shnayder, V., Chen, B.R., Lorincz, K., Fulford-Jones, T.R., Welsh, M.: Sensor networks for medical care. Technical Report TR-08-05. Division of Engineering & Applied Sciences, Harvard University, Cambridge (2005)
2. Milenković, A., Otto, C., Jovanov, E.: Wireless sensor networks for personal health monitoring: issues and an implementation. Comput. Commun. **29**(13), 2521–2533 (2006)
3. Cao, H., Leung, V., Chow, C., Chan, H.: Enabling technologies for wireless body area networks: a survey and outlook. IEEE Commun. Mag. **47**(12), 84–93 (2009)
4. Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., Leung, V.C.: Body area networks: a survey. Mob. Netw. Appl. **16**(2), 171–193 (2011)
5. Ehyaie, A., Hashemi, M., Khadivi, P.: Using relay network to increase life time in wireless body area sensor networks. In: IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops, pp. 1–6. IEEE (2009, June)
6. Braem, B., Latre, B., Moerman, I., Blondia, C., Demeester, P.: The wireless autonomous spanning tree protocol for multihop wireless body area networks. In: 2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, pp. 1–8. IEEE (2006, July)
7. Ali, A., Irum, S., Khanzar, F., Khan, F.A.: A cluster-based key agreement scheme using keyed hashing for Body Area Networks. Multimed. Tools Appl. **66**(2), 201–214 (2013)
8. Kim, K., Lee, I. S., Yoon, M., Kim, J., Lee, H., Han, K.: An efficient routing protocol based on position information in mobile wireless body area sensor networks. In: 2009 First International Conference on Networks & Communications, pp. 396–399. IEEE (2009, December)
9. Miao, F., Jiang, L., Li, Y., Zhang, Y.T.: Biometrics based novel key distribution solution for body sensor networks. In: 2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 2458–2461. IEEE (2009, September)
10. Liu, J., Kwak, K.S.: Hybrid security mechanisms for wireless body area networks. In: 2010 Second International Conference on Ubiquitous and Future Networks (ICUFN), pp. 98–103. IEEE (2010, June)
11. Bao, S.D., Zhang, Y.T., Shen, L.F.: Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. In: 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference (2005)
12. Ramli, S.N., Ahmad, R.: Surveying the wireless body area network in the realm of wireless communication. In: 2011 7th International Conference on Information Assurance and Security (IAS), pp. 58–61. IEEE (2011, December)

13. Kumar, R., Mukesh, R.: State of the art: Security in wireless body area networks. Int. J. Comput. Sci. Eng. Technol. (IJCSET) **4**(5), 622–630 (2013)
14. Ragesh, G.K., Dr. Baskaran, K.: An overview of applications, standards and challenge in futuristic wireless body area networks. IJCSI Int. J. Comput. Sci. Issues **9**(1), 180–186 (2012)
15. Sudha, R., Dr. Devapriya, M.: An energy saving approach in wireless body sensor networks for health care monitoring. Int. J. Appl. Eng. Res. (IJAER) **11**(7), 4797–4802 (2016)
16. Sudha, R., Dr. Devapriya, M.: Enhanced bio-trusted anonymous authentication routing technique of wireless body area network. In: Biomedical Research 2016 in Special Issue, pp. S276–S282 (2016)

RETRACTED CHAPTER

An Efficient Replica Management Based Disaster Recover Using Elephant Herding Optimization Algorithm

K. Sasikumar[1(✉)] and B. Vijayakumar[2]

[1] BITS Pilani, Dubai, United Arab Emirates
sasikumarkll75@gmail.com
[2] Department of Computer Science, BITS Pilani, Dubai Campus, Dubai, United Arab Emirates

Abstract. Now-a-days, more services depend on Information Technology (IT) systems. Some of these services such as health care service and financial service are very crucial to the customers. Even a very small amount of data loss or a short downtime could lead to huge economic crisis or social issues. So most of the important business and public services use disaster recovery technique for protecting important data and reduce the downtime caused by catastrophic system errors. In this paper, we proposed an efficient replica management based disaster recover using Elephant Herding Optimization Algorithm (EHO).in this paper, initially, the data are uploaded into could with the help of EHO algorithm. Then, to avoid data loss, we create the replicas for each data. Finally, the request based data are back up and retrieved.

Keywords: Data replica · Disaster · Loss · Cloud computing · Recovery · Herding optimization algorithm · Uploading

1 Introduction

Cloud computing has become very common in many fields and various businesses as the cloud users have to pay only for the resources that are being actually utilized. Cloud service providers have been providing different services based on the needs of the users. Rapid growth in technology and the large scale usage of internet have to lead to the era where a very huge amount of data is being handled every day [1]. This has caused a huge range of cloud expansion. The very first necessity for cloud storage is that it should be capable of delivering data reliability efficiently and effectively at a reasonable cost. But providing reliable storage at a reasonable cost can be very difficult especially in large scale systems [2]. The cost of cloud storage and the reliability of data stored in the cloud are two primary concerns in current cloud storage systems [11]. So as to lower the utilization of cloud storage while fulfilling all the data reliability requirements, a cost-effective technique that ensures a minimum number of replicas can be used. The system failure can happen anytime in the cloud as it cannot be protected with absolute security. In such cases, the data might get corrupted or totally get lost [3]. To tackle this situation, the data in the cloud are replicated and stored in the cloud in another geographical location. These data can be recovered after the disaster strikes. This is known as the disaster recovery process [12].

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 392–399, 2020.
https://doi.org/10.1007/978-3-030-37051-0_45

The important issue about Disaster Recovery is that it has to provide an effective data backup and recovery process with high data availability while maintaining low costs. The disaster recovery solutions should be capable of recovering IT systems, critical data and components to guarantee normal business operation [4]. These solutions assist systems in surviving unforeseen or extraordinary failures whether they are caused by users or natural catastrophic events [5]. Cloud-based disaster recovery solutions can be very helpful in dealing with the issue of designing a fault tolerant strategy to store, process and share an enormous amount of data. Most of the effective solutions generally replicate the data and infrastructure to a remote cloud. But a replication method has to be established prior to the disaster for the recovery to take place [6]. Various kinds of strategies have been adopted in disaster recovery systems such as continuous synchronization of data or backing up of data at regular interval. Disaster recovery is one of the primary approaches for data security and data reliability in the cloud.

A real-time distributed wide area storage system SeWDress has been designed, analyzed and implemented by Zeng et al. [7] for disaster recovery. Network failures and disk failures are considered in this work. An efficient data organization method RSR AII, called Replication-based Snapshot Redundant Array of Independent Image files, which consolidates erasure-coding and replication strategy has been introduced. The results have been very effective. Wu and Ni [8] have introduced a new disaster recovery technique. The system has been combined with P2M and P2P to generate a hierarchical IT infrastructure spread across various locations. The results have shown that it guarantees to maintain the data with high availability and avoid data losses. Dhanujati and Girsang [9] have provided a detailed study on the evaluation, planning, and implementation and testing of the disaster recovery solution. All the data gathered from these studies have been stored in Data Center-Disaster Recovery Center for future use. Suguna and Suhasini [10] have presented a new approach in which the massive data storage process has been analyzed and the Enriched Genetic Algorithm has been utilized for efficient disaster data recovery. Results have shown that the presented approach has been suitable for many of the data disaster recovery processes.

2 Proposed Replica Management

The main objective of the proposed methodology is to recover the data when a disaster occurs in the cloud. In distributed computing, enormous information storage is one of the extraordinary challenging tasks in term of dependable storage of delicate information and nature of storage administration. Among different cloud safety issues, data disaster recovery is the hugest issue which is required to be considered. Because the disaster occurs in customer side means, the cloud definitely has the backup data but disaster occur in the cloud means data will be lost. It will definitely affect the customers. So, in this paper, we develop a replica management based data disaster recovery process using Elephant Herding Optimization Algorithm (EHO). EHO algorithm is a recently developed optimization algorithm; it captures the herding behavior of elephants. The proposed work comprised into four phases namely (i) file uploading phase, (ii) replica generation phase, (iii) data backup phase and (iv) disaster recovery phase the overall diagram of disaster recovery is given in Fig. 1.

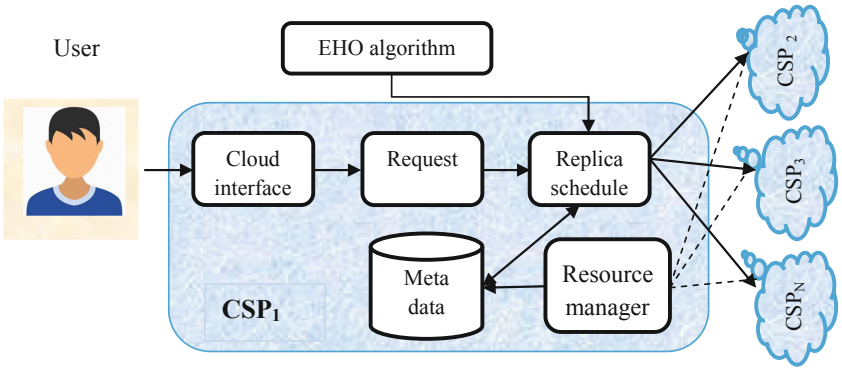


Fig. 1. Proposed methodology of recover data

2.1 Data Uploading Process

Nowadays, many companies or organizations have been uploading their data and building their business into the cloud. For the data uploading process, each file of the incoming file should be stored in a minimum transfer cost node. To upload the files, the client must provide his/her information like that name and password. The valid authentication client can connect to the cloud and upload the data file by providing its details namely data name and email. Let us consider, cloud has N number of node (Ni, i = 1,2,…,N) and M number of data file (Fj,j = 1,2,…,M). To reduce the complexity of the recovery process, in this paper, we schedule the upcoming files and stored on cloud node using Elephant Herding Optimization Algorithm (EHO).

Step 1: Solution initialization
Solution initialization is an important process for scheduling. Here, we schedule uploading the file into the corresponding cloud node. To decrease the complexity of the recovery process, in this paper scheduling process is included. Initially, we randomly assign each file to a different node (clan). Here, the solution is represented as an elephant. For example, we consider ten files and three nodes. The randomly assigned initial elephant is given in Eq. (1).

$$S_i = \{1, 3, 2, 3, 3, 1, 2, 1, 1, 2\} \tag{1}$$

The length of the elephant represents the total number of files. The Eq. (1) represents file 1 stored in clan 1, file 2 is stored in clan 3 and file 3 will stored in clan 2 like that all the files present in the elephant are stored.

Step 2: Fitness calculation
After elephant initialization, the fitness of each elephant is calculated.

Step 3: Solution Updation using EHO algorithm
After fitness calculation, in each clan, the elephant's positions are updated using the following equation,

$$S_i^{new} = S^i + \mathrm{A} * \left(S_{best} - S^i\right) * r \tag{2}$$

After that, the fittest elephant positions are updated in each clan, which is described in the Eq. (3)

$$S_{new}^i = \mathrm{B} * S_{center} \tag{3}$$

$$S_{center} = \sum_{i=1}^{n} S^{i,d} / \eta e \tag{4}$$

Then the worse elephants presented in the clans are separated using the following equation,

$$S_{worst}^i = S_{\min} + (S_{\max} - S_{\min} + 1) * rand() \tag{5}$$

Based on the above equations, the elephants and their positions are updated.

2.2 Replica Generation

To avoid the data file from disaster, we generate the replica files. In this paper, we generate three replicas for each file and store the replica file to a different node. In this any node will be affected by the disaster, we can retrieve the data from another node.

2.3 Data Backup Process

In the Data backup process, the user sends the request to the cloud service provider and retrieves the corresponding data file. The step by step process is explained below;

Step 1: Initially, the client sends the backup request to the cloud service provider CSP. Then, CSP transfer request to request buffer to check the client is already registered or not. The request is canceled when the client has not registered already.
Step 2: Then replica scheduler read every request from the request buffer and find out each request storage location. In this paper, we create three replicas for each file. All three replica locations are found out.
Step 3: Cloud service provider save all the replica location on Metadatabase when the transmission is over. After that, completed requests are deleted from the request buffer.
Step 4: Then, the Cloud Service provider sends an acknowledgment to clients to capture corresponding data, which can be used to restore certain data from CSP.

3 Result and Discussion

The proposed replica management based disaster recovery process is explained in this section. The performance of the proposed approach analyzed in terms of scheduling time, uploading time, memory utilization and cost.

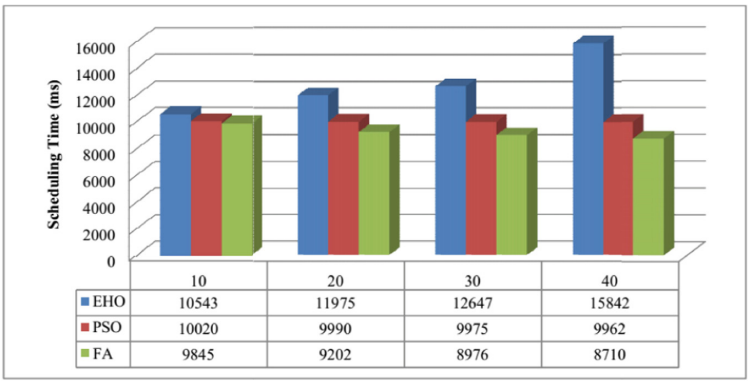


Fig. 2. Proposed based on scheduling time performance analysis

Figure 2 shows the performance of the proposed EHO approach along with existing Particle Swarm Optimization (PSO) and Firefly Algorithm (FA) based on the scheduling time. The iterations of 10, 20, 30 and 40 have been taken for analysis. On iteration 10, the scheduling time of EHO is 10543 ms, the scheduling time of PSO is 10020 ms and the scheduling time of FA is 9845 ms. The order of value is the same for all the remaining iterations. The scheduling time has to be lower for an approach to be efficient. Here the proposed approach has the lowest scheduling time. The performance analysis of the proposed algorithm, PSO and FA based on uploading time has been shown in Fig. 3. On the iteration of 40, the uploading time of the proposed EHO approach is 2416 ms, the uploading time of PSO is 2643 ms and the uploading time of FA is 2864 ms. the order of the values has been the same for all the remaining iterations. An approach can be known as the efficient one when it takes the lowest time to upload data. Here, the proposed EHO approach has the lowest uploading time. In terms of memory utilization, approaches which consume or use lesser memory are known as the effective approach. The performance analysis of the proposed EHO, PSO and FA based on memory utilization has been shown in Fig. 4. Here the memory utilization of the proposed EHO approach for all the iterations is 2.56, 3.08, 3.46 and 4.34. The memory utilization of PSO is 3.52, 3.75, 4.43 and 4.96. The memory utilization of FA is 4.52, 5.43, 6.13 and 8.48. On analyzing all these values, it has been clear that the proposed EHO approach has utilized lesser memory. Figure 5 shows the overall data backup cost for the proposed EHO approach, PSO and FA approach. When the iteration is 10, the backup cost of the proposed EHO approach is 2.45, the data backup cost of PSO is 3.95 and the data backup cost of the FA is 4.26. The proposed EHO approach has the lowest cost when compared with the other two. This order of values is the same for all the remaining iterations. On analyzing all the performances, it can be concluded that the proposed EHO approach has performed superior to PSO and FA approaches in terms of scheduling time, uploading time, memory utilization and data backup cost.

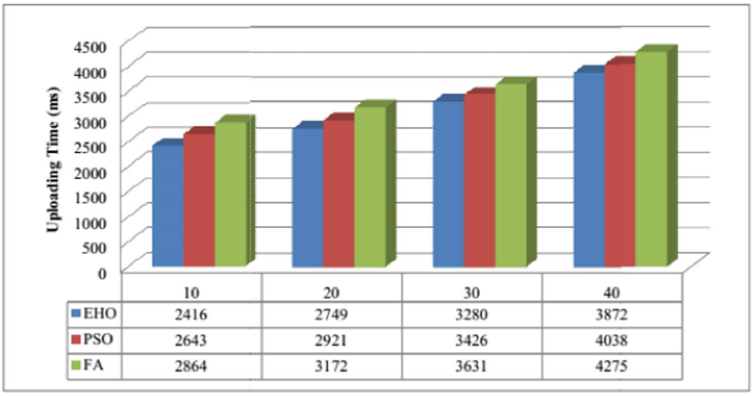


Fig. 3. Proposed algorithm performance depends on uploading time

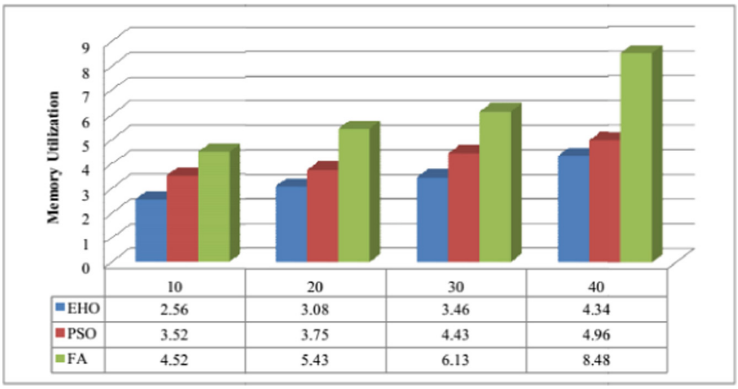


Fig. 4. Proposed algorithm performance depends on memory utilization

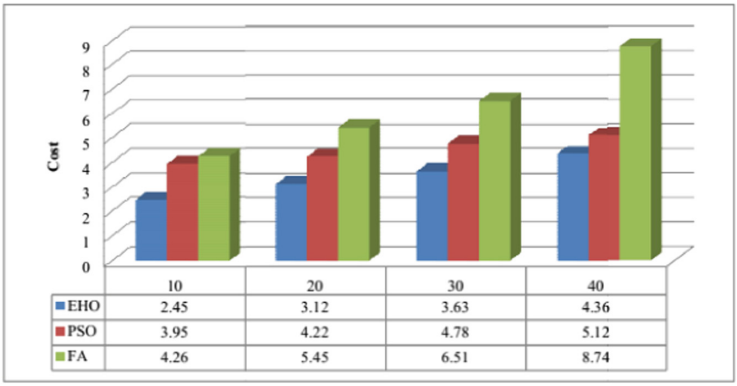


Fig. 5. Cost of overall backup data

4 Conclusion

Replica management based data disaster recovery process is explained in this paper. The proposed approach involves four major phases where each phase has its own functionalities. The data have been uploaded to the remote servers in the first phase. EHO algorithm has been used here to schedule and upload the files on the cloud node. Replica of the files has been generated and stored in various locations in phase two of the presented approach. Three replicas have been generated for each file. This helps in retrieving a file at least from any one of the locations. The third phase involves the backup process of the replicated data. The user's backup request to the cloud service provider triggers this phase. The locations of the replicas have been shared with the user so that the user can access those locations and retrieve data. Data retrieval has been the fourth and final phase of the proposed approach. Here, the users are authorized and their data have been retrieved. The proposed approach has presented a much better performance than the existing PSO and FA methods in terms of scheduling time, uploading time, memory utilization and overall data backup cost. İn future work, we will incluide the security scheme in replication process. This will be increse the system performance. Moreover, we will include hybrid optimization algorithm for fitness calculation.

References

1. Alshammari, M.M., Alwan, A.A., Nordin, A., Abualkishik, A.Z.: Disaster recovery with minimum replica plan for reliability checking in multi-cloud. Procedia Comput. Sci. **130**(C), 247–254 (2018)
2. Li, W., Yang, Y., Yuan, D.: A novel cost-effective dynamic data replication strategy for reliability in cloud data centres. In: Proceedings of International Conference on Dependable, Automatic and Secure Computing, Sydney, NSW, Australia, pp. 496–502 (2011)
3. Mendonca, J., Andrade, E., Endo, P.T., Lima, R.: Disaster recovery solutions for IT systems: a systematic mapping study. J. Syst. Softw. **149**, 511–530 (2019)
4. Andrade, E., Nogueira, B.: Dependability evaluation of a disaster recovery solution for IoT infrastructures. J. Supercomput., 1–22 (2018)
5. Andrade, E., Nogueira, B., Matos, R., Callou, G., Maciel, P.: Availability modeling and analysis of a disaster-recovery-as-a-service solution. Computing **99**, 1–26 (2017)
6. Gu, Yu., Wang, D., Liu, C.: DR-cloud: multi-cloud based disaster recovery service. Tsinghua Sci. Technol. **19**(1), 13–23 (2014)
7. Zeng, L., Veeravalli, B., Wei, Q., Feng, D.: SeWDReSS: on the design of an application independent, secure, wide-area disaster recovery storage system. Multimed. Tools Appl. **58** (3), 543–568 (2012)
8. Wu, Z., Ni,Y.: A disaster-recovery IT framework based on disaster indexing measurement mechanism in e-government. In: 2009 International Conference on Management of e-Commerce and e-Government, pp. 87–90. IEEE (2009)
9. Dhanujati, N., Girsang, A.S.: Data center-disaster recovery center (DC-DRC) for high availability IT service. In: 2018 International Conference on Information Management and Technology (ICIMTech), pp. 1–9. IEEE (2018)

10. Suguna, S., Suhasini, A.: Enriched multi objective optimization model based cloud disaster recovery. Karbala Int. J. Mod. Sci. **1**(2), 122–128 (2015)
11. Gharat, A.A., Mhamunkar, D.E.: Disaster recovery in cloud computing. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **4**(5) (2018)
12. Khoshkholghi, M.A., Abdullah, A., Latip, R., Subramaniam, S.: Disaster recovery in cloud computing: a survey. Comput. Inf. Sci. **7**(4) (2014)

An Efficient High Utility Pattern Mining for Finding Time Based Customer Purchase Behavior

V. S. Aziya Shirin(✉) and Joona George

Depatment of CSE, ICET, KTU University, Kerala, India
aziyashirin@gmail.com, joonageorge@gmail.com

Abstract. Utility mining is a prospering trend in data mining area. High utility itemsets are those ones that yield high profit when sold together or alone, in other words groups of items that generate high returns/profits in the customer transaction database. Regard of finding high profitable products, this is necessary to understand the recent preference of the customer. Detecting of HUP in a single phase with customer purchase behavior for a time period is addressed in this paper. In this paper not only consider the individual profit and quantity of each item in a transaction but also consider the customer preference of an item for a given time period. We propose an algorithm and a list structure for finding high utility patterns over large volume of data on the basis of sliding window technique and time cube. The objective is to discover groups of items periodically purchased by customers and generate large profits to the sales revenue.

Keywords: High utility pattern mining · Sliding window technique
Time based mining

1 Introduction

Our work inspires us to follow the problems of the industrial area. If a set of certain products generates high profit, managers can set up more profitable production plans to increase the production of these products so that the plant's revenue can be maximized. And the manager also has to consider customer preference for a specific period of time. For example, customer-friendly product information for a specific period of time is significantly more essential than the products currently in use. Although few items before generate high profits, if they currently not generate high profits, they are less important. In this regard, if customers purach some products frequently for a particular period of time, then we may understand that at this time period these particular products are valuable products . Therefore, plans can be drawn up in industrial areas on the basis of such information in order to maximize profits. The time they can be observed is therefore important.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 400–407, 2020.
https://doi.org/10.1007/978-3-030-37051-0_46

2 Related Work

A Two-Phase Algorithm [1] uses apriori-*like* approach for generating candidate patterns. In this process, for the calculation of TWU values of produced patterns, additional database scan is needed. The number of patterns generated at each level is therefore very large, so that extensive computational resources are consumed here for the mining process.

Sliding window techniques are used in the earlier time of HUPM [4, 7, 8]. THUI Mine was proposed to mine high utility patterns in a window. Since this algorithm has indistinguishable issues of two-stage, tree-based algorithm, for example, HUPMS [5] and SHU-Growth [6] have been proposed. SHU-Growth decreases the assembled TWU values of its structure. Hence, the candidate patterns that SHU-Growth generates is far lesser than HUPMS. But these two algorithms have limitations as they need enormous runtime to calculate the candidate pattern's actual utility. So we are proposing a time-based high utility pattern mining algorithm based on sliding window technique that does not produce candidate patterns.

Table 1. Example database

	TID	ITEMS	TU	TC
TB1	**T1**	A(3), B(2),C(5), E(2)	24	D1
	T2	A(2),B(3), C(4)	21	D1
TB2	**T3**	A(1), C(3),E(2)	10	D1
	T4	C(1), D(2)	10	D2
TB3	**T5**	B(1),C(2)	7	D3
	T6	A(2),B(2),E(1)	11	D3

Table 2. External utilities of items

Item	A	B	C	D	E
External utility	2	3	2	4	1

3 Proposed System

Table 1 shows an example database. Each number in a "blanket" indicates the internal utility of an item. Table 2 presents the external utilities of items. The following definitions are employed in the previous studies.

3.1 Mining High Utility Patterns Over Data Streams Using Sliding Window Technique

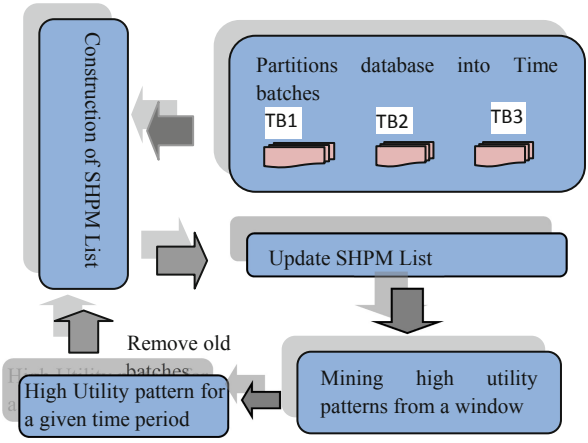


Fig. 1. Procedure of algorithm

An algorithm for High Utility Pattern Mining (HUPM) based on the time cube and sliding window technique is introduced in this section. Introduce a list structure here that helps to avoid the generation of candidates to remove the utilization of computational resources to verify the patterns of candidates. There is also a new pruning strategy to reduce HUPM's search space dependent on the sliding window model. Photograph. Figure 1 Shows our algorithm's complete procedure.

3.2 Problem Definition

Let D is given data stream and it can be split into multiple time batches in the basis of transaction time. Time batch, TB = $\{T_1, T_2, \ldots, T_n\}$, is a transactions set. n is the size of each time batch. Diversely window has set of batches SW = $\{TB_1, TB_2, \ldots, TB_m\}$ is a set of time batches and size of window is indicated by m. An user specifies the sizes of a window and the time period.

3.3 Construction of List Structure

At first, SHPM List is created for every pattern in transaction contain only single item. In other words every item in the given stream of data changes into 1 length pattern. The list of 1 length patterns are called global lists. Global lists are kept up in main memory the whole time all together to process data. A pattern list is made out of each transaction, which includes the pattern as its secondary pattern. So as to save all vital data for enerating high utility patterns which does not generate candidate pattern, wtid, an identifier of transaction; wup, pattern's utility; wu, pattern's remaining utility.

The remaining utility [9] is used as a pattern's vastly underestimated utility to trim unimportant patterns and lessen HUPM's search space using list structures. Subsequently, the information of the most seasoned group can be expelled from records effectively.

3.4 Updating Global SHUP-Lists

The proposed algorithm's mining process can be led to discover high utility patterns from the window on the off chance that a window is full of recent batches. Be that as it may, before leading the mining procedure, the wu values in the global SHPM-Lists ought to be refreshed dependent on an ideal TWU rising request so as to play out the mining procedure too effectively. The cause is that for the mining forms that use list structures, the development of records dependent on a TWU rising request is recognised as the more productive way [13].

3.5 Mining High Utility Patterns from the List Structure

Mining procedure of the algorithm performed well after ru values of global SHPM Lists are fully updated. The algorithm's mining process is performed based on the depth - first search method. The algorithm consolidates three global lists of three distinct patterns so as to produce the contingent rundown of an pattern, which is a ultra pattern of the three pattern. The blend of three lists are carried out by looking at the sections of the three records.

3.6 Mining Patterns with TCs

Let I = {i1, i2, …, In} Be a set of items in a database and D. Each transaction is associated with an identifier transaction ID (TID), a time stamp ts a set of items. For all transactions, ts ay T is the total time span of the database. Let st, et[t] where st is the

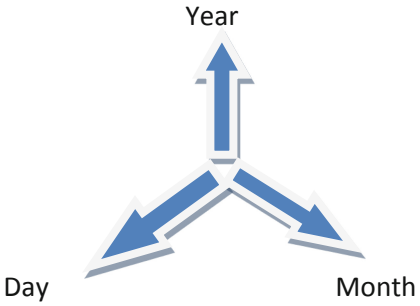


Fig. 2. Example of three time hierarchies

time of beginning and et is the time of end. And st < and so on. For example, (3, 8) Month is the 3rd to 8th month interval. TC is defined to deal with temporary portions of transactions. Figure 2 is a pictorial representation of a database partitioned three-time hierarchy. Instead, for more than three time hierarchies, the term hyper cube is used. A partitioning of equal length is used according to the minimum interval of the user, knowing the hierarchy of time and its domain. Initial cubes are called Basic Time Cubes (BTCs) [11].

Time hierarchy shown in Fig. 2, It is possible to consider an hour, a day, a month to define a BTC $1 \times 1 \times 1$. It is not possible to overlap any two elements in BTC such that $BTCi \cap BTCj = \varnothing$ [11].

3.7 Algorithm 1: SHPM Algorithm [10]

Carry four inputs, database D, minimum utility threshold mu, batch size TB, and window size SW. Above all else, D is divided into different batches. The transactions that belong to the batch are processed one by one for each batch. By collecting transaction utilities, TWU of an item is acquired for each item in a transaction.

Algorithm 2: Mining [10]

Input - a set of lists, ***L***;
HP : A set of High utility patterns;
Mu : A minimum utility threshold ;

Function: Mining (L,HP)

1. For each list l in L
2. If the pattern's utility in l is greater than or equal to mu
3. Enter the pattern into HP;
4. End if
5. For each list l' that can combined with l
6. If psum + rsum of I is no less than mu
7. Through combine I' and I create a new list in L
8. End if
9. End for
10. recursively call the function mining
11. Call functionMining(L,Hp,mu)
12. End for

Furthermore, if there is no list in global SHUP - Lists, the item list will be constructed. And new transaction entry will be added to the list. If a window is filled with data of recent batches, processes are performed from the window for mining high utility patterns. First, Wu entry fields are updated in TWU's optimal upward order. High utility patterns are then mined by calling the Mining process from the window. Users will be provided with the results of the mining process.

The Mining algorithm is used to perform SHPM, the proposed algorithm's recursive mining process. To carry out recursive mining processes, the procedure receives the following parameters. The first parameter L is a set of SHPM-lists of k-lengths patterns diversely. Mu and HP is used in the current window respectively to determine high utility patterns and to store high utility patterns extracted in the memory. First, the algorithm selects items from List one after another. If the utility of pattern is in l is greater than mu then its added to HP. Then generate a new list using combine two lists. If the summation of psum and rsum is no less than mu, considering the batches of two lists, the function call joins two lists to create a new one. The function calls itself after all lists are combined to perform recursive mining processes.

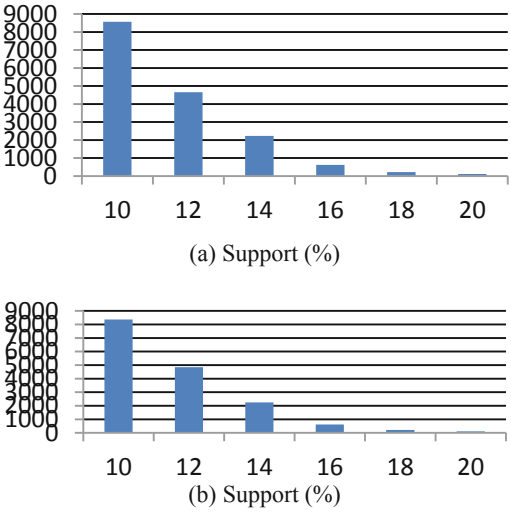


Fig. 3. Solution time of the proposed algorithm against different minimum supports (a) $\alpha = 30\%$. (b) $\alpha = 50\%$

4 Result Analysis and Discussion

The dataset is a synthetic transaction database made from 01/01/2016-00:00:00 to 01/01/2017-00:00:00 by 100 items. Then a pattern is selected as a solution for the target. The goal behind using such a large data set for analysis is to ensure that any high utility pattern mining problem can be handled by our proposed algorithm. Time hierarchies of the time stamp, i.e. month, day, hour, a specific time interval is selected to increase a pattern. Objectset{65,73,92} is a high utility pattern from the apriori. We assume that this pattern is frequent in the first three months of 2016 between 7 and 9 A. M., 1st and 2nd days.

This time interval contains 3 = 2 = 3 BTCs. 100 transactions are increased for each BTC, including only items 65, 73, and 92. The proposed algorithm is coded by the Java programming language and runs on a notebook computer using an Intel Corei7, 2.5 GHz CPU with 16 G of memory and running windows 10. Target solution, i.e. pattern {65,73,92}, has been mined at a reasonable time in the specified time interval as expected. Figure 3 Displays the relationship between the time of the solution and the minimum density supports. The lower the minimum support, as we can see, the higher the time of the solution. It is also worth noting that in addition to the target solution, many other useful patterns are found with support level below 20 percent. While there are no significant differences between solution time with different density threshold, we now guarantee that found data patterns are valid and there has been no overestimation of time periods.

5 Conclusion

This paper introduce a technique used to extract the utility of itemsets, which finds high utility patterns without generating candidates with customer purchasing behavior at particular time period. It is therefore feasible for the establishment of cost effective production plans in different industrial areas. In order to manage the time based data a list structure called SHPM List was drawn up. And For reducing the search space of high utility pattern mining introduce a pruning strategy sliding window. For future work, we will design alternative algorithms for High utility pattern extraction.

References

1. Liu, Y., Liao, W., Choudhary, A.: A two-phase algorithm for fast discovery of high utility itemsets. In: Proceedings of 9th Pacific-Asia Conference, pp. 689–695 (May 2005)
2. Chu, C.-J., Tseng, V., Liang, T.: An efficient algorithm for mining temporal high utility itemsets from data streams. J. Syst. Softw. **81**(7), 1105–1117 (2008)
3. Krishnamoorthy, S.: Pruning strategies for mining high utility itemsets. Expert. Syst. Appl. **42**(5), 2371–2381 (2015)
4. Ahmed, C., Tanbeer, S., Jeong, B.-S., Lee, Y.-K.: Efficient tree structures for high utility pattern mining in incremental databases. IEEE Trans. Knowl. Data Eng. **21**(12), 1708–1721 (2009)

5. Ahmed, C., Tanbeer, S., Jeong, B.-S., Choi, H.-J.: Interactive mining of high utility patterns over data streams. Expert Syst. Appl. **39**(15), 11979–11991 (2012)
6. Ryang, H., Yun, U.: High utility pattern mining over data streams with sliding window technique. Expert. Syst. Appl., 214–231 (2016)
7. Kim, D., Yun, U.: Efficient mining of high utility patterns with considering of rarity and length. Appl. Intell. **45**(1), 152–173 (2016)
8. Ryang, H., Yun, U., Ryu, K.: Fast algorithm for high utility pattern mining with the sum of item quantities. Intell. Data Anal. **20**(2), 395–415 (2016)
9. Liu, M., Qu, J.: Mining high utility itemsets without candidate generation. In: Proceedings of the 21st ACM international conference on Information and Knowledge management (October 2012)
10. Yun, U., Lee, G., Yoon, E.: Efficient high utility pattern mining for establishing manufacturing plans with sliding window control. IEEE Trans. Eng. Manag. **64** (2017)
11. Ghorbani, M., Abessi, M.: A new methodology for mining frequent itemsets on temporal data. IEEE Trans. Eng. Manag. **64** (2017)
12. Yun, U., Kim, D., Ryang, H., Lee, G., Lee, K.: Mining recent high average utility patterns based on sliding window from stream data. J. Intell. Fuzzy Syst., 3605–3617 (2016)
13. Liu, X., Guan, J., Hu, P.: Mining frequent closed itemsets from a landmark window over online data stream. Comput. Math. Appl. **57**(6), 927–936 (2009)
14. Kusiak, A., Shah, S.: Data-mining-based system for prediction of water chemistry faults. IEEE Trans. Ind. Electron., 593–603 (2006)
15. Tseng, V., Shie, B.-E., Wu, C.-W., Yu, P.: Efficient algorithms for mining high utility itemsets from transactional databases. IEEE Trans. Knowl. Data Eng., 1772–1786 (2013)
16. Xiao, Y., Zhang, R., Kaku, I.: A new framework of mining association rules with time-windows on real-time transaction database. Int. J. Innov. Comput. Inf. Control **7**(6), 3239–3253 (2011)

Plant Disease Detection Using Deep Learning

Gresha S. Bhatia(✉), Pankaj Ahuja, Devendra Chaudhari, Sanket Paratkar, and Akshaya Patil

Computer Engineering Department, Vivekanand Education Society's Institute of Technology, Mumbai, India
{gresha.bhatia, 2015pankaj.ahuja, 2015devendra.chaudhari, 2015sanket.paratkar, 2015akshaya.patil}@ves.ac.in

Abstract. India is an agrarian economy, with three-quarters of its rural population relying on agriculture as their primary means of livelihood. Agriculture shares 17% of the country's GDP. With rising demands due to the ever-growing population, increasing farm productivity is the need of the hour. However, annually more than one-third of the crop yield is affected by the diseases in India. Thus, identification of the disease in the early stage is essential to provide proper treatment. Traditionally, the disease identification is done by visual examination, which often is done after major damage has already been done to the crop. With the help of state of art technologies like deep learning and cloud computing, the same can be achieved on a real-time basis. With the help of Convolutional Neural Network architectures, researchers propose a system that focuses on detection and identification of the plant disease with a mere click of leaf picture and provides solutions. Furthermore, the system also generates heat maps, which provides insights about disease spread in a region, thereby easing out the data analysis process.

Keywords: AI in farming · Cloud computing · Machine learning · Crop disease detection

1 Introduction

Crop diseases affect the yield of the crop to a large extent. The farmer based on their past knowledge and an intuition tries to identify and take remedial steps accordingly [1]. However, researchers in this attempt to automate the process, only require an infected leaf as an input.

The Application guides the farmer to take a proper image considering the light as well as orientation thereby minimizes the computations further. Pre-processing is done with the help of scaling and segmentation before feeding into convolutional neural networks. The proposed system thus identifies the diseases and proposes the measures

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 408–415, 2020.
https://doi.org/10.1007/978-3-030-37051-0_47

to be taken considering the geographic conditions like soil, weather. The data analysis model captures the geolocation of the region where the query was generated, at the same time and effectively generates statistics with the help of heat maps. Such a system can prove to be useful for the farmers to get assistance on a real-time basis regarding the crop disease queries. Also, it can help the scientific fraternity, government and private organizations to get insights about the region-wise spread of disease.

2 Overall View

As shown in Fig. 1. farmer will click an image through a smartphone camera and the same will be uploaded to the firebase datastore. In the result of successfully uploading of image, Firebase datastore returns a downloadable image URL which in turn is fed to the own custom API running over Azure cloud service. Client side will wait for the image to be processed and ResNet 50 model will then eventually predict the disease class to which the leaf belongs over the cloud. If the received result is of healthy of status then no remedial solution is mapped and the message is displayed to the farmer. Otherwise, the mapping will be done between disease and its remedial solution and the same will be displayed over the farmer's smartphone application screen. Meanwhile, in the background, a disease Case will be created in object-oriented approach where the location of Farmer, image_url and infected disease name will be recorded for the data analysis purpose which can be used by any organization in order to get insights of the area under the spread of plant disease.

As shown in Fig. 2. After receiving the image_url from the smartphone at Web Service (API) hosted at Cloud Service image is being downloaded at the server side. As model requires the image to be resized in the format of 227 $\times$ 227 pixel pre-processing steps are performed. Before feeding to the ResNet50 model image is first checked whether an image is of a leaf or not. Further prediction steps are performed only when the condition of integrity of the image is satisfied. ResNet 50 model will then make a prediction on the 38 classes of diseases based on the input image. Based on the disease detected remedial solution is suggested. All the generated information is then parsed into the JSON formatted string and returned to the client end with an appropriate status code.

3 Implementation

As detection of disease from a provided leaf picture is a difficult task to learn for human as well as the machine. As more features are required to be learned by the network to classify the image among 38 classes, Residual Network is being used because of the following reasons:

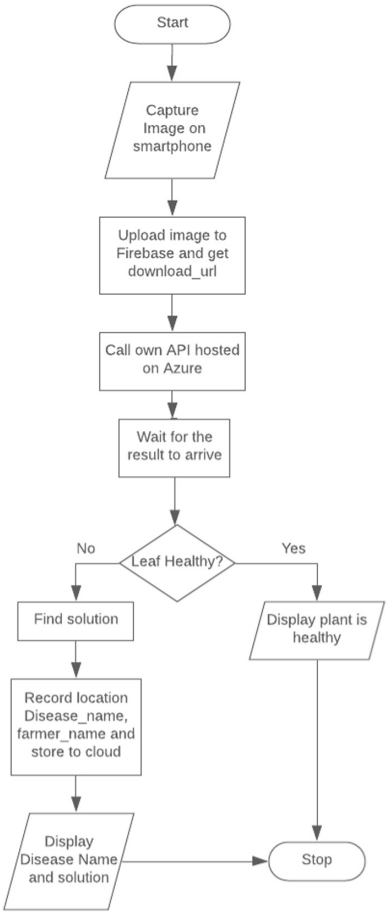


Fig. 1. Client-side flow of action

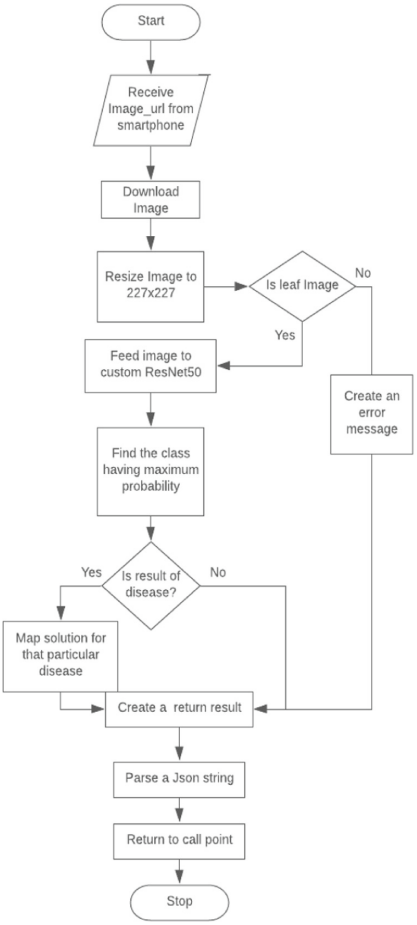


Fig. 2. Flowchart of API side working

1. Deeper CNN is required to learn complex features.
2. Deeper the network more problem of vanishing gradient arises.
3. Deeper the network more problem of Exploding gradient arises.

In order to avoid these problems, Residual Network creates a shortcut link between multiple stages thus remembering the image fed for the larger part of the network.

The system inputs image from farmer and image is then fed to Residual Network using CNN in foreground outputs the predicted disease if any. The input image is rescaled to the size of (227,227,3) and fed to the ResNet shown in Fig. 3. After being processed inside the network result is extracted from the network specifying the class number to which the leaf disease is being assigned.

Complete Network is broken into 5 stages excluding Input and Output Layer. Inputted image is padded with zeros with size (3,3) in order to keep the pixels at edge

safe for deeper layers [2]. In stage 1, Image is the convoluted with kernel_size of (7,7) and 64 such filters are used to make the depth of 64 [3, 4].

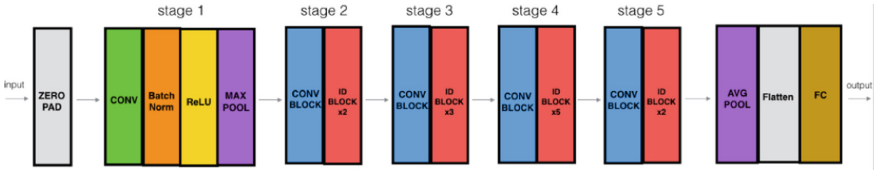


Fig. 3. ResNet 50 model structure

Table 1. Kernel size, number of ConvBLOCK and number of Identity Block stagewise breakdown

	Kernel size	Number of ConvBLOCK	Number of identity block
Stage 1	(7,7)	0	0
Stage 2	(3,3)	1	2
Stage 3	(3,3)	1	3
Stage 4	(3,3)	1	5
Stage 5	(3,3)	1	2

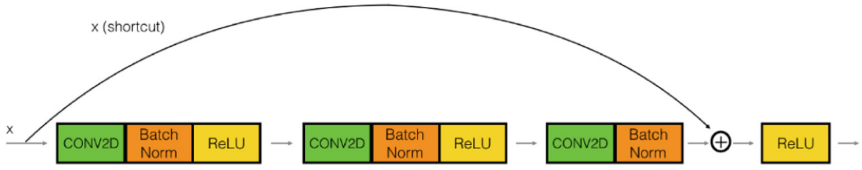


Fig. 4. Identical block

Similar patterns are used for further 4 stages as well. Table 1 shows the kernel_size used for convolution at that stage, the number of Convolutional Blocks and Identical Blocks used.

As shown in Fig. 4 there are three components in Identical Block.

Each component is convoluting the output received from the previous layer (x) then normalized result is then passed through ReLU activation function [5, 6]. However, before applying the activation function in stage 3 intermediate result is added with the previous layer output (x).

Table 2 shows the stagewise distribution of the number of filters used for convoluting each component.

Table 2. Identical block number of filters

Stage	Conv2D	Conv2D	Conv2D
Stage 2	64	64	256
Stage 3	128	128	512
Stage 4	256	256	1024
Stage 5	512	512	2048

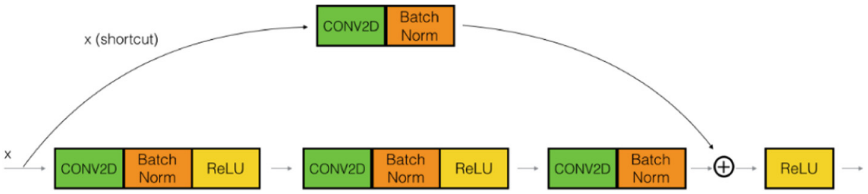


Fig. 5. Convolution block

Table 3. Convolutional block number of filters

Stage	Conv2D	Conv2D	Conv2D	Conv2D (shortcut)
Stage 2	64	64	256	256
Stage 3	128	128	512	512
Stage 4	256	256	1024	1024
Stage 5	512	512	2048	2048

Convolutional Block is same as that of Identical Block with one additional component as shown in the Fig. 5 where the component (CONV2D shortcut) will make previous layer output (x) compatible for addition with the intermediate output received from the last component in the sequence before applying the ReLU activation function.

Table 3 shows the stagewise distribution of the number of filters used for convoluting each component with one additional column for shortcut component.

The result obtained from stage 5 is then average pooled and flattened [7]. Moreover, the flattened layer is then converted to a fully connected layer having 38 output unit representing distant classes applied under SoftMax activation function to output maximum probability of prediction class [8].

4 Evaluation

The output from the model shown in Fig. 3 will be 38 values ranging from 0 to 1. These output values will be then log (q(x)) and expected value for that particular unit is represented by p(x). Both entities are multiplied and summed over the dataset. Result obtained is multiplied with −1 in order to get a positive entity as shown in formula number 1.

$$H(p,q) = -p(x)\,log(q(x)) \tag{1}$$

The categorical cross entropy loss function used in formula number 1 then optimized with the help of Adam optimizer in order to minimize the loss and model will change its weights eventually learning the complex features. Results obtained from the model are then checked based on the accuracy which is computed with formula as following [9, 10].

$$Accuracy = \frac{Number\ of\ examples\ correctly\ labeled}{Total\ number\ of\ examples} \tag{2}$$

5 Graphs and Reports

Data is split into 75% training data, 12.5% Validation data and 12.5% Testing data. Model is trained for 14 epochs. Accuracy for training dataset keeps on increasing but validation set accuracy increased to epoch number 10. Thus, epoch number 10 gives the optimal weights as epoch number 10 onwards model starts to overfit over the training dataset and doesn't perform well on validation data [11]. The graph of Accuracy versus Number of training epochs is shown in Fig. 6.

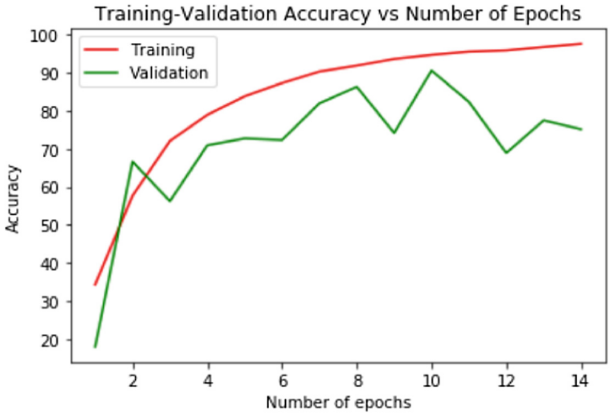


Fig. 6. The training accuracy versus Epochs in Red curve and validation accuracy versus Epochs in green curve.

Table 4. Accuracy breakdown for ResNet50 model

	Train	Validation	Test
Alone	97.50%	90.50%	92.52%
Combined	98.32%		

The results shown in Table 4 are obtained after the training the model for 14 iterations. Combined training accuracy obtained on a number of images 17,752 is 98.32%. Test accuracy obtained on a number of images 2,192 is 92.52%.

As shown in Table 5 ResNet 50 is giving maximum accuracy for the given labeled dataset of Plant Disease Detection. Other methods were close enough to generate similar results but applying the shortcut link in Residual Network benefitted the model in remembering features learned in earlier stages of Convolutional Neural Network.

Table 5. Accuracy comparison with the other CNN architecture

Model	Training	Testing
ResNet 50 [12]	98.32%	92.52%
AlexNet [13]	95.35%	87.78%
VGG16 [14] (small)	97.84%	76.82%
VGG16 [14] (big)	98.04%	86.59%
MobileNet	87.47%	87.63%

6 Conclusion

With the help of state of art technologies like Deep learning, the process of disease detection, identification can be semi-automated with minimal human intervention. The proposed system achieves 92.52% of accuracy which proves to more reliable compared to the other algorithms studied. The remedial measures proposed by the system can be followed by the farmer to cure the infected plant. Data analysis can be done by the government as well as private organizations from the insights through heat maps generated to analyze the region-wise disease spread. Altogether the system proves to use to boost the farm throughput.

7 Future Scope

The system proposed is a semi-automated solution for the problem faced by farmers. However, human intervention can also be eliminated with the help of drones/robots that monitor the field with an onboard camera. With the help of IoT sensors, the system can directly supply the amount of the prescribed solution in the right proportion. Hence, the cure can also be taken care of automatically. Thus, the proposed system can be made completely autonomous.

References

1. Bhatia, G.S., Ahuja, P., Chaudhari, D., Paratkar, S., Patil, A.: FarmGuide one-stop solution for farmers. Asian J. Converg. Technol. **5**(1)
2. https://medium.com/machine-learning-algorithms/what-is-padding-in-convolutional-neural-network-c120077469cc

3. https://towardsdatascience.com/deciding-optimal-filter-size-for-cnns-d6f7b56f9363
4. https://www.saama.com/blog/different-kinds-convolutional-filters/
5. https://keras.io/layers/convolutional/#conv2d
6. https://keras.io/layers/normalization/#batchnormalization
7. https://keras.io/layers/pooling/#averagepooling2d
8. https://keras.io/layers/core/#dense
9. Janocha, K., Czarnecki, W.M.: On loss functions for deep neural networks in classification, submitted on 18 Feb 2017
10. Kingma, D.P., Lei Ba, J.: Adam: a method for stochastic optimization. In: Published as a Conference Paper at ICLR (2015)
11. Ghasemian, A., Hosseinmardi, H., Clauset, A.: Evaluating overfit and underfit in models of network community structure, submitted on 1 Mar 2018
12. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. Cornell University Library, submitted on 10 Dec 2015
13. ImageNet classification with deep convolutional neural networks. https://papers.nips.cc/paper/4824-imagenet-classification-with-deep-convolutional-neural-networks.pdf
14. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. Cornell University Library, submitted on 4 Sep 2014 (v1)

Study and Implementation of Ethernet Based Synchronization in Distributed Data Acquisition System

Jismi S. Manjaly[1(✉)], Abi K. Krishnan[2], and P. L. Bonifus[1]

[1] Rajagiri School of Engineering and Technology, VLSI and Embedded Systems, Kochi, India
jismimanjaly149@gmail.com,
bonifus@rajagiritech.edu.in
[2] Naval Physical Oceanographic Laboratory, SCH, Kochi, India
abi@npol.drdo.in

Abstract. In the recent past, acoustic detection and ranging techniques has become more advanced and sophisticated. In general, the sonar systems consist of distributed data acquisition systems. For accurate ranging these systems needs to be synchronized in time. This can be achieved by custom synchronization techniques or through standard mechanisms like IEEE 1588 PTP (precision time protocol). This project outlines the implementation of a synchronization mechanism with minimal hardware support. The main objective is that it will minimize custom hardware requirements. Using a standard hardware interface like Ethernet will rule out any signal integrity related issues at the physical layer. The accuracy of synchronization across the systems has to be measured and tuned. The implementation will be done on the Microzed board using the Vivado 2018.1.

Keywords: IEEE 1588 · Precision time protocol · Vivado

1 Introduction

The clock synchronization, a subject that has become considerably relevant in some industrial fields such as automation, robotics and sensor networks. This is especially important for automated control systems, wherein the knowledge of the exact time of an event is critical for the correct function of the entire control process. Synchronization protocols are used to precisely synchronize independent clocks throughout a distributed system. Synchronization allows transactions between distributed systems to be controlled on time basis.

Periodic Clock synchronization is necessary in distributed systems as the internal clocks of several computers may have offsets. Even when initially set accurately, the clocks may slowly drift apart, because of the inherent difference in the accuracy of different clock sources. There are several factors that occur as a repercussion of clock rate differences. The precise time data has an incredible significance for distributed systems in computerization innovation. Protocols like IEEE 1588 [8] focuses on

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 416–423, 2020.
https://doi.org/10.1007/978-3-030-37051-0_48

distributing synchronized time stamps across the network with an accuracy of under microsecond by means of Ethernet systems.

Synchronization is the process of taking multiple devices and making their information identical. The synchronization accuracy required depends on the application under consideration. Some applications might require the time to be synchronized between the distributed systems with a tolerance of few milli seconds. But this variation might be completely unacceptable to some other applications like autonomous vehicles or distributed digital signal processing. The aim of this implementation was to achieve a distributed timestamp with an accuracy better than 10 μs. The implementation is done using a Microzed board [10], which is a development platform for Xilinx ZYNQ FPGA [7]. The achieved accuracy was measured using a PPS signal generated on the GPIO pins available in the PMOD interface of the board [9].

2 Literature Review

Fubin et al. and Yubo et al. [1] proposed a mechanism for improving the accuracy of IEEE 1588 in synchronization protocol. The authors realized that IEEE 1588 synchronization protocol plays a major role in the packet based synchronization mechanism, also enables accuracy in sub Micro–Second range. From the principle of IEEE 1588 it is clear that there are several factors affecting the accuracy of grand master and slave devices. They are offset between master and slave devices, transmission delay in the network and finally the position of time stamp generation. Mahmood et al. [2] and Exel et al. proposed an IEEE 802.11 wireless local area network synchronization (WLAN) system using the IEEE 1588 precision time protocol and software assisted time stamps. In this work authors investigated the individual sources of delay and jitter mechanism. The author also proposed a novel measurement to quantify the hardware and software related delay and jitter mechanisms.

The IEEE 1588 [3–5] convention assumes a noteworthy job to give a high level of exactness and accuracy both in wired and remote systems. Dissimilar to other synchronization protocol [6], it has the adaptability across different time stamping methods with varying accuracy. From the writing overview, we have seen that different sifting methods have been examined to improve the slave exactness. The execution of the IEEE 1588 protocol has been assessed for a Master-Slave progressive system. The primary objective of this proposal is to explore ways to implement the well established IEEE 1588 protocol on a hardware which is not PTP aware and compare the accuracy in different time stamping scenarios.

3 Architecture Design and Implementation

In this section we describe the basic architecture of clock synchronization, and we desribes the IEEE 1588 synchronization protocol.

3.1 IEEE 1588 Synchronization

It is based on a message exchange mechanism. These messages are routinely exchanged between the master and slave so as to decide the offset and the message travel delay through the network. The realization mechanism [11] shown in Fig. 1.

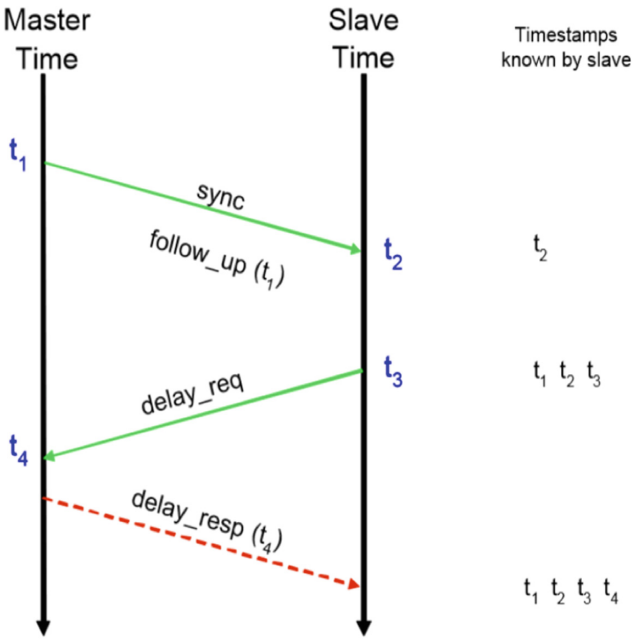


Fig. 1. One-step clock

One-Step Clock

The One-Step clock strategy exchanges three time estimation messages among master and slave:

1. Sync Message
2. Delay-Request message
3. Delay-Response message

The specific steps are as follows:

Step 1: At the time of t_1 (based on master clock), the master clock send sync message to slave. The slave system receives the message after the network transmission delay. The slave records the time in the local clock, when the sync message is received, as t_2.

Step 2: At the time t_3 (based on slave clock), the slave send Delay Req message to master clock by unicast transmission, and marks the causing time stamp. The master marks the time from the local clock, when the Delay Req message is received, as t_4.

Step 3: The master sends Delay Resp message to slave, in which it embeds the time t_4. Therefore, the slave obtains four time stamp: t_1, t_2, t_3, t_4.The difference between the Master and the Slave timer is denoted by t_{offset} and the time taken by the message to travel from one system to another is denoted by t_{delay}. Delay and offset are calculated by Eqs. (1) and (2).

3.2 Architecture Design

The time stamping of the messages between the master and slave is the critical element in deciding the accuracy of synchronization. The variability in the process will deteriorate the performance of the algorithm. Closer the time stamping to the wire, better will be the accuracy. For best result, the time stamping has to be done at the Ethernet PHY level [9]. This requires special PHY devices which are PTP aware and this may not be feasible in the already existing hardware modules. The next opportunity to time-stamp the packet is when the packet enter/leave the Ethernet MAC. This is also specific to the MAC IP used and will not be portable across designs. In proprietary Ethernet MAC IPs it may not be feasible to implement custom time stamping. In this implementation hardware dependency is completely avoided, at the penalty of accuracy, and the time stamping is done in the software. Figure 2 shows the software based time stamping.

$$Delay = \frac{(t_2 - t_1) + (t_4 - t_3)}{2} \tag{1}$$

$$Offset = \frac{(t_2 - t_1) - (t_4 - t_3)}{2} \tag{2}$$

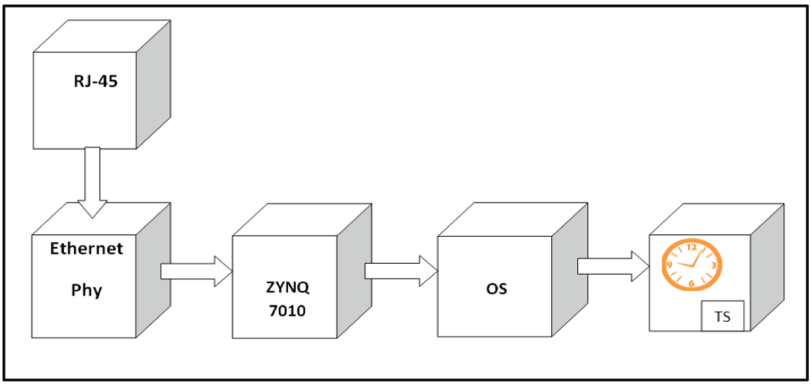


Fig. 2. Software based time stamping

3.3 Implementation

The software based time stamping can be done with the help of any high resolution timer available in the system. In our implementation, the Triple time counter (TTC) in ZYNQ FPGA was used to implement the time stamping. Once initialised the timer runs independently without any processor involvement. The time can be adjusted by the processor at any instant through a set of registers.

In order to measure the achieved synchronization accuracy, a PPS output is generated with the help of the GPIO of the ZYNQ [10]. The PPS signal is generated based on the TTC timer and hence directly provides an indication of the distributed time synchronization. TTC is configured to generate interrupt at periodic intervals to generate the PPS signal. The GPIO output is routed to the PMOD header on the evaluation board. Two Microzed boards were used for implementation and testing, one of them acting as the master and the other as slave. The PPS signal from both the boards through the PMOD header was connected to the CRO for the measurement. To study the impact of variability in the application software timing, on the accuracy of synchronization, two methods were used to implement the algorithm.

1. Ethernet data transmission with IP stack
2. Raw Ethernet Data Transmission.

Ethernet Data Transmission with IP stack

In this mode, the application is configured to run on an operating system and a separate IP stack. FreeRTOS was chosen as the operating system and lwIP stack was used [12]. Both are open source software, integrated in to the Xilinx Vivado SDK along with the required BSPs for Zynq. lwIP was configured in the socket mode, so that standard socket programming can be directly used in the application development. The presence of OS and IP stack provides abstraction and lot of flexibility in the application development, but introduces extra overhead in terms of the execution time.

Raw Ethernet Data Transmission

In this mode, the application is written in the bare metal mode, where in the application directly runs on the processor, without any OS and IP stack. In this mode Ethernet data is transmitted by directly initiating the DMA transfer from the memory to the Ethernet MAC, by the application software. Hence the overhead of the OS and IP stack does not exist in this case. Based on the method mentioned in the Sect. 3.1, message exchange is carried out in both the modes and time values t_1, t_2, t_3 and t_4 are obtained. From these, the delay and offset are calculated by the slave system. The timer at the slave is then adjusted with the offset value to match the Master timer.

4 Experimental Setup and Result

Figure 3 shows the test setup for the accuracy measurements. Two Microzed boards are connected to each other through Ethernet cable. The PPS output from both the systems are connected to the CRO. Master program was downloaded to one of the boards and

slave program to the other. The same setup was used for the testing of both bare metal application and application with OS and IP stack. The time difference between the edges of the PPS signals from both the boards were measured for different timer resolutions. Timer resolution was varied with the help of prescalar register of the TTC timer. Figure 4 shows the output of the CRO, after synchronization message exchange between the systems, and the corresponding timer corrections. Table 1 lists the time accuracies achieved in both the configurations for different timer resolutions.

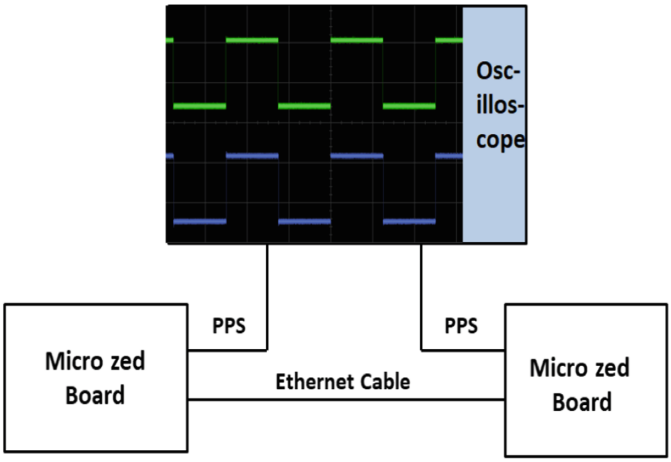


Fig. 3. Setup diagram of synchronization accuracy test of IEEE 1588

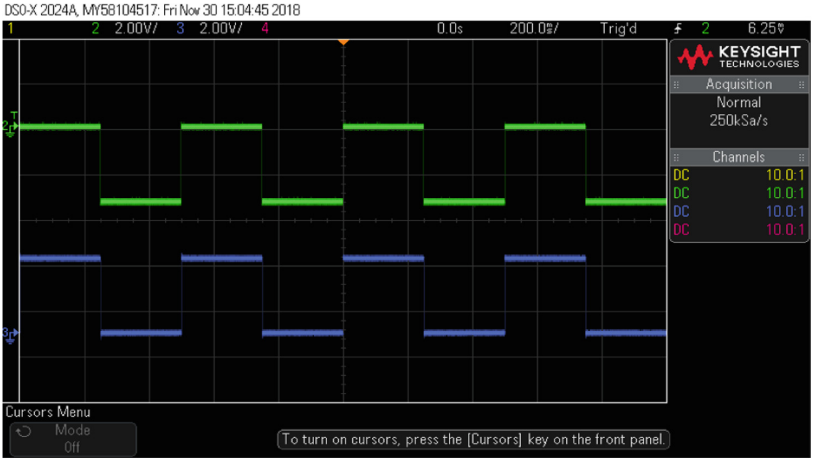


Fig. 4. Syncronized output signals

Table 1. Achieved synchronization accuracy

Methods	TTC prescaler config		
	1 Hz	4 Hz	8 Hz
Ethernet data transmission with IP stack	4.8 µs	2.4 µs	1.9 µs
Raw ethernet data transmission	1.3 µs	940 ns	890 ns

5 Conclusion

One-Step clock message exchange method is implemented and tested on a PTP unaware hardware using software Time-Stamping. The achieved accuracy was close to 1 µs and it deteriorated with software overheads. The deterioration of the accuracy with OS and IP stack can be attributed to the variability in the processing delay in the IP stack from packet to packet. For applications requiring synchronization times of the order of 10 µs and above, the software time stamping method can be used. For applications requiring sub-microseconds accuracy, hardware based time stamping at Ethernet MAC or PHY will have to be explored.

A suggestion for future work is the IEEE 1588 time stamps should be generated in hardware or the timestamp should be captured as close as possible to the hardware. During hardware based time stamping, if the packet exchanges are instantaneous there will be no delay and the time difference can be computed accurately.

Acknowledgements. This work was supported by the Naval Physical Oceanographic Laboratory and Rajagiri School of Science and technology.

References

1. Fubin, P., Yubo, Y., Lei G., Liangliang, S.: The accuracy of IEEE 1588 time synchronization protocol and its improvement. In: IEEE 12th International Conference on Electronic Measurement & Instruments (2015)
2. Mahmood, A., Exel, R., Member, IEEE, Sauter, T.: Fellow, IEEE: delay and jitter characterization for software-based clock synchronization over wlan using ptp. IEEE Trans. Ind. Inform. **10**(2) (2014)
3. Mahmood, A., Exel, R.: Servo design for improved performance in software time stamping assisted WLAN synchronization using IEEE 1588. In: Proceedings of Emerging Technology and Factory Automation (ETFA), Cagliari, Italy, pp. 1–8 (Sep 2013)
4. Mahmood, A., Gaderer, G., Trsek, H., Schwalowsky, S., Kero, N.: Towards high accuracy in IEEE802.11 based clock synchronization using PTP. In: Proceedings of IEEE Symposium on Precis on Clock Synchronization (ISPCS), Munich, Germany, pp. 13–18 (Sep 2011)
5. Ronen, O., Lipinski, M.: Enhanced synchronization accuracy in IEEE1588. In: 2015 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), pp. 76–81. IEEE (2015)
6. Ullmann, M., Vogeler, M.: Delay attacks implication on NTP and PTP time synchronization. In: ISPCS 2009 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication Brescia, Italy (12–16 Oct 2009)
7. https://www.xilinx.com/support/documentation/user_guides/ug585Zynq-7000TRM.pdf

8. http://www.ti.com/lit/an/snla098a/snla098a.pdf
9. http://zedboard.org/sites/default/files/documentations/5276-MicroZed-HWUG-v1-7-V1.pdf
10. http://adiuvoengineering.com/microzed_chronicles.pdf
11. http://soc-e.com/wp-content/uploads/2013/02/ieee1588_120926_lq1.pdf
12. https://www.st.com/content/ccc/resource/technical/document/application_note/fd/5d/64/cf/7c/38/4c/30/DM00036052.pdf/files/DM00036052.pdf/jcr:content/translations/en.DM00036052.pdf

Prevention of DDoS Attack Through Trust Management System for VANET Environment

Piyush Chouhan(✉) and Swapnil Jain

SVVV, Indore, India
pchouhan06@yahoo.com, swapniljain76@gmail.com

Abstract. DDoS (Distributed Denali of Service) attack majorly issues on vehicular Ad hoc network (VANET). When two or more vehicle exchanges information to each other either direct or indirect, DDoS attack effects on VANET networks. VANET networks can manage communication by using trust management model for predication and detection of DDoS attacks. Trust model based on Hash encryption key and Identity based technique will work ageist DDoS attacks node. Trust Management System is divided in to three Steps. Step-I: **System Initialization**, Step-II **Trust-Value Updating** and Step-III: **Vehicle to Vehicle Authentication and Trust Evaluation**. Its method applies scenario 20 nodes, 40 nodes, 60 nodes, 80 nodes, and 100 nodes and totally taken 15% malicious nodes on a given scenario. With the help of NS2 simulation tool through which calculate PDR, E2E and Throughput parameters during Simulation. Analysed result based on three protocol AODV, DDoSAODV and TAODV that's by TODV perform better result compare to another protocols on the bases of parameters.

Keywords: DDoS attacks · VANET · Trust model · Hash function · NS2 AODV

1 Introduction

Wireless mobile methods under nodes have been part in wireless mobile structure which contains different nodes. Auto two wheeler & four wheeler transferring & applying devoted precise amplitude connection property [1]. Also maintain auto two wheeler & four wheeler connection under exchange which provides comfort & relief for users with support of connecting information. Safety organization merges intersection mark contact compressing, auto car-stake clash warning, and lane situation advice & location elaborate support. In the same manner consolation organization merges auto car leftovers, automatic motor way payment collection, entertainment & World Wide Web [2]. Moreover under wireless mobile methods of nodes, safety has been important factor as comfort information that has growth essential documents connected. Decision & spot build safety arrangement apply for knowing originality in auto car & information, that differentiates with each but might unable to handle safety problems completely [3]. Assurance authority compulsorily authorized assurance limit in source & comfort information. Additionally under wireless mobile methods nodes, assurance authority possesses text excellent experiment & very low performance

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 424–435, 2020.
https://doi.org/10.1007/978-3-030-37051-0_49

process but on the other hand it's remaining a complex task which described in given research article [4]. On the other hand a free safety inquiry under wireless mobile methods junction that wherein a junction assures comfort information brings to second junction. Mark under applying assurance authority & committee facilitate each junction under wireless mobile methods for differentiating false junction [5].

I. Trust Organization & Structure: Under Wireless mobile method of nodes, assurance earlier safety provides an important part to made well established wireless mobile systems of nodes under adjacent situation. Outstanding assurance controlling systems necessarily merge continuation in requested features, which given as [6] redistributed assurance authority, functional, elegant in safety matter, regulate for various dimensions, vigour, layout limit safety. Assurance may design in middle under authorized layout [7]. Graphically build for authorization & growing under its own preparing form. Main task in assurance committee have been confirm authorized distribution in middle of nodes wherein few assurance controlling systems are suggested. Assurance systems categorizes as [6, 7]: documents set assurance systems: clarify reliability in classmates, messages having assurance systems core surround getting reliability in messages & build up assurance systems. Primarily verify reliability under assistant determined feature in message. Assurance controlling in middle of nodes greatly build on binary types which may be express as straightforward & circular methods [8].

II. Related Works: This paper proposed neighbour correspondence based trust in which board conspire for verified interchanges under Wireless mobile method of nodes. Also authorized redistributed, versatility & strength accompanied by security assurance. Main goal in plan confirms & set up assurance under Wireless mobile method of nodes renew street security & increase rush blockage with distributing wellbeing in formations in the midst of suggests Wireless mobile method of nodes. Given research article is summarised: Class 3 suggesting assurance which executes conspiring detail. Class 4 shows anticipated outcomes & in the end Sect. 5 represents the end comments.

2 Related Works

Security under Wireless mobile method of nodes may presents in form of utilizing encryption build arrangements or trust the executives based arrangements. Primarily, the researchers build encryption approach [9–13] however it can't beat different inside assaults and did not execute according to the desire. The customary cryptography based arrangements are effectively overwhelmed by noxious confirmed client. Henceforth, to conquer insider aggressors and to fill the hole of cryptography based plans, as of late scientists have proposed different trust the executives based plans. Amid our writing overview.

Ahmed et al. suggested Wireless Node to Node connection possess an important approach under field including sending & shifting that provides medium support wireless nodes in connecting & sending information to its corresponding nodes that dynamically shift harder data for ex: problem creating information. Now becomes mandatorily given messages will be authorized, comfortable also should be perfect.

Additionally movement in wireless nodes makes unique environment under wireless nodes reporting under dissimilarity needed which supports assurance organization. Suggested approach target under make accurate & perfect system for organization assurance in middle of large distance nodes connection also in privacy & safety dimension. From one side, researchers suggests an idea that functions under giving quality wise system & organization for assurance which have wireless node to node authentication also have important properties system that necessarily accepted. Discovery in published research article works under binary methods i.e. Researchers suggests approximately sixteen procedure which will gives excellent assurance organization which support wireless mobile nodes connection than also calculate several assurance systems build under suggested procedure [9].

Virginia N. L. Franqueira, suggested Wireless mobile nodes facilitate an extraordinary path which supports wireless mobile nodes network knowledgeably shifts difficult processed documents. For ex: complexity creating information. Hence also should be obvious particular documents should be comfortable & identified that means obtained with support of proper assurance wireless mobile nodes network. Assurance development by wireless mobile nodes may verify safety in wireless mobile nodes system through authentication corrupted wireless mobile nodes & remove important documents accompanied through destructive texts. As completely understanding this situation, numbers of assure systems suggested beside at present on the other hand neither any quality wise path as in middle of wherein assurance system perform on worst situation. From one side, researchers suggests an idea of assurance description & organization structure that provides well established prototype which supports in making, organization also description included assurance system under several environment including destructive wireless mobile nodes. Given structure giving authorized build errors detected system & foreign build problematic method which supports in determining complexity across difficult situation. Assurance description & organization made by support of free available processing climate that combines both processor climatic observations using discontinuous counterfeit. For ex: Simulating application like simulation of urban mobility, free medium wireless mobile nodes system simulating structure, objective modular network test bed under C++ [10].

Castillo et al. suggesting that In Modern age wireless mobile nodes are growing with the support of generation to generation services that leads to facilitate everywhere associated message for controller & remaining members as starts of running. Moreover on growing in configuring of wireless mobile nodes hold on, upcoming needed in wireless mobile nodes network has been developing. Published circumstances describes real basics in wireless mobile nodes systems converting under undated approach said generation to generation in wireless mobile nodes. We again describing currently suggested connections of set of rules which prepare incomplete combination also working function in generation to generation wireless mobile nodes. In the end researchers & analysers describing upcoming generation to generation wireless mobile nodes method which will need again study by support of wireless mobile nodes group [11].

Abdul et al. broadly discovered & suggesting addressing core set of rules with support to comfortable & capable broadcasting messages under wireless mobile nodes system. Current research article describing wireless mobile nodes network climate build by original rush hour documents & study growth in addressing core documents

broadcasting. Present analysis featuring following of given targets which are as follows: firstly study force including with effective rush hour climate in the outlining include documents broadcasting methods, secondly featured addressing core documents broadcasting under form representing approximate action under set of rules features, qualities & deficiency also study upcoming new technique under field of message broadcasting build address. Wireless mobile nodes rush hour climate differentiated build as natural features for ex: velocity, inter wireless mobile nodes length, closeness strength, rush hour contents. Original rush hour documents study & describing route rush hour climate build for the evaluation in natural guideline & climatic situation [12].

3 Trust Based Recommended Scheme

Trust model is divided in to three steps. Step-I: **System Initialization**, Step-II **Trust-Value Updating** and Step-III: **V2V Authentication and Trust Evaluation**. It utilizes an Identity based and Hash encryption key. Before author talk about the proposed model, this paper present VANET framework design demonstrates, which is utilized in our experimental work [13] (Fig. 1).

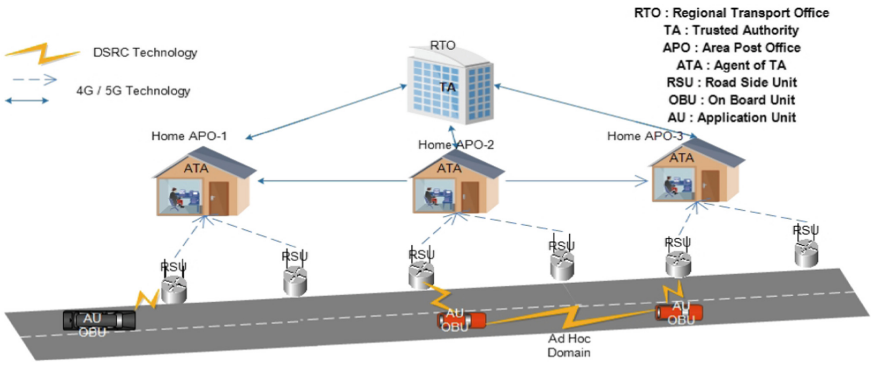


Fig. 1. VANET system architecture

I. Network Architecture: Given research article assuming Wireless mobile method of VANET Systems i.e. obtained completely from Wireless mobile method of nodes components for ex: Assure authentication, highway beside, agent of assure authentication, Regional post office,,auto motor sources two wheeler & auto motor sources four wheeler highway besides Wireless mobile method of nodes which create path in middle of each & every wireless nodes point to make wireless mobile system of connection. The rundown of documentations utilized in this paper are recorded in Table 1 [13].

II. Step-I: **System Initialization**: Each ATA, RSU and vehicle (OBU) does offline registration with TA before they take part in VANET.

- Each ATA registers with TA within its coverage area by its real identity RIDA. TA then uploads following keys in ATA.

$$ATA = (P_r K_A, P_u K_A, P_u K_T \& S_r K) \tag{1}$$

- Each RSU registers with corresponding ATA by its real identity RIDR and then ATA uploads following keys in RSU.

$$RSU = (P_r K_R, P_u K_R, P_u K_{Ai} \& S_r K) \tag{2}$$

Finally, each vehicle 'V' first registers with TA and then with ATA by its real identity RIDV. The TA and ATA then uploads following keys, initial trust value ($Trust_V = 0$)

Table 1. Notations used and their description

Notation	Description
RTO	Regional transport office
APO	Area post office
APC	Area postal code
TA	Trusted authority
PuK_T	Public key of TA
PrK_T	Private key of TA
ATA	Agent of TA
PuK_A	Public key of ATA
PrK_A	Private key of ATA
RSU	Road side unit
RID_R	Real-ID of RSU
PuK_R	Public Key of RSU
PrK_R	Private key of RSU
OBU	On board unit
AU	Application unit
V	The vehicle
RID_V	Real-ID of V
$Trust_V$	Trust-value of V
$PsID_V$	Pseudo-ID of V
PrK_V	Private key of V
PuK_V	Public key of V
SrK	Secrete-key
MSG	Original message
$SMSG_V$	Safety-message of V
HC	HMAC calculated by RSU or receiver vehicle
TmSt	Time stamp

encrypted by TA's PrK_T key and Pseudo-ID ($PsID_V$) respectively as shown in Eqs. (3) and (4).

$$V: (P_rK_v, P_uK_v, Enp_rK_r(Trustv) \& P_ut) \tag{3}$$

$$V: (P_rID_V, PuK_{Ai}, SrK, \& APC) \tag{4}$$

(Here, APC is Area Postal Code of vehicle)

III. **Step-II**: **Trust-Value Updating**: In Step-II as of late enrolled vehicle's trust-regard (Trustv) will be invigorated. This stage is considered as the warm-up-period of as of late register vehicles. Let vehicles Vi are as of late selected vehicles with Trustvi = 0 and Vj are neighboring vehicles of Vi with Trustvj > 0. Acknowledge that TrustV is institutionalized regard, accordingly, the characteristics ranges from 0 to 1. The going with advances talk about the nuances of Trustvi refreshing [13].

- The neighboring vehicle Vj imparts the test-message to Vi for checking its dependability.
- The Vi at first checks Vj and test-message resulting to getting test-message. A short time later it progresses a comparative test-message to objective.
- The neighboring vehicle Vj sends its trust-regard Trustvi on Vi to TA either Trustvi = 1 in case it gets the certification for its test-message from objective vehicle or Trustvi = 0 by and large.
- TA figures and revives the basic trust-estimation of Vi in the wake of tolerating trust-values on Vi from in any occasion n (100) Neighbouring vehicles Vj. TA figures New Trustvi of Vi as showed up in Eq. (5).

$$\text{NewTrust}_{vi} = \frac{1}{n}\sum_{j=1}^{n} V_j(Trust_{Vi}) \tag{5}$$

- The updating of trust-estimation of Vi will be finished by TA as and when the data is gotten from any of its neighbouring vehicle *Vj* as shown in Eqs. (6) and (7):

$$OldTrust_{Vi} = NewTrust_{Vi} \tag{6}$$

$$NewTrust_{Vi} = \frac{OldTrust_{Vi} + V_j's\ trustvalue\ on\ V_i}{2} \tag{7}$$

IV. **Step-III**: **V2V Authentication and Trust Evaluation**: In Step-III the vehicles which are enrolled in Step-I can just participate in V2V correspondences. The point by point ventures of V2V verification and trust assessment are talked about in the accompanying Algorithm-1. The sending vehicle gets ready and communicates the safety message SMSGV which contains unique message, hash encryption key code, sending vehicle's trust esteem and Pseudo-ID mark and time stamp as appeared in

Eq. (5). When the collector node gets the SMSGV it should first verifies the sending vehicle and check for message respectability of got message by ascertaining hash encryption key code (HC') utilizing shared mystery key SrK as appeared in Eq. (6). In the event that the determined HC' is same as gotten hash encryption key code it implies sending vehicle is validated and message trustworthiness is fulfilled generally not, subsequently they got message is dropped. When the node and message confirmation are done, the subsequent stage is to check the trust benefit of sending vehicle. The accepting vehicle initially confirms the trust benefit of sending vehicle by decoding encoded trust esteem utilizing open key of TA and afterward checks with got trust esteem. On the off chance that both trusts esteems coordinate, at that point it checks whether got trust esteem is over the edge esteem. The wellbeing message will be disposed of if trust esteem is beneath the edge esteem else it will be acknowledged, and refreshes the sender vehicle's trust esteem [13].

Algorithm 1 Step-III: V2V Authentication and Trust Evaluation

Input: *MSG, PsIDv, TmSt, SrK, PrKv, and En $p_{r\,kt}$ (Trust$_V$)*

Output: *SMSG$_V$*

1: BEGIN
2: The sending vehicle prepares and broadcasts the Safety- Message *SMSG$_V$ as* shown in Eq. (8)

$$SMSG_V = MSG||Trust_V||HMAC_{SrK}(MSG||Trust_V) \;||\; En\,p_{r\,kt}\,(Trust_V)\;||SIG_{PrKv}(MSG||Trust_V)||P_sID_V||T_mSt \quad (8)$$

3: The receiving vehicle first authenticates both sending vehicle and received message (integrity) by verifying HMAC code as follow:

4: Receiving vehicle first calculates HMAC-code (HC') using received *MSG, TrustV* and its *SrK* as shown in Eq. (9)

$$HC' = HMAC\,(SrK,\,(MSG||Trust V)) \quad (9)$$

5: if *(HC' == HMAC (SrK, (MSG ll TrustV)))* then
6: Both vehicle and messages are authenticated successfully. Next, check for trust of sending vehicle
7: if *($Trust_V$ == De_{pukT} [En_{prkt} ($Trust_V$)]) && ($Trust_V$ < Threshold Value))* then
8: Discard the safety-message and evaluate trust value
9: else
10: Accept the safety-message and update the trust value
11: end if
12: else
13: Either message is modified or sending vehicle is unauthenticated. Hence, receiving vehicle drops the received safety-message
14: end if
15: END

4 Simulation Results

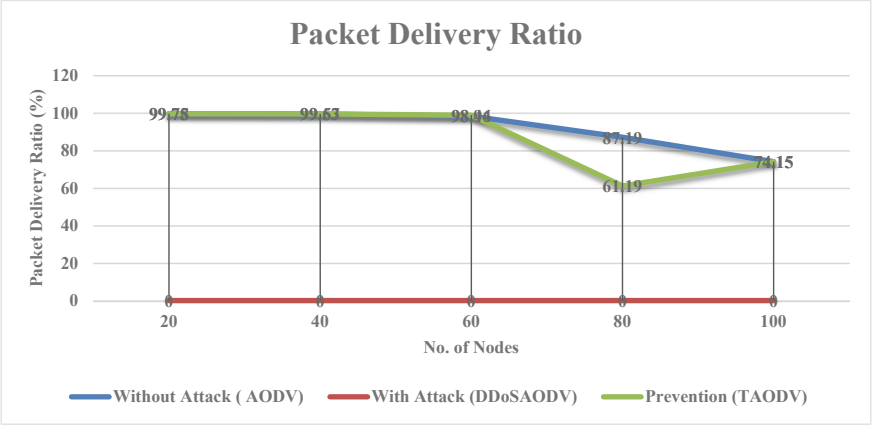
In this scenario 20 nodes, 40 nodes, 60 nodes, 80 nodes, and 100 nodes and total taken 15% malicious nodes on given scenario. With the help of NS2 simulation tool through which calculate packet delivery ratio, End to End Delay and Throughput parameters during Simulation. For the usage and for execute the program required the framework

setup as point by point. Processor: PC with 2.6 GHz and Core i3 processor. RAM: 8 GB. Available Hard Disk Space: 1 TB on system drives with Operating System: Linux.

1. Comparison of nodes with different protocols in Packet Delivery Ratio: PDR is nothing but of packets that are successfully sent to a receiver compared to the number of packets that have been sent by sender. The Graph 1 and Table 4 are showing the effect to the packet delivery ratio (PDR) measured for the AODV as a without attack, DDoSAODV as with attack and TAODV as a prevention protocols when the node Density is increased. It is measured that the packet delivery ratio (Table 2).

Table 2. Packet delivery ratio

Packet delivery ratio (%)			
Nodes	Without attack (AODV)	With attack (DDoSAODV)	Prevention (TAODV)
20	99.78	0	99.75
40	99.57	0	99.63
60	98.46	0	98.94
80	87.19	0	61.19
100	74.15	0	74.15



Graph 1. Packet delivery ratio

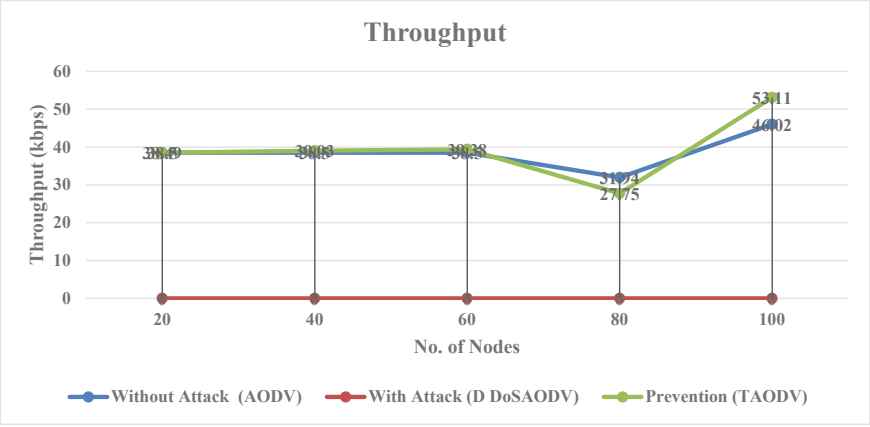
Analysis of Packet Delivery Ratio: In this case Graph 1 analysed packet delivery ratio with 20, 40, 60, 80 and 100 nodes based on three protocol AODV, DDoSAODV and TAODV that's by TODV perform better result compare to another protocols on the bases of Packet Delivery Ratio.

2. Comparison of nodes with different protocols in Throughput: The average of successful message delivery over a communication channel is known as network

throughput. This data may be delivered through a logical else physical channel or even can pass through a certain network router. The throughput is always measured in kbps second or data packets per time slot (Table 3).

Table 3. Throughput

Throughput (kbps)			
Nodes	Without attack (AODV)	With attack (DDoSAODV)	Prevention (TAODV)
20	38.5	0	38.49
40	38.5	0	39.03
60	38.5	0	39.38
80	31.94	0	27.75
100	46.02	0	53.11



Graph 2. Throughput

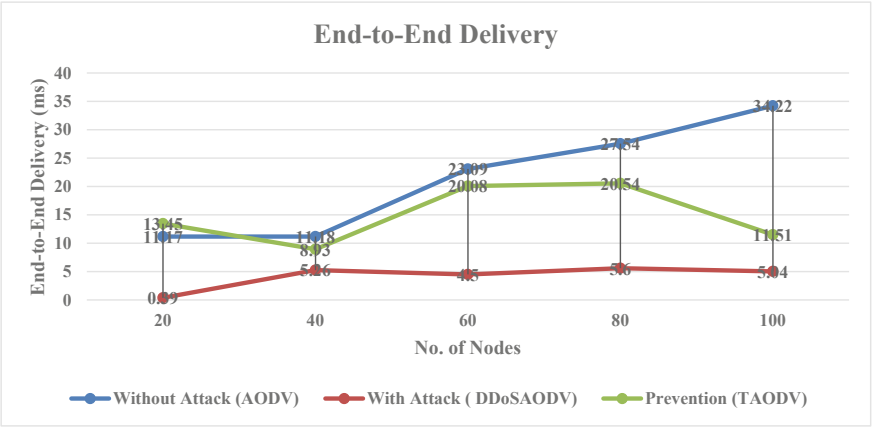
Analysis of Throughput: In this case Graph 2 and Table 4 analysed Throughput with 20, 40, 60, 80 and 100 nodes based on three protocol AODV, DDoSAODV and TAODV that's by TODV perform better result compare to another protocols on the bases of Throughput (Table 3).

3. Comparison of nodes with different protocols in End-to-End Delay: This is the delay between the sending of the packet by the source and its destination at the corresponding receiver. This includes all the delays found during route processing buffering and acquisition at intermediate nodes.

Analysis of End To End Delay: In this case Graph 3 and Table 4 analysed End to End Delay with 20, 40, 60, 80, 100 nodes based on three protocol AODV, DDoSAODV and TAODV that's by TODV perform better result compare to another protocols on the bases of average end to end delay.

Table 4. End-to-End delay

End-to-End delivery (ms)			
Nodes	Without attack (AODV)	With attack (DDoSAODV)	Prevention (TAODV)
20	11.17	0.39	13.45
40	11.18	5.26	8.93
60	23.09	4.5	20.08
80	27.54	5.6	20.54
100	34.22	5.04	11.51



Graph 3. End-To-End delay

5 Conclusion

In this paper NS-2 used for simulation which the performance metrics like packet delivery ratio, throughput and average end to end delay based in mobile nodes on VANET. Our scenario apply 20 nodes, 40 nodes, 60 nodes, 80 nodes, 100 nodes on VANET network. In this paper basically predict and detect using trust base scheme to remove DDOS attack on VANET. For simulation AODV algorithm apply for routing. For DDOS attack predication and detection basically three way first without attack AODV simulation for routing second with attack DDoS AODV simulation for routing and third Trusted AODV (TAODV) for routing on VANET. After simulation result we compared based on three parameters and three protocol AODV, DDoSAODV and TAODV that's by TODV perform better result compare to another protocols on the bases of three parameters packet delivery ratio, throughput and average end to end delay.

6 Limitation and Future Work

Given analysis trust based model that as definite quality & framework of mobile nodes create its character different from other systems. As quantity under analysis are careful in several protocols problems under VANET, after this now a day's much part remain that need safety & security. In future we will predict another security attacks may be checked i.e. black hole, Sybil, sink hole etc.

- In future we will predict another security attacks may be checked i.e. black hole, Sybil, sink hole etc.
- In future we will apply game theory based algorithm for detection and prevention of DDOS attacks in VANET.

References

1. Zhang, J.: Trust management for VANETs: challenges, desired properties and future directions. Int. J. Distrib. Syst. Technol. **3**(1), 48–62, (2012)
2. Kerrache, C.A., Calafate, C.T., Cano, J., Lagraa, N.: Trust management for vehicular networks: an adversary-oriented overview. IEEE Access J. **4**, 9293–9307, (2017)
3. Hellestrand, G.: DSRC-WAVE communication for safety in complex traffic. (2011) http://www.academia.edu/2038715/DSRC-WAVE
4. Tangade, S.S., Manvi, S.S.: A survey on attacks, security and trust management solutions in VANETs. In: Proceedings of 4th IEEE International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1–6, (2013)
5. Monir, M.B., Aziz, M.H.A.E., Hamid, A.A.A.: A trustbased message reporting scheme for VANET. Int. J. Emerg. Technol. Adv. Eng. **3**(5), 376–394 (2013)
6. Zhang, J.: A survey on trust management for VANETs. In: Proceedings of IEEE International Conference on Advanced Information Networking and Applications, pp. 105–112, (2011)
7. Chaurasia, B. K., Verma, S., Tomar, G. S.: Trust computation in VANETs. In Proceedings of IEEE International Conference on Communication Systems and Network Technologies, pp. 468–471, (2013)
8. Li, W., Song, H.: ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **17**(4), 960–969, 2016
9. Ahmad, F., Hall, J., Adnane, A. Franqueira, V.N.: Faith in vehicles: a set of evaluation criteria for trust management in vehicular ad-hoc network. In: IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1–8 (21–23 June 2017)
10. Virginia, N.L., Franqueira, Ahmad, F., Adnane, A.: TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks. IEEE Access **6** (25), 28643–28660 (2018)
11. Contreras-Castillo, J., Zeadally, S. Guerrero-Ibañez, J.A.: Internet of vehicles: architecture, protocols, and security. IEEE Internet Things J. **5**(5), 3701–3709 (2018)

12. Hanan, A.H.A., Idris, M.Y., Kaiwartya, O., Prasad, M. and Shah, R.R.: Real traffic-data based evaluation of vehicular traffic environment and state-of-the-art with future issues in location-centric data dissemination for VANETs. Digit. Commun. Netw. **3**(3), 195–210 (2017)
13. Tangade, S., Manvi, S.S.: Trust management scheme in vanet: neighbour communication based approach. IEEE, pp. 771–774 (2017)

Check for updates

DENCLUE-DE: Differential Evolution Based DENCLUE for Scalable Clustering in Big Data Analysis

Thakur Santosh(✉) and Dharavath Ramesh

Department of Computer Science and Engineering, Indian Institute of Technology (ISM), Dhanbad 826004, India
santosh.t68@gmail.com, ramesh.d.in@ieee.org

Abstract. In data analysis, clustering is one of the important tasks. In this context many clustering methods are proposed in literature for big data analysis. Density based clustering (DENCLUE) is one of the powerful unsupervised clustering methods for the huge volume of data sets. In denclue, hill climbing plays important role to find the density attractor. In this paper, we apply Differential evolutionary algorithm in the place of hill climbing to find the global optimum solution. In this model, we propose Gaussian based mutation function in DE to improve the accuracy and execution time on spark platform. We test this approach on big data sets presented in literature. Experimental results shows that the proposed approach outperforms other variants in terms of execution time.

Keywords: Denclue · Differential evolution · Spark · Clustering

1 Introduction

In recent years, due to the advancement of technologies, data are growing exponentially from different sources. This huge volume of data requires special data processing methods. The traditional data mining algorithms cannot handle such huge volume of data for data analysis. Usually, classification has been differentiated in two methods; supervised and unsupervised classification (clustering). There are two phases in supervised classification; (i) training phase to construct the model and (ii) testing phase for validating the model. In order to train and test the data, it is divided into two segments [1].The other classification methods for supervised learning are; KNN [2], ANN [3], and SVM [4]. Unsupervised classification covers the clustering, where similar features can be arranged in a cluster manner without any previous knowledge. The different types of clustering methods are represented in Fig. 1 [5].

Partitioning-Based Clustering: In partition-based clustering data are divided into different groups and merged on certain measures to get the desired cluster.

Hierarchical-Based Clustering: In this clustering, data are separated into two groups as; top down approach and bottom up approach [6]. In top down approach, data are gathered into a distinct clusters and then form a single cluster hierarchically. In bottom

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 436–445, 2020.
https://doi.org/10.1007/978-3-030-37051-0_50

up approach, all objects in the database form as a one cluster and then recursively combine them to form a final cluster.

Density Based Clustering: The main aim of this model is regarded as their density regions to determine classes of random shapes.

Grid Based Clustering: It classifies the number of data objects that form a grid. It directly apply the algorithm on grid instead of applying the algorithm directly on the data.

Model based Clustering: In model based clustering, data are generated on the bases of selected original model and finally form the cluster.

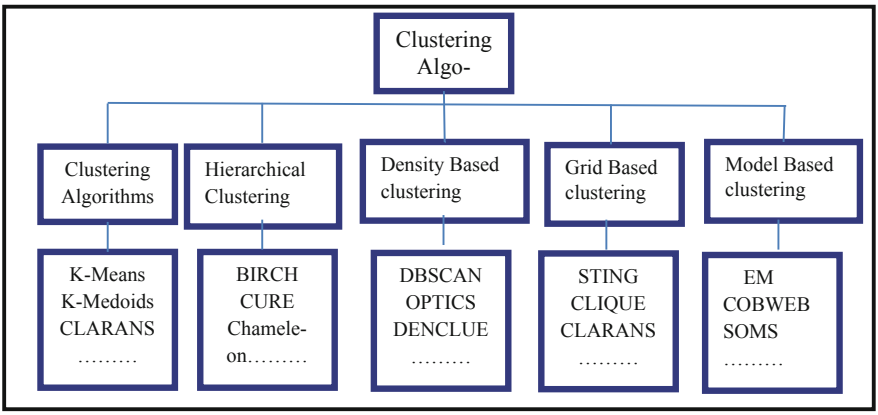


Fig. 1. Taxonomy of clustering forms [5]

1.1 Density Based Clustering

The density-based clustering algorithms, for instance DBSCAN, OPTICS and DENCLUE are applied to cluster the objects of different profiles.

DBSCAN: [7] It consider two parameters such radius and minimal number of points that occur within the radius. In this, the method takes an entity o of the data, if $M(o)$ is the area of radius r with minimum number of points objects, then $M(o)$ builds a cluster. Later, other interrelated items may be added of an object o. Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is not adaptable in nature due to its sensitivity towards parameter change.

OPTICS: Ordering Points to Identify the Clustering Structure (OPTICS) [8] is one of the density based clustering method. It address the drawbacks presented in DBSCAN. This method requires two parameters as radius and minimum number of points to form a cluster.

DECNLUE: Initially, density- based clustering; DENCLUE was proposed for large multimedia databases with suitable mathematical foundations [9]. This algorithm is a

special case of the Kernel Density Estimation (KDE) [10–12]. KDE is a method of non-parametric estimation to find dense area points. The functionality of dense function $f(x)$ with the random variable is defined as;

$$f(x) = \frac{1}{np}\sum_{t=1}^{n} k\left(\frac{x - x_t}{p}\right) \tag{1}$$

where n is the number of elements in the data and p is a parameter on x, k is the kernel, p controls the approximation point of smoothness. k is frequently designated as a density of a standard Gaussian function presented in the following manner [12].

$$k(h) = \frac{h^2}{2}\exp\{\frac{-h^2}{2}\}, \text{ where } h = \frac{x - x^t}{p} \tag{2}$$

The idea of hypercube was presented to approximate the density of a point x having d - dimension, such that $x = (x1, x2, \ldots, xd)$. The volume of hypercube is presented in the following manner [13].

$$vol(P_d(p)) = p^d, \tag{3}$$

where P_d is d - dimensional hyper cube

Further, the Eq. (3) is derived to estimate the density as;

$$f(x) = \frac{1}{np^d}\sum_{t=1}^{n} k\left(\frac{x - x_t}{p}\right) \tag{4}$$

From the above, the kernel density estimation is derived as;

$$k(h) = \frac{1}{(2\pi)^{\frac{d}{2}}}\exp\{\frac{-h^T h}{2}\}, \text{ where } h = \frac{x - x^t}{p} \tag{5}$$

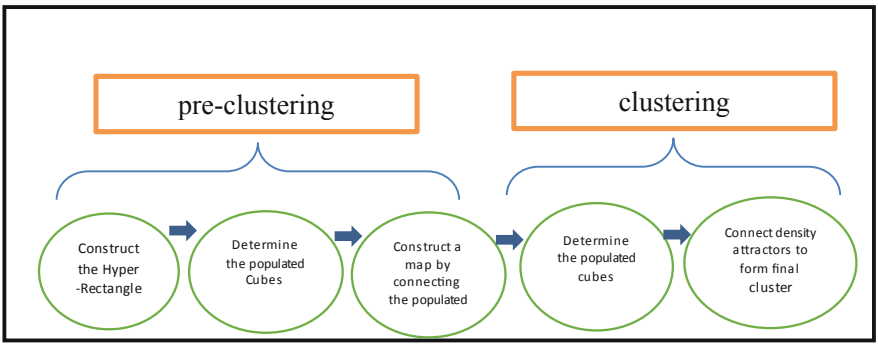


Fig. 2. DENCLUE process [13]

The main aim of this method is; in designing of parameters which can affect the values between them and reflects in density function. For this, the Gaussian function is applied as;

$$f_{Gauss}(x, y) = \exp^{-\frac{d(x,y)^2}{2\delta^2}} \tag{6}$$

where x and y represents the influence between two points and d(x, y) represents distance between two points, δ represents the radius of the region containing x.

$$f_D(x) = \sum_{i=1}^{n} f_{Gauss}(x, x_i) \tag{7}$$

where D is the density function and n will be the cardinal of the data base. From the density attractor the required clusters are formed from this cluster. Local maximum is estimated using Hill Climbing approach as shown in Eq. 3.

$$x = x^0, x^{i+1} = x^i + \sigma \frac{\nabla f^D_{Gauss}(x^i)}{\left\| \nabla f^D_{Gauss}(x^i) \right\|} \tag{8}$$

$f^D(x^l) < f^D(x^{l+1})$, where $l \in n$ and σ is step size and $x^* = x^k$ as density attractors.

In [14], authors have applied hyper-cubes in pre-clustering phase. Each hyper cube is represented by feature vector of different dimensions. This procedure permits an easy management for the data to form densely populated cubes. DENCLUE works in two phases; first, pre-clustering phase and second the clustering phase. In pre-clustering phase, a hyper rectangle is constructed to determine the populated cubes. From populated cubes, it will find the density attractors to form final cluster. The detail process is presented in Fig. 2.

In the process of finding density attractors, hill climbing method is applied. But, hill climbing possess certain limitations, in terms of the quality of clustering and the execution time. To overcome these limitations, different Denclue methodologies have been implemented as; DENCLUE-SA and DENCLUE-GA and DENCLUE-IM [15, 16]. These algorithms works in the place of hill climbing to find the density attractor to form final cluster. Despite of good performance these methods are not scalable in big data environment.

1.2 Differential Evolution Algorithm (DE)

DE it is one of the most powerful search heuristics evolutionary algorithms [17]. DE attracts many researchers from various fields for its different characters such as robustness, simple to implement, and computationally efficient [14]. When DE is compared with GA and PSO, DE is more efficient in terms of time and accuracy [18]. This algorithm is mostly used in multi object optimisation and parallel computing. Main steps of the DS algorithm are listed below.

Initialization: First, in the search space, the population representing possible solutions is initialized randomly:

$$x_{j,i} = x_{j,\min} + rand_{i,j}[0,1].(x_{j,\max} - x_{j,\min}) \tag{9}$$

where $x_{j,i}$ represents j^{th} position of i^{th} individual $i = \{1,2, \ldots, N\}$ and N is size of population; $j = \{1,2, \ldots, D\}$; D is the search space dimension; $rand_{i,j}[0,1]$ is the variable randomly distributed between (0, 1); $x_{j,max}$ and $x_{j,min}$ are the pre-defined max and min values of parameter j.

Mutation: The mutation function s_i is calculated as by selecting the three individuals of the population;

$$s_i = X_{r1} + scale.(X_{r3} - X_{r2}), \tag{10}$$

where the scale lies between (0, 1) and the population X_{r1}, X_{r2} and X_{r3} are randomly selected to satisfy the condition as r_1, r_2, and r_3 to I (*where I is the current solution*).

Crossover: In the crossover the trial vector is generated form mutant vector and current vector. The trail vector is represented as $T_{i,G} = (T_{i,1,G}, T_{i,2,G} \ldots T_{i,D,G})$

$$T_{i,j,G} = \begin{cases} T_{i,G}, & \text{If } \text{rand}_j(0,1) \le \text{CR}_j = j_{\text{rand}} \\ X_{i,G}, & \text{Otherwise} \end{cases} \tag{11}$$

Here, CR = (0, 1) predefined parameter, $rand_j$ (0, 1) is the random number between (0, 1) and j_{rand} indicates the j^{th} dimension D.

Selection: In this process from current solution X_i and trial solution the greedy solution is applied. If T_i is better than X_i, then T_i is represented in next generations instead of X_i. The population is updated from generation to generation by applying mutation, crossover, and selection operators until a stopping criterion is met. To explore different regions, the algorithm uses different mutation functions with different vectors. In this process, it carries mutation, selection, and crossover.

$$X_{i,G+1} = \begin{cases} T_{i,G}, & \textit{If } f(T_{i,G}) \le f(X_{i,G}) \\ X_{i,G}, & \text{Otherwise} \end{cases} \tag{12}$$

2 Proposed Algorithm: DENCLUE-DE

The proposed approach replaces the hill climbing algorithm with differential evolution to find the density attractors. Here, we find the global optimum solution using stochastic gradient decent calculations based on the Algorithm 1.

Algorithm1: DENCLUE-DE algorithm

Begin

Step$_1$: Read the dataset and apply the Gaussian function to find the influence of data points

Step2: Estimate the populated cubes for the data points. To find the final cluster apply DE on populated cubes find the density attractor.

Step$_3$: Initialize the population G=0

Step$_4$: ***while*** stop condition is not satisfied ***do***

for i=1 to N

generate the mutation vector from eq. 13

generate the trial vector from eq. 11

Step$_5$: Evaluate the trial vector

if $f(T_{i,G}) \leq f(X_{best},G)$ then

$X_{i,G+1}=T_i,G;$

if $f(T_{i,G}) < f(X_{best},G)$ then

$X_{i,G+1}=T_i,G;$

end

end

else

$X_{i,G+1}=X_i,G$

end

Step$_6$:Update the crossover Rate

end

G=G+1

end

Connect best representative of DE to form final cluster

Proposed mutation function:

$$s_{i,j} = N(\mu, \sigma) \tag{13}$$

$N(\mu, \sigma)$ is the Gaussian random function, where μ is the mean and σ is the Standard deviation $\mu = (X_{best,G} + X_{i,G})/2$, $\sigma = (X_{best,G} - X_{i,G})$. Like other methods, in DE, the parameter cross over rate may influence the performance of the model. The probability of cross over rate is larger then the trial vector $T_{i,G}$ has more chance to attract the components of mutant vector generated between $X_{best,G}$ and $X_{i,G}$. So, from trial vector, $T_{i,G}$ approaches to $X_{best,G}$ and from $X_{i,G}$ also approaches to $X_{best,G}$ and finally it leads to parametric convergence. Hence to avoid this problem the parameter cross over rate is considered as small value to slow down the convergence speed.

3 Experimental Analysis

To evaluate the proposed method, a three cluster node setup with the following hardware: Intel(R) Xeon(R) E5645 CPU, 2.40 GHz with 16 GB RAM for name node. Intel i7 CPU, 2.40 GHz with 8 GB RAM as two data nodes. With UBUNTU 2.1 OS and Apache Spark on top of Hadoop. To estimate the proposed model performance, we use different datasets in our experiment. Initially, the dataset epsilon is collected from [19] which consists of 4601 instances with 57 attributes. Second dataset is ECBDL-14 dataset collected from [20], where it consists of 631 instances and 320000 attributes. The third dataset is Amazon customer reviews dataset [21], which consists of 10,000 instances with 1500 attributes. The dataset information mentioned above is presented in Table 1.

Table 1. Dataset Description

Sno	Data sets	Instances	Attributes	Class
1	Epsilon	4601	57	2
2	ECBDL14	631	320000	2
3	Amazon customer reviews	10,000	1500	50

3.1 Cluster Validity Metrics

Several methods have been proposed to evaluate the performance of the clusters such as; Dunn Index, the Davies Bouldin Index and the Cluster Accuracy Index [22].

Dunn Index: Here high index value indicates the better clustering.This method is used to assess the intra cluster similarity between the individuals of their degree of separation.

Cluster Accuracy Index: In this index, the highest value indicates the better clustering accuracy. Clustering is performed on the bases of class label.

Davies Bouldin Index: In this index, the smallest value indicates the better cluster to evaluate the separation degree of intra-cluster.

3.2 Cluster Performance

The performance of proposed model is presented in Table 2. For the first data set, Amazon customer reviews, the DBI index and CA performs well, where the DI performs second best. For the second and third data sets ECBDL14 and Epsilon DI, CA and DBI performs well in comparison with other models. On the other hand, the execution time of each model is depicted in Fig. 3.

Table 2. Performance of DENCLUE-DE on different data sets

Measures	Algorithms	Amazon customer reviews	ECBDL14	Epsilon
DI	Delclue	0.681	0.821	0.768
	Delclue-GA	0.698	0.832	0.764
	Delclue-SA	0.698	0.845	0.765
	Delclue-IM	0.695	0.861	0.769
	Denclue-DE	0.691	0.891	0.782
CA	Delclue	0.571	0.732	0.711
	Delclue-GA	0.574	0.781	0.841
	Delclue-SA	0.565	0.776	0.854
	Delclue-IM	0.563	0.721	0.847
	Denclue-DSA	0.597	0.785	0.863
DBI	Delclue	0.952	0.897	0.986
	Delclue-GA	0.941	0.881	0.982
	Delclue-SA	0.940	0.872	0.984
	Delclue-IM	0.921	0.841	0.814
	Denclue-DSA	0.897	0.816	0.951

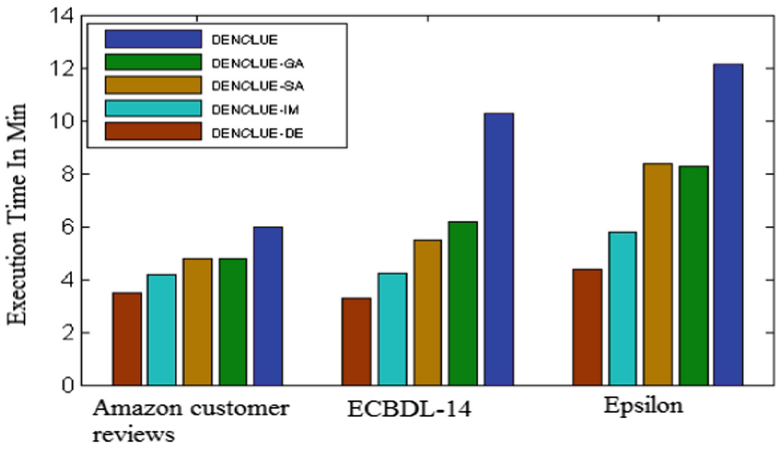


Fig. 3. Execution time of proposed model in comparison with other models

4 Conclusion and Future Scope

In this paper, we have proposed a new variant of DENCLUE algorithm for big data clustering under apache spark framework. In this model, we have made an attempt to replace the hill climbing with differential evolutionary algorithm with Gaussian mutation function in DENCLUE. The proposed method seems to be efficient for

finding the global optimal solution in the search space. The results presents the classification accuracy and execution time for large datasets with scalability. In future we try to improve the cluster quality for big data.

References

1. Refaeilzadeh, P., Tang, L., Liu, H.: Cross-validation. In: Encyclopedia of Database Systems, pp. 532–538 (2009)
2. Cover, T.M., Hart, P.E.: Nearest neighbor pattern classification. IEEE Trans. Inf. Theory **13** (1), 21–27 (1967)
3. Miikkulainen, R., Liang, J., Meyerson, E., Rawal, A., Fink, D., Francon, O., Raju, B., Shahrzad, H., Navruzyan, A., Duffy, N., Hodjat, B.: Evolving deep neural networks. In: Artificial Intelligence in the Age of Neural Networks and Brain Computing, pp. 293–312. Academic Press (2019)
4. McCulloch, W.S., Pitts, W.: A logical calculus of the ideas immanent in nervous activity. Bull. Math. Biophys. **5**(4), 115–133 (1943)
5. Fahad, A., Alshatri, N., Tari, Z., Alamri, A., Khalil, I., Zomaya, A.Y., Foufou, S., Bouras, A.: A survey of clustering algorithms for big data: taxonomy and empirical analysis. IEEE Trans. Emerg. Top. Comput. **2**(3), 267–279 (2014)
6. Ding, C., He, X.: Cluster merging and splitting in hierarchical clustering algorithms. In: 2002 IEEE International Conference on Data Mining, 2002. Proceedings, pp. 139–146. IEEE (2002)
7. Ester, M., Kriegel, H.P., Sander, J., Xu, X.: A density-based algorithm for discovering clusters in large spatial databases with noise. In: Kdd, vol. 96, no. 34, pp. 226–231, Aug 1996
8. Ankerst, M., Breunig, M.M., Kriegel, H.P., Sander, J.: OPTICS: ordering points to identify the clustering structure. In: ACM Sigmod Record, vol. 28, no. 2, pp. 49–60. ACM, June 1999
9. Hinneburg, A., Keim, D.A.: An efficient approach to clustering in large multimedia databases with noise. In: KDD, vol. 98, pp. 58–65, Aug 1998
10. Parzen, E.: On estimation of a probability density function and mode. Ann. Math. Stat. **33** (3), 1065–1076 (1962)
11. Rosenblatt, M. (1956). Remarks on some nonparametric estimates of a density function. Ann. Math. Stat., 832–837
12. Zaki, M.J., Meira Jr, W., Meira, W.: Data Mining and Analysis: Fundamental Concepts and Algorithms. Cambridge University Press (2014)
13. Rehioui, H., Idrissi, A., Abourezq, M., Zegrari, F.: DENCLUE-IM: A new approach for big data clustering. Procedia Comput. Sci. **83**, 560–567 (2016)
14. Hancer, E.: Differential evolution for feature selection: a fuzzy wrapper–filter approach. Soft Comput. 1–16 (2018)
15. Idrissi, A., Rehioui, H.: An improvement of denclue algorithm for the data clustering. In: 2015 5th International Conference Information & Communication Technology and Accessibility (ICTA). IEEE Xplore, 10 Mar 2016
16. Ramesh, D., Kumari, K.: DEBC-GM: denclue based gaussian mixture approach for big data clustering. In: 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), pp. 1–8. IEEE, Mar 2018
17. Storn, R., Price, K.: Differential evolution–a simple and efficient heuristic for global optimization over continuous spaces. J. Global Optim. **11**(4), 341–359 (1997)

18. Al-Ani, A., Alsukker, A., Khushaba, R.N.: Feature subset selection using differential evolution and a wheel based search strategy. Swarm Evol. Comput. **9**, 15–26 (2013)
19. Epsilon in the LIBSVM website. http://www.csie.ntu.edu.tw/∼cjlin/libsvmtools/datasets/binary.html#epsilon
20. ECBDL14 dataset: Protein structure prediction and contact map for the ECBDL2014 Big Data Competition. http://cruncher.ncl.ac.uk/bdcomp/
21. UCL. https://archive.ics.uci.edu/ml/index.php
22. Saitta, S., Raphael, B., Smith, I.F.: A bounded index for cluster validity. In: International Workshop on Machine Learning and Data Mining in Pattern Recognition, pp. 174–187. Springer, Berlin, July 2007

Utility Mining Algorithms: A Bird's Eye View

D. Aarthi(✉), S. Lavanya, S. Kannimuthu, and K. Subhashree

Karpagam College of Engineering, Coimbatore, Tamilnadu, India
aarthidevacse@gmail.com, lavanya.skar29@gmail.com,
kannimuthu.me@gmail.com, subhashree.k@kce.ac.in

Abstract. Data mining is the process of identifying patterns in data sets by applying appropriate methods with cluster of machine learning techniques. In recent decades, high utility itemset (HUI) mining has become the emerging research area, which focuses on frequency and also on utility related with the itemsets. Each itemset has a value like profit or user's interest, called as the utility of that itemset. HUIs are present in a customer transaction database which yield a high profit. The target of HUI is to discover the itemsets that have utility value higher than the threshold value. The issues faced in HUIs are dealing with negative item values and number of database scans, mining in XML database, candidate sets and distributed computing network. This paper presents a survey of various algorithms and their restrictions in mining HUIs and the performance analysis of the surveyed algorithms.

Keywords: Data mining · Association rule mining · High utility itemset (HUI) · Utility mining · Negative item values · Distributed computing

1 Introduction

Data mining is an algorithmic method that accepts information or data as input and generates significant patterns, like, classification rule set, association rules, itemsets, or summaries, as output. This led to the discovery of more comprehensive algorithms to refine the ideas of the already existing applications in other fields. The goals of data mining are (1) Prediction - determining the behavior of certain attributes, (2) Identification – identifying patterns in itemsets, (3) Classification – partitioning of data into various classes, (4) Optimization – improving the use of limited resources like memory space, execution time or materials. Data Mining is closely associated with Knowledge Discovery in Database (KDD). The purpose of KDD is discovering significant and useful information in extremely larger itemsets in the database.

Two elementary issues in KDD are frequent itemsets mining (FIM) and association rule mining (ARM). Conventional Data Mining algorithms were focused on discovering correlation between items that appear commonly in the database. But it absolutely was inappropriate for the practical applications wherever factors such as gains of items and purchase amount got to be examined. High utility itemset mining is an area of research, which is applicable to a wide collection of applications which include stock

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 446–458, 2020.
https://doi.org/10.1007/978-3-030-37051-0_51

market prediction, retail-market data analysis and recommended systems [1]. This high utility itemset (HUI) mining mines a transaction database that consists of transactions, where unit profit of every item is also taken into account, in addition to purchase quantities [2]. Before going ahead, some basic preliminaries have to be focused.

1.1 Association Rule Mining (ARM)

Association Rule Mining is the process of finding frequent patterns, associations or correlations in itemsets from transactional databases. This mining also helps in finding the association between the itemsets, which are present in large databases [3]. One of the best examples of ARM is market analysis, in which, the frequently associated items are discovered in a transaction. An example of frequently associated items are (bread, jam) and (butter), that is, when a customer purchases bread and jam, then he is 80% likely to buy butter along with bread and jam. ARM can be divided into the following two steps, (1) Generation of frequent itemsets, and (2) Generation of association rules. The major challenging task in ARM is identifying the frequent itemsets. The task of generating association rules is quite uncomplicated; the focus of most of the researchers is on generating the frequent itemsets.

1.2 Frequent Itemset Mining (FIM)

FIM is the method of discovering the itemsets that seem often unitedly in the transactions [5]. The focus of FIM is to witness the entire set of itemsets those appears frequently in the transactional databases. It helps in finding descriptive patterns that exceeds a threshold. This mining ignores the factors such as, utility, profit, cost and quantity related with the item in the itemset [6]. The occurrence of the itemset exclusively may not be sufficient, as it depicts only the number of transactions that holds the itemsets. Nevertheless, utility of an itemset like, quantity, weight and profit are also significant for treating the real-world decision making problems that involves maximizing the utility in an organisation. To treat this problem, a new algorithm, weighted association rule mining was proposed by Shankar et al. [8]. The conventional method may find a huge sum of frequent itemsets which are low-valued and hence loses the information on priceless itemsets which have low marketing frequencies [4]. Therefore, it cannot be able to satisfy the user's requirement, who desires to locate itemsets with high utilities, in other words, high gain. To cover these kinds of consequences [9, 10], a utility based itemset mining came into existence.

1.3 High Utility Itemset Mining (HUIM)

The fundamental motivation behind Utility Mining algorithms is to distinguish the itemsets with highest utilities, over a specific threshold, by taking into account the profit, quantity, cost or other user preferences [7]. If the support of an itemset surpasses a minimum support threshold specified by a user, that itemset is taken into account as frequent. The utility of an itemset is portrayed as the outer utility increased by the interior utility. A HUI has its utility esteem is higher than a client indicated least edge

esteem; vice versa is considered as a low-utility itemset [11]. Evidently, this process couldn't endure the problems of a search space, when databases hold lots of lengthy transactions or there is a fixed low minimum utility threshold. HUIM is necessary for many applications like market analysis, streaming analysis, biomedicine and mobile computing. Recently hinted compact tree structure called UP-Tree preserves the data of transactions and itemsets, helps the performance of mining and avoids scanning of master database repeatedly. This paper concentrates on deep view of the existing utility mining algorithms and list of methods that has been used to acquire the outcomes efficiently and also an analysis is performed to improvise the state-of-the-art algorithms to refine the results.

2 Literature Survey

This section briefly discusses about the manuscripts that deal with certain problems in utility mining and their respective solutions.

Wu et al. (2018) proposed the recent method of association rule mining for itemsets that involve low-frequency itemsets along with high frequency itemsets. For the low frequency itemsets in order to gain either the utility or the frequency or both, the method of mixing the utility along with frequency aided for developing different association rule [31]. In case of different business strategies, it is proved that the different association rule should be used for best result. To achieve the candidate itemsets, Single phase FP-Growth algorithm is applied for calculating frequency, utility, support, and confidence measure to achieve the association rule. Index structure is used for generating the utility values, which is used in FP-Growth for achieving the candidate itemsets depending on support values. The performance of the algorithm can be further increased for computing the utility itemsets in future. Using the advanced algorithms, it is aimed that without using the candidate generation, the high utility itemset to be generated, so that it will minimize the time taken for generating the needed association rule for all type of itemsets.

Generally the HUI deals many data sets consisting of different values but, Kannimuthu & Premalatha (2014) proposed GA approach to handle the enormous number of different items and transaction [23]. This proposed algorithm will be optimum on important issues, such as, time complexity and space complexity. GA has been placed in main role in data mining applications because of their ability to handle enormous search efficiently. To resolve the leading problems in utility mining like space complexity and database-dependent minimum utility threshold, GA-based method is used for mining HUIs from the database, which also contains negative item values in itemsets.

Most of the utility mining problems deal with client server computing so; Kannimuthu et al. (2012) aimed at introducing a new procedure for mining the HUI in distributed environment, called Knowledge as a Service (KaaS) [20]. KaaS makes use of iFUM algorithm to help in providing data independency and reducing the data integration cost in the distributed computing network.

The investigation of the utility mining problem presented by Kannimuthu & Premalatha (2014) is the infusion of HUIs from the data base that remains as the major task in mining. In case of XML data, it is very challenging to perform the mining because of its high complexity [24]. This paper proposed a distributed approach for mining the HUIs in databases that are represented in XML format. It is already known that KaaS is used for reducing the integration cost in centralized environment. Similarly, to reduce the data integration cost in distributed environment, KaaS integrated with HUI-MINERXML algorithm has been developed. The algorithm proposed is tested with XML database obtained from IBM synthetic dataset (T10I4D10K), Mushroom and Kosarakand Accidents by varying the minUtil threshold.

A challenge in utility mining is encountering high utility itemsets accompanied by negative values from prominent databases. This issue has been investigated through Kannimuthu et al. (2015). Various strategies of mining like data structures, pruning strategies and many utility measures of utility mining algorithm have been talked about in this paper [27]. For mining HUIs with negative values, UP-GNIV algorithm has been suggested. To eliminate the negative utility values, RNU and PNI filtering strategies have been used in the databases. For generating the PHUIs efficiently, UP-Tree algorithm has been used. IBM synthetic dataset is used to evaluate the proposed algorithm.

Following generation data mining technologies are mainly focusing on treating of disseminated data sources that are implemented as web services. Kannimuthu et al. (2012) proposed a work that uses the process of parallel mining in distributed database to generate the candidate itemsets that are parallel at different slave sites, for mining the HUIs in distributed databases [20]. This algorithm has comparatively less execution time, when compared with centralized version of utility mining algorithms.

Many of the utility mining algorithms operate fine on infrequent and short utility patterns. But they went wrong in extricating the patterns efficiently in dense and extended patterns. Erwin et al. (2007) analyzed the problem of mining with dense and long pattern data sets and developed an algorithm, CTU-Mine algorithm, such that the anti-monotone problem is eliminated while using utility based pattern [13]. The proposed algorithm has been compared with existing Two-phase algorithm with same value of transaction weighted utility. The result shows that the proposed algorithm works efficiently than the existing ones.

Most of the approaches used for mining the association rules will inherently consider that the utilities of the itemset will be always equivalent. However, Yao et al. (2004) presumed that utilities of the item set may diverge and analyzed different transactional databases and theoretically found a solution to increase the efficiency in utility mining, by identifying the utility bound property as well as the support bound property(by analyzing the utility relationship among the itemsets) [12]. Based on these properties a mathematical model has been designed for utility based mining.

Even though there are innumerable significant perspectives based on HUI itemset, there occurs a problem in producing large number of candidate item set when database consist of lots of long transaction. To handle this issue, Tseng et al. (2010) presented a resourceful algorithm named UP-Growth for mining HUI itemset miming from transactional databases. UP-Tree data structure has been proffered for preserving the information of HUIs [18]. Hence, the potential HUIs can be effectively prompted from the UP-Tree by scanning the database only twice. In the demonstrations, synthetic and real datasets have been employed to judge the performance of the algorithm. The mining production has been improved extensively because the proposed strategies effectively reduced the search space and the number of candidates. The UP-Growth algorithm outperforms when there are lots of long transactions present in the database.

The discovery of temporal high utility patterns in data streams has been a major challenging task. However the main limitation of FIM is it does not eliminate the non-periodic itemset, so that the efficiency of mining will be decreased which lead to decline in the profit of the retails. Viger et al. (2016) proposed an algorithm for filtering the non-periodic pattern in the database. A built-in disadvantage of the conventional high-utility item set mining procedure is that they are incompatible in discovering the recurring customer behaviour on purchase [29]. For example, some products can be bought by the customer frequently for every week or month. This limitation can be overcome by the use of periodic high-utility item set mining. This type of mining algorithm detects the class of items that are bought by the customers periodically for generating high gain. This algorithm helps in filtering a high amount of non-periodic patterns for discovering the needed periodic high-utility itemsets only.

The detection of High utility pattern in the data stream owing to immense application on numerous domains was a demanding task. Liu & Qu (2012) discloses that Utility-list data structure provides the pruning information for HUI-Miner along with the item sets utility information. A very immense number of candidate itemsets are being processed by conventional algorithms during the mining process. Candidate generation process has been skipped while using HUI-Miner for mining high utility item sets [21]. This obviates the utility computation and costly generation of candidates. This HUI-Miner procedure has improved production concerning memory consumption and running time.

FIM has a concern that it presumes all items has same significance and generates the itemset which produces low profit. To resolve this issue, HUIM [26] algorithm has been proposed, which resolves the issue to some extent, but the utility of an itemset is neither monotonic nor anti-monotonic. So to make the algorithm more efficient, Viger et al. (2014) proposed an algorithm called FHM (Fast High-Utility Miner), which consolidates the strategy EUCP (Estimated Utility Co-occurrence Pruning)that is used to scale down the number of joins during the mining of high-utility item sets by utilizing the utility-list data structure. This pruning approach is experimentally proved to diminish the search space by 95% and is faster than HUI-Miner algorithm by six times.

HUIs mining continues to be very time consuming, though it is a foremost mining algorithm for countless applications. Zida et al. (2016) brought in EFIM to revamp the efficiency of mining in terms of execution time and memory consumed. This algorithm depends on two upper-bounds for pruning the search space, namely, local utility and sub-tree utility [29]. These upper-bounds are calculated using an array-based utility algorithm called as Fast Utility Counting. This approach calculates the upper bound in linear time and space. High-utility Database Projection (HDP) and High-utility Transaction Margin (HTM) are the two techniques that are used for database projection and transaction merging in order to reduce the cost of database scans. EFIM algorithm consumes comparatively less memory than other algorithms such as, FHM [ref 2], UP-Growth + , HUP-Miner, HUP. EFIM out performs on both dense and sparse datasets.

HUIs are mined in complex event sequences by incorporating utility mining with episode mining. Wu et al. (2013), discovered UP-Scan algorithm, in order to estimate the utility of episodes, the external as well as internal utilities are considered. Complex event sequences holding concurrent events are taken into consideration, which provides users with high utilities and information concerning the relationships between episodes [22]. UP-Scan (Utility episodes mining by Spanning prefixes) has been introduced for mining the entire set of high utility episodes efficiently. TWU model and EWU (Episode – Weighted Utilization) model has been used for episode mining and for high utility episode mining tasks respectively. DGE (Discarding Global unpromising Events) and DLE (Discarding Local unpromising Events) have been introduced and are integrated with UP-Scan algorithm to diminish the number of candidates and to increase the performance of those tasks regarding execution time and memory consumption. Exploratory results on real and synthetic datasets indicate that UP-Scan algorithm performs better than baseline approach and has good scalability measures, especially under higher minimum utility threshold. Serial episodes containing simultaneous events are only considered. Other kinds of episode such as injective episodes, parallel episodes, and closed episodes have not been taken into account.

Even though there are many papers regarding HUI mining, there aren't many researches on the incremental database. Ahmed et al. (2009) proposed three tree structures for handling incremental databases, with the presently available memory size for operations such as insertions, modifications and deletions [16]. The $IHUP_L$Tree is easy to construct and handle, since there is no requirement for any restructuring operation, despite of, gradual revision of the databases. $IHUP_{TF}$-Tree requires less memory, whereas, $IHUP_{TWU}$ Tree requires less time for execution. To obviate the level-wise candidate generation and test methodology, a pattern growth approach has been used. The entire above mentioned tree structures follow "BUILD ONCE, MINE MANY" property, that are satisfactory for interactive mining. All the three structures need two dataset scans at the max. These tree structures are effective for interactive and incremental high utility pattern mining. These perform better than the conventional algorithms in regard to execution time and memory usage. They are scalable to handle a large number of distinct items and transactions.

A dispute of utility mining is locating HUIs with negative values from transactional databases. This concern has been scrutinized through Philippe Fournier-Viger (2014), who proposed an efficient algorithm named FHN (Fast High-Utility itemset miner with Negative unit profits), which can be used for mining HUIs, where item units may be positive or negative [17]. This algorithm provides a supplement to FHN algorithm for HUI mining. Practical outcomes manifest that the FHN algorithm is almost 500 times faster and uses at the max of 250 times less memory when compared with HUINIV-Mine algorithm. This algorithm outperforms on the dense datasets too.

Chu et al. (2019), handles the problem of detecting high utility item sets with negative item values in large databases. HUINIV-Mine identifies high utility item sets with negative item values in large databases [32]. The proposed HUINIV-Mine helps in identifying high utility item sets with negative value in less high TWUI effectively, such that, the mining time taken for execution of high utility item sets with negative values can be reduced. This algorithm generates fewer candidate item sets for finding high utility item sets with negative item values with higher performance compared to other traditional algorithms.

Viger and Zida (2015) proposed FOSHU (Fast On-Shelf High Utility item set miner) algorithm to mine high utility item sets consisting of negative utility values and considering shelf time of items. This algorithm doesn't hold the candidates in memory, as it is a single phase algorithm and relies on a depth first search strategy [28]. In this algorithm, mining of itemsets are done in all time periods simultaneously, instead of mining each period separately and performing post-processing of the results of each time, which is costly. This algorithm introduced an idea of using total order, where negative items handle negative external utility values efficiently than the traditional algorithms. The experimental results confirm that FOSHU is faster than three orders of magnitude and uses up to ten times less memory than TS-HOUN.

3 Comparative Analysis

The comparative analysis of various utility mining algorithms, the itemsets used by these algorithms, their results on various problems in utility mining, the data set used have been discussed in Table 1.

Table 1. Comparative analysis of various utility mining algorithms.

Sno	Year	Itemset used	Problem discussed	Algorithm Proposed	Result obtained	Dataset used	Total no of trans actions	Average no of transactions	Future work of paper
1	2004	Utility itemset	Utility mining problem	Transaction utility and external utility [12]	Increase in profit Efficient in utility mining	Theoretical analysis			Comparison with other itemset mining algorithm has to be done
2	2007	High utility itemset	Mining in long and dense dataset	CTU mine [13]	Eliminate Anti-monotone problem	IBM quest Data generator T10I5D50K	10,000	10	Negative value itemset is to be considered
3	2007	High utility itemset	Optimization problem	High-Yield Partition tree [14]	Highest yield for each and every size given	IBM data set	2003 revenue data with	21	To extend the work to mine in distributed database
4	2009	High utility itemset	Mining in vertical distribute d database	WIT-tree technique TWU- Mining distribute [15]	Reduce search space Runtime is more efficient	BMS-POS Retails	515597 88162	1656 16469	Mining HUI in horizontal distributed database
5	2009	High utility itemset	Mining Incremental Database	IHUPL tree IHUPTF tree IHUPTWU [16]	Incremental and interactive HUP mining Very efficient and scalable	Mushroom Retail Kosarak Chain-store	8124 88162 990002 1112949	23 10.3 8.1 7.2	Negative value itemset mining in incremental database
6	2010	High utility itemset	Transactional database with lots of long text	HUI Miner UP-Growth UP-tree [17]	Reduced execution time when database contain lots of long text	BMS-Web view Chess T10I6D100 K	1000 K 40000000		Mining has to be done in distributed network
7	2012	High utility itemset	Transactional database in distributed network	FUM-D [18]	Overcomes error and pitfalls	IBM synthetic dataset Supermarket store	1000000 20000	1000 7007	Discover high utility itemset with negative values
8	2012	High utility itemset	Utility mining in Distributed database	iFUM [19] Kaas	Increase productive and promote the profit in XML	Online shopping cart system	–	10	This algorithm may be extended to transactional

(*continued*)

Table 1. (*continued*)

Sno	Year	Itemset used	Problem discussed	Algorithm Proposed	Result obtained	Dataset used	Total no of trans actions	Average no of transactions	Future work of paper
9	2013	High utility itemset	Mining in complex event sequence	UP-Scan [20] EWU DGE DLE	Reduced execution time and memory consumption	IBM generator Food mart Retail Chain store	10000 4141 88162 1112949	12 4.4 10.3 7.3	Window-based occurrence, non-overlapped/overlapped minimal occurrence is to be addressed in future
10	2014	High utility itemset	Mining the negative value itemset	Genetic algorithm HUPEUMU-GRAM [21]	Increased scalability and efficiency	IBM data generator	10000	10	The algorithm has to be extended to work in distributed database
11	2014	High utility itemset	XML database in distributed network	MINERXML [22]	Transparency Parallelism Interoperability Fault tolerance	IBM Synthetic Mushroom Kosarak Accidents	100000 8124 990002 340183	6144 963 49859 59663	Mining has to be extended to deal with negative value itemssets
12	2014	High utility itemsets	Existing HUI Miner algorithm perform costly operations for each pattern	FHM [23]	Reduce the number of join operation upto 95% and 6% faster in execution	Chain store BMS Kosarak Retail	1112949 59601 990000 88162	7.26 4.85 8.09 10.30	Future work is to explore other optimizations for itemset mining, sequential pattern mining and sequential rule mining
13	2014	High utility itemset Transactional Database	Handling negative value itemset	FHN [24]	500 times faster execution and 250 times lesser memory space consumption	Mushroom Retail Kosarak Chess Psumb Accidents	8124 88162 41270 3196 49046 340183	23 10.30 8.09 35 74 3380	To investigate other interesting problems involving utility mining in itemset mining
14	2015	High utility itemset	Mining with negative value itemset	UP-GNIV [25] RNU	Remove the negative value using UP-tree pruning	IBM dataset T10I4D100 k T20I4D100	100000	1–10	Mining interesting patterns using optimization algorithms
15	2015	High utility itemset Transaction Database	Handle the database with negative unit profit	FOSHU [26]	1000 times faster in execution and 10 times less memory consumption	Mushroom Retail Accidents Chess Pusmb	8124 88162 340183 3196 49046	23 10.3 33.8 35 74	To explore other interesting problems involving utility in itemset mining such as sequential pattern mining

(*continued*)

Table 1. (*continued*)

Sno	Year	Itemset used	Problem discussed	Algorithm Proposed	Result obtained	Dataset used	Total no of trans actions	Average no of transactions	Future work of paper
16	2016	High utility itemset	Inappropriate to discover recurring customer purchase	PHM [27]	Filter the non- periodic pattern, aster and efficient	Retail Mushroom Chain store Food mart	16470 119 461 1559	10.30 23 7.23 4.4	To consider designing alternative algorithms to mine PHUIs
17	2016	High utility itemset	HUIM is expensive in both time and space	EFIM [28] HDP HTM	Efficiently discover HUI Low power consumption Linear space and time is used	Accidents BMS Chess Connect Food mart Mushroom Chain store	340183 59601 3196 67557 4141 8124 1112949	33.8 4.8 37 43.0 4.4 23.0 7.2	To redesign EFIM as a distributed algorithm to be able to mine very large databases
18	2018	High utility itemset	Considering LUI and Generating pattern	HUIM [29] FIM & UIM FP- growth	Accurate measure which increase sales and reduce time	Chess Connect Pumsb Accidents Mushroom Retail	10000 20000 30000 50000	4	To use the approaches descried in the advanced algorithms to generate the high utility itemsets without candidate generation, and thus reduce the time required to generate our desired association rules

4 Conclusion

The frequent itemset mining was discovered on the proposition that the itemset that appear more customarily in the transactional databases are considered to be in the top of user's wish list. Still, in reality, the mining of itemsets, by taking into account only the frequency of itemset, is a challenging task, as it has been proved in many applications that the itemsets that bestow to the most are not inevitably the frequent itemsets. Utility mining attempts to bridge this gap by making use of utility factors such as profit, quantity or cost based on user's view. This paper delivered a quick analysis of the various algorithms involved in mining of high utility itemsets from transactional databases. Most of the algorithms were focused on reducing the number of scans done on candidate itemset generation and finding the high utility itemsets with negative values. In future, we will be developing an algorithm for high utility itemset mining.

References

1. Zhang, C., Almpanidis, G., Wang, W., Liu, C.: An empirical evaluation of high utility itemset mining algorithms. Expert Syst. Appl. **101**, 91–115 (2018)
2. Pillai, J., Vyas, O.P.: Overview of itemset utility mining and its applications. Int. J. Comput. Appl. **5**(11), 0975–8887 (2010)
3. Zhong, R., Wang, H., Institute of Computer, Shaoguan University, Shaoguan, Guangdong Province: Research of commonly used association rules mining algorithm in data mining. In: International Conference on Internet Computing and Information Services, 978-1-4577-1561-7 (2011)
4. Kayastha, J., Wankhade, N.R.: A survey paper on frequent itemset mining techniques. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **6**(12) (2016). ISSN: 2277 128X
5. Patel, S., Madhushree, B.: A survey on discovering high utility itemset mining from transactional database. In: Information and Knowledge Management, vol. 5 (2015). www.iiste.org. ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
6. Khot, Y., Kulkarni, M.: Survey on high utility itemset mining from large transaction databases. Int. J. Emerg. Trends Technol. Comput. Sci. (IJETTCS), **3**(4) (2014)
7. Bhattacharya, S., Dubey, D.: High utility itemset mining. Int. J. Emerg. Technol. Adv. Eng. **2**(8) (2012). ISSN 2250-2459
8. Shankar S, Pursothaman T, Jayanthi S: Novel algorithm for mining high utility itemsets. In: International Conference on Computing, Communication and Networking (2008)
9. Han, J., Pei, J., Yin, Y.: Mining frequent patterns without candidate generation. In: ACM SIGMOD International Conference on Management of Data, pp. 1–12 (2000)
10. Tseng, V.S., Wu, C., Shie, B., Yu, P.S.: UP-growth: an efficient algorithm for high utility itemset mining. In: ACM SIGKDD International Conference on Knowledge Discovery Data Mining, pp. 253–262 (2010)
11. Surawase, K.: Efficient Discovery of High Utility Itemset CPGCON-15, Ingle M.D (2015)
12. Yao, H., Hamilton, H.J., Butz, C.J.: A foundational approach to mining itemset utilities from databases, SDM(2004)
13. Erwin, A., Gopalan, R.P., Achuthan, N.R.: CTU-mine: an efficient high utility itemset mining algorithm using the pattern growth approach. In: 7th IEEE International Conference on Computer and Information Technology (CIT), Aizu-Wakamatsu, Fukushima, pp. 71–76 (2007). https://doi.org/10.1109/cit.2007.120

14. Hu, J., Mojsilovic, A.: High-utility pattern mining: A method for discovery of high-utility item sets. Pattern Recognit. **40**(11), 3317–3324 (2007). ISSN: 0031-3203
15. Vo, B., Nguyen, H., Le, B.: Mining high utility itemsets from vertical distributed databases. In: 2009 IEEE-RIVF International Conference on Computing and Communication Technologies, Da Nang, pp. 1–4 (2009)
16. Ahmed, C.F., Tanbeer, S.K., Jeong, B., Lee, Y.: Efficient tree structures for high utility pattern mining in incremental databases. IEEE Trans. Knowl. Data Eng. **21**(12), 1708–1721 (2009)
17. Fournier-Viger, P. FHN: efficient mining of high-utility itemsets with negative unit profits. In: Luo, X., Yu, J.X., Li, Z. (eds.) Advanced Data Mining and Applications. ADMA 2014. Lecture Notes in Computer Science, vol 8933. Springer, Cham (2014)
18. Tseng, V.S., Wu, C.-W., Shie, B.-E., Yu, P.S.: UP-Growth: an efficient algorithm for high utility itemset mining. In: Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'10), pp. 253–262. ACM, New York (2010)
19. Subramanian, K., Kandhasamy, P., Subramanian, S.: A novel approach to extract high utility itemsets from distributed databases. Comput. Inf. **31**, (6+) (2012)
20. Kannimuthu, S., Premalatha, K., Shankar, S.: Investigation of high utility itemset mining in service oriented computing: deployment of knowledge as a service in E-commerce. In: Fourth International Conference on Advanced Computing (ICoAC), Chennai, pp. 1–8 (2012)
21. Liu, M., Qu, J.: Mining high utility itemsets without candidate generation. In: Proceedings of the 21st ACM International Conference on Information and Knowledge Management (CIKM'12), pp. 55–64. ACM, New York (2012)
22. Wu, C.-W., Lin, Y.-F., Yu, P.S., Tseng, V.S.: Mining high utility episodes in complex event sequences. In: Ghani, R., Senator, T.E., Bradley, P., Parekh, R., He, J. (Eds.) Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'13), pp. 536–544. ACM, New York (2013)
23. Kannimuthu, S., Premalatha, K.: Discovery of High Utility Itemsets Using Genetic Algorithm with Ranked Mutation. Appl. Artif. Intell. **28**(4), 337–359 (2014)
24. Kannimuthu, S., Premalatha, K.: A distributed approach to extract high utility itemsets from XML Data, World Academy of Science, Engineering and Technology, International Science Index 87. Int. J. Comput. Electr. Autom. Control Inf. Eng. **8**(3), 498–506 (2014)
25. Fournier-Viger, P., Wu, C.-W., Zida, S., Tseng, V.S.: FHM: faster high-utility itemset mining using estimated utility co-occurrence pruning, foundations of intelligent systems. Springer International Publishing (2014)
26. Fournier Viger, P.: FHN: efficient mining of high-utility itemsets with negative unit profits, vol. 8933, pp. 16–29 (2014). https://doi.org/10.1007/978-3-319-14717-8_2
27. Subramanian, K., Kandhasamy, P.: UP-GNIV: an expeditious high utility pattern mining algorithm for itemsets with negative utility values. Int. J. Inf. Technol. Manag. **14**, 26–42 (2015)
28. Fournier-Viger, P., Zida, S.: FOSHU: faster on-shelf high utility itemset mining–with or without negative unit profit. In: Proceedings of the 30th Annual ACM Symposium on Applied Computing (SAC'15), pp. 857–864. ACM, New York (2015)
29. Fournier-Viger, P., Lin, J.C.W., Duong, Q.H., Dam, T.L. PHM: mining periodic high-utility itemsets. In: Perner P. (eds.) Advances in Data Mining. Applications and Theoretical Aspects. ICDM 2016. Lecture Notes in Computer Science, vol 9728. Springer, Cham (2016)
30. Zida, S., Fournier-Viger, P., Lin, J.C.W., et al.: Knowl. Inf. Syst. **51**(595), 0219–1377 (2017). Springer London

31. Wu, J.M.-T., Zhan, J., Chobe, S.: Mining association rules for low-frequency itemsets. PLoS ONE **13**(7): e0198066 (2018)
32. Chu, C.-J., Tseng, V.S., Liang, T.: Efficient mining of temporal high utility itemsets from data streams (2019)

A Survey of Datalink Layer Protocol for IoT

Dipasree Dey(✉), Jayanti Dansana, and Ashutosh Behura

KIIT Deemed University, Bhubaneswar, India
dipasreedey93@gmail.com, {jayantifcs,ashutoshfcs}
@kiit.ac.in

Abstract. The Internet of Things helps in filling the space between the real world and the virtual world, which is one of the forthcoming networking regions. Our daily lives have been changed by the role of the mobile appliance. Devices can interact among themselves where protocol played a key role in IoT implementation. The simple protocol of IoT technology is designated here. We can classify the IoT protocols into four categories such as data link layer protocol, network layer protocol, transport layer protocol, application layer protocol. Depends on the disparate benchmark, comparison of data link protocols is done. After comparing all protocols, we can't determine which integration of protocol is the best for the implementation of IoT.

Keywords: Bluetooth · Cellular · Data link layer protocol · IoT protocol stack

1 Introduction

The updated version of Internet technology is IoT. Before IoT comes into picture internet technology is used for connecting each and everything in the globe but sometime. Some techniques like Zwave, Bluetooth, Cellular, and ZigBee, Wi-Fi etc. are prevailing techniques but for the advancement of the system of the Internet of Things, there are many techniques present. Liable on the various parameter such as range, the requirement of data, safety, battery usage, handiness, cost and some other factors of several protocols one can choose which one is the finest. Internet protocol has the advantages of reliability and flexibility. Depending on these factors, the Internet Engineering Task Force (IETF) make another protocol for connection among the IoT appliances. Based on the topic of different layers of standards protocol of IP stack, several kinds of white paper are introduced by the Internet Protocol for Smart Objects (IPSO) alliance and also published about adaptation layer by which smart objects can be communicated. We can define IoT stack which is consist of 5 layers i.e. application layer, transport layer, network layer, data link layer, and physical layer. Figure 1 describes the layers of IoT stack [1].

1.1 Physical Layer

The physical layer [1] is basically used for connecting physical medium with the mechanical or electrical interfaces to achieve a synchronous communication. It takes care of bit-level transmission between them. It takes care of the physical connections of

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 459–466, 2020.
https://doi.org/10.1007/978-3-030-37051-0_52

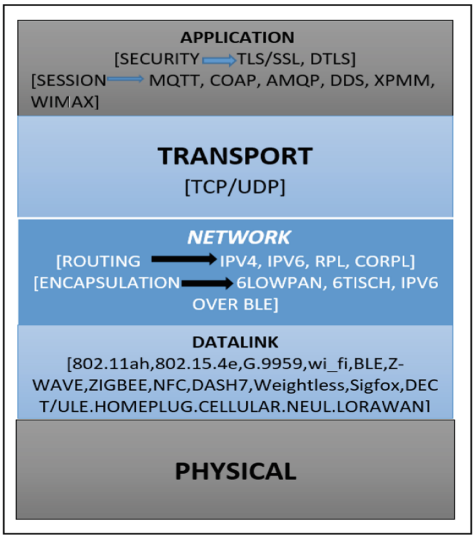


Fig. 1. IoT stack

the networks like cabling, a standard of cabling, connectors and its types etc. but not the physical medium.

1.2 Data Link Layer

It is the 2nd layer of the IoT protocol stack. It is obtain the process, by which the data is sent through the medium like the radio wave, copper wave. It is also obtain the process, by which packets are coded through the medium [2].

1.3 Network Layer

This layer responsible for sending IP datagram from source network to destination network. It executes the task of the host addressing and packet routing. The datagram hold the source and destination address, by which source to destination route is decides This layer has two sublayers: Routing layer and Encapsulation layer in network stack.

1.4 Transport Layer

This layer has the ability to transfer the end to end messages in a particular network. By the help of handshake or without handshake protocol message transferring is done. Congestion controls and segmentation functions are execute here.

1.5 Application Layer

The application layer has standardizes communication depends to set up host-to-host data transfer, it is depend on transport layer. It is divided into two sub layer one is security layer and another is session layer [1].

2 Related Work

This section presented, the survey of data link layer protocols related papers worked. Salman [1] presented a survey paper, which is describe about the different standards like IEEE, IETF supported IoT technologies and data link layer, network layer, application layer and session layer protocols briefly discussed. Mohammed et al. [6] presented a review paper on enabling technologies and describe some protocols and use cases. Pathak and Tembhurne [4] this paper provides a general view of IoT and it's used standards. Patel and Tusher [3], compare various internet of things protocol. They can conclude which combination of protocol can be used together to get the best way for the implementation of IoT.

3 Data Link Layer Protocols

In [1] this section presents different type of data link layer protocols.

3.1 IEEE 802.11 (Wi-Fi)

IEEE 802.11 is broadly used in wireless local area network (WLAN). The speed of the data transmission rate is 1 Mb/s up to 6.75 GB/s. It has low cost. It uses CSMA/CD. Network topologies defined are star and mesh. It's network communication is bi-directional and its power consumption is less convenient i.e. 100 mw. It uses direct sequence spread spectrum techniques. It supports Advance encryption standards (AES) [1].

3.2 IEEE 802.3 (Ethernet)

IEEE 802.3 is a first broadly used in local area network technology (LAN). It is simplest than token local area network. The speed of the data transmission rate is 10, 100, 1000 Mbps. It has a very cheap cost. It uses CSMA/CD methods. IEEE 802.1 network architecture is used in the IEEE 802.3 technology [2].

3.3 IEEE 802.15.4

This standard is famous for WPAN. It Operates on ISM band. and Uses CSMA/CD methods. Power consumption is minimized due to infrequently occurring very short packet transmissions with low duty cycle (<1%). Transmission, for most cases, is line of sight (LOS) and Standard transmission range varies between 10 m–75 m and the Best case transmission range achieved outdoors can be up to 1000 m and Networking

topologies defined are star and mesh. It is suitable for home networking, automotive networking and industrial networking [1].

3.4 ZigBee

It operates on 2.4 GHz like Bluetooth and Wi-Fi. It is based on the IEEE 802.15.4 protocol. Data rate range around 250 kbs and the physical range are around 10–100 m [10]. ZigBee is suitable for home automation, it has some significant advantages like it uses low power, higher reliability, high scalability, larger nodes count. Zigbee has three types: ZigBee coordinator (ZC), ZigBee router (ZR) and ZigBee End Device (ZED) [8]. Zigbee network tree has a root, this root known as Zigbee coordinator. There is single hop connectivity to any other devices. ZigBee router (ZR) is Capable of running Program, as well as relaying information between nodes connected to it. ZigBee End Device (ZED) has the ability to communicate with the parent node and to collect information it cannot depend on other devices. Nodes are permitted to sleep for a certain time for that battery life is extended. Memory requirements and cost of ZEDs are quite low, as compared to ZR or ZC [11].

3.5 Z-Wave

It [3] is a technology intended for home automation products. It is also a low power RF Communication Technology which basically works in the band 1 GHz. Z-Wave used for reliability and short latency communication for transmitting small packet and Data rate of 100 kbits/s. It does not require coordinator because it supports the mesh network type topology. So a greater number of devices can be connected up to 232. It supports quality data transfer in a faster way so widely used nowadays in the home environment and LAN. The standard used nowadays is 802.11n which deliver an efficient throughput, which is of hundreds of megabits per second. It is good for transferring data but the disadvantage is that power consumption is very high which is not appropriate for the IoT devices [2].

3.6 NFC

It works inside the range of 4–10 cm and has a less power consumption than others i.e. 15 mA. It is a simple contactless two-way communication technology among electronic gadgets. It let numerous contactless operation like amount transfer, digital content, and contact of electronic expenditures like card without any contact. Basically it is similar to RFID technology. NFC is used in Low-power home automation systems, Parcel tracking, Computer game synchronized toys, Information tags in posters and advertisements, Smartphone based payments [12].

3.6.1 NFC Device Types

All NFC types are similar but communicate in different ways. So very animated NFC technology which is known as the **FELICA**, is commonly found and mostly used in JAPAN. The contemporary once, **TYPE A** and **TYPE B** NFC are used in the rest part

in the world. Primarily NFC devices are two types: passive and active device. Passive devices contain information which is readable by other devices [8] (Fig. 2).

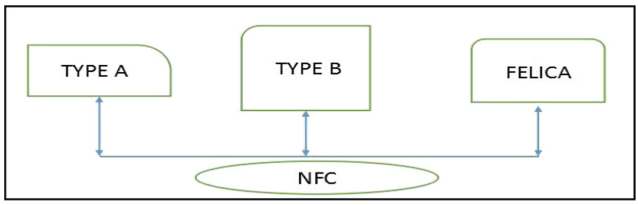


Fig. 2. NFC types

3.7 Sigfox

Sigfox is a company, founded in 2009 which is emerged in Toulouse, France. It gives a web application interface for device management. It uses ultra narrow band technology. It has standby time is very high i.e. 20 years with 2.5 mAh battery as compared to 2 years for cellular. It is a scalable network in which any number of devices are connected up to kilometers. Power consumption is less so it is suitable for smart application such as security device, street lightening etc. and operates in 1 GHz band wireless network. It is also used in agriculture, healthcare, intelligent buildings, public transport, and utilities [3].

3.8 Nuel

It is just like Sigfox, functioning in the sub-1 GHz band and also customs TV whites pace spectrum to achieve greater scalability, greater coverage, less power, and less cost wireless network. Nuel is a weightless technology particularly intended for IoT and also it contends with GPRS, 3G, CDMA, and LTE WAN solutions. It consumes less battery as 20–30 mA batteries can run up to 10–15 years and data rates can be from few kbps to 100 kbps for the same link [2].

3.9 LoRaWAN

It is also similar to Sigfox and Nuel used for WAN. Consumption of battery is 10 mA so battery life upturns to 10 years. It is optimized for low power costs. The Data rate range of LoRaWAN is 0.3 up to 50 kbps and physical rage is around 2–5 km in an urban area and 15 lm in the suburban area It is used in smart city and industrial purpose [3].

3.10 Cellular

It supports high data rate and long distance transmission of IoT data with the help of GSM/3G/4G but it has a disadvantage of high power consumption. The important factor in this technology is Square EE and CELL1.0 low-cost development board and

linking board with Raspberry Pi and Arduino platform. It provides data projection with low power consumption and low transfer rate by the help of sensor-based with lowering the bandwidth [10].

3.11 Bluetooth

It is heavily used for IoT connectivity. This is particularly used for short-range communication personal area network and to transfer data using Bluetooth between two mobile devices. This mobile devices, of course, need to have the Bluetooth radio to be supported and now most of the mobile phones particularly the smart phones they are all enabled with Bluetooth. So one can transfer files, music, videos so on and so forth. One of the good thing about Bluetooth is security. In Bluetooth there are three types of radio, class a, class b and class c. class a range is 100 m basically it is used for industrial purpose then class b range is 10 m which is used for mobile devices and class 3 range is 1 m [9].

3.12 HART & Wireless HART

It is the latest release of highway addressable remote transducer (HART) protocol [1]. HART standard was developed for networked smart field devices. The wireless protocol makes the implementation of HART cheaper and easier. HART encompasses the most number of field devices incorporated in any field network. Wireless HART enables device placements more accessible and cheaper-such as the top of reaction tank, inside a pipe, or at widely separated warehouse. Main difference between wired and unwired versions is in the physical, datalink and network layers. Wired HART lacks a network layer [8].

4 Conclusion

In IoT, There is existed many technologies which are a part of the datalink link layer protocol. In all of them, it is difficult to find out which one better. This paper is presented here with a brief description of the data link layer protocol. They are used in many different types of application. In this paper, different types of the data link protocol are compared using the different type of factor like cost, privacy, battery life, spreading factor, complexity, data rates etc. but which one is best for faster and secure for IoT application does not conclude. In future work, I will research on LoRaWAN data link layer protocol on IoT devices. It has low power consumption, less cost and used in many IoT applications. Comparing of these data link layer protocol is given on above Table 1.

Table 1. Comparison of data link layer protocols

IoT protocol	IEEE 802.11	IEEE 802.15.4	Zigbee	Neul	LoRAWAN	Cellular	ZWAVE	Sigfox
IEEE standard	802.11	802.15	802.15.4	Neul	802.15.4	GSM/GPRS/UMTS /HSPA(3G)/LT E(4G)	ITU-T G.9959	Sigfox
Frequency band	900 MHz	902–928 MHz	2.4 GHz	900 MHz (ISM)	Various	900/800/1900/2100 MHz	908.42 MHz	900 MHz
Max signal rate	42 Mbps	50 $kbps^{-1}$ Mbps	250 KB/S	FEW BPS UP TO 100 KBPS	0.3–50 KBPS	35–170 kbps(GPRS)	0Kbit/s or 100 kbit/s	10–100 BPS
Nominal range	1 km	100 m	10 M	10 km	2.5 km (Urban) 15 km (sub urban)	36 km maximum for GSM	~30 M	30–50 km (rural), 3–10 km (urban)
Cryptography	AES 128	AES 128	AES block cipher	AES encryption partially address	AES encryption	AES encryption/RC4	AES encryption	AES with no key OTA transmission
Network type	WLAN	WLAN	WPAN	LTE WAN	WAN	LAWN	WPAN	UNB (LPWA)/WAN
Spreading	SC, OFDM	TDMA CCK	DSSS	UHF spectrum	DSSS	WSDMA	FHSS	BPSK
Power consumption	100 MW	100 MW	~40 mA	20–30 mA from 2XAA battery	TX current (24–44 mA) RX current (12 mA)	4.5 MWH	~2.5 mA	~50 μW
Fully bi-directional	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Topology	Star	Star	P2P, Star	Star	Star	Cell topology	Mesh	Star
MAC	CSMA/CA	CSMA/CA	Unslotted CSMA/CA	CDMA	Unslotted aloha	CDMA	CA	Unslotted aloha
Multihop	2 hops	Yes	Yes	Yes	Yes	Yes	Optimum hop 2 max hop 5	Yes
Complexity	Lowlevel	Low level	Low level	Very low level	Very low level	High level	Low level	Low level
Battery lifetime	Long time	Long period	Years	Low battery life	Up to 10 years	Low	Long time	Very low
Privacy	Less	Less	Mid	Less	Less	More	More	Less
Cost	Less	Less	Average	Less	Less	More	Average	Less

References

1. Salman, T., Jain, R.: A survey of protocols and standards for Internet of Things, April 2017. https://www.researchgate.net/publication/320616226
2. Choudhari, S., Rasal, T., Suryawanshi, S., Mane, M., Yedge, S.: Survey paper on Internet of Things: IoT. IJESC **7**(4) (2017)
3. Patel, A., Champaneria, T.A.: Study and comparison of various internet of things protocols. Int. J. Adv. Eng. Res. Dev. **2**(12) (2015)
4. Pathak, A.D., Tembhurne, J.V.: Internet of Things: a survey on IoT protocols. In: 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT) (2018)
5. Alahari, H.P., Yalavarthi, S.B.: A survey on network routing protocols in Internet of Things (IOT). Int. J. Comput. Appl. **160**(2), 0975–8887 (2017)
6. Mohammadi, M., Aledhari, M.: Internet of Things: a survey on enabling technologies, protocols and applications. Factor **6**(81). https://doi.org/10.1109/comst.2015.2444095
7. Dragomir, D., Gheorghe, L., Costea, S., Radovici, A.: A survey on secure communication protocols for IoT systems. https://doi.org/10.1109/siot.2016
8. Connectivity-Technology. https://www.youtube.com/watch?v=d9QfVpCG00Y&list=PLaxu2gn-9WXMf_ln5pMvxjf043jzof4-i&index=7. Accessed 21 Jul 2017
9. Pareek, M., Buriya, S.: A study of link layer protocols in IoT. Int. J. Futur. Revol. Comput. Sci. Commun. Eng. **4**(2), 355–359. ISSN: 2454-4248
10. Lee, J.S., Su, Y.W., Shen, C.C.: Comparative study of wireless protocols: Bluetooth, UWB, Zigbee and Wi-Fi. In: The 33rd Annual conference of IEEE Industrial Electronics society (IECON), 5–8 Nov 2007, Taipei, Taiwan
11. Kaur, H., Sharma, S.: A comparative study of wireless technologies: Zigbee, Bluetooth LE, Enocean, Wavenis, Insteon and UWB. In: Proceedings of the International Conference on Recent Trends in Computing and Communication Engineering—RTCCE 2013 (2013)
12. Sethi, P., Sarangi, S.R.: Internet of Things: architectures, protocols, and applications. J. Electric. Comput. Eng. (2017)

ASL Recognition and Conversion to Speech

Simran Kharpude(✉), Vaishnavi Hardikar, Gautam Munot,
Omkar Lonkar, and Vanita Agarwal

College of Engineering, Pune, India
{kharpudesl15.extc, hardikarvsl5.extc, munotgsl5.extc,
lonkarodl5.extc, vsa.extc}@coep.ac.in

Abstract. The deaf & dumb (or the Mute community) find it a tedious task to converse with ordinary people through sign language. This stands as a hindrance in even the most basic of their activities. It affects their personal development, interpersonal relations and limits the contributions they could otherwise make to society. The prime motive of this project is to provide an easy to use platform for the hard of hearing people to express themselves despite the sign language barrier. We aim to achieve this motive through gesture recognition. Using gesture recognition, we compute the mathematical interpretation of human hand gestures to recognize the signs conveyed by American Sign Language. The system enables real-time hand gesture and speech recognition and provides an innovative and simpler mode of communication for the mute people.

Keywords: American sign language · Background subtraction · OpenCV
Python speech recognition · Convolutional neural network · Tensorflow-GPU
Real-time

1 Introduction

According to marxentlabs.com, "The general definition of gesture recognition is the ability of a computer to understand gestures and execute commands based on those gestures". In our project we have used gesture recognition to recognize American Sign Language. American Sign Language is the third most commonly used language in the United States. About 2 million people in the world use ASL. This language uses finger spellings, hand shapes and gestures to indicate certain concepts and ideas. The ASL vocabulary or dictionary database is more readily available than other local sign languages. Hand shapes and hand structure varies considerably from person to person and hence the dataset required to train a model for such an application should be dynamic and vast. Hence there is a need for heavy preprocessing. Preprocessing is done to remove unwanted features from the gestures and reduce the dataset size by some extent. It additionally helps to improve accuracy of recognition. After processing, machine learning algorithms are applied to extract desired features which are further used to obtain the required output. Complex applications also use neural networks along with machine learning to train the network. Existing models for this application hardly provide a means for two way communication and rarely any scope for scalability.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 467–474, 2020.
https://doi.org/10.1007/978-3-030-37051-0_53

The motivation of our project is to provide a robust method for overcoming hurdles faced while communicating with the hard of hearing people without any knowledge of the sign language. The project is designed keeping in mind the objective of providing an easy to use, fast, less complex and background independent solution for a communication model for the mute community.

Our project can be divided into 2 parts as follows:

Gesture Recognition (Input) & conversion into speech (Output).

Speech Recognition (Input) & back conversion into Text (Output).

The extent of preprocessing that we have applied is what makes our project unique. The novel idea being that we have tried to implement a model which has extremely minimal memory requirements which results in comparatively low processing time even while extracting tens of thousands of features.

2 ASL Gestures Dataset

We have trained our system for 47 gestures which includes 26 English alphabets, 10 digits and 11 most commonly used signs enough to introduce oneself. The dataset consists of 2400 static, black and white, flipped images for each of the 47 classes. All images have a size of 50 by 50 pixels [7]. Our system has provisions for additions in the dataset and training of new gestures as per the user (Fig. 1).

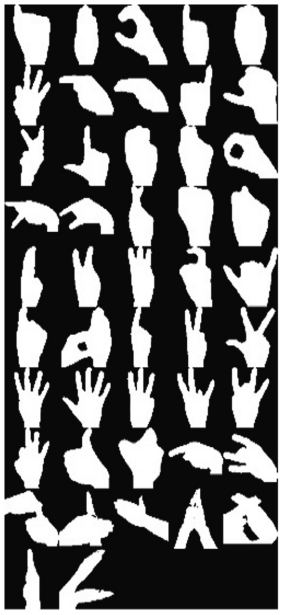


Fig. 1. Preprocessed input gestures

3 Background and Drawbacks of the Current Sign Language Recognition Methods

There have been several attempts of recognizing sign language in real time. Most of these methods require additional hardware for detecting hand movement or hand shape. Such hardware includes smart gloves [2], accelerometers, flexure sensors, etc. These sensors and devices increase the overall cost of the system and make it difficult for the hard of hearing people to afford the system.

Additional hardware increases the complexity in terms of interfacing all nodes onto the same platform. This limits the flexibility of the project and also its future scope. Not only is this complex from a development point of view but it also becomes difficult to maintain such devices over several years. Implementation of this idea can be done on many software platforms. One approach is to design a whole system based on MATLAB [5, 6]. Image processing is easier when done in MATLAB, but the software has many drawbacks such as the size required is very large. Hence, we have used Python as it is a very user-friendly language and has ample libraries which simplifies implementation of complex functions.

Another algorithm based on hand detection using skin color histograms has also been proposed [4]. This does not provide accurate threshold images of the gestures as it is extremely sensitive to ambient lighting conditions. Shadows formed on the hand while making varying hand shapes results in incorrect gesture recognition. Thus, this method is error prone (Fig. 2).

Fig. 2. Example of hand detection using skin color histogram

4 Brief Methodology

1. We use a 4 layered CNN model to train 47 gestures (47 classes)
2. We have used background subtraction technique to create and recognize gestures
3. Recognized gestures are displayed as text
4. The text is then converted to speech
5. The second party can reply in speech which is then recognized and displayed as text
6. For speech processing, pyttsx3 and speech libraries have been used (Fig. 3).

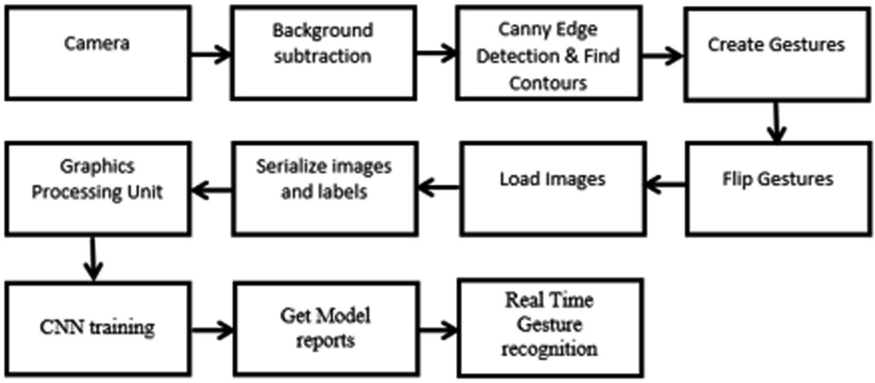


Fig. 3. Flow diagram of our method

5 Algorithm

Gestures are created using background subtraction technique. For the first 30 frames, the system calibrates and finds the running average of the present frame from previous frame. This running average is stored as our reference background. Any change in this background is then detected and is subtracted [8]. The resultant image is processed for edge detection using Canny Edge Detection Algorithm [11] to improve the accuracy, Gaussian blur as well as Binary Thresholding [9] and the contours are calculated to find the area of pixels under the detected region and for shape analysis. These gestures are then fed into the network in binary format as processing hand gestures in RGB format is subject to errors due to various skin shades. Processing power required for color image processing is thrice as much required for binary image processing. RGB format leads to unnecessary wastage of resources such as storage and increased complexity. For this application, we have obtained satisfactory results with binary images as we require only the boundary of the gesture. Hand boundaries are traced using contours and this is used to segment the image into hand and non-hand areas [1, 9].

Training is done using CNN built with Keras using minimum lines of code. Due to our large dataset, we require effective down sampling which is achieved using CNN [10].

For prediction, we use Keras predict [12]. Prediction begins only when the area of pixels covered in the bounding rectangle are greater than 7000.

The predicted gesture is mapped to its respective label from the database which is displayed as text using OpenCV and is then converted to speech using Python text to speech algorithm. The prediction is displayed and converted to speech only for those symbols for which the prediction probability is greater than 80%. The default speech rate is 200 words per minute (Fig. 4).

Our system allows the listener to respond as and when he/she wants to. The words spoken by the listener are converted to text that can be read by the mute person (Figs. 5 and 6).

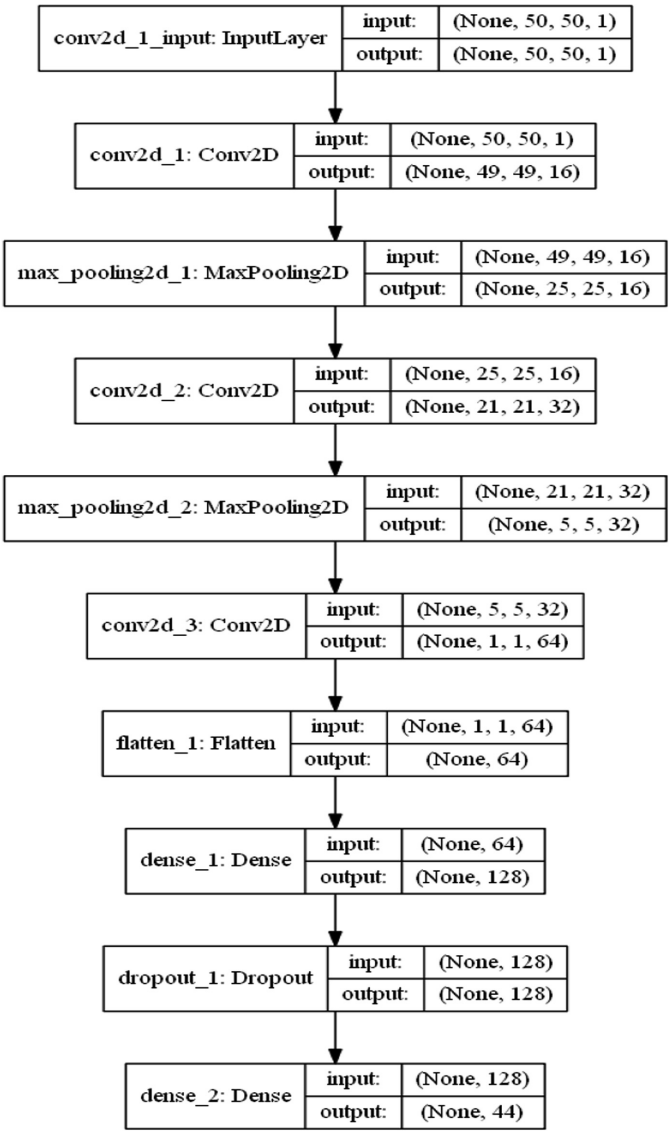


Fig. 4. CNN model

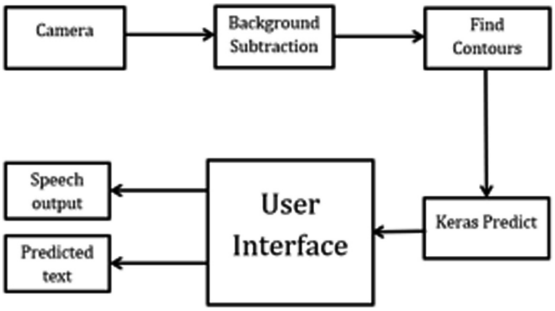


Fig. 5. Block diagram of the working

Fig. 6. Hand detection using background subtraction

6 Results and Discussion

Prediction accuracy of the model over 10 epochs is found to be 97.89%. We chose 10 as the optimal number of epochs as this gave us the least validation error i.e. Misclass percentage according to the Table 1 below.

Table 1. Overall results of the model

Parameters	Values
Average prediction time during training	0.001034 s
Average prediction time during real time recognition	0.003519 s
Time taken to predict 18800 test images	7 s
Prediction accuracy of the model	97.89%
Misclass	2.11%

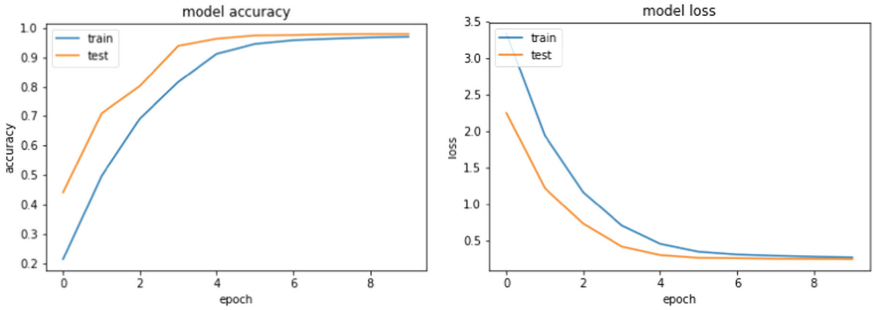


Fig. 7. Accuracy and loss graphs per epoch for the CNN model

It can be seen that the prediction time and the complexity of our model is very less. The accuracy that is achieved during training is reflected during the real time recognition (Fig. 7).

7 Conclusion

The above results provide support to our novel contribution. It can also be inferred that the objective of our project has been achieved. We have been successful in implementing a simple and scalable two way communication model by using background subtraction, image processing in OpenCV and CNN.

To convert this project into a viable product, we need to implement it on a portable device like a mobile phone. To do this we need to create a desktop application for the laptop and an application on our mobile phone using android studio [3]. We propose to do this by making a service on the laptop that will connect to the Android app on phone. Thus, our laptop will act as a server which has access to our CNN model and the rest of the recognition system. Through the app on the phone, we will send requests to the server to record a real time video and to recognize the gesture. The server will process results and send it back to the app.

References

1. Hussain, I., Talukdar, A.K., Sarma, K.K.: Hand gesture recognition system with real-time palm tracking. In: 11th IEEE India Conference: Emerging Trends and Innovation in Technology, INDICON 2014. Institute of Electrical and Electronics Engineers Inc. (2014)
2. Elmahgiubi, M., Ennajar, M., Drawil, N., Elbuni, M.S.: Sign language translator and gesture recognition. In: 2015 Global Summit on Computer & Information Technology (GSCIT), pp. 1–6 (2015)
3. Loke, P., et al.: Indian sign language converter system using an android app. In: Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA, January 2017. Institute of Electrical and Electronics Engineers Inc., pp. 436–439 (2017)

4. Gupta, M., Meha, G., Prateek, D.: Sign language to speech converter using neural networks. Int. J. Comput. Sci. Emerg. Technol. **14**(3) 2044–6004 (2010)
5. Butte, A., Jadhav, S., Meher, S.: *Hand Gestures And Speech Recognition System For Deaf-Dumb* (2018)
6. About American Sign Language. https://www.startasl.com/american-sign-language, August 2016
7. Sign Language Recognition. https://github.com/Evilport2/Sign-Language (2018)
8. Background subtraction. https://gogul09.github.io/software/hand-gesture-recognition-p1. Accessed 06 April 2017
9. OpenCV documentation. https://docs.opencv.org/4.0.0/
10. CNN Keras. https://www.tensorflow.org/guide/keras
11. Gonzales, R.C., Woods, R.E.: *Digital Image Processing*
12. Raschka, S.: *Python Machine Learning* (2015)

Efficient Fuzzy-Based Multi-constraint Multicasting with Fault Tolerance Routing Mechanism

N. Sivapriya(✉) and T. N. Ravi

Department of Computer Science, Periyar E.V.R. College(A), Trichy, India
nmsivapriya@gmail.com, proftnravi@gmail.com

Abstract. A very efficient and well-known computing environment is Mobile Adhoc Network (MANET). However, the node capacity and delay are affected during the data transmission due to its mobility. To tackle this problem, Multi-criteria Enhanced Optimal Capacity-Delay Tradeoff with Efficient Fuzzy-based Multi-constraint Multicast Routing (MEOCDT-EFM2R) method has been proposed to solve the optimal route selection problem where the multiple network metrics are taken into consideration. However, it requires fault tolerance-based Cluster Head (CH) selection since it does not handle any transmission or link failure in the network. Therefore in this paper, Efficient Fuzzy-based Multi-constraint Multicast Fault Tolerance Routing (MEOCDT-EFM2FTR) method is proposed to efficiently handle the transmission failure in the network. In this method, the CH for each cluster is chosen depending upon on the maximum nodal weight which is stored in the routing table. Initially, each and every node computes its weight with different network metrics like residual energy, mobility speed, computational power and fault tolerance. Then, the node with the highest weight is elected as CH of a specific cluster and each CH coordinates itself as a ring to tolerate any transmission failure by choosing a new CH. So, the new CH takes the responsibility of initial CH to complete the transmission without degrading the network performance. Finally, the simulation gives the evidence for the performance effectiveness of the MEOCDT-EFM2FTR method compared to the MEOCDT-EFM2R for throughput, routing overhead, delay, etc.

Keywords: Mobile ad-hoc network · Clustering · Multi-casting · Cluster head election · Fault tolerance · Transmission failure

1 Introduction

MANET is a kind of decentralized wireless network consisting of several mobile nodes that can transmit data with each other directly or indirectly via wireless links. Even though, it is extremely challenging since each node has a limited computing power resource, little storage and a short transmission range. Nodes that do not fall within the communication range of other nodes can transmit data through relay nodes. The non-deterministic mobility model incurs synchronized and random topological changes. Due to the dynamic nature of network such as wireless links and limited bandwidth

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 475–484, 2020.
https://doi.org/10.1007/978-3-030-37051-0_54

availability, the topological changes become more frequent that causes network efficiency.

Nowadays, these networks have been deployed in distributed applications such as inter-node transmission, information exchange, data aggregation, key distribution, group communication, privilege grant, etc. [1] During the implementation of this kind of applications, specifically in MANET, the Cluster Head (CH) is a crucial component that is responsible for coordinating these activities [2]. Therefore, it is very helpful to include a CH for providing the critical decisions in a simple manner. As a result, a CH selection is a popular research challenge in distributed networks. In Multi-criteria Enhanced Optimal Capacity-Delay Tradeoff with Efficient Fuzzy-based Multi-constraint Multicast Routing (MEOCDT-EFM2R) method [3, 4], optimal node selection within the cluster of network during data transmission was achieved by considering the multiple network metrics like delay, bandwidth, Link Stability Factor (LSF) and residual energy. These metrics were converted into a single metric named fuzzy cost or communication cost by using fuzzy logic method to find an optimal path from source to the destination that reduces end-to-end delay. However, the link or nodes failure was not efficiently handled that reduces the network performance.

Hence in this paper, Efficient Fuzzy-based Multi-constraint Multicast Fault Tolerance Routing (MEOCDT-EFM2FTR) method is proposed. The main aim of this method is selecting the CH and constructing the ring of all CH to tolerate any link or node failure in the network during transmission. Initially, the network is split into different clusters where each node has its own information such as computational power, residual energy, mobility speed and fault tolerance. Based on these metrics, each node calculates it node weight and distributed with each other. Then, the node with the highest weight is picked as CH and each CH arranges itself in a ring. If any transmission fails through specific CH, then a new CH is selected in a constant time based on the ring. Therefore, a new CH transmits the data packet to the destination without packet loss. Thus, this MEOCDT-EFM2FTR method achieves fault tolerant routing between source and destination in the network.

2 Related Work

Democratic leader finding algorithm with fault tolerance [5] was proposed for large-scale MANET. This algorithm was proposed based on the general parliamentary polity followed by the democratic countries which always provides the existence of an executive for coordinating and monitoring various activities and also for taking decisions regarding affairs or issues in the state. This parliament concept brings in failure resiliency to this algorithm and ensures greater availability of leader, especially on occurrence of failure. However, it reduces the resource availability and increases the energy consumption.

An Adaptive Secondary Cluster head-Aided Clustering (ASCAC) scheme [6] was proposed for group communication in MANET. In this scheme, a token circulation method was proposed by using an adaptive secondary CH-aided clustering algorithm. The initial Cluster Head was selected depending on the link degree between nodes and mobility of each node. As well, a secondary CH was set inside each cluster by taking

the part of the functions of the initial CH such as functionalities of clustering, token monitoring, storage of data related to clustering, etc. If initial CH fails, then secondary CH will get the chance to maintain track of the token circulation. However, average number of primary CH changes was not reduced efficiently. Leader election algorithm using Fibonacci heap structure [7] was proposed in wireless networks. In this method, the Fibonacci heap tree was used to select the leader by computing the minimum key of the Fibonacci heap. However, the resultant structure was complicated. Also, it requires high memory space.

An energy efficient CH selection for fault tolerant routing [8] was proposed in MANET for maximizing the CH energy and reducing the single link failure. However, energy consumption was still not reduced efficiently. Weight-based K leader election algorithm [9] was proposed in MANET. At first, very few coordinator nodes were chosen locally and those nodes using diffusing computation approach gather the weights of left over nodes. Then, the coordinator nodes were collaborated together and the weights of all the nodes in the network were collected by the highest weight coordinator to elect the final leaders. However, the election time was high.

An adaptive fault tolerant, non-blocking and coordinated check pointing algorithm [10] was proposed for cluster-based MANET. In this algorithm, least number of mobile hosts in the cluster was encouraged to record checkpoints. By using this algorithm, the unwanted checkpoints were minimized by maintaining exact dependencies among processes and piggybacking check pointing sequence numbers on to the normal messages. However, it does not handle the concurrent failures and multiple executions at the same time.

A security fault-tolerant routing [11] was proposed for multi-layer non-uniform clustered Wireless Sensor Network (WSN). Initially, the multi-layer non-uniform clustered network topology was established. Then, the trust model and fuzzy logic were used in the CH selection process for evaluating the qualification of sensors to become a CH. Additionally, the priority level and the trust value were also used for selecting the security CH as the next hop. Through the selected CH, a path was constructed between different layers. Further, a fault-tolerant algorithm was proposed based on rollback strategy for improving the security and fault-tolerant of the network. However, network lifetime was less.

3 System Model

In this section, the proposed MEOCDT-EFM2FTR method is explained in brief. Initially, the entire network nodes are split into many clusters [12]. For all the clusters, each node has its own information i.e., network metrics such as Residual Energy (E_r), Mobility Speed (MS), Computational Power (CP) and Fault Tolerance (FT). Such information of each node can distribute with each other for selecting their Cluster Head CH during data transmission. The considered network metrics are defined as:

- Residual Energy (E_r): It is defined as the energy level in a node after receiving or transmitting the data packets i.e., remaining energy of a node. It can be computed according to the distance between two nodes as:

$$E_r(N_i) = \sum_{i=1}^{n} E_r[distance(N_i, N_{i+1})] \tag{1}$$

- Node Mobility Speed (MS): It represents the rate at which a node moves from one location to another. It is calculated as follows:

$$MS = \frac{1}{|i,j|} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{T} \int_0^T RS(i,j,t)dt \tag{2}$$

$$\text{Where } RS(i,j,t) = \left|V_i(t) - V_j(t)\right| \tag{3}$$

  Here, (i,j) refers the number of distinct node pair, n is the total number of nodes in the network, $RS(i,j,t)$ is the Relative Speed between nodes i and j at time t, $V_i(t)$ and $V_j(t)$ are velocity of node i and j respectively at time t and T refers the total simulation time.
- Fault Tolerance (FT): It is the ability of preventing and enhancing the network reliability from any node failure or link failure.

$$\text{Where } k_{SD} = \sum_{i=1}^{k} \delta(P_i) \tag{4}$$

$$FT = 1 - e^{-k_{SD}} \tag{5}$$

$$\delta(P_k) = 1 - \frac{|P_k \cap P_o|}{|P_o|} \tag{6}$$

  Here, P_o refers the shortest path between the source S and destination D, P_k refers one of the paths between node S and node D, $\delta(P_k)$ is the number of paths constructed by the routing protocol.
- Computational power: It defines the node's computational ability. If the network topology happens to change, the participant node may be in a situation to leave the computation because of the forced termination or power off. Further, this may lead to link failure. Therefore, a fault tolerance model is required to recover the network from the node crashes.

Once these network metrics are known, the combined weight for each node is computed based on the weight associated with each metrics as follows:

$$W(N_i) = w_1 E_r(N_i) + w_2 MS(N_i) + w_3 CP(N_i) + w_4 FT(N_i) \tag{7}$$

In Eq. (7), w_1, w_2, w_3 and w_4 are the weighting factors for their corresponding network metrics. The weighting factors are chosen arbitrarily such that $w_1 + w_2 + w_3 + w_4 = 1$.

For each node, their combined weight is computed. Then, the computed node weights are stored in the routing table which is distributed to each other nodes in the network. According to this information, the node with the highest weight is opted as

CH for that particular cluster. Moreover, each CH forms itself as a ring. During this process, only a distinct single ring is constructed from all the CH in the network. In Fig. 1, a data transmission is carried out through an optimal route which is selected based on MEOCDT-EFM2FTR method. If any node or transmission fails in the network, then a ring of a CH is used to elect the new CH to complete the data transmission without any packet loss.

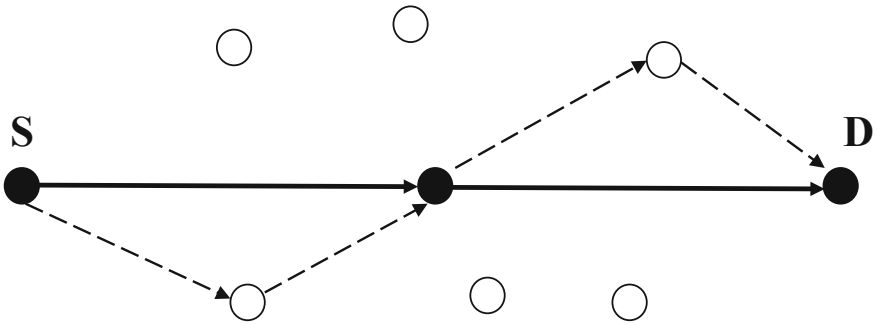


Fig. 1. Fault tolerant network

4 Simulations and Analysis

Here, the efficiency of the proposed MEOCDT-EFM2FTR method is analyzed and compared with the existing MEOCDT-EFM2R method by using Network Simulator version 2 (NS2.35). The considered performance metrics are throughput, routing overhead, end-to-end delay, Energy Cost per Packet (ECP), Packet Delivery Ratio (PDR), packets dropped. The simulation parameters are given in Table 1.

Table 1. Simulation parameters

Parameters	Value
Number of nodes	40
Node's speed	0.01 m/s
Network simulation area	1500 × 1500 sqm
Frequency	2.4 GHz
Radio range	250 m
MAC Protocol	IEEE 802.11
Packet size	512 bytes
Packet type	RTP/UDP
Transmission Power	15 dBm
Number of channels	2
Channel capacity	2 Mbps
Transmission rate	4 Mbps

(*continued*)

Table 1. (*continued*)

Parameters	Value
Packet interval	2 ms
Traffic source	CBR
Node mobility	0–20 m/s
Mobility model	Random way point
Propagation model	Free space propagation
Traffic rate	4 packets/s
Initial energy	50 J

4.1 Throughput

Throughput is the number of bits received at the destination within a given time.

Table 2. Comparison of throughput (kbps)

Mobility speed (km/h)	MEOCDT-EFM2R	MEOCDT-EFM2FTR
10	54	58
15	52	56
20	50	54
25	48	52
30	46	50
35	44	48
40	42	46
45	40	44

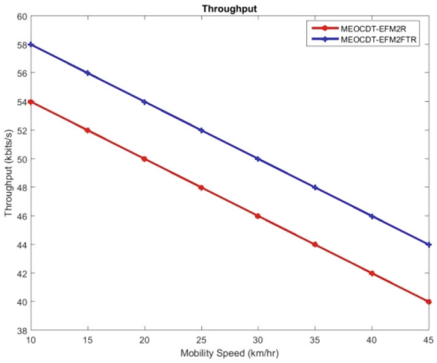


Fig. 2. Comparison of throughput

Table 2 gives the throughput comparison of proposed with existing technique for different mobility speeds is carried over. In Fig. 2, x-axis denotes the mobility speed in km/hr and throughput in kbps is in the y-axis. Based on the analysis, it is evidently clear that the proposed MEOCDT-EFM2FTR method receives higher throughput than the MEOCDT-EFM2R method.

4.2 Routing Overhead

It is the total number of routing packets in the network.

Table 3. Comparison of routing overhead

Number of connections	MEOCDT-EFM2R	MEOCDT-EFM2FTR
10	0.071	0.063
15	0.085	0.072
20	0.094	0.081
25	0.099	0.089
30	0.106	0.097
35	0.116	0.106
40	0.124	0.116
45	0.135	0.127

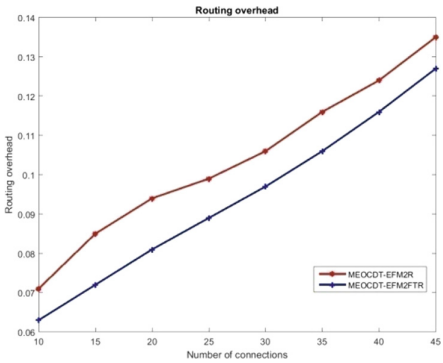


Fig. 3. Comparison of routing overhead

Table 3 gives the routing overhead of proposed with existing technique and also compared for different number of connections. In Fig. 3, x-axis takes number of connections and routing overhead values in the y-axis. From the prior analysis, it is concluded that the proposed MEOCDT-EFM2FTR method has reduced overhead than the MEOCDT-EFM2R method.

4.3 End-to-End Delay

End-to-End Delay is the time elapsed between transmitting the data packet from the source and receiving the packet at the destination.

Table 4. Comparison of end-to-end delay (ms)

Mobility speed (km/h)	MEOCDT-EFM2R	MEOCDT-EFM2FTR
10	0.0093	0.0089
15	0.0094	0.0090
20	0.0095	0.0091
25	0.0096	0.0092
30	0.0097	0.0093
35	0.0098	0.0094
40	0.0099	0.0095
45	0.0100	0.0096

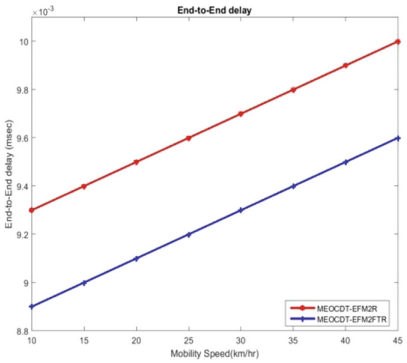


Fig. 4. Comparison of end-to-end delay

Table 4 shows the comparison of proposed with existing method in terms of end-to-end delay for different mobility speeds. In the Fig. 4, x-axis denotes the mobility speed in km/hr and the end-to-end delay values in milliseconds in y-axis. From the

prior analysis, it is evident that the end-to-end delay of the proposed MEOCDT-EFM2FTR method is comparatively less than the MEOCDT-EFM2R method.

4.4 Energy Cost Per Packet

Energy Cost per Packet (ECP) is the ratio between the average energy consumption over the number of data packets successfully received at the destination node.

Table 5. Comparison of ECP

Mobility speed (km/h)	MEOCDT-EFM2R	MEOCDT-EFM2FTR
10	8.8	8
15	9.5	8.8
20	10.4	9.5
25	11	10.2
30	11.8	11
35	12.6	11.7
40	13.8	12.6
45	14.3	13.4

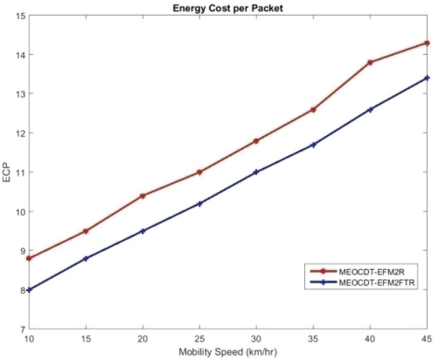


Fig. 5. Comparison of ECP

Table 5 shows the comparison of proposed with existing method for the energy cost required for a packet in different mobility speeds. In the Fig. 5, x-axis denotes the mobility speed in km/hr and y-axis denotes the ECP values. Based on the comparative analysis, it is evident that the ECP of the MEOCDT-EFM2FTR method is minimum than that of MEOCDT-EFM2R method.

4.5 Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is the fraction of the total number of data packets received to the number of data packets transmitted over the communication channel.

Table 6. Comparison of PDR(%)

Mobility speed (km/h)	MEOCDT-EFM2R	MEOCDT-EFM2FTR
10	96	97.2
15	94.9	96
20	93.8	95
25	92.8	94
30	91.2	92.6
35	89.5	90.9
40	88	89.4
45	87.1	88

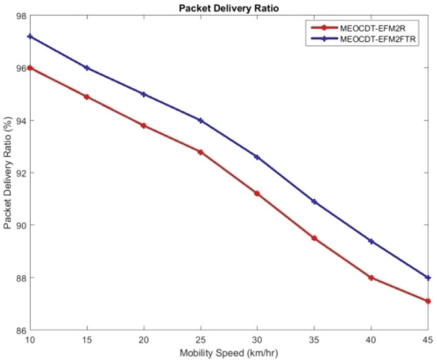


Fig. 6. Comparison of PDR

Table 6 compares proposed with existing method in terms of PDR for different mobility speeds. In the Fig. 6, x-axis denotes the mobility speed in km/hr and the PDR values in % y-axis. From the analysis, it is concluded that the PDR of the proposed MEOCDT-EFM2FTR method is most promising than the MEOCDT-EFM2R method.

4.6 Packets Dropped

It is the sum of packets dropped due to the queue overflow.

Table 7. Comparison of packets dropped

Mobility speed (km/h)	MEOCDT-EFM2R	MEOCDT-EFM2FTR
10	104	95
15	120	109
20	140	125
25	152	139
30	159	148
35	167	159
40	180	170
45	200	186

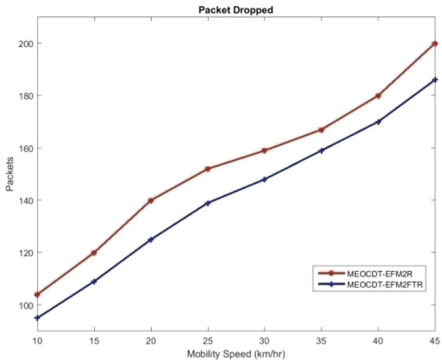


Fig. 7. Comparison of packets dropped

Table 7 shows that the proposed strategy excels than the existing method in terms of packets dropped for different mobility speeds. In the Fig. 7, x-axis denotes the mobility speed in km/hr and the number of dropped packets in y-axis. From the analysis, it is concluded that the total number of packets dropped by the proposed MEOCDT-EFM2FTR method is less than the MEOCDT-EFM2R method.

5 Conclusion

In this paper, MEOCDT-EFM2FTR method is proposed for MANET to enhance the fault tolerant CH and multicast routing path selection algorithm. In this method, the fault tolerant CH for each cluster is elected based on the weight of nodes in the network. The combined weight with the network metrics such as residual energy, mobility speed, computational power and fault tolerance is computed. The failure of node or transmission is solved by selecting a new CH by using a ring structure between each CH. Thus, this method ensures the fastest and fault tolerant CH selection in MANET without degrading the network performance under different mobility conditions. Finally, the simulation results are evaluated through NS2 and compared with the MEOCDT-EFM2R method to demonstrate the efficiency of the proposed method. From this analysis, it is concluded that the proposed MEOCDT-EFM2FTR method achieves higher performance than the existing method.

References

1. Mohandas, R., Krishnamoorthi, K., Sudha, V.: energy sensitive cluster level security selection scheme for MANET. Wireless Pers. Commun. **105**(3), 973–991 (2019)
2. Bentaleb, A., Boubetra, A., Harous, S.: Survey of clustering schemes in mobile ad hoc networks. Commun. Netw. **5**(02), 8 (2013)
3. Jia, R., Yang, F., Yao, S., Tian, X., Wang, X., Zhang, W., Xu, J.: Optimal capacity-delay tradeoff in MANETs with correlation of node mobility. IEEE Trans. Veh. Technol. **66**(2), 1772–1785 (2017)
4. Sivapriya, N., Ravi, T.N.: Multi-criteria node rank based time limited neighbor detection for enhanced optimal capacity-delay tradeoff in MANETs. Int. J. Res. Anal. Rev. **6**(1), 469–474 (2019)
5. Sharma, S., Singh, A.K.: Democratic Leader finding algorithm for large mobile ad hoc networks. In: 31st International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 304–312. IEEE Press (2011)
6. Subathra, P., Krishnan, P.R., Sivagurunathan, S.: A cluster-based reliable token circulation scheme for group communication in MANET. Arab. J. Sci. Eng. **37**(3), 647–664 (2012)
7. Jain, A.K., Sharma, R.: Leader election algorithm in wireless environments using fibonacci heap structure. Int. J. Comput. Technol. Appl. **3**(3), 34 (2012)
8. Narayanan, A.E., Devi, R., Jayakumar, D.A.V.: An energy efficient cluster head selection for fault-tolerant routing in MANET. Int. J. Eng. Technol. **5**(2), 1281–1289 (2013)
9. Raychoudhury, V., Cao, J., Niyogi, R., Wu, W., Lai, Y.: Top k-leader election in mobile ad hoc networks. Pervasive Mob. Comput. **13**, 181–202 (2014)
10. Mansouri, H., Badache, N., Aliouat, M., Pathan, A.S.K.: Adaptive fault tolerant checkpointing algorithm for cluster based mobile ad hoc networks. Procedia Comput. Sci. **73**, 40–47 (2015)
11. Ye, Z., Wen, T., Liu, Z., Song, X., Fu, C.: A security fault-tolerant routing for multi-layer non-uniform clustered WSNs. EURASIP J. Wirel. Commun. Netw. **192** (2016)
12. Pathak, S., Jain, S.: An optimized stable clustering Algorithm for mobile ad hoc networks. EURASIP J. Wirel. Commun. Netw. **51** (2017)

Performance Evaluation of Filtering Techniques in Filtered OFDM for 5G Technology

Hardik B. Tank(✉), Bhavin S. Sedani, and Nirali A. Kotak

Gujarat Technological University, Ahmedabad, Gujarat, India
{hbtank, nakotak}@ldce.ac.in,
bhavin_s_sedani@yahoo.com

Abstract. Filtered orthogonal frequency division multiplexing is one of the most promising candidate waveforms for 5G and beyond technology for the upcoming wireless communication system. Filtered OFDM ensures all the advantages of the orthogonal frequency division multiplexing technique with additional advantages in terms of spectrum efficiency and robustness in high SNR system and also in some specific cases, ideal spectrum utilization can be achieved by F-OFDM which can completely eliminate the guard band. This paper aims at comparing the performance of various filters by different windowing techniques such as rectangular, triangular, bartlett and hanning window to complex window function such as Kaiser, Nuttall's Blackman-Harris, root raised cosine window which can be applied to Filtered OFDM in terms of spectrum confinement, BER improvement and overall throughput betterment. In this research work, multiple windowing techniques have been simulated with Filtered OFDM and their performance has been evaluated. Based on the simulation results, Filtered OFDM with complex window function such as Kaiser, Nuttall's Blackman-Harris, root raised cosine can be seen as the potential candidate for future generation wireless communication system in terms of betterment in spectrum efficiency and improved out of band interference.

Keywords: 5G · Filtered OFDM · Windowing techniques · Root raised cosine window · Kaiser window · Nuttall's Blackman-Harris window

1 Introduction

Fifth generation mobile communication system is the upcoming phase after the 4G LTE that is long term evaluation standards. 5G technology should not be limited only for the mobile communication system but it will cover almost all the sectors such as various industries, semiconductor vendors, various manufacturing firms any many more. 5G will reach not only specified for cell phones but it will reach to almost all industries. Huge demand for wireless based services such as to carry video and other rich content services and IoT (internet of things) based services are the major push toward the race to fifth generation technology. To fulfil this major objectives next generation technology will provide large broadband speed, ultra reliable connectivity and ultra low latency for minimum delay in the communication.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 485–495, 2020.
https://doi.org/10.1007/978-3-030-37051-0_55

In order to improve the data rate and spectral efficiency we can depart physical layer of 5G from 4G LTE in number of ways. Coding Schemes, channel models, power amplifier design, modulation schemes all need to be designed and developed according to meet the 5G standards. To improve spectral efficiency by limiting out-of-band emissions new radio waveforms including: Filtered OFDM (F-OFDM), Windowed OFDM (W-OFDM), and Cyclic Prefix OFDM (CP-OFDM) is proposed by the 3GGP.

2 System Model

OFDM, as a multi carrier modulation technique, has been widely adopted by 4G communication systems, such as LTE and WiMAX. It has many advantages: robustness to channel delays, single-tap frequency domain equalization, and efficient implementation. But the main limitations of this technique in spite of several advantages are the loss in spectral efficiency due to higher side lobes and the strict synchronization requirements. New modulation techniques are, thus being considered for 5G communication systems to overcome some of these factors [8].

A new waveform in 5G should be able to support diverse service and deployment scenarios in a carrier band and provide very good spectrum localization, while inheriting the advantages of OFDM. Further justifying these benefits in this document some preliminary analysis is done with the prime contenders for the next generation mobile communication waveform. Waveform candidates for considerations can be roughly categorized in as OFDM based orthogonal waveform as Universal-Filtered (UF-OFDM), windowing-OFDM, and filtered-OFDM belong to this category, in which complex-domain orthogonality of OFDM symbols is maintained [6] (Fig. 1 and Table 1).

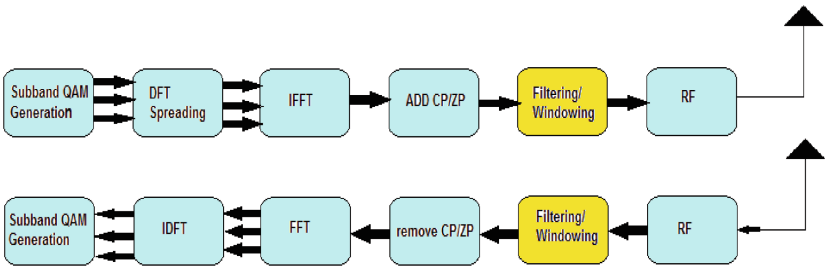


Fig. 1. Block diagram of OFDM-based orthogonal waveform scheme

Table 1. OFDM-based orthogonal waveform schemes

Category	Waveforms	DFT spreading	Prefix	Frequency localization scheme
OFDM based multi-carrier	UF-OFDM	No	ZP	Sub-band filtering
	Windowing OFDM	No	CP	Windowing
	f-OFDM	No	CP	Sub-band filtering

Because of the following advantages of filtered OFDM over other waveform contenders we have selected it for the further implementation of designing the next generation waveform [6].

- Filtered OFDM supports the dynamic configurations to enable mixed service application and various deployment scenarios where each sub-band can serve its own target application or deployment, while the mutual impacts is greatly minimized.
- Filtered OFDM waveform can be easily adapted to support RAN slicing and hence provides a future proof design within a carrier band.
- It maintains the complex-domain orthogonality within the sub-band as OFDM waveform, and hence inherits all benefits of OFDM and could reuse all the OFDM transmitter and receiver schemes.
- Due to the orthogonality of the waveforms it is much more amicable to MIMO as well as Massive MIMO for the future technologies.
- F-OFDM shows better out-of-band radiation performance, so it can enable very high spectrum utilization [7].

3 System Design

The current 4G LTE standard is centered around traditional OFDM structure with 1024 FFT size, 64 QAM modulation technique with 600 subcarriers over the AWGN medium with 18 dB of SNR. The following snapshots are the simulation results of the aforementioned system i.e. 4G LTE with simple OFDM structure.

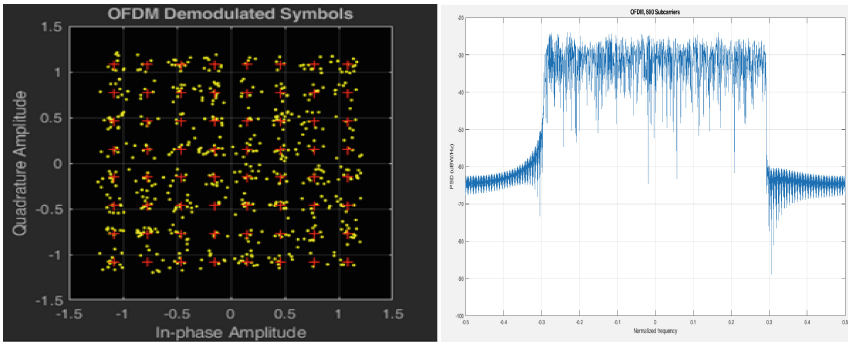


Fig. 2. Constellation and PSD of OFDM system.

From the above results it can be easily identified that there is a huge scope of further improvement in terms of the increment in spectral density by removing out of band emission and also the decrement in BER as per the constellation diagram where in 64 points are quiet scattered.

To improve the performance of the existing scheme, the signal generated after inverse FFT (IFFT) will be divided into number of resource blocks (RBs) and then applied to a specific window/filter with a typical passband that has:

Sharp transition
Flat characteristics in the passband
High out-of-band rejection.

Such characteristics form the base of F-OFDM system wherein to separate one band of frequencies from the other, Windowed-sinc filters are used. The basic properties of windowed sinc functions are: they are very stable, the performance of filter can be increased by minor mathematical changes and computational speed can be increased by changing the order of FFT. To meet above criteria a filter with rectangular frequency response such as sinc impulse response can be used, but sinc impulse response is not causal in nature so windowed function can be used which limits the non-causality and it ends to zero at both the ends and hence offers smooth transition. The ideal filter response for F-OFDM can be constructed by the implementation of various Windowed functions.

In first phase of this research work, it has been proven that filtered OFDM technique with basic filtering/windowing aspect will be the better contender over current 4G LTE with traditional OFDM that leads towards the development of one of the blocks of upcoming 5G systems. Moreover in the second phase, with the implementation and analysis of different windowing techniques in the F-OFDM itself, still further improvement in the filter characteristics can be obtained which can decide the appropriate window function for 5G system.

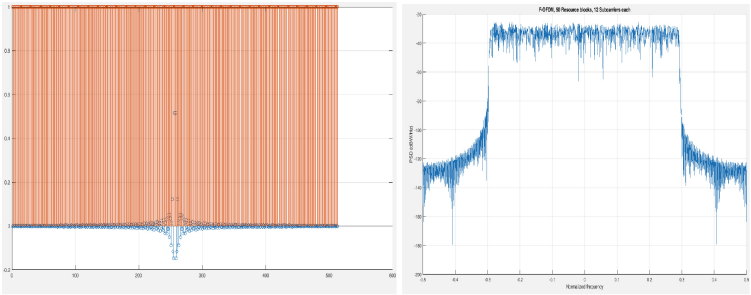
The following section illustrates the simulation results for the realization of F-OFDM technique with multiple windowing techniques which clearly shows the improvement in the above discussed parameters wrt traditional OFDM technique that has been shown in Fig. 2.

4 Simulation Results

In this evaluation, we apply different windowing techniques and based the results obtained; the appropriate window function can be selected that will be suitable for the 5G Filtered OFDM.

[1] **Rectangular Window**:

Here the simulation is carried out by considering a rectangular window of length L in the column vector w, this window function is provided for completeness; a rectangular window is equivalent to no window at all (Fig. 3).



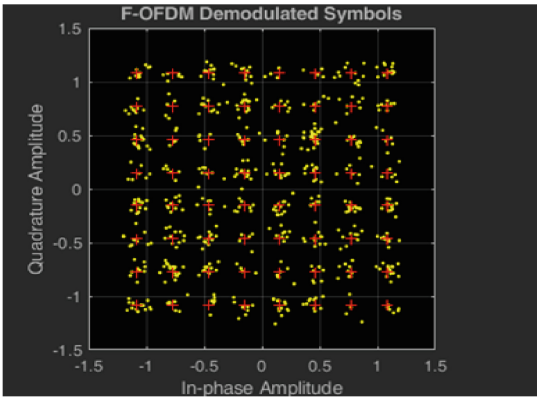


Fig. 3. Window response, constellation and PSD of F-OFDM system with rectangular window function.

[2] **Triangular Window**:

This window function will give M-point triangular window in the column vector, w and triangular window has the coefficients as below, (Fig. 4).

For M odd:

$$tri(n) = \begin{cases} \frac{2n}{M+1}, & 1 \le n \le \frac{M+1}{2} \\ 2 - \frac{2n}{M+1}, & \frac{M+1}{2} + 1 \le n \le M \end{cases}$$

For M even:

$$tri(n) = \begin{cases} \frac{(2n-1)}{M}, & 1 \le n \le \frac{M}{2} \\ 2 - \frac{(2n-1)}{M}, & \frac{M}{2} + 1 \le n \le M \end{cases}$$

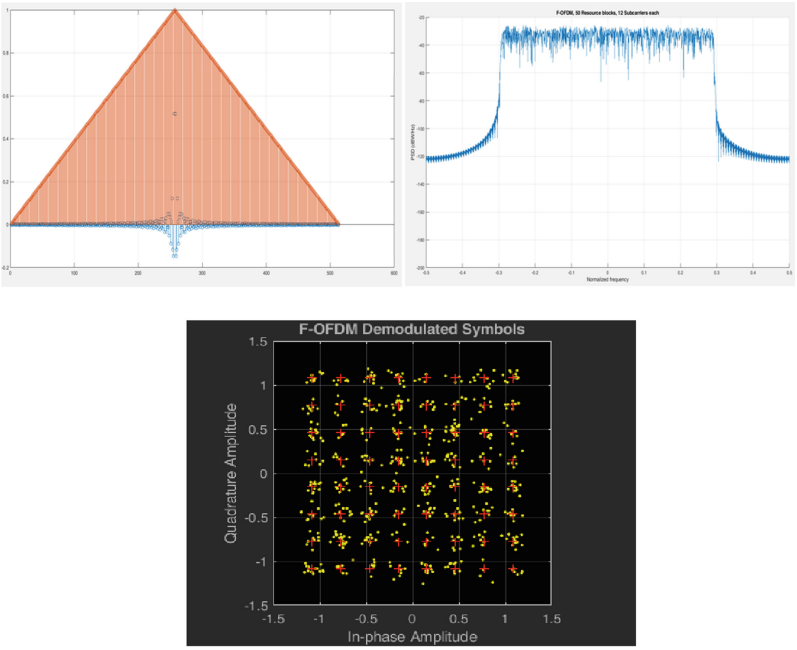


Fig. 4. Window response, constellation and PSD of F-OFDM system with triangular window function.

[3] **Bartlett window**:

This window function will give an M-point Bartlett window in the column vector w, where M is equal to positive integer. The coefficients of Bartlett window are as under

$$brtlt(n) = \begin{cases} \frac{2n}{M}, & 1 \le n \le \frac{M}{2} \\ 2 - \frac{2n}{M}, & \frac{M}{2} \le n \le M \end{cases}$$

The window length N = M + 1. There is a huge similarity between Bartlett window and triangular window. Triangle window is nonzero at first and last sample while Bartlett window has zeros at initial and final samples (Fig. 5).

[4] **Hanning Window**:

The following equation generates the coefficients of a Hann window:

$$hnng(n) = 0.5\left(1 - \cos\left(\frac{2\pi n}{M}\right)\right), \quad 0 \le n \le M$$

The window length N = M + 1 (Fig. 6).

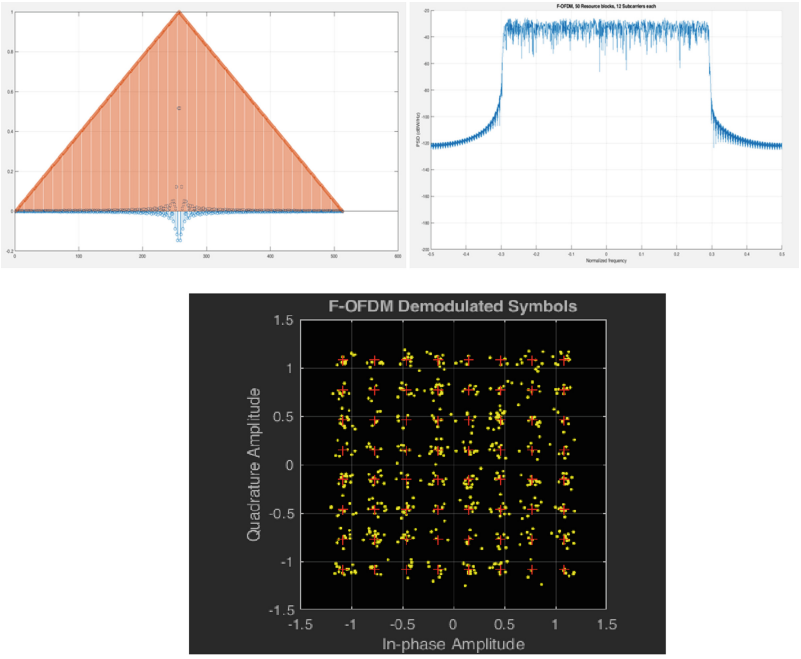


Fig. 5. Window response, constellation and PSD of F-OFDM system with Bartlett window function.

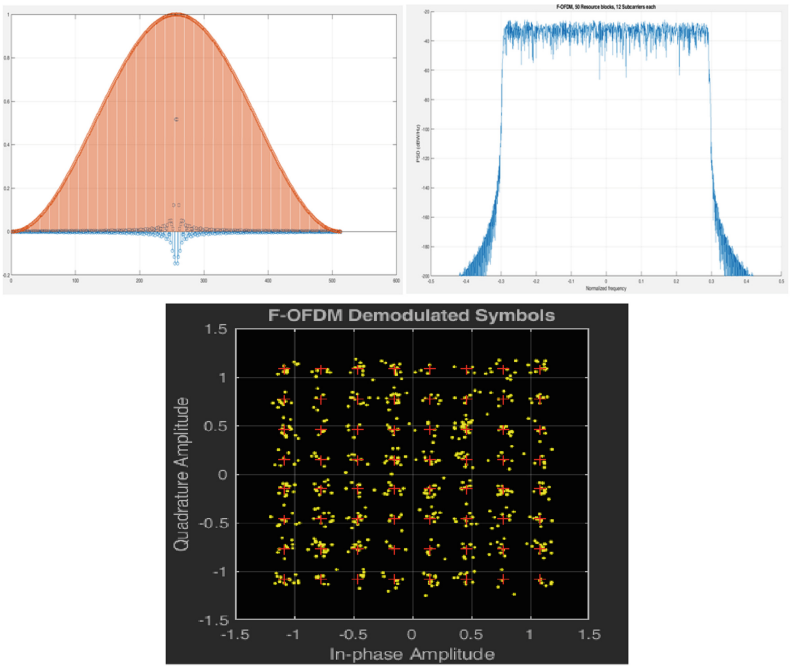


Fig. 6. Window response, constellation and PSD of F-OFDM system with Hanning window function.

[5] **Kaiser Window**:

The following equation is used to calculate the coefficients of a Kaiser window:

$$ksr(n) = \frac{I\left(\beta\sqrt{1-\left(\frac{n-M/2}{M/2}\right)^2}\right)}{I.\beta}. \quad 0 \le n \le M$$

beta = 0.5, where I is the modified Bessel function with zero order. The length of the window is $N = M + 1$. For the designing of an FIR filter with side lobe attenuation of α dB, the Kaiser window function should be implemented by using the following β.

$$\beta = \begin{cases} 0.1102(\alpha - 8.7), & \alpha > 50 \\ 0.5842(\alpha - 21)^{0.4} + 0.07886(\alpha - 21), & 50 \ge \alpha \ge 21 \\ 0, & \alpha < 21 \end{cases}$$

The increment in value of β will increase the width of the main lobe and reduces the amplitude of the side lobes as well thereby increases the attenuation (Fig. 7).

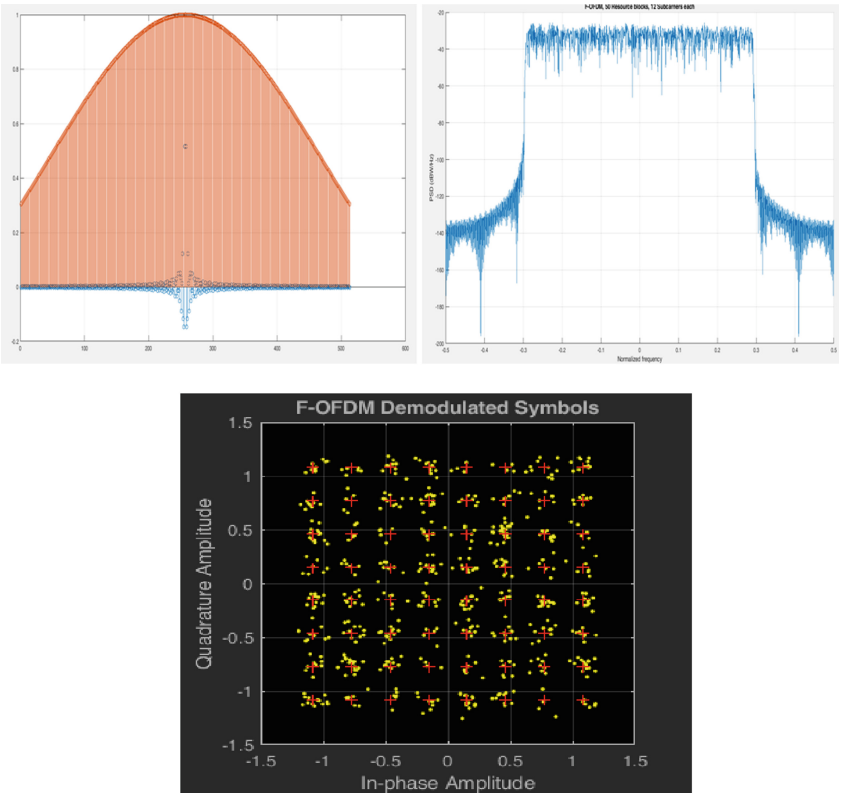


Fig. 7. Window response, constellation and PSD of F-OFDM system with Kaiser window function.

[6] **Nuttall's Blackman-Harris Window**:

A Nuttall described N-point, 4 term, symmetric Blackman-Harris window can be defined by this window function. Here the maximum number of side lobes is minimized that is why the window is minimum. To anticipate this, the coefficients are different than Blackman Harris. The following equation defines the symmetric Nuttall window:

$$nutl(n) = a - b.cos\left(\frac{2\pi n}{M-1}\right) + c.cos\left(\frac{4\pi n}{M-1}\right) - d.cos\left(\frac{6\pi n}{M-1}\right)$$

where n = 0,1,2, …, M − 1.

The following equation defines the *periodic* Nuttall four-term Blackman-Harris window

$$nutl(n) = a - b.cos\left(\frac{2\pi n}{M}\right) + c.cos\left(\frac{4\pi n}{M}\right) - d.cos\left(\frac{6\pi n}{M}\right)$$

where n = 0, 1, 2, … M − 1.

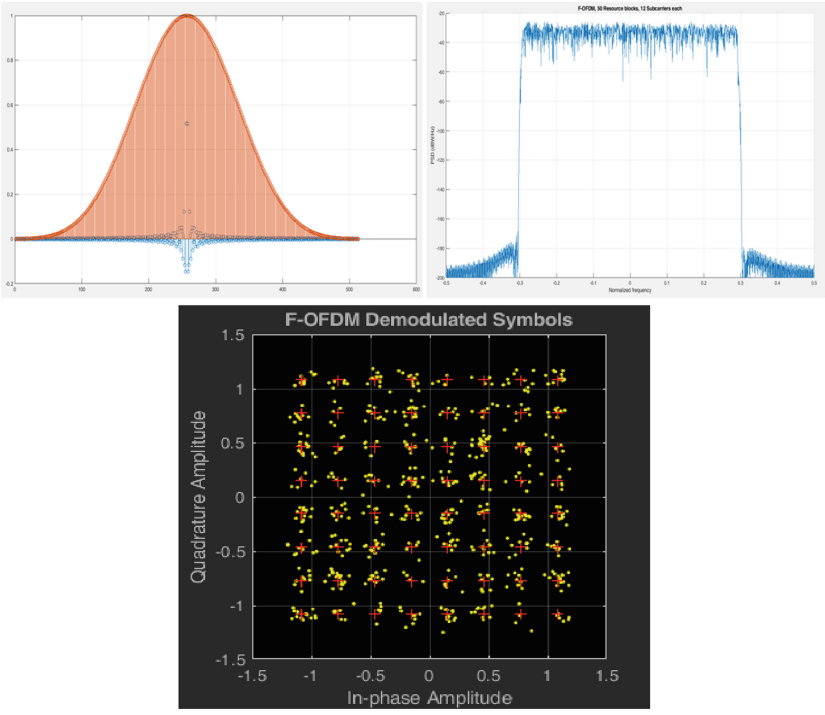


Fig. 8. Window response, constellation and PSD of F-OFDM system with Nuttall's Blackman-Harris window function.

The periodic window is N-periodic.

The coefficients for this window are, a = 0.3635819, b = 0.4891775, c = 0.1365995, d = .0106411 (Fig. 8).

[7] **Root Raised Cosine Window [RRC Window]**:

To minimize the ISI we implemented the raised cosine filtering that has been used to separate the transmitter and receiver filter, so raised cosine filter is combined effect of transmitter and receiver filter. By varying the parameter we can set the root raised cosine filter shape (Fig. 9).

$$rrc(n) = \left[0.5\left\{1 - cos\left(\frac{2\pi n}{M-1}\right)\right\}\right]^{\alpha} \quad \text{where} \quad \alpha = 0.6, \mathrm{M} = 513.$$

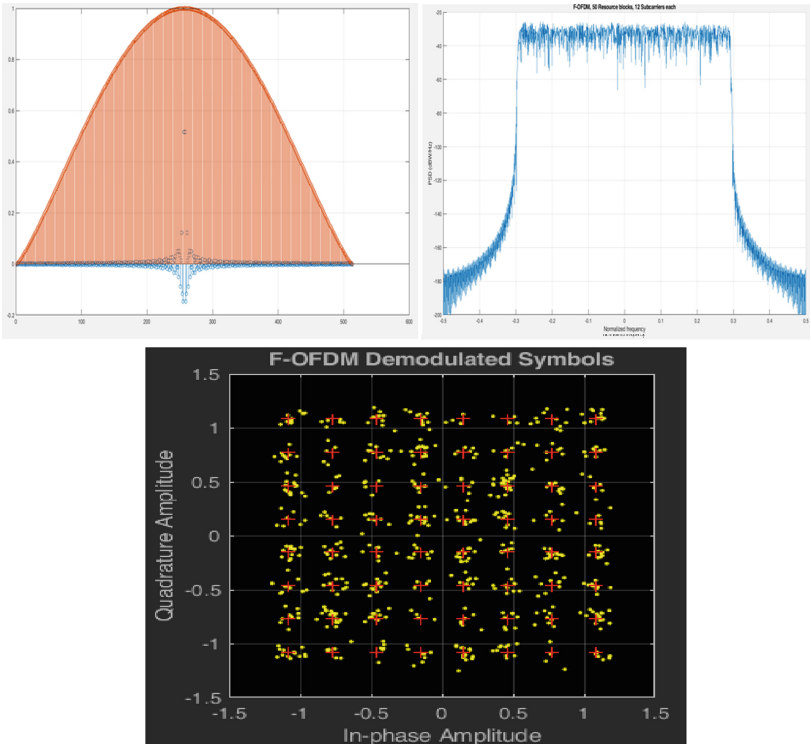


Fig. 9. Window response, constellation and PSD of F-OFDM system with root raised cosine window function.

5 Comparative Analysis of Windowing Functions

Based on the simulation results obtained in Sect. 4 for different windowing functions in F-OFDM, the following comparison can be made amongst the all techniques so as to select the best candidate in F-OFDM which leads towards the modular realization of 5G system.

Window function	Transition	Pass band characteristic	OOB rejection	BER at SNR = 18 dB
Rectangular	Gradual	Inflate	Very low	1×10^{-3}
Triangular	Gradual	Inflate	Low	8.3×10^{-4}
Bartlett	Gradual	Flat	Low	8.3×10^{-4}
Hanning	Sharp	Flat	Low	5.5×10^{-4}
Kaiser	Gradual	Flat	High	5.5×10^{-4}
Nuttall's Blackman Harris	Sharp	Flat	High	4.5×10^{-4}
Root raised cosine window	Sharp	Flat	Very high	4.5×10^{-4}

6 Conclusion

The main focus of this research work is on F-OFDM technique and its implementation using multiple windowing aspects so as to analyze the best candidate over the traditional OFDM in 4G LTE system thereby leading towards the upcoming 5G standard. Based on the simulation results, it can be clearly derived that the requirement of flat passband, sharp transition band to minimize guard band and sufficient stop band attenuation will be fulfilled by the F-OFDM technique with Nutella's Blackman Harris window, Kaiser window and Root Raised Cosine window functions.

References

1. Abdoli, J., Jia, M., Ma, J.: Filtered OFDM: a new waveform for future wireless systems. In: IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Stockholm, 2015, pp. 66–709 (2015)
2. Guan, P., Wu, D., Tian, T., Zhou, J., Zhang, X., Gu, L., Benjebbour, A., Iwabuchi, M., Kishiyama, Y.: 5G field trials—OFDM-based waveforms and mixed numerologies. IEEE J. **35**(6) (2017)
3. Nagul, S.: A review on 5G modulation schemes and their comparisons for future wireless communications. In: Conference on Signal Processing and Communication Engineering Systems (SPACES), Date of Conference, 4–5 Jan (2018)
4. Zhang, L., Ijaz, A., Xiao, P., Molu, M., Tafazolli, R.: Filtered OFDM systems, algorithms and performance analysis for 5G and beyond. IEEE Trans. Commun. **66**(3) (2018)
5. Yang, L., Xu, Y.: Filtered-OFDM system performance research based on Nuttall's Blackman-Harris window. In: IEEE 17th International Conference on Communication Technology (ICCT) Date of Conference, 27–30 (2017)
6. R1-162152. OFDM based flexible waveform for 5G. 3GPP TSG RAN WG1 meeting 84bis. Huawei, HiSilicon (2016)
7. R1-165425. F-OFDM scheme and filter design. 3GPP TSG RAN WG1 meeting 85. Huawei, HiSilicon (2016)
8. Sedani, B.S., Kotak, N.A.: Transition from 4G to 5G technology: high speed mobile communication perspective. In: International Conference on Recent Developments in Science, Engineering, Management and Huminities (2018)

Multifactor User Authentication Mechanism Using Internet of Things

S. G. Santhi(✉) and M. Kameswara Rao

Department of Computer Science and Engineering, Annamalai University, Chennai, India
ssau2009@gmail.com, mkraoau2016@gmail.com

Abstract. Internet of Things (IoT) is one of key areas of research, where number of smart devices is connected to internet. In IoT network Users operate various devices which process and exchange data with other devices and end users. User Verification is a major aspect in web based applications. One of the most well known evidence solutions used right now are the alphanumeric-based plans. Graphic critical solutions are offered to control the way users are ready to examine graphic styles pictures greater than reviewing alphanumeric secrets. Lexicon Attacks are focused on clients who select weak passwords. Graphical passwords offer enough security for such assaults. In this paper we suggest a two step authentication approach combining graphical passwords and Internet of Things.

Keywords: Two step authentication · Graphical password · Internet of things

1 Introduction

Safety has been a massive matter in relation to proof is important because it could prompt a quick violation of human security as a result of being able to view a resource by unapproved people. Distinctive sorts of validation components have been utilized to keep information secure and private. A standout amongst the most utilized confirmation instruments is text based verification frameworks since they are basic and advantageous to use with negligible expense. Nonetheless, literary passwords have a few downsides: simple to overlook and a great many people will in general use passwords that are basic and simple to be retained. Thus, these passwords can be speculated with very little exertion, they can likewise be effectively split and inclined to bear surfing assaults. Graphical secret phrase plans are used widely than literary passwords as various subjective and mental examinations demonstrated that individuals can recall pictures much superior to recollecting words [1]. In this work we proposes a two step verification process where clients get verified in the first step using their graphical password and in the second step using clients own IoT device registered during registration process.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 496–502, 2020.
https://doi.org/10.1007/978-3-030-37051-0_56

2 Literature Survey

Graphical confirmation methods could be partitioned into two fundamental classes: acknowledgment based and review based [2]. Acknowledgment based frameworks are otherwise called cognometric frameworks or search metric frameworks. What expanded the fame of graphical secret key plans are the down sides and obstructions in the usage of varieties of validation strategies, for instance, literary passwords, bio-metric and numerical PIN verification plans. Right away, solid printed passwords are challenging to retain. Acknowledgment based frameworks requires recognizable evidence of target pictures among a specialized amount of distracter objects. Diverse kinds of pictures have already been utilized, for instance, faces, images, regular articles, arbitrary expressions, so forth. The outstanding capacity of individuals perceives recently seen pictures make the acknowledgment based calculations famous. The most significant productive methods were exhibited in [3] where an acknowledgment based systems was proposed. The proposed graphic verification plan been dependent on hash illustration innovation. Due to their structure, the customer should opt for a specific number of pictures from loads of unpredictable pictures produced by a program. Afterward, the customer will probably be approached to decide on pre-chosen pictures to be confirmed. The outcomes recognized that 90 of the members could accept utilizing that technique, while only 70 succeeded utilizing material based accounts and pins. Irrespective of the reason, the ordinary sign-in time is lengthier than the standard methodology. The shortcoming of one's structure could possibly be that the machine needs to save lots of the photos per customer in plain content. Furthermore, the easiest way toward picking loads of pictures from the photo database could possibly be boring and tedious for the client. The work in [4] presents two story acknowledgment based techniques utilizing symbols to take care of the issue that acceptance based graphic secret term options have that they'll do not have an enormous place created for many web applications.

An ImagePass is undoubtedly an affirmation based strategy presented in [5]. Amid the enrollment organize, the shopper begins with a substantial amount of 30 pictures to peruse to produce a mystery expression. Amid the shopper login, ImagePass demonstrates a photo grid of 4×3 which is a blend of certifiable pictures and phony. Since ImagePass is undoubtedly an affirmation based structure, the shopper would need to begin to see the veritable pictures in the correct growth of approval. Position of the Pictures will vary for each sign-in. The database of ImagePass contains the photographs as numbers interesting to every single picture for that entire endorsement time span. Audit based structures require the purchaser to reproduce a picture he/she made or picked upfront during the selection sort out. Audit based plans is separated into two standard social affairs: unadulterated survey based and provoked survey based techniques [6]. Unadulterated review based structures are in general called Locimetric systems while incited survey structures will be in like manner termed as Drawmetric structures [7, 8]. The unadulterated survey based mechanisms are not useful to the users in emulating their passwords. One example is, Draw-A-secret (DAS), Grid Methods, Passdoodle is unadulterated audit designs [9, 10]. A touch screen can be used in the mechanism to draw the doodle. Another method considered snap A-Secret which unites

both locimetric and cognometric plans was presented in [11]. This blueprint allows the commitment of one's riddle over the correspondence with the image. Around the First step, customers must make somebody picture by superseding express locales of one's main picture. Right should the customer believe that the prevailing picture is perfectly for making a mystery key, he/she affirms anyone picture. Another cross breed contrive was developed in [12] in the name called PassHands. It will be the variety of graphical based affirmation passwords in addition to a biometric based palm development. This chart requires palm pictures constructed from human as a substitute for routinely used faces. In the midst of the login organize, nine relatively estimated pictures arranged with the palm are graded at a 3 × 3 system capriciously where among the many photos can be a mystery word picture and others are deluding pictures. The provoked survey based Schemes give customers one or two signs to empower the criminals to maximum benefit exact mystery word which assists them later around the sign-in stage. These signs and experiences are going to be shown as spots inside a picture which customers can select several of them. The principal flagged audit based arrangement and graphical mystery word plot when all is claimed in done was designed by Blonder. In this arrangement the mystery key constructed with explicit concentrations at a mystery expression picture. The buyer sets the mystery key by investigating predefined territories. Inside login arrange the purchaser picks comparative concentrations or regions around the identical right demand to login. Along these lines, this arrangement has various security issues, for example, spyware ambushes, bear surfing, creature power, and dictionary attacks. Pass Point security system has a sign-in stage where customers must pick the best spots around the correct demand to sign to the structure. The qualification in PassPoint may customer can tap on any point while in the mystery word picture which it wasn't open in Blonder's arrangement. PassPoint is progressively secure concerning brute power and lexicon ambushes yet for now not fixable to peeping and spyware strikes. Another approval plan called S3PAS [13] graphical system was developed. Inside enrollment, the purchaser picks and sports the mystery key he/she needs. Inside login screen, the artistic mystery state characters are subjectively showed up in a picture arrange where customers will want to tap at the cognizant imperceptible triangles surrounded with the mystery expression components or type characters which may have an area with each mystery expression triangle. Similar works are reported in [14–18].

3 Proposed Two Step Authentication Process

In this section, we propose Two Step, a mix of Graphical secret phrase and IoT Device Authentication.

Authentication Phase

Step 1: Graphical Password Selection

In stage one, a client is requested her client name and graphical password. The graphical password interface contains a set of icons (25 icons in a 5 × 5 grid) and the

user can select his choice of icons with a predefined number of clicks per icon as his password (Fig. 1).

Fig. 1. Proposed graphical password interface

For example the user can select icons and the number of clicks to be made during password verification as shown in Fig. 2. Let us assume the icons are numbers 1 to 25 from left to right in the 5 × 5 grid. Alice may select his graphical password icons numbered {2, 5, 14, 17, 22} and number of clicks per icons as {2, 2, 1, 1, 3} respectively.

Fig. 2. Selection of icons and number of clicks

During verification phase the user has to select the same icons and click that much number of times on his choice of icons as registered in the registration phase.

Step 2: IoT Device Registration

Every User must get their IoT Device get registered with the proposed IoT application platform. Enrolling an IoT gadget includes arranging the gadget as a gadget type, giving the gadget a name, and giving gadget data.

Verification Phase

Graphical Password Verification: During verification phase the user has to enter the graphical password selected in registration phase. The graphical interface with 5 × 5 set of icons jumbled in a random fashion. The user has to identify his icons and click on the pass icon as per the pre- registered number of clicks at the registration phase (Fig. 3).

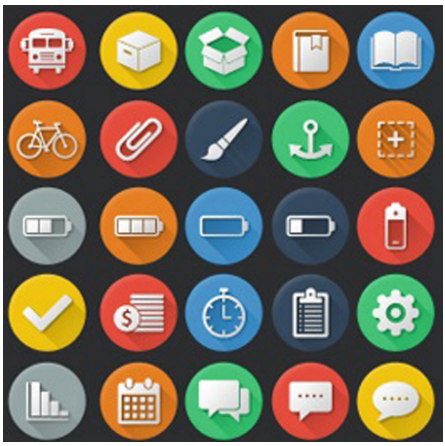


Fig. 3. Graphical password Interface with random shift in icon positions

If the user didn't find his pass icons in phase I he can slide the interface such that a new set of icons can be seen on the interface in which the user identifies his pass icons (Fig. 4).

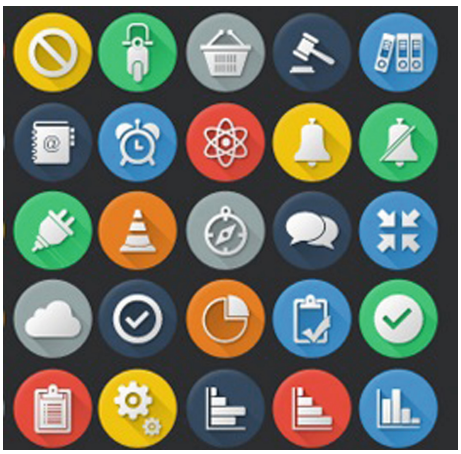


Fig. 4. New set of icons after a slide

The user has to select the same icons and click that much number of times on his choice of icons as registered in the registration phase.

IoT Device Verification: The user is authenticated in Step 2 by getting connected with his IoT device as registered during registration phase. The user has to submit the gadget type, gadget name, and the application connects to the IoT device for verification of its device ID which was registered at registration phase.

4 Usability and Security

Assaults on graphical passwords incorporate word reference assault, spyware assault, peeping assault and social designing assault. The proposed strategy is impervious to spyware and social designing assaults as a result of its two step verification process. The client can likewise incorporate his preferred quantities in the spaces which will build the security of the proposed work. On the security perspective, the customer tendency of selection of clicks for each icon makes the proposed strategy impenetrable to bear surfing strikes. The client can misinform the assailant who is playing out the shoulder surfing assault by pivoting his preferred wheels toward any path, while keeping a look on his mystery numbers. At each time the client signs in the icons in the openings are rearranged which make the assault increasingly trouble-some. In the event that a customer neglects to login with in 3 endeavors, the secret phrase must be reset. In this manner with an extensive secret phrase space and the pivot alternative with more hubs indicating, the shoulder surfer can be misinformed.

5 Conclusion

Graphic confirmation programs are confirmed an running exploration zone which methods to enhance the delivery of confirmation frameworks. The enthusiasm of our function is that we challenge that other approval structures have specific issues. The situation that we had with the abstract passwords is they are difficult to review, weak against various forms of attacks, for example; carry exploring and term research ambushes. In like manner, biometric and PIN based check designs are expensive to execute or apply on a broad scale. Graphical mystery key designs are generally proposed to greatly help customers with bettering recollect their passwords. This work presents a two step authentication process using graphical validation system and IoT Device Verification. The proposed validation mechanism is compelling against the various assaults. What's more, not normal for printed passwords, on the off chance that the graphical secret word was seen by an assailant, it is troublesome for the aggressor to produce the proper graphical secret word alongside IoT Device identification. The Work can be extended using public and private keys and a specific protocol for exchange of encrypted information among the IoT device and server.

References

1. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N.: PassPoints: design and longitudinal evaluation of a graphical password system. Int. J. Hum. Comput. Stud., 102–127 (2005)
2. Eljetlawi, A.M., Ithnin, N.: Graphical password: comprehensive study of the usability features of the recognition base graphical password methods. In: 3rd International Conference on Convergence and Hybrid Information Technology (2008)
3. Sabzevar, A.P.: Universal multi-factor authentication using graphical passwords. In: International Conference on Signal Image Technology and Internet Based Systems, pp. 625–632 (2008)
4. Mayer, A., Monrose, F.: The design and analysis of graphical passwords. In: Proceeding of The 8th UNISEX Security Symposium (1999)
5. Wu, T.-S., Lee, M.-L., Lin, H.-Y., Wang, C.-Y.: Shoulder-surfing-proof graphical password authentication scheme. Int. J. Inf. Secur. **13** (2014)
6. Zhu, B.B., Yan, J., Xu, N.: Captcha as graphical passwords a new security primitive based on hard AI problems. In: Proceedings of the IEEE Transactions on Information Forensics and Security, vol. 9, pp. 891–904 (2014)
7. Malek, B., Orozco, M.: Novel shoulder-surfing resistant haptic-based graphical password. Proc. Euro Haptics (2006)
8. Kameswara Rao, M., Yalamanchili, S.: Novel shoulder-surfing resistant authentication schemes using text-graphical passwords. Int. J. Inf. Netw. Secur. (IJINS) (2012)
9. Dunphy, P., Yan, J.: "Draw a secret" graphical passwords. In: 14th ACM Conference on Computer Communications Security (CCS), pp. 36–47 (2007)
10. Zhao, H., et al.: S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In: Advanced Information Networking and Applications Workshops, AINAW 2007 (2007)
11. Gao, H., et al.: A new graphical password scheme resistant to shoulder-surfing. In: International Conference on Cyberworlds. IEEE, Singapore (2010)
12. Sreelatha, M., Shashi, M., Anirudh, M., Md Sultan Ahamer, Manoj Kumar, V.: Authentication schemes for session passwords using color and images. Int. J. Netw. Secur. Its Appl. **3**(3) (2011)
13. Lashkari, A.H.: A secure recognition based graphical password by watermarking. In: International Conference on Computer and Information Technology, vol. 7, no. 1, pp. 164–170 (2011)
14. Apoorva, N., Lokesh, P.N., Rao, M.K.: Random grid size based graphical password authentication. J. Adv. Res. Dyn. Control. Syst. **10**(2) (2018)
15. Kameswara Rao, M., Usha Switha, T., Naveen, S.: A novel graphical password authentication mechanism for cloud services. Adv. Intell. Syst. Comput. **433** (2016)
16. Kameswara Rao, M., Vidya Pravallika, C., Priyanka, G., Kumar, M.: A shoulder-surfing resistant graphical password authentication scheme. Adv. Intell. Syst. Comput. 413 (2016)
17. Kameswara Rao, M., Phaneendra Kumar, C.V., Haritha, K.: Graphical password based authentication for mobile devices. Int. J. Appl. Eng. Res. **10**(2) (2015)
18. Kameswara Rao, M., Aparna, P., Avinash Akash, G., Mounica, K., Sampath Kumar, G.: A graphical password authentication system for touch screen based devices. Int. J. Appl. Eng. Res. **9**(18) (2014)

Auto Emergent System (AES)

S. Sureshkumar(✉), M. Saad Ahamed, P. Sanjay, and R. Saravanan

Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore 641022, India
sureshkumar.s@srec.ac.in, saad.ahamed.m@gmail.com, saravanan26lll999@gmail.com, sanjay.ps@yahoo.com

Abstract. Nowadays, due to the exploding growth of vehicles which paves a way for the unusual population in the road traffic, accidents are becoming more and more common among people. There are various factors which causes accidents. This paper lists out the classification of accidents and various solutions provided to avoid accidents as well as to overcome from accidents when it is encountered. Classification of accidents includes accidents by pedestrians, cyclists, mass casualty and animal accidents. The various solutions to avoid as well as to overcome accidents include usage of smart phones, VANET and GSM along with GPS. The proposed solution detects the accident and sends ambulance to the accident area by the usage of sensors. In this paper a derived factor named Crash rate analysis is used to determine the number of ambulances required for the accident area to take up the recovery process. This work is intended to provide better and faster lifesaving solutions for the road accidents.

Keywords: Road accidents · Crash rate · GPS · GSM · VANET · Firebase PIR sensor · Airbag sensor

1 Introduction

Fatal rate in India is increasing steadily day-by-day. Major causes are due to the road accidents. Statistics show that the major reason for the death of people in road accident is due to the delay in the reach of hospital and treatment process. When an accident takes place, an ambulance is called for rescue process and the victim is taken to the Hospital for treatment. Ambulances play a major role in this tedious process. The challenges in rescuing the victim are calling the ambulance from the spot of accident, allocation of number of ambulances based upon the number of victims, fetching the location of accident by the ambulance using GPS, to reach the spot as soon as possible and to take the victim to the Hospital as soon as possible.

The notable limitation of other proposed solutions for the automatic road accident rescuing system is that the system fails to detect the people count in the automobile and allocating insufficient number of ambulances. The reasons for the late arrival of ambulance include traffic congestion of automobiles in Indian Roadways, Improper allocation of pathway to the ambulance in traffic signals. So, the ambulance gets caught in vehicular queueing.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 503–512, 2020.
https://doi.org/10.1007/978-3-030-37051-0_57

This can be resolved using Internet of Things (IoT) [10] which interconnects the devices and provides the essential solutions for those problems. This domain provides us the use of existing hardware in an innovative way to meet the circumstances.

In this paper, we concentrate on proper scheduling of the ambulances to reach the victim's spot and to save the victim's life by taking them to the proper facilitated hospital based upon the patient's critical condition by resolving the traffic congestion problems and eliminating the delay factor in reaching destinations.

2 Classifications of Accidents

Road accidents has become more and more common these days. Injuries due to these accidents are the major cause for death in many countries. Accident refers to the undesired or unplanned incident which results in damage or injury. A road accident is something which occurs on a road open to public circulation in which at least one person is injured or killed.

There are various classifications of road accidents which is classified based on the reasons it takes place. Some of the various classifications of road accidents are:

2.1 Pedestrians

One of the most common road accidents that occur is hitting a pedestrian while driving an automobile [1, 2]. It may be due to:

i. Driver - The driver may lose control with the automobile or he/she may be drunk.
ii. Pedestrian - The Pedestrian may not obey road safety rules which may subject to a road accident.
iii. Automobile - The internal parts of the automobile may get damaged due to time factor or any other physical damage and the driver may lose control over the vehicle and which may lead to a road accident.

2.2 Pedal Cyclists

The pedal cyclists move slower than the other vehicles. Hence in a situation where a driver of particular vehicle overtakes other the cyclist almost doesn't come under the consideration of the driver and gets hit. A study says that pedal cyclists are more vulnerable than motorcyclists [3].

2.3 Animal Collision

It is the accident that takes place between the vehicle driver and the animals on the path. The reasons may include low visibility of light at night time and over speeding [4].

2.4 MCI (Mass Casualty Incident)

Mass or Multiple casualty incidents is defined as any incident wherein a large number of medical facility is required to save the victims. These types of road accidents occur when a large number of vehicles get collided or huge vehicles get collided with each other. A large number of people get damaged due to this kind of road accident and large medical facility is required to save the victims. This incident serves as an example for a MCI [5].

3 Types of Rescue Systems

There are various number of solutions proposed for the detection of road accidents. Some of the solutions are:

i. *Using Smartphones*: Various systems which provides solution to detect the road accidents is mostly based on smartphones [6]. This method uses the accelerometer and airbag deployment monitors to detect the road accident and send the message to the response center. The smartphone acts as a third person to notify about the accident. The sensors in the smartphone are used to detect the location of the accident and it sends the location of accident to the response center to fetch help on time.
ii. *Using VANET*: VANETs (Vehicular Ad-hoc Network) are also used to detect the accidents [7]. Airbag and crash sensor play a major role in this method. When an accident is sensed by these two sensors, the signals are transmitted to the micro-controlled based system. Global Positioning System (GPS) is used to locate the accident and GSM is used to share the location. The rescue team gets alert message with the help of VANET. The VANET unit consists of:
   (a) *On-board Units:* It is fixed inside the vehicle.
   (b) *Road-side Unit*: It is fixed along the road. Once when accident is detected communication takes place between these ObU and RbU and finally signals reaches the rescue team and hence rescue is done by the team. The communication between the board units may be of Vehicle-to-Vehicle, Infrastructure-to-Infrastructure, or Vehicle to Infrastructure.
iii. *Using GSM and GPS*: Using a microcontroller based infrared road accident detection system, the road accidents can be detected [8, 9]. In this method:
   (a) Sensors-Used to detect the accident.
   (b) GPS-Used to locate the place of accident.
   (c) GSM-Used to transmit the location.

Although these methods serve as a path for detecting the accidents there are a few limitations [11] in these methods which make these methods less efficient. The Table 1 lists out few limitations of these above-mentioned methods.

Table 1. Limitations of present rescue system

System	Limitations
Smartphones	Not every person owns a smartphone and there is a chance for getting failure of the smartphone. The probability of detecting the all the accidents that occur using smartphones is very less. Moreover, different smartphones have different response times and sensitivity which should be taken into account
VANET	Improper Environmental conditions fail this VANET system. The efficiency of VANET gets affected in places like intersection and subways
GPS and GSM	This method fails in the case of color of the automobile. IR sensor is used in GSM and GPS method which detects the accident based on the principle of Reflection. Hence this method fails in the case of dark colored vehicles in which absorption of IR rays occur rather than reflection due to which the signals cannot be transmitted

4 Different Types of Vehicles and Accident Detections

There are various types of vehicles in existence, which differs a lot in their size and speed. The no of passengers also differs according to the size of the vehicle.

Some of the common vehicles in existence and their accident detection mechanism are:

a. *Motorcycles*: Motorcycle accidents are also getting increased and there are some safety measures such as helmet. Nowadays, Smart helmets can detect the accidents using adrenaline secretion of human wearing the helmet and gyroscopic condition of the vehicle.
b. *Cars*: Mostly these type of vehicles uses airbag sensors to detect the accidents that happened to it.
c. *Trucks*: Damages to the truck drivers and passengers during a truck accident is rare. Thus, the same airbag sensor is also used here.
d. *Buses*: Buses may contain larger number of passengers in it and it is easy to detect the accident with help of same airbag sensor or vibration sensor. But detecting the injured passengers due to accident is little difficult in this case (Fig. 1).

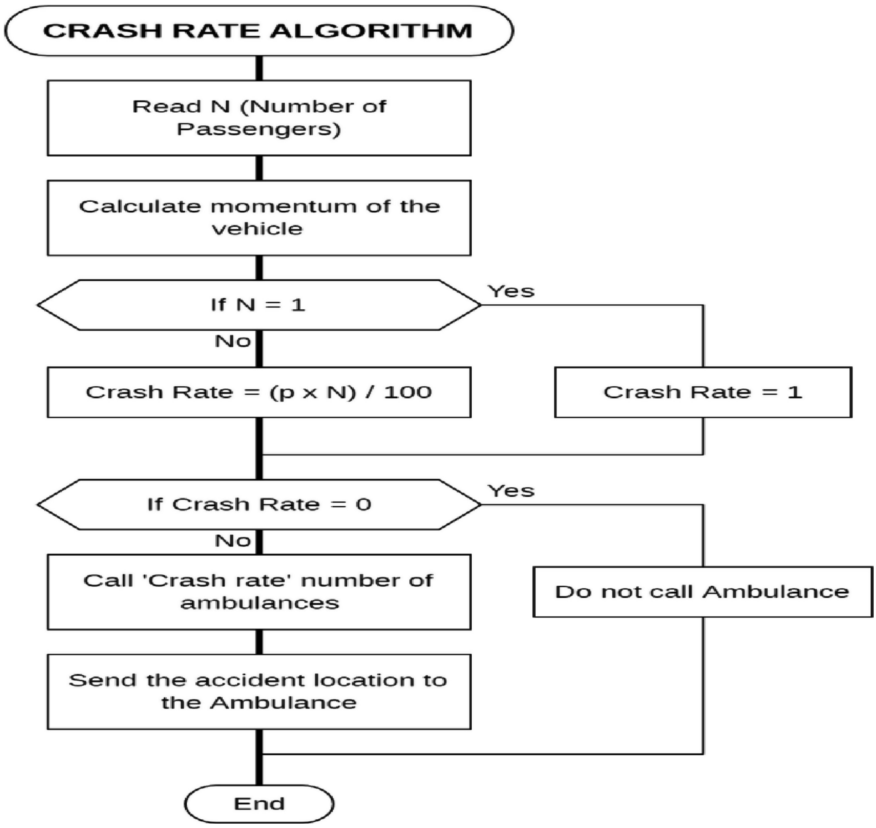


Fig. 1. Flowchart for crash rate algorithm

5 Proposed Solution

The above stated problems can be rectified using Auto Emergent System. The process of the device execution is detailed below (Fig. 2):

5.1 Accident Detection

Various types of road accidents can be detected using Airbag sensors (cars, trucks, buses, etc.) and Accident detection helmet (bikes). Thus, we don't want any of the additional sensors [13] to be used to detect the accidents. Airbag sensors are well developed to detect the accidents by experiencing a sudden deceleration. It works with 95% accuracy in detecting the accident. So, the output has been cascaded as the input of AES device. This input invokes the device to call for the ambulance.

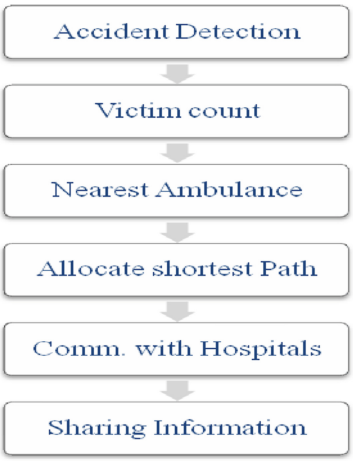


Fig. 2. Work flow

5.2 Victim Count

It's important to consider the number of passengers travelling in the automobile. Call for the insufficient number of ambulances may also cause death of the passengers. So, it's important to calculate the number of passengers. Hence, AES includes a Passive infrared Sensor (PIR) to identify and store the number of passengers in the automobile and to update the count once if the doors were opened or closed.

Call for the additional number of ambulances may also lead to the inconvenience for the ambulances. This is solved by calculating the **crash rate** of the automobile and to call for the ambulance accordingly. Thus, the process is detailed in below:

We use our own crash rate algorithm to find the crash rate of the accident which helps in finding the number of ambulances required for the accident rescue.

Mathematical model:

Recent maximum speed of the vehicle is updated to the AES device frequently. Once if the vehicle meets with an accident, the crash rate found using the following perspectives.

The maximum numbers of passengers for the common vehicle are listed below in Table 2:

Table 2. Standard maximum passengers count table

TPYE	Bike	Car	Truck	Bus
Max passengers	**2**	**5 or 7**	**2**	**50**
Level count	**1**	**1**	**2**	**2**

Fig. 3. Simple architecture of AES

The above graphical representation illustrates the simple architecture of Auto Emergent System (AES) (Fig. 3)

1. Detecting the accident and sending the info to cloud server.
2. Cloud server searches for the nearest ambulance from the location of 1.
3. Searching for the ambulance (red).
4. Found the nearest ambulance (green).
5. The ambulance reaches the accident spot.

The above listed are some of the commonly used vehicles on road. The maximum count can be varied according to the type of the vehicle. Level count is based on the weight of the vehicles. Heavy vehicles are given 2 whereas others are 1.

The crash rate of the vehicle is calculated using the following formula:

T = Type of the vehicle
N = Number of passengers (T)
c = Level count (T)
s = Maximum speed at the time of accident

$$\textbf{CRASH RATE (R)} = (s \times N) / (c \times 100)$$

Only for $\mathbf{N \neq 0, 1}$
If N = 1, CRASH RATE (R) = 1
If N = 0, CRASH RATE (R) = 0
Calls 'R' number of ambulances when the AES device is invoked.

Model Calculation:

Consider a car of weight 1500 kg hits a pillar at a speed of 60 kmph. There are 4 people inside a car. Now, **N = 4**

$$\mathbf{c = 1}$$
$$\mathbf{s = 60}$$

Crash rate = $(60 \times 4)/(1 \times 100)$

Crash rate = 2

Call 2 ambulances for the rescue process.

5.3 Search for the Nearest Ambulance

Locating the nearest ambulance is the most important task in this tedious process. First of all, the location details such as latitude and longitude of the crash zone was fetched using inbuilt GPS in the AES device. Fetched location details of the automobile was sent to the cloud server and the cloud server searches for the nearest ambulance using the tracking device in every ambulance which has been tracked and updated to the cloud server.

Likewise, the nearest ambulance was identified and details were passed to reach the spot as soon as possible and rescue the victim's life.

The first nearest ambulance was given 30 s of time to accept the task. If the first ambulance fails to accept in exceptional cases, it will be passed to the next nearest ambulance and the process will be continued. This helps to avoid the time delay, if suppose the ambulance driver was busy.

5.4 Allocate the Shortest Path

To look for the shortest and less traffic route to reach the destination using Google maps traffic analysis. The shortest route is allocated from the Ambulance to the accident spot and accident spot to the nearest hospital.

Traffic congestion also leads to the increase in the duration of ambulance to reach the hospital. Hence, this can be resolved by making the signals on the way of the ambulance to the hospital to be in green until it crosses the traffic signal from before its 5 km of distance.

As a next part of reducing the traffic, notification alert is sent to the automobiles on the way of ambulance to the hospital. The notification alert can either be sent to the mobile phones of the neighbour vehicles or to its infotainment system which is connected to internet.

5.5 Finding the Need Based Hospital

According to the critical situation of the patient, Ambulance searches for the proper facilitated hospital. Check for the availability of emergency ward, doctor and pathological requirements [12]. The live location of the Ambulance is also shared to the hospital. This communication provides a better platform to allocate a better facilitated hospital to the patient.

5.6 Sharing Data

All information is shared to the registered contacts (family, friends) of AES device through its app. And also, the nearest cop was alerted about the incident respective to the location. The location details such as latitude and longitude of the accidental area and the details of the victim such as vehicle number and the number of ambulances required are sent to the Google firebase through the GSM module which is connected with the microcontroller. The real-time database of the firebase is used to send an data from the victim.

People near the accident can also check the active status of ambulance by entering the vehicle no. in the commonly accessible website (Fig. 4).

Fig. 4. Sharing data to other vehicles

6 Conclusion

This system brings out a better solution which has a greater impact in saving a human's precious life. This also resolves the number of ambulances required for particular accident based upon the crash rate algorithm by the type of the vehicle and number of passengers in the vehicle accordingly. It is found that, the crash rate analysis provided in this system gives better results when compared to the existing systems. This system reduces the disadvantages found in the previous systems and provides a standard solution for reducing the number of accidents.

7 Future Work

Integrating the system with Google Fi Sim cards as it shifts to the best network in the given area and also it can send message to the ambulance driver in the poor network coverage areas. It can also be implemented fire accidents and send the messages to fire engines. It can also be implemented in streets such as VANET so that accidents can be detected and sent to the user thereby reducing the chance for accidents to happen. The information about the accident is sent to the doctors who are nearby the accidental area who are off duty so that they can provide instant first aid to the victims thereby increasing the chances of saving the life of the victim.

Acknowledgment. The authors would like to thank the Management, Director, Principal and Head of the Department of Computer Science and Engineering of Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India for their motivation and the support rendered to carry out this work.

References

1. Malik, Y.S.: Road accidents in India—2016. In: Ministry of Road Transport and Highways, Government of India, New Delhi (August 2017)
2. Zia, Y., Sabir, M., Saeed, I.U., et al.: Pedestrian injuries and fatalities by patterns in reported road traffic crashes–Islamabad. J. Pak. Med. Assoc. **64**(10), 1162–1165 (2014)
3. Department for Transport: Facts on pedal cyclists. Last accessed on 1 May 2017. https://www.gov.uk/government/uploads/system/uploads/attachment data/file/447674/pedal-cyclists-2013-data.pdf
4. Khalil, U., Javid, T.: Automatic road accident detection techniques: a brief survey published on IEEE 2017
5. Delvalle Institute Office of Public Health Preparedness: What is mass casualty incident? Last accessed 1 May 2017
6. White, J., Thompson, C., Turner, H., Dougherty, B., Schmidt, D.C.: Wreck watch: automatic traffic accident detection and notification with smartphones. Mob. Netw. Appl. **16**(3), 285 (2011)
7. Praveena, V., Sankar, A.R., Jeyabalaji, S., Srivatsan, V.: Efficient accident detection and rescue system using ABEONA algorithm. Int. J. Emerg. Trends Technol. Comput. Sci. **3**(5) (2014)
8. Iyyappan, S., Nandagopal, V.: Automatic accident detection and ambulance rescue with intelligent traffic light system, published on arjeeie 2017
9. Sri Krishna Chaitanya Varma, Poornesh, Tarun Varma, Harsha. Automatic vehicle accident detection and messaging system using GPS and GSM modems. Int. J. Sci. Eng. Res. **4**(8) (2013)
10. IEEE Journal based on Internet of things: a brief study "published in 2018". http://iot.ieee.org/journal
11. Beshah, T., Ejig, D.: Learning the classification of traffic accident types. In: Published on 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems
12. Bangar, V., Chaskar, N., Kurhade, S., Borhade, B.M.: Smart ambulance rescue system with patient monitoring. Imp. J. Interdiscip. Res. (IJIR) **3**(12) (2017)
13. Fremantle, P., Kopp, O., Leymann, F., Reinfurt, L.: A detailed analysis of IoT platform, architectures: concepts, similarities, and differences. Inst. Arch. Appl. Syst. (2018)

Cloud Container Placement Policies: A Study and Comparison

Piyush Mishra(✉), Shubham Bhatnagar, and Avita Katal

School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India
suyashmishra96@gmail.com,
shubham.bhatnagarr@gmail.com, akatal@ddn.upes.ac.in

Abstract. Virtualization is a core technique used for running multiple applications and services at the same time. In addition to effectively increasing the utilization rate of bare metal hardware, virtual machines are also used for replicating test environments. However, the emergence of containers has been seen as an enhancement to virtualization. This paper discusses the concept of containers, how they function, and provides a theoretical analysis of containerization with reference to virtualization. In the end, the performance of container migration policies provided as part of CloudSim framework, namely First Fit, Least Full, Most Full and Random is evaluated using allocated number of hosts, containers, and virtual machines.

Keywords: Containers · Virtualization · Placement policies · Cloudsim

1 Introduction

Virtualization is described as the creation of a logical instance from a given physical instance. It is categorized into various types, depending on the entity being abstracted. This includes application virtualization, network virtualization, desktop virtualization, server virtualization and various types of hardware virtualization. The use of virtual machines has increased the utilization rate of available processing power, which was not being utilized to maximum extent earlier. To create and manage virtual machines, a software/firmware known as hypervisor or virtual machine manager, is used. It sits on top of the underlying host hardware and is responsible for facilitating the interaction between the virtual machines and the hardware resources of the host. Virtualization has been an essential component in implementing cloud computing, providing it the essential characteristics which includes scalability and elasticity.

Deriving from the concept of virtualization is the container technology [2]. It is an implementation of operating system (OS) virtualization which uses the kernel of the underlying OS to provide an encapsulation for deploying and launching applications. This does not limit the use of containers to applications only. They can also run virtual machines as well as clusters. Containers sit on top of a physical server and its host OS, e.g. Linux or Windows. Each container shares the host OS kernel and usually, the binaries and libraries too. Shared components are read-only. Containers are "shareable"

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 513–524, 2020.
https://doi.org/10.1007/978-3-030-37051-0_58

and can be used on a variety of public and private cloud deployments, accelerating development and test by quickly packaging applications along with their dependencies.

2 Containerization

A feature of the Linux kernel is 'namespace' [1]. A process has some resources allocated to it, such as process ID, hostname and file systems. The isolation of the resources utilized by a group of processes and then virtualizing it is done by namespace. Thus, each process is associated with some namespace (there are six kinds of namespaces supported by Linux kernel) and it can only access the resources falling under its own namespace. Hence, namespace provides a type of isolation. The memory in a modern operating system is divided into two categories: kernel space, which can only be accessed by the kernel and a user space, where user processes and other secondary processes run. The process of containerization involves the existence of multiple, isolated user spaces, each referred to as a container. Each container shares the underlying Linux kernel but functions in isolation from the other containers. Figure 1 describes the basic architecture of a container based virtualization i.e. containerization.

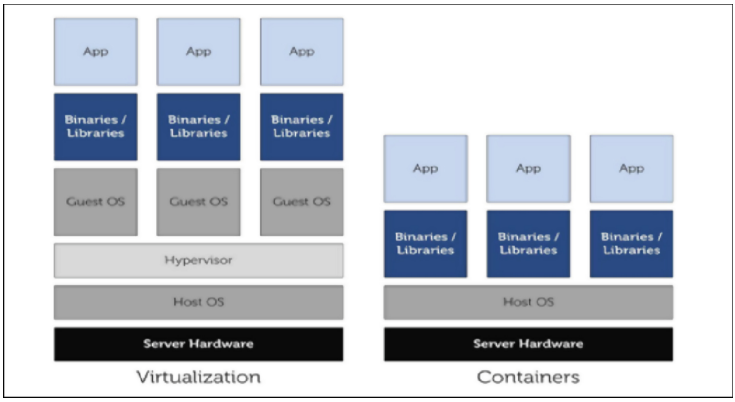


Fig. 1. Container architecture does not require a firmware/software like hypervisor

A container provides the run time environment for an application such that dependency on the underlying hardware is abstracted. A container typically consists of the application, the libraries, configuration files, binaries required by it, and the dependencies, combining all of these into a single package.

I. Types of Containers
   (a) OS Container – It permits the running of a complete OS i.e. the capability of running multiple processes. It permits the configuration of multiple applications, as done on an actual OS. Containers of this type are usually built from existing templates which define a structure and configuration. Usually, these templates are different flavors of Linux. Also known as system containers,

they share the kernel of the host OS and therefore provide quicker startup and low performance overhead. These are not to be considered as a separate guest operating system.

(b) Application Container - This container is designed to deploy a single application or a service within an application without the need for a VM. By providing the desired configuration environment that the application requires, the problem incompatibility and easy distribution is taken care of.

An important feature of containers is the usage of 'copy-on-write' technique. Consider a host node comprising of many containers. Each container will have the configuration files of the host. However, they are provided to the containers as a symbolic link. All the containers will share the resource (the files in this case) and only if a container attempts to modify the file, a copy of the files is provided to it onto which write operation is done. This technique facilitates resource management. The file system of a container has a special mount point on the host node which enables the host to check the files, if needed.

Containers are beneficial when it comes to debugging since they can replicate the production environment effectively. Also, a container is small size, typically in megabytes. Containers have a few limitations as well. The dependence on the kernel of the host can cause compatibility issues. Containers can exploit kernel vulnerabilities by using the root access they are given to the kernel. Moreover, the state of the container is not saved if the host is directly powered off.

3 Containerization Tools

Numerous container creation and orchestration tools have been released in recent times. This work briefly discusses three of them—LXC, LXD, and Docker. LXD is an extension to LXC.

I. Linux containers(LXC)
It is an interface which allows the creation/management of containers [3]. It derives its functionalities by combining the concepts of control groups and namespaces. Control groups is a feature of the linux kernel which maintains a group of processes that share a common criteria of limitation on usage of resources. Features such as monitoring the resources being utilized by a group of processes, the priority order of various gropus and control options, like checkpointing are available through a control group's interface. The LXC version currently in use is not restricted just to namespaces and control groups but also uses other kernel capabilities such as the kernel security option. LXC also makes use of Seccomp, which provides a process the option to filter the system calls that it receives and the chroot call which isolates files running inside the environment it provides from the other files on the system.

II. LXD
It can be understood as a hypervisor which manages linux containers [4]. LXD is a daemon container tool built using LXC and uses REST API as the communication medium. The security aspects of LXD are handled using the same

features as the LXC. This tool gives a complete operating system within the container and allows tools utilized for application deployment in a virtual machine (VM) to be used in the container. Hence, it is suitable for system containers.

Any LXD container has the following components: a file system, the image and runtime state. Each container also has an entity known as profile, which stores the configuration details of the container and all of its devices. Also, LXD allows unprivileged containers, which overcomes the security concern of using a privileged LXC container.

III. Docker

This project [5] started out as LXC containers modified for single application deployment. It can be thought of as the combination of application and the base image used for creating the container to present the application as a single process. Docker container uses the concept of union mount, which allows multiple file systems to be layered on top of each other but appear as single file system. The base image, similar to the one used to create a container, is also used in case of Docker. The Docker platform consists of two parts: Docker Engine, the tool which creates and manages the execution of containers and DockerHub, which is an SaaS offering of Docker, where users can share their images/repositories. It also allows repositories to be downloaded. The components of Docker Engine [6] are described in Fig. 2.

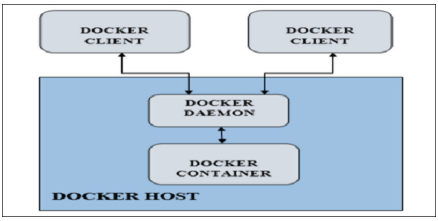


Fig. 2. Components of Docker engine

The main components of a Docker Engine are:

(a) Client: It is the interface for accessing Docker. Using CLI, the client connects and communicates to the server (Docker daemon) via REST API. Docker Engine follows client-server architecture.
(b) Docker Daemon: Responsible for the creation and distribution of containers.

The images (templates) that are used for creation of Docker container are often combined into a library (collection), known as a registry. These registries can be either public or for private use. DockerHub serves as a public registry. A 'Dockerfile' consists of a base image onto which instructions are executed, therefore resulting in the creation of new layers on top of the image. Each instruction adds one layer. Thus, if an image is to be built, the Dockerfile needs to be read. Figure 3 shows the layered file system that a Docker container follows.

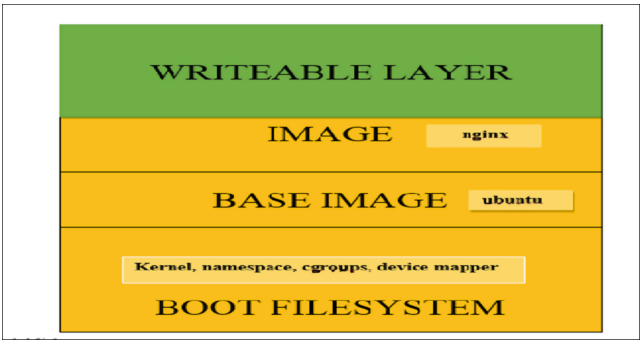


Fig. 3. Layered architecture of Docker container

In Fig. 3, the bootfs makes the base of the container. On top of it, a base image is loaded, which is a Linux distribution. Each instruction executed in the Dockerfile commits a layer on top of the base image. In the above diagram, the container has nginx installed. The top most layer denotes where the next instruction commit will occur. When the container is initially loaded, the writeable layer is empty.

The comparison performed between Docker and LXD on benchmarks such as CPU performance, memory, I/O storage and stateful snapshot [7] shows that they are on par with each other. There are certain stability issues regarding LXD in terms of live migration and disk performance.

4 Comparison with Virtualization

Containerization which is based on OS level virtualization, differs from virtualization in certain aspects:

I. Overhead
   Figure 4 shows the components of a virtual machine and a container. The virtual machine shares the physical hardware of the host while maintaining a separate, private copy of the layers above the physical processor - it uses an operating system of its own which may be completely different from the host operating system. The VM maintains a copy of the required libraries as well as any code written by the user. On the other hand, the container maintains a separate copy of only the libraries required and any code that the user writes in the container. The operating system is shared with the host, in addition to the physical hardware and processor.
   Thus, the overhead in creating a container is less as compared to the creation of a virtual machine instance. The average boot-time of Docker container is lesser than the time required by a VM [8].

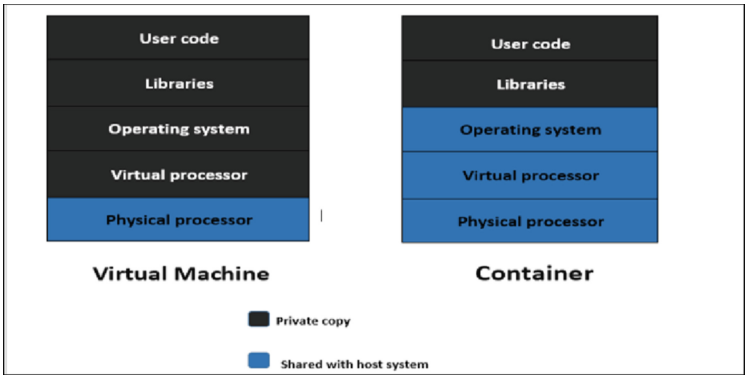


Fig. 4. Comparison of VM and container architecture

II. Portability
Containers share the underlying OS kernel. This limits the migration of containers across servers. For example, a Linux container can't be run on a Windows server.
Virtual machines can be migrated to any system if the required hypervisor is available. A VM instance has its own operating system, applications and libraries. Thus, the dependency on the host system is less as compared to containers.

III. Isolation
Containers have a larger attack surface as compared to virtual machines. Since containers are run through root access, vulnerability is high. Also, the access to OS kernel provides an attack entry point. VMs' run in isolation from one another. Since they use virtualized hardware and are monitored by the hypervisor, attacking the host system is difficult as compared to containers. Also, a breach in one VM doesn't compromise with the security of other VMs.

IV. Support Tools
Containerization is a relatively new concept when compared to virtualization. Existing container management tools like Kuberenetes and DockerUI are being assessed and updated regularly. On the other hand, there is no dearth of virtualization management software/tools. Also, when it comes to orchestration and management, the tools available in the market for virtual machines exceed that of containers in quantity.

V. Size
The space occupied by a single container is lesser than the space required by a VM. Thus, a system can host a greater number of containers as compared to virtual machine instances.

VI. Scalability
Containers are suitable for running microservices. Each container performs a specific task. Therefore, containers are difficult to scale if workload increases/decreases. In contrast, resource provisioning in case of a VM is simple using a hypervisor.

The comparison performed between KVM and Docker in tests based on network latency, bandwidth, memory access, block I/O and memory bandwidth [9] shows that Docker either equals or exceeded KVM in performance. Containerization and virtualization have their own merits and demerits. The two are complementary to each other. Containers are suitable for testing in early phases. The reason is that the provisioning/removal of containers is suitable for production environments. They should not be used for monolithic applications. Instead, containers are suitable for microservice architectures, where each container can deal with one module. On the other hand, virtual machines are suitable for running legacy applications. If different operating systems are required, virtualization is the key. It is also important to note that containers are stateless, i.e. once the host system is powered off, the contents are lost. There is no failover and live migration in case of containers. For specific workloads, containerization is suitable. Thus, VMs are suitable for addressing hardware level problems and for launching servers. They are preferred when security is more important than utilizing a lightweight solution. The flexibility in utilizing hardware resources is best done through virtualization. Containerization is suitable for DevOps where it enhances the development process, thus increasing the speed and quality of the delivered product.

5 Container Placement Policies in CloudSim

The CloudSim Framework [10] provides the functionality of container simulation. In this paper, the container migration policies that come packaged with the CloudSim frame work are analyzed for the effect on their performance when the number of Hosts, VMs and containers are varied. The following policies are taken into consideration:

I. First Fit
   Container is allocated to the first VM which can provide sufficient resources to the container. E.g. There are two VMs namely VM#1 and VM#2 with 18637 available MIPS each and the created container requires 10000 MIPS. The container will move to VM#1 in accordance with First Fit allocation policy.
II. Least Full
   Container is allocated to the VM which has the highest resources available i.e. least full VM out of all active VMs. E.g. There are two VMs namely VM#1 and VM#2 with 18637 and 15000 available MIPS respectively and the created container requires 10000 MIPS. The container will move to VM#1 in accordance with Least Full allocation policy.
III. Most Full
   Container is allocated to the VM which has sufficient but lowest resources available i.e. most full VM out of all active VMs. E.g. There are two VMs namely VM#1 and VM#2 with 18637 and 15000 available MIPS respectively and the created container requires 10000 MIPS. The container will move to VM#2 in accordance with Most Full allocation policy.

IV. Random
Container is allocated to active VMs at random. E.g. There are two VMs namely VM#1 and VM#2 with 18637 and 15000 available MIPS respectively and the created container requires 10000 MIPS. The container can move to any VM at random in accordance with Random allocation policy.

For a given number of hosts, VMs and containers, the number of container migrations that occur for each policy is recorded. Each policy is tested thrice by allocating it different number of hosts, VMs and containers. In this experiment, the performance of the policies is recorded when the number of hosts, VMs and containers available are 350, 800 and 5002 respectively, the second time when 525 hosts, 1200 VMs and 7502 containers are allocated, then finally for 700 hosts, 1600 VMs and 10002 containers. The experiment is based on a nearly linear increment in the number of resources allocated. The number of hosts is increased by 125 each time, the number of virtual machines is increased by 400 each time, and the number of containers is increased by 2500 each time. The experiment is repeated 50 times for each set of {number of hosts, number of VM, number of containers} values to record total container migrations and to calculate average total container migrations for each set. Finally, a graph of Average Total Container Migrations vs Number of containers is plotted to compare the policies. Table 1 shows the values of the general parameters used for simulation in CloudSim.

Table 1. General parameters and their values

hostSelectionPolicy	vmAllocationPolicy	OL threshold	UL threshold	VMSPolicy	ContainerSPolicy	totalSimulationTime	Scheduling Interval
First Fit	MSThreshold-Under	0.80	0.70	VmMaxC	MaxUsage	10000 units	300 units

Table 2 shows the cloudlet specifications used for simulation in CloudSim. A single type of cloudlet has been used.

Table 2. Cloudlet related parameters and their values

Cloudlet length	30
Cloudlet PES	1

Table 3 shows the container specifications used for simulation in CloudSim. Three types of containers have been used.

Table 3. Container related parameters and their values

	Container MIPS	Container PES	Container RAM	Container Bandwidth
Container Type 1	4658	1	128 MB	2500
Container Type 2	9320	1	256 MB	2500
Container Type 3	18636	1	512 MB	2500

Table 4 shows the VM specifications used for simulation in CloudSim. Four types of virtual machines have been used.

Table 4. VM related parameters and their values

	VM 1	VM 2	VM 3	VM 4
VM MIPS	37274/2	37274/2	37274/2	37274/2
VM PES	2	4	1	8
VM RAM	1024 MB	2048 MB	4096 MB	8192 MB
VM Bandwidth	100000	100000	100000	100000
VM Size	2500	2500	2500	2500

Table 5 shows the host specifications used for simulation in CloudSim. Three types of hosts have been used.

Table 5. Host related parameters and their values

	Host MIPS	Host PES	Host RAM	Host bandwidth	Host storage
Host 1	37274	4	65536	1000000	1000000
Host 2	37274	8	131072	1000000	1000000
Host 3	37274	16	262144	1000000	1000000

For the first test set, 350 hosts, 800 VMs and 5002 containers are allocated for use. The experiment is repeated 50 times and total container migrations for each policy are recorded. Table 6 shows 5 entries from the 50 observations, and the complete table is available on GitHub [11]

Table 6. Total container migrations at 350 Hosts, 800 VMs, 5002 Containers

First Fit	5125	6118	6084	6125	6037
Least Full	6694	6531	6694	6583	6498
Most Full	7019	6917	6733	6913	6770
Random	6738	6896	6570	6807	6724

For the second test set, 525 hosts, 1200 VMs and 7502 containers are allocated for use. The experiment is repeated 50 times and total container migrations for each policy are recorded. Table 7 shows 5 entries from the 50 observations, and the complete table is available on GitHub [12].

Table 7. Total container migrations at 525 Hosts, 1200 VMs, 7502 Containers

First Fit	8983	8773	8778	8753	8661
Least Full	9173	9362	9530	9287	9233
Most Full	9339	9402	9441	9483	9573
Random	9722	9738	9456	9679	9680

For the third and final test set, 700 hosts, 1600 VMs and 10002 containers are allocated for use. The experiment is repeated 50 times and total container migrations for each policy are recorded. Table 8 shows 5 entries from the 50 observations, and the complete table is available on GitHub [13].

Table 8. Total container migrations at 700 Hosts, 1600 VMs, 10002 Containers

First Fit	11477	11550	11298	11576	11410
Least Full	12095	12320	12311	12287	12267
Most Full	12567	12593	12335	12606	12796
Random	12604	13023	13187	12405	12890

Table 9 shows the average total container migrations for each set of hosts, VMs, and containers. Figure 5 shows the graphical representation of the results obtained in Table 9.

Table 9. Average total container migrations

Hosts, VMs, Containers	First Fit	Least Full	Most Full	Random
350,800,5002	6137.96	6627.24	6925.86	6787.92
525,1200,7502	8879.34	9266.94	9338.98	9752.86
700,1600,10002	11470.96	12252.1	12600.7	12969.7

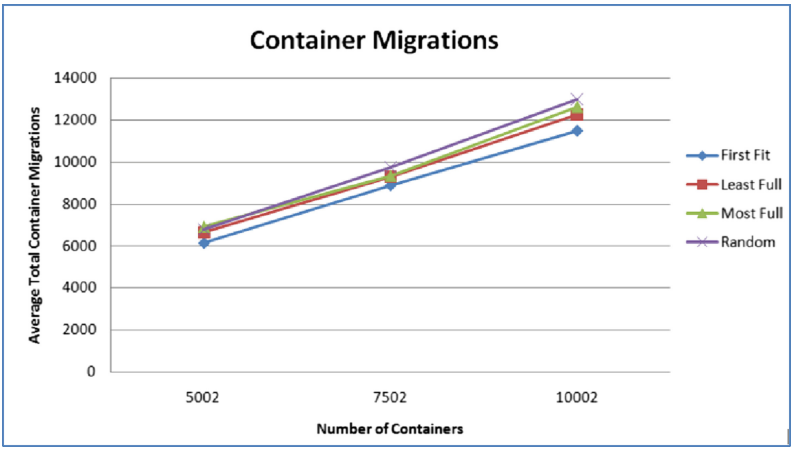


Fig. 5. Average total container migrations vs number of containers

Similar line graphs are obtained for average total container migrations vs number of hosts, and average total container migrations vs number of virtual machines (VMs). It can be seen from Fig. 5 and Table 9 that First Fit Container Allocation policy gives least number of container migrations followed by Least Full. Random performs better than Most Full at 5002 containers. However, when number of containers are increased, Most Full performs better than Random.

6 Conclusion and Future Work

The above experiment gives an idea of how the container placement policies behave when the number of hosts, VMs and containers are changed linearly. Out of the four inbuilt container allocation policies, First Fit performs better than others having the least container migrations in this specific scenario.

The following points can be taken into consideration when it comes to extending this work:

I. Varying the general parameters listed in in Table 1 which have been kept constant for this simulation.
II. Identifying container placement policies that have been recently implemented as part of research initiatives and comparing them against the existing ones.
III. For the experiment, the values of number of VMs, hosts and containers were incremented linearly. Further experiments could be performed with other types of increments such as exponential, squared, cubic, etc.
IV. More vigorous comparison between virtual machines and containers using parameters not listed in Sect. 4 of this paper.
V. Comparison of latest container orchestration tools available in the market such as Docker, Kubernetes, etc.

References

1. Rosen, R.: Resource management: Linux Kernel namespaces and cgroups (2017). http://cs.ucsb.edu/~rich/class/old.cs290/papers/lxc-namespace.pdf. Accessed 15 Oct 2017
2. Ernst, D., Bermbach, D., Tai, S.: Understanding the container ecosystem: a taxonomy of building blocks for container lifecycle and cluster management. In: IEEE Second Workshop on Container Technologies and Container Clouds, Berlin, Germany (2016)
3. Linux containers: LXC—Introduction, Linuxcontainers.org. https://linuxcontainers.org/lxc/introduction/. Accessed 12 Mar 2016
4. Linux containers: LXD—Introduction, Linuxcontainers.org. https://linuxcontainers.org/lxd/. Accessed 14 Mar 2017
5. Kumar, R.: An introduction to Dockers: from monolithic to containerized environment. Int. J. Sci. Res. **5**(12), 457–458 (2016)
6. Docker Overview, Docker.com. https://docs.docker.com/engine/understanding-docker/. Accessed 25 Dec 2017
7. Gupta, S., Gera, D.: A comparison of LXD Docker and virtual machine. Int. J. Sci. Eng. Res. **7**(9), 1414–1416 (2016)

8. Seo, K.-T., Hwang, H.-S., Moon, I.-Y., Kwon, O.-Y., Kim, B.-J.: Performance comparison analysis of Linux container and virtual machine for building clouds. Adv. Ser. Technol. Lett. (Netw. Commun.) **66**, 105–111 (2016)
9. Felter, W., Ferreira, A., Rajamony, R., Rubio, J.: An updated performance comparison of virtual machines and Linux containers. In: 2015 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), pp. 171–172 (2015)
10. Piraghaj, S.F., Dastjerdi, A.M., Calheiros, R.N., Buyya, R.: Container CloudSim: an environment for modeling and simulation of containers. In: Cloud Data Centers, Software: Practice and Experience, vol. 47, no. 4, pp. 505–521 (2017), ISSN: 0038-0644
11. Bhatnagar, S.: Container migrations data. https://github.com/shubham-bhatnagar/Container-Migrations-Data/blob/master/Hosts%20350_VMs%20800_Containers%205002.xlsx. Accessed 28 Nov 2017
12. Bhatnagar, S.: Container migrations data. https://github.com/shubham-bhatnagar/Container-Migrations-Data/blob/master/Hosts%20525_VMs%201200_Containers%207502.xlsx. Accessed 28 Nov 2017
13. Bhatnagar, S.: Container migrations data. https://github.com/shubham-bhatnagar/Container-Migrations-Data/blob/master/Hosts%20700_VMs%201600_Containers%2010002.xlsx Accessed 28 Nov 2017

Internet of Energy: A Deep Learning Based Load Prediction

Jahanvi Sharma[1(✉)] and Ritu Garg[2]

[1] Banasthali Vidyapith, Vanasthali, Rajasthan, India
Jahanvi.sharma0495@gmail.com
[2] National Institute of Technology, Kurukshetra, India
ritu.59@nitkkr.ac.in

Abstract. Smart grid being the major component of our power system is progressing fast to become more flexible and interactional. For the proper operation and planning in these systems, the load forecasting is of prime concern. In spite of the fact that many traditional methods are present for load forecasting but still a prediction of electrical load is needed to be explored further as the variation from time and surrounding weather conditions make it too complex. In this paper, we present deep learning based recurrent neural network approach for the short term load prediction using data captured from smart meters. This framework helps us to handle the over-fitting problem and uncertainty issues. The Tensor flow as a deep learning platform is used for our implementation. We compared our proposed model with the autoregressive integrated moving average model (ARIMA) and Fbprophet model and it is manifested that the proposed model outperforms in terms of RMSE, MSE, and MAE.

Keywords: Smart grid · Smart meter · Deep learning · Load forecasting · Internet of energy

1 Introduction

Smart grids play a significant role in smart energy as being the power network with the aim to make a sustainable and secure electric supply [1, 2]. Smart grid when working together with the Internet of things forms a sustainable energy model known as the Internet of Energy (IoE) [3]. Internets of things enabled smart metering systems and are essential for smart homes as they optimize home energy [4]. The data is processed through the smart metering infrastructure [2], IoT technologies [5] and sensing methods [6, 7]. Smart meters give economic and environmental benefits by collecting and processing data within a short span of time [8]. Smart grids introduce a bi-directional flow of electricity linking the consumer and supplier. Further, the forecasting of the load is mandatory as electricity is produced and consumed at the same time in smart grids. A single fault in forecasting can change the whole consumption pattern that results in an increase in the cost [9]. Thus, accurate forecasting is important as it assists in capacity planning of the power system and provides the consumer with the

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 525–533, 2020.
https://doi.org/10.1007/978-3-030-37051-0_59

knowledge of self-consumption pattern [10]. Power load forecasting is categorized as long, medium and short term load forecasting.

In this paper, forecasting has been performed for smart homes. The unpredicted behavior of the consumer and a periodic factors like weather, residual noise [11, 12] results in the formation of uncertainty. Thus, to handle it, we used the concept of deep learning which has a huge number of cascaded deep hidden layers all together forming a network. Deep learning is a technique of machine learning which provides the ability of automatic feature extraction [4, 13]. Our proposed load forecasting model works in two phases. In the first phase, the data value is collected through the smart meters at homes [14]. Preprocessing is carried out and missing values are handled through the MICE algorithm. Further, the smart database of homes is generated by pooling. In the second phase, the recurrent neural network algorithm is applied for short term load forecasting. Finally, the load value is predicted.

2 Literature Review

Innumerable research works exist under the field of short term load forecasting. Kandil et al. [15] used an artificial neural network for load forecasting. In addition, a drawback associated with it is the overfitting issue and the subjective determination of model structure [16]. Support vector regression model helps to overcome the disadvantage caused by the artificial neural network by providing the regularization technique and the kernel method implementation [17, 18]. However, the support vector regression model has an issue with processing i.e. longer time span is needed for processing which becomes an obstacle and is solved through deep learning. Deep learning with its automatic feature extraction ability reduces the time taken for a process and understands the non-linear relations more accurately. Due to its advantages in the field of forecasting, the researchers moved towards its usage. Zhang et al. [19] proposed autoencoder algorithm in deep learning for electricity price forecasting [20]. Further, Kong et al. [21] used long short term memory forecasting model for residential load forecasting. Li et al. [4] come up with IoT based load forecasting for smart grid considering the intraday load forecasting and daily consumption estimation network is recognized in order to improve the precision of forecasting. Zhong et al. [22] bring forward big data architecture that uses decision tree and smart meter data and clustering is applied for load prediction. Cao et al. [23] deploy ARIMA that is an autoregressive integrated moving average model for load prediction.

In the above-mentioned research works, there is an issue of overfitting. In this paper, we proposed the use of deep neural networks for load forecasting as they have deep hidden layers cascaded to form a network. By merging the homogeneous data coming from various household profiles, expands the volume and diversity. In the first phase, by applying the pooling, we have overcome the problem of overfitting and in the second phase, the recurrent neural network is used to predict the load accurately. Finally, we compared our proposed technique with the existing state of art techniques.

3 Proposed Model for Load Forecasting

This section provides a detailed description of our proposed model for load forecasting. Figure 1 shows the steps used to build the model.

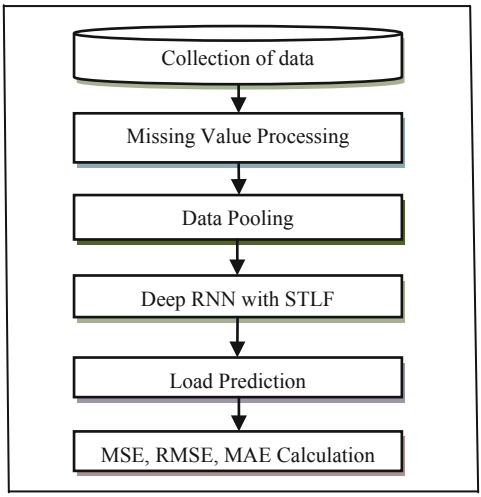


Fig. 1. Steps for building a load forecasting model

First, the daily household data is gathered through sensors and then the pre-processing technique is applied to handle the missing values. Further, we used deep learning and recurrent neural network technique for load forecasting. At last, we compared our model with two different models and evaluate their performance with standard evaluation metrics.

3.1 Data Set

We work on the high-resolution data provided by UMass. The study was done on the homes of western Massachusetts [14]. Our aim is to gather the multitude of data as we work on breadth. Internet of things is responsible for the monitoring of the household power consumption as different sensors provide the external plus internal value of data which is collected through different smart meters and further used for accurate prediction of the load.

3.2 Missing Value Processing

Due to malfunction of any sensor or meter, the collected data may contain missing values and outliers. However, deep learning has difficulty in processing these values and results in misleading us by giving wrong output. Thus, it becomes a necessity to pre-process the data before performing any analysis. For handling of these missing values, we use an R package named as Multivariate Imputation by Chained Equation (MICE) [24]. MICE have various methods for handling the missing values and

distinguish the ordered, unordered, numerical and binary data. MICE algorithm provides different imputations. Here, we imputed the missing value with three different imputations. Thus, by viewing the component and their missing proportion we can impute the appropriate result in the place of missing value.

Figure 2 shows the scatter plot which depicts the missing vs. not missing ratio between the smart home components. The red dot in scatter plot denotes the missing value while the blue denotes the values which are present in our dataset. While the other illustrates the missing value handling through the MICE algorithm. A density plot is plotted with the three different imputations resulting through mice algorithm. The density plot is used for this purpose as it visualizes the distribution of data over a continuous time period or interval.

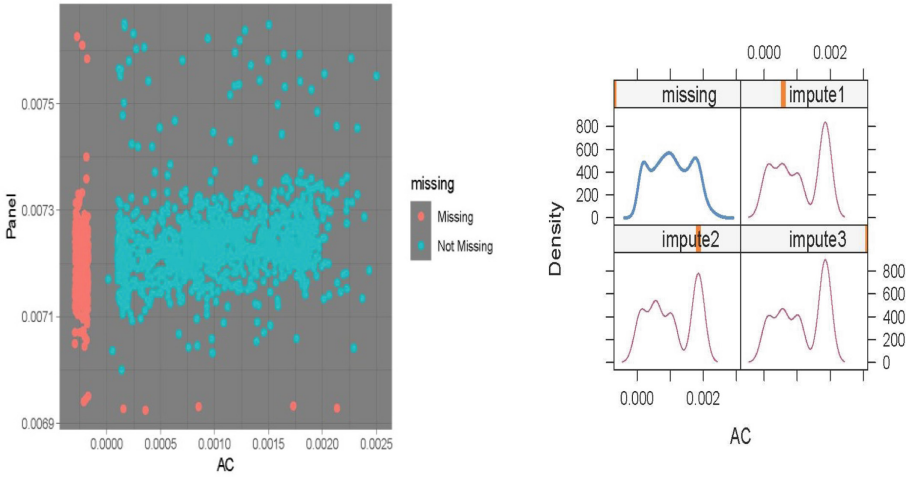


Fig. 2. Missing value pre-processing with the MICE algorithm.

3.3 Load Forecasting Using Deep Learning

Our next step is to predict the load as our data has been pre-processed and it works in two phases: (1) Pooling the load profile (2) Deep RNN based short-term load prediction. The outcome of the first phase feeds into the second phase. Design of both phases has been discussed in detail in the following section.

Phase 1: Load Pool: Sometimes the historical load profile is not sufficient for processing and can lead to a problem. Thus, to overcome this problem we pool the data from different households such that the diversity and volume are increased. As shown in Fig. 3, we split and label the data of two homes. Further, we make the training and test pools of these customers. At last, we merge the training pool and test pool of these customers. Through this, the data is scaled and thus solves the overfitting problem. In addition, uncertainties are resolved as if the diversity raises then the knowledge of these uncertainties rises too. Once the load pool is generated, it acts as input to the next phase and our algorithm can be applied to this new pool.

The *second phase* uses various techniques like deep learning which has the ability to extract feature. Further, the recurrent neural network algorithm is applied for short term load prediction of smart homes.

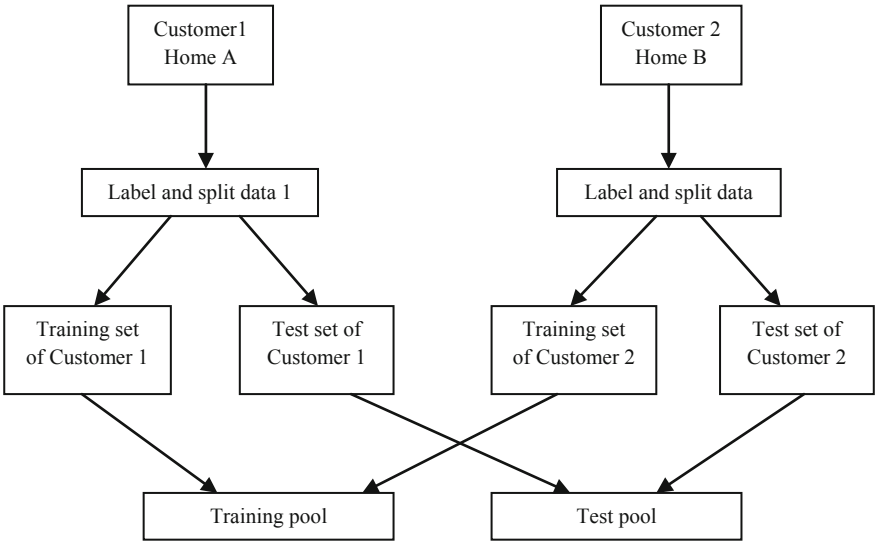


Fig. 3. Load pool construction with different smart homes load profile.

Deep Learning: Deep learning being a part of machine learning selects only the more appropriate features and here each input is transformed into a more abstract composition [25]. Various application of deep learning is in various fields as computer vision, drug design, natural language processing and many more. In addition, because of its two superior properties i.e. to understand the highly non-linear relationships and the shared uncertainties accurately they are preferred than the shallow network [26].

Recurrent Neural Network (RNN): The recurrent neural network helps to construct the correlations between previous input information and the current affecting factors. Various patterns are recognized whether the numerical time series or text. They are named as recurrent due to the fact that with any element in input they always perform the same calculation. A difference in outputs is only seen through the difference in hidden layers, as they are dependent on value at the last time stamp plus the current state. Backpropagation through time (BPTT) is a gradient based technique that helps recurrent neural network with the goal to reduce the network error. Following equations defines the recurrent neural network with time.

$$A^{(t)} = F\left(H^{(t)}; w\right) \tag{1}$$

$$H^{(t)} = G\left(H^{(t-1)}, X^{t}; w\right) \tag{2}$$

where $A^{(t)}$ being the outcome of RNN at time t and $X^{(t)}$ represents the input of RNN at time t, whereas $H^{(t)}$ stand for the state of hidden layers at t time.

Phase 2: Short-term load forecasting using deep RNN: This phase train and test the load for the forecasting on a Tensorflow deep learning platform. Figure 4 describes that once the load pool is generated, we initiate the RNN process by selecting the parameters. After this selection, the training batches are fetched. Further, we observe the network convergence once it is minimized we perform the testing on our household pool. Thus, at last, obtain the forecasted load values.

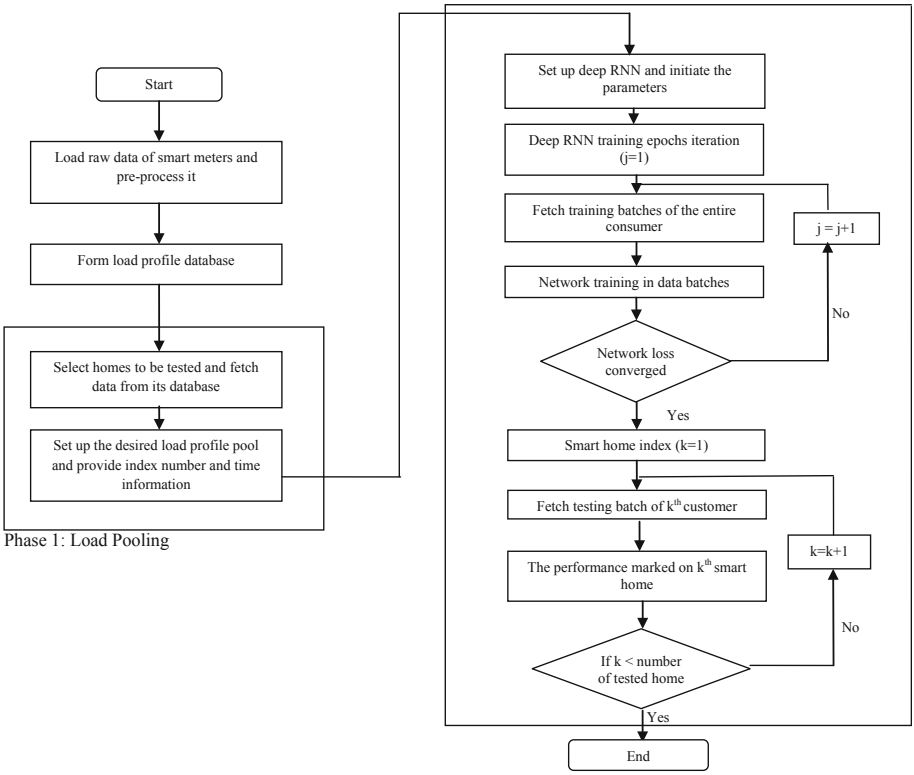


Fig. 4. Flowchart of the proposed model building with its two phases

4 Experimental Results and Analysis

Smart homes data has been collected through smart meter from western Massachusetts [14]. The dataset has been trained and tested under a timestamp of 30 min each for complete one-year duration. An autoregressive integrated moving average model (ARIMA) and Fbprophet model have been chosen as base models for the comparison with our proposed model. Tensorflow platform is selected to build the forecasting model. The main criterion is pooling, train and test model for short term load forecasting with recurrent neural network algorithm.

Root mean square error (RMSE), Mean absolute error (MAE) and Mean squared error (MSE) are the metrics used as a performance measure for our model.

$$\mathrm{RMSE} = \sqrt{\frac{\sum_{i=1}^{N}(\bar{y}_i - y_i)^2}{N}} \tag{3}$$

$$\mathrm{MAE} = \frac{\sum_{i=1}^{N}|\bar{y}_i - y_i|}{N} \tag{4}$$

$$\mathrm{MSE} = \frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y}_i)^2 \tag{5}$$

where y_i being the target value and $\bar{y}_i$ represents the forecasted result. Here, the test set size is denoted by N.

Figure 5 shows the comparison of three load forecasting methods on our dataset with the original output. After setting the Python environment we forecast our model using pybrain, scikit-learn and other machine learning libraries. Training set to test set ratio is set 70:30. Fbprophet and autoregressive integrated moving average model (ARIMA) have their forecasted performance less than our proposed deep recurrent neural network. As the yellow line in the power consumption graph shows the highest prediction with the given dataset. Thus, our method for prediction is efficient. The proposed model performance is further estimated through the considered metrics (RMSE, MSE and MAE) and the results are depicted in Fig. 6. RMSE value shows the standard deviation for our forecasted and observed values. Lower is the value better is the result. Furthermore, MAE and MSE defined as Eqs. 4 and 5 are used for comparison and result shows that more the value is near to zero and non-negative better is the estimate. Thus, results clearly signify that the RMSE, MSE and MAE values for our model is better and achieve efficient outcomes in comparison to the other two base models considered.

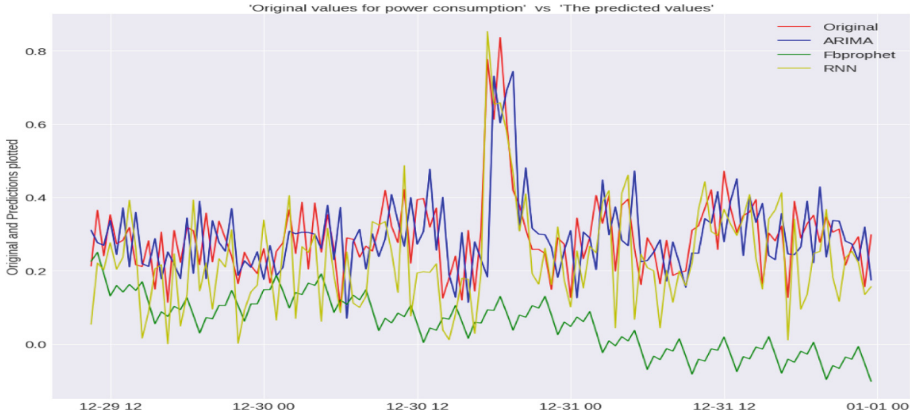


Fig. 5. Original/predicted value of ARIMA, Fbprophet, and RNN

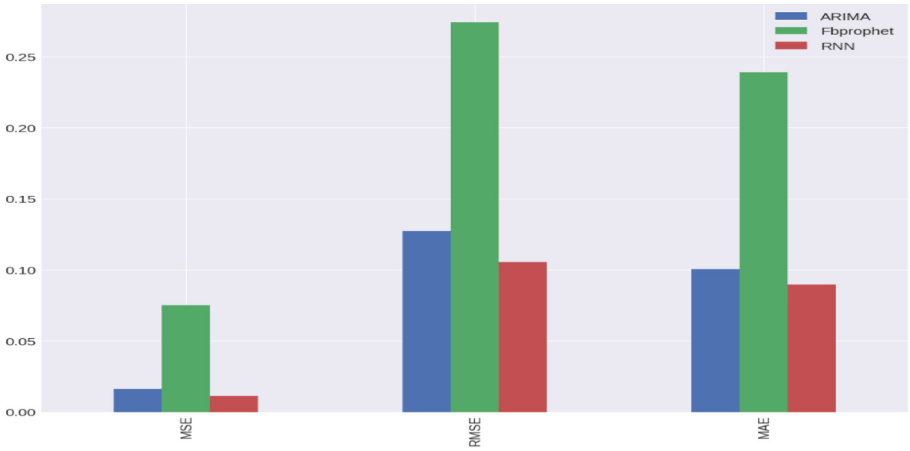


Fig. 6. MSE, RMSE and MAE values of different forecasting models

5 Conclusion

In this paper, we proposed the short term load forecasting for smart homes with deep learning technique under high volatility and uncertainty. In addition, as the load is pooled between the customers, hence more quick learning of layers is obtained which helps us to overcome the overfitting problem. Further, our forecasting models have been evaluated using evaluation metrics RMSE, MAE, MSE and results analysis show that our proposed model achieve better results and has good performance. In the future, work can be expanded by working on the dissimilar batch of customers with the usage of more external features.

References

1. Yu, X., Cecati, C., Dillon, T., Simox0303es, M.G.: The new frontier of smart grids. IEEE Ind. Electron. Mag. **5**, 49–63 (2011)
2. Alahakoon, D., Yu, X.: Smart electricity meter data intelligence for future energy systems: a survey. IEEE Trans. Industr. Inf. **12**, 425–436 (2016)
3. Bui, N., Castellani, A.P., Casari, P., Zorzi, M.: The internet of energy: a web-enabled smart grid system. IEEE Net. **26** (2012)
4. Li, L., Ota, K., Dong, M.: When weather matters: IoT-based electrical load forecasting for smart grid. IEEE Commun. Mag. **55**, 46–51 (2017)
5. Shah, S.H., Yaqoob, I.: A survey: Internet of Things (IoT) technologies, applications, and challenges. In: 2016 IEEE Smart Energy Grid Engineering (SEGE), pp. 381–385 (2016)
6. Ma, H., Zhao, D., Yuan, P.: Opportunities in mobile crowd sensing. IEEE Commun. Mag. **52**, 29–35 (2014)
7. Hernández, L., Zorita, C.B., Aguiar, J.M., Carro, B., Sánchez-Esguevillas, A., Mauri, J.L., Massana, J.: A survey on electric power demand forecasting: future trends in smart grids, microgrids and smart buildings. IEEE Commun. Surv. Tutor. **16**, 1460–1495 (2014)

8. Mauri, J.L., Tomás, J., Canovas, A., Parra, L.: An integrated IoT architecture for smart metering. IEEE Commun. Mag. **54**, 50–57 (2016)
9. Fahiman, F., Erfani, S.M., Rajasegarar, S., Palaniswami, M., Leckie, C.: Improving load forecasting based on deep learning and K-shape clustering. In: 2017 International Joint Conference on Neural Networks (IJCNN), pp. 4134–4141 (2017)
10. Paoletti, S., Casini, M., Giannitrapani, A., Facchini, A., Garulli, A., Vicino, A.: Load forecasting for active distribution networks. In: 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, pp. 1–6 (2011)
11. Wang, Y., Xia, Q., Kang, C.: Secondary forecasting based on deviation analysis for short-term load forecasting. IEEE Trans. Power Syst. **26**, 500–507 (2011)
12. Wang, Y., Chen, Q., Zhang, N., Wang, Y.: conditional residual modeling for probabilistic load forecasting. IEEE Trans. Power Syst. **33**, 7327–7330 (2018)
13. LeCun, Y., Bengio, Y., Hinton, G.E.: Deep learning. Nature **521**, 436–444 (2015)
14. Barker, S.K., Mishra, A.M., Irwin, D.E., Cecchet, E., Shenoy, P.J., Williams, J.A.: Smart*: an open data set and tools for enabling research in sustainable homes
15. Kandil, N., Wamkeue, R., Saad, M., & Georges, S.W.: An efficient approach for shorterm load forecasting using artificial neural networks. In: 2006 IEEE International Symposium on Industrial Electronics, vol. 3, pp. 1928–1932 (2006)
16. Sapankevych, N.I., Sankar, R.: Time series prediction using support vector machines: a survey. IEEE Comput. Intell. Mag. **4** (2009)
17. Warrior, K.P., Shrenik, M., Soni, N.: Short-term electrical load forecasting using predictive machine learning models. In: 2016 IEEE Annual India Conference (INDICON), pp. 1–6 (2016)
18. Chen, B.J., Chang, M.W.: Load forecasting using support vector machines: a study on EUNITE competition 2001. IEEE Trans. Power Syst. **19**(4), 1821–1830 (2004)
19. Zhang, G., Patuwo, B.E., Hu, M.Y.: Forecasting with artificial neural networks: The state of the art * (1997)
20. Wang, L., Zhang, Z., Chen, J.: Short-term electricity price forecasting with stacked denoising autoencoders. IEEE Trans. Power Syst. **32**, 2673–2681 (2017)
21. Kong, W., Dong, Z.Y., Hill, D.J., Luo, F., Xu, Y.: Short-term residential load forecasting based on resident behaviour learning. IEEE Trans. Power Syst. **33**, 1087–1088 (2018)
22. Li, J., Song, Z., Zhong, Y., Zhang, Z., Li, J.: Short-term load forecasting based on improved extreme learning machine. In: 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA), pp. 584–588 (2017)
23. Cao, X., Dong, S., Wu, Z., & Jing, Y. (2015). A data-driven hybrid optimization model for short-term residential load forecasting. In: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 283–287
24. Buuren, S.V.: Mice: multivariate imputation by Chained Equations in R (2011)
25. Almalaq, A., Edwards, G.: A review of deep learning methods applied on load forecasting. In: 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 511–516 (2017)
26. Din, G.M., Marnerides, A.K.: Short term power load forecasting using Deep Neural Networks. In: 2017 International Conference on Computing, Networking and Communications (ICNC), pp. 594–598 (2017)

Alert Generation Framework from Twitter Data Stream During Disaster Events

M. Hasla(✉) and K. P. Swaraj

Department of Computer Science & Engineering, Government Engineering College, Thrissur, India
haslaaa@gmail.com, swaraj.gec@gmail.com

Abstract. Twitter like microblogging site is used by millions of people to share their daily lives. During a natural disaster, the situational updates posted by users will get mixed with millions of other tweets and will be difficult to monitor manually in real time. Also, timely identification of situational updates, along with the location is very important for the rescue and relief operations during the disaster event. The tweets with contextual information posted during disaster provide information regarding the need or availability of resources and services, the number of casualties, infrastructures damage, and warnings or cautions. Some disaster-related tweet may not have any actionable information. This paper presents an alert generation framework, which will intake the tweets posted during the disaster, detects, classifies and geocodes the tweets belonging to each class, which provide actionable information, in order to alert the concerned authorities about the current situation in a timely manner.

Keywords: Twitter · Disaster · Tweets · Classification · Geocoding

1 Introduction

Micro-blogging sites like Twitter, Facebook are an important source of real-time information, especially during natural disasters, epidemics and other emergencies [3]. Earlier people depended on the news on television, radio for the information during emergency situations. Nowadays people rely on these websites for sharing and knowing about important situational and actionable information like the scarcity of food or other resources, missing people, injury or death toll in a particular location, situational awareness, etc.

The tweets with contextual information can be utilized by the authorities like local government or humanitarian organization, for the disaster management purpose and for gaining an overall picture of the ongoing disaster event. On average 6000 tweets are sent per second, 3.5 million tweets in a minute and 500 million tweets per day. This rate increases drastically during disaster events. So if any relief team or humanitarian organization wanted to monitor these tweets posted at a faster rate in real time, manually monitoring is nearly impossible in this scenario. So an automated system is required for this purpose. Also, different kinds of actionable information will be posted and will be mixed up all together. So for the monitoring to be easier, the tweets belonging to each category should be previewed in its respective classes.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 534–541, 2020.
https://doi.org/10.1007/978-3-030-37051-0_60

Another issue is the same post will be retweeted by multiple users, and thus increases the volume of tweets posted during the disaster event. Also, regarding the number of casualties, many peoples post similar tweets, as 700 people died, 700 lost their lives, 700 killed, etc. As concerned with the relief team and victims, timely identification of situational update along with the location mentioned in the tweets is very important for the relief purpose.

The framework presented in this paper is an alert generation framework. It will intake the disaster related tweets from the Twitter data stream in real time, filter out the irrelevant tweets based on some set of features, classifies the tweets into multiple classes, summarizes the tweets in each class and geotags each tweet in each class in a timely manner. The performance of the framework is measured against three benchmark dataset: Nepal earthquake 2015, Typhoon Hagupit 2014, Uttarakhand flood 2013.

The rest of the paper is as follows: Related work is discussed in Sect. 2. Section 3 describes the alert generation framework. Section 4 discusses the experiment result with test data and real-time tweets. Finally, Sect. 5 is the conclusion with a brief description of the findings and future works.

2 Related Works

People post a lot of tweets during natural disasters. These tweets were used by many kinds of research for exploiting the usefulness of Twitter during the emergency situation. Some works focussed only on a particular disaster [7]. Most of the works have focussed on retrieving disaster related tweets [2, 10], classifying tweets posted during disaster into disaster related or not, on identifying and matching the tweets related to resource or service requested [6] and extracting summarizing the disaster related situational tweets [8]. A work by Anirban et al. [11] developed NLP based classifier for identifying the tweets which provide situational awareness during disaster events. For training the classifier they have used tweets posted during both natural and man-made disaster and also have used low-level lexical features for classification. Singh et al. [9] proposed a disaster related tweet classification framework, in order to identify tweets the victims asking for help and for predicting the location of the user, based on their old tweets. Sreenivasulu et al. [5] modeled a system based on the informative words present in the tweets posted during the disaster in order to detect the resource related tweets. Support vector machine classifier is trained using these informative words. The training and testing were done on the same as well as different disaster datasets.

Aupetit et al. [1] developed an interactive tool for monitoring the crisis situation which provides a different level of views of the event. Tweets are classified into subcategories using supervised classifier. Hong et al. [4] proposed a semi-automatic framework, which extracts and compares the conversation between the people and local government during the snowstorm. It was done at various spatiotemporal levels using st-LDA and geotagged tweets only.

However, timely identification of situational update along with location is an important aspect as concerned to the relief team and volunteering services. If the relief team and volunteers get the requests from the user in a timely manner, they can easily

provide the requested service or resource as early as possible. Classifying the contextual tweets into different useful classes will help the disaster monitoring faster, as they needn't go through the entire tweet stream.

3 Alert Generation Framework

The alert generation framework collects the disaster related tweets, filter out the irrelevant tweets, classifies it into different classes and geocodes the location mentioned in it.

3.1 Disaster-Related Tweet Retrieval

During a disaster event, a lot of tweets will be posted on Twitter, along with some hashtags or key terms. **#NEQuake, #NepalEarthquake, #NepalQuake**. These were some of the hashtags used during Nepal earthquake. Similarly, tweets related to a particular ongoing disaster can be retrieved using a particular key term or hashtag from the twitter streaming data.

3.2 Preprocessing of Tweets

The retrieved tweet be will in JSON format. It contains tweet text along with metadata like time at which the tweet is posted, user id, tweet id, etc. Also, the tweet text may contain twitter specific symbols like RT (retweet), @ - (mention), URLs, etc. So the tweet text is preprocessed in order to remove these symbols.

For example,

Original tweet - RT @rConflictNews: #NepalEarthquake causes avalanche in Everest, at least 8 killed - RT http://t.co/iMiDvzGUC

Preprocessed tweet - causes avalanche in Everest, at least 8 killed.

3.3 Filtering Out Non-contextual Tweet

The tweets retrieved using keyword based method will have some irrelevant tweets also. The tweets with situational update contain information like need or availability of resources or emergency services, number of casualties, infrastructure damage and caution or warning, etc. All the tweets other than this has to be filtered out. A supervised classifier is trained using tweets from three different disaster dataset. Information about the disaster and dataset are given in Table 1. A classifier trained on tweets from multiple disasters can easily classify any tweets from any future disaster event. So here the classifier is trained using tweets posted during earthquake, flood, and typhoon. Since terminologies differ during different disaster event and certain words are found only in either contextual tweet or in the irrelevant tweet [8, 12]. For the classification, each tweet is converted into a vector of word-level features. The feature vector is characterized by numerals, location, religious terms, adverbs like so, too, really etc. casualties related terms like killed, injured, missing etc., infrastructure and other

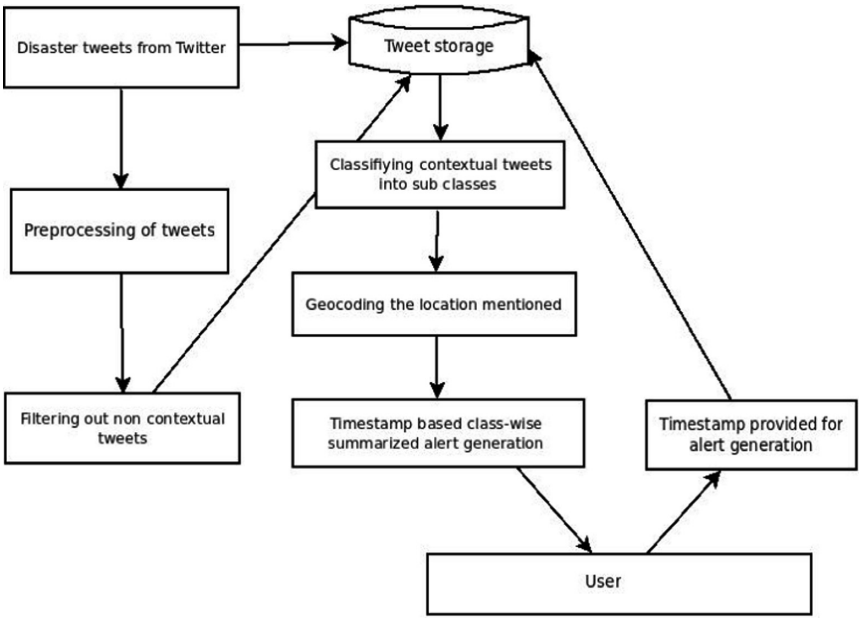


Fig. 1. System architecture

utilities, religious terms like pray, God, Lord etc., Questions and exclamatory phrases and words like warning, alerts, precaution etc.

Table 1. Train and test data set of different disaster events

Disaster	Total no. of tweets	Training set	Testing set
Nepal Earthquake	19970	15820	4150
Typhoon Hagupit	5000	4000	1000
Uttarakhand flood	5000	4000	1000

Each feature vector is labeled with its corresponding class as either 0 or 1. '0' means an irrelevant tweet and '1' means it provides contextual information 10 fold cross-validation of each model is done and the result is given in Table 2. The selected classifier is Support Vector Machine (kernel = rbf and gamma = 0.5) and has an accuracy of 86.4% and F1-score of 89.4%. After the classification, tweets with label '0' is filtered out and tweets with contextual information remain.

3.4 Classification of Contextual Tweets into Subclasses

The contextual tweets contain information like number of casualties, infrastructure damage, resources and services (provided and requested) and any cautions, etc. So the tweet belonging to each category has to be classified to its respective classes.

Table 2. Cross validation result

Model	Accuracy	Precision	Recall	F1-score
Linear SVC	0.816 ±0.032	0.816	0.918	0.863
SVM (kernel ='rbf', gamma = 'auto')	0.863 ±0.033	0.874	0.914	0.893
Random forest classifier	0.859 ±0.033	0.867	0.921	0.892
Logistic regression	0.817 ±0.032	0.818	0.916	0.863
Bernoulli Naive Bayes	0.839 ±0.034	0.837	0.925	0.878
SVM (kernel ='rbf', gamma = 0.5, probabilty = True)	0.864 ±0.031	0.871	0.922	0.894

Each class is characterized by a set of keywords. For instance, some of the casualty related keywords are "killed", "dead", "died", "victims", "injured" etc. Service related keywords are "emergency", "contact number", "helpline", "rescue" etc. Infrastructure damage related words are "damaged", "collapsed", "crashed" etc. The keywords related to caution are "warning", "caution", "alert" etc.

3.5 Geocoding of Tweets

It is important to identify the location mentioned in a tweet, especially for the tweets belonging to resource and service requested and infrastructure damage. Geocoding provides the exact geo-coordinates of a location, which will be useful for the rescue operators and relief teams for easily identifying the location. By named entity recognition, location entities can be identified and using geocoder (Open Street Map) the coordinates of that location can be obtained.

4 Result

The tweets from test data and real time tweets were given as input to the system along with time (hh:mm) and date (Day Mon Date) as argument. The tweets with situational information during that particular period were classified into different subclasses, namely, "Resources and emergency service", "Number of casualties", "infrastructure and utilities damaged" and "warning or caution" in a timely manner. Also for resource and emergency service tweets and infrastructure and utilities damage related tweets, geocoding is also done. For each location specified in the tweet, corresponding geo-coordinates are also provided. The time based class-wise result obtained for Nepal earthquake test data-2015 (Sat Apr 25 12:50) and the real-time tweets during Cyclone Idai in Mozambique-2019 (Thu Mar 21 04:43) are given in Tables 3 and 4.

Table 3. Nepal Earthquake related alert during Sat Apr 25 12:50 (test data)

Sat Apr 25 12:50		Location
Resource and emergency services (requested and provided)	IAF C-130 J Super Hercules with 40 NDRF personnel and 4 tons of relief about to land Kathmandu	Kathmandu [27.708796,85.320244]
	Modi govt sending IAF C130 Hercules and Globemaster aircraft to Nepal with relief material	
Number of causalities	China – 7 killed	
	India – 35 killed	
	Bangladesh – 2 killed	
	Nepal – 700 killed	
Infrastructure damage	Death toll rising rapidly with reports of massive damage near epicenter	
	Gorkha, Dading, Nuwakot districts all houses flattened	Gorkha [27.9952021,84.6264697] Dading [33.4985472,116.3548108] Nuwakot [27.9656478, 83.05917396]
Caution or warning	Just in from a friend in Nepal, People in Nepal are advised to stay away from buildings n walls thru the night	
	AFAD search + rescue crews on high alert due to today's NepalEarthquake	

Table 4. Cyclone Idai related alert during Thu Mar 21 04:43 (Real time data)

Thu Mar 21 04:43		Location
Resource and emergency services (requested and provided)	7,550 UK aid shelter kits and 100 family tents arrived in Mozambique today	Mozambique [−19.302233, 34.9144977]
	Breaking News 30 tonnes trucks carrying aid can now reach Chimanimani CycloneIdai	
	MSF has set up a stabilization centre at skline, 20 km away from Chimanimani, eastern Zimbabwe to support to.	Zimbabwe [−18.4554963, 29.7468414]
Number of causalities	Mozambique – Thousands killed	
Infrastructure damage		
Warning		

5 Conclusion

During disaster events, a large number of tweets are posted at a faster rate. The government officials and rescue teams can make use of these tweets for getting contextual updates in different locations during the disaster. The alert generation framework will extract the disaster related tweets, which provide contextual information, geocodes the tweet, and generates time based class level alert based on these tweets posted during a particular time. The geo-coordinates in the tweet helps the rescue team and other organizations to locate the people in need and plan the relief operations efficiently. The dataset used in the work is tweets posted during Nepal earthquake, Uttarakhand flood and Typhoon Hagupit. Also, real time tweets are also used to test the framework. Hence, from the result, it was seen that the user can obtain the alert based on both past tweets and real-time tweets. The proposed system is significant in countries where government-sponsored disaster monitoring systems are not available.

Since the alerts are generated purely based on the tweets posted during the disaster, the authenticity and truthfulness of each tweet posted are questioned here. So a rumor free alert generation framework from tweet during the disaster is required, which is planned as future work.

References

1. Aupetit, M., Imran, M.: Interactive monitoring of critical situational information on social media. In: Social Media Studies Proceedings of the 14th ISCRAM Conference Albi, France (2017)
2. Imran, M., Castillo, C., Lucas, J., Meier, P., Vieweg, S.: Aidr: artificial intelligence for disaster response. In: Proceedings of WWWcompanion, pp. 159–162 (2014)
3. Rudra, K., Banerjee, S., Ganguly, N., Goyal, P., Imran, M., Mitra, P.: Summarizing situational tweets in crisis scenario. In: Proceedings of the 27th ACM Conference Hypertext and Social Media. ACM, pp. 137–147 (2016)
4. Hong, L., Fu, C.,Wu, J., Frias-Martinez, V.: Information needs and communication gaps between citizens and local governments online during natural disasters. Inf. Syst. Front. **20** (5) (2018)
5. Sreenivasulu, M., Sridevi, M.: Mining informative words from the tweets for detecting the resources during disaster. In: International Conference on Mining Intelligence and Knowledge Exploration. Springer International Publishing AG 10682, pp. 348–358 (2017)
6. Basu, M., Ghosh, S., Ghosh, K., Choudhury, M.: Overview of the FIRE 2017 track: Information retrieval from microblogs during disasters (IRMiDis)—working notes of FIRE 2017. In: CEUR Workshop Proceedings, vol. 2036, pp. 28–33 (2017)
7. Anbalagan, B., Valliyammai, C.: #ChennaiFloods: leveraging human and machine learning for crisis mapping during disasters using social media. In IEEE 23rd International Conference on High Performance Computing Workshops (2016)
8. Rudra, K., Ghosh, S., Ganguly, N., Goyal, P., Ghosh, S.: Extracting and summarizing situational information from the twitter social media during disasters. ACM Trans Web **12** (3), 17, Article 35 (2018)
9. Dwivedi, Y.K., Singh, J.P. Rana, N.P., Kapoor, K.K.: Event classification and location prediction from tweets during disasters. Application of or in disaster relief operations. Springer (2017)

10. Yuzawa, A., Ichikawa, H., kobayashi, A.: Extracting Tweets related to disaster information by using multiple co-occurrence relation of words. In: IEEE International Conference on Smart Computing (2018)
11. Anirban, S., Rudra, K., Ghosh, S.: Extracting situational awarness from microblogs during disaster events. In: 7th International Conference on Communication Systems and Networks, Social Networking Workshot, CCOMSNETS (2015)
12. Imran, M., Mitra, P., Castillo, C.: Twitter as a lifeline: human-annotated Twitter corpora for NLP of crisis-related messages. In: Proceedings of the Tenth International Conference on Language Resources and Evaluation (LREC), Paris, France (2016)

Potential and Extention of Internet of Things

Animesh Nag(✉), Anand Kesharwani, Bharti Sharma, Ishu Gupta, Abhishek Tiwari, and Ashutosh Kumar Singh

National Institute of Technology, Kurukshetra, Haryana, India
nag.animesh56@gmail.com, anandkesharwani100@gmail.com

Abstract. The cheap availability of portable devices and processing elements has triggered the emergence of IOT. It is an integration of powerful computers with large number of tiny devices that support automation and smart decision making in all walks of life that may be agriculture, battle field, industry, office or home. Thus, IOT has very wide range of applications. However, the success of such applications heavily depends on efficient handling of numerous challenges related to computation and communication because huge volume of data needs to be aggregated, transported and processed at faster rate. We illustrate the potential of IOT and various technologies used to realize it and reap benefits. The paper also makes a mention of a futuristic application which is a wearable device that assists to protect victims from various threats.

Keywords: Sensors · IOT · RFID · NFC · ZigBee

1 Introduction

The Internet of Things (IOT) is the connectivity or network of devices referred to "things" which is embedded with different types of sensors, electronic equipment, software and most importantly network connectivity through which they can send and receive data. "Things" in IOT means devices with network connectivity and has built-in sensors such as motion sensor, humidity sensor, temperature sensor. Example-GPS devices which are attached with farm animals, device which monitors health like the heartbeat, blood pressure, pulse. The IOT devices are implanted with a high processing unit, sensors, and devices for network connectivity to do a particular work. these devices may include various sensors, Global Position System (GPS), actuator, Radio Frequency Identification (RFID), wi-fi, Bluetooth and many more components [1].

The general Architecture of IOT compromises of the user, service providers, management unit, Networks, and devices. See Fig. 1.

1.1 Facts About IOT

The Internet of things is a very hot topic and is going to serve each of us very soon. Let us see some interesting facts. In 2019 we will be having more than 4.9 billion IOT devices. The first IOT machine was ATM which was developed in 1974. By the end of 2020, the number of devices which will be connected to the Internet will reach to more than 50 billion. By 2020 there will be more than 6 billion smartphone users.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 542–551, 2020.
https://doi.org/10.1007/978-3-030-37051-0_61

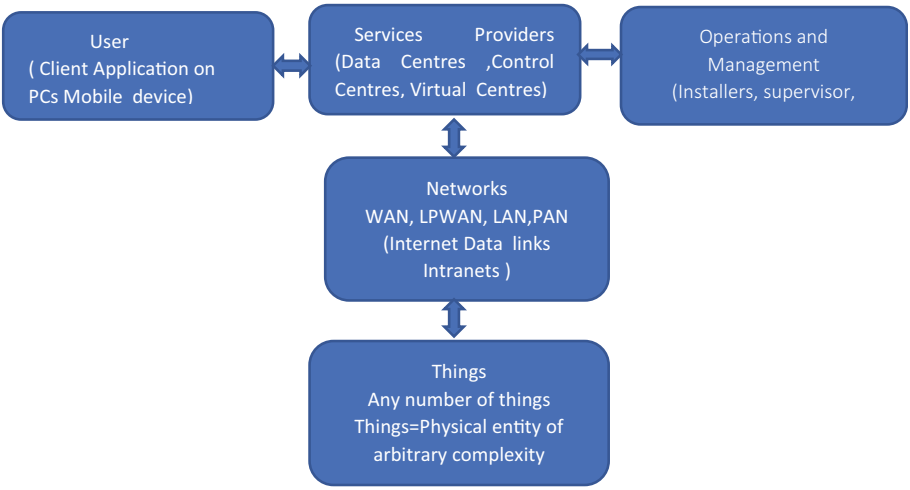


Fig. 1. General IOT system architecture

1. The perspective of IOT is to connect most of the appliances we have in our home. E.g. TV, refrigerators, camera, coffee maker, doors. Multinational companies like Google and Samsung know the potential of IOT and henceforth are intensively working on it [2].
2. More than 250 million vehicles will be connected to the internet by 2050 which will make driving easier and provide automated driving. Google's self-driving cars have already been developed which can drive on their own 10,000 miles per week.
3. There is a growth of 223% in the global market of wearable devices, with Apple selling more than 3 million Apple watches.
4. By 2020 clothes having internet connectivity will be the new trend as estimates predict more than 10 million pieces of smart clothing will be shipped by then. For the purpose of tracking and identification, Radio Frequency Identification (RFID) tags are being used extensively and its market is worth $11 billion.
5. The Internet of things will be adding more than $10 trillion to the global GDP in the next 20 years and the impact on the economy will be more than $12 trillion by 2026. According to CISCO IOT has the potential to generate more than $5 trillion over the next ten years in the public sector [2].

2 Technologies Used in IOT

2.1 Sensors in IOT

The main component of IOT Applications are sensors which senses the environment and transmits the information to the microcontroller for further processing. Some commonly used sensors are listed below see Table 1.

Table 1. Represents the types of sensors and its types

Sensors	Explanation	Types
Temperature sensor	A temperature sensor is a device, typically, a thermocouple, that provides temperature measurement through an electrical signal [9, 10]	a. Thermistors b. Infrared sensors c. Thermometers
Proximity sensor	A proximity sensor is a sensor able to detect the presence of nearby objects without any physical contact	a. Inductive b. Magnetic, including magnetic proximity fuse c. Radar
Pressure sensor	A pressure sensor is a device for measuring the pressure of gases or liquids [11]	a. Inductive b. Reductive
Humidity sensor	Humidity is defined as the amount of water present in the surrounding air [12]	a. Capacitive Humidity Sensors b. Resistive Humidity Sensors c. Thermal Conductivity Humidity Sensors
Accelerometer and gyroscope	The accelerometer is based on vibration and measures the amount of linear acceleration A gyroscope is based on the principle of the rigidity of space and determines the angular position [11]	a. Micro-Electro-Mechanical System (MEMS) Accelerometer

2.2 Near Field Communication (NFC)

In recent years, NFC is extensively used to establish a connection between NFC enabled devices to transmit data. The devices can be connected by simply bringing two devices together or in the vicinity of the other device that can range to less than 3–4 inches. It is used to transmit data, device pairing, making payments, NFC tags (used to store small data), NFC business cards (transmit your business cards details digitally in another mobile). It does not need pairing as in Bluetooth [13].

2.3 Radio Frequency Identification Technology (RFID)

RFID contains a small chip and an antenna that contains data, which can be identified by an RFID reader. It uses radio waves for the transmission of data. It does not require a line of sight view between the RFID tag and the RFID reader and can be identified without the need of an operator from a distance up to 100 m which depend on frequency. It can be used in a big supermarket where it is attached with clothes to prevent it from being shoplifted. It can also be used for object tracking and identification [14].

The RFID tags are categorized into two types: Active RFID tags and Passive RFID Tags. The difference between them is that Active tags consist of the power source and

passive tags do not consist of any power source. Passive tags are cost-efficient and are durable as they draw power from the electromagnetic waves emitted by the reader [15, 16]. The comparison between the tables is given in Table 2.

Table 2. Comparison between Active RFID and Passive RFID

Features	Active	Passive
Power	Battery operated	No internal power
Range	Long range (100 m+)	Short range (3 m)
Typical data storage	Large read/write data (128 kb)	Small read/write data (128b)
Cost	More expensive	Less expensive
Used in tracking	Queue free toll payment system	Smart labels, passports
Required signal strength	Low	High

2.4 Actuator

An actuator is a component fitted inside a machine which converts the electrical energy into another form of energy which is required. Example Lights, fan, Heating coils, display in television and motors, in smart homes locking and unlocking of doors, switching on or off the lights in a room, alerting the people in case of fire.

2.5 ZigBee

Today communication standards with high data rates are available but they require low energy consumption at lower bandwidths but such low energy consumption devices were not present. Zigbee technology is a low cost and consumes very low power and this feature of Zigbee makes it beneficial for communication purpose in various applications of smart home and industry. It consumes low energy is reliable and is cost-efficient. Its range is from 10 to 100 m [17].

A comparison of similar technologies is done in the Table 3 which gives an insight into the differences between them. Difference between WIFI, ZigBee, Bluetooth and NFC based on their range and date rate has been shown in Fig. 2.

3 Applications

IOT's application is being extensively used in various sectors of medical, smart homes, vehicle, agriculture, industry, education and many more see Fig. 3. The percentage of IOT application used in various sectors is given in Fig. 4.

3.1 IOT in Medical and Health Care

IoT sensors can be attached to the human body to collect accurate and real-time medical information such as heart rate, Blood pressure, the pulse of a human body. The data obtained can be analyzed and used for analysis. Hence patients can be monitored

Table 3. Comparison between NFC, RFID, Bluetooth, Wi-Fi.

Features	NFC	RFID	Bluetooth	Wi-Fi
Maximum operating range	10 cm	3 m	100 m	100 m
Operate frequency	13.56 MHz	Varies 1	2.4 GHz	2.4/5 GHZ (802.11 N)
Directional communication	Two way	One way	Two way	Two way
Bit Rate	106/212/424 kbps	Varies 13	22 Mbps	144 Mbps
Potential uses	E-Tickets Credit card payment membership card	Tracking item, EZ-pass	Communicate between phones, peripherals device	Wireless internet

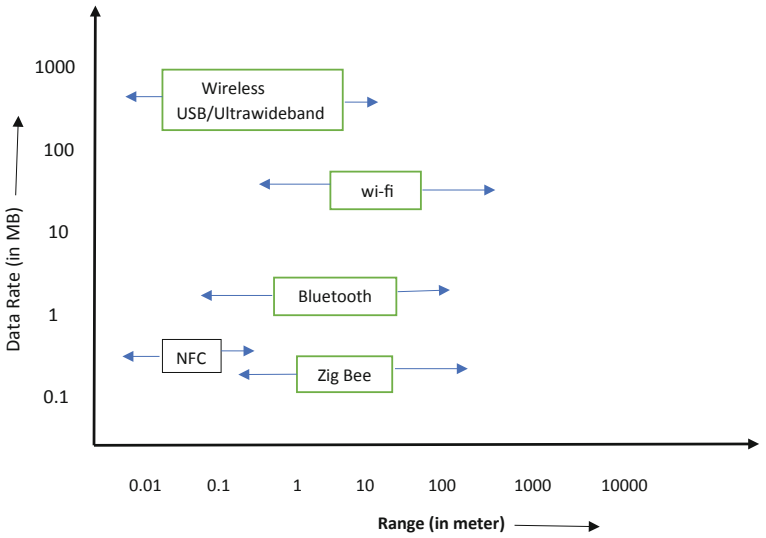


Fig. 2. Comparison between similar technologies.

at any point of time and prevent any kind of mishappening. Equipment like medical fridges can monitor and control of the temperature inside freezers storing various kind of medicines, vaccines, and organic elements which require a particular range of temperature [3].

3.2 IOT for Smart Home

The standard of living of our generation is changing tremendously so smart home is going to become an essential part of our life. Devices such as automated doors, windows, refrigerator, washing machine, smart lights, can work on their own by sensing

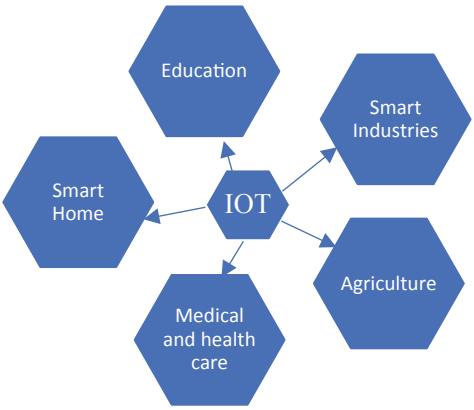


Fig. 3. Application of IOT in various areas.

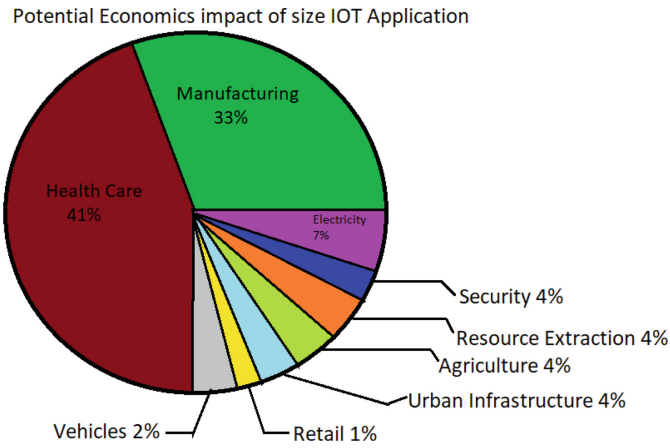


Fig. 4. Impact of IOT applications in various fields.

the presence of human being, temperature, rain. We can also control them with the help of our smartphones [4].

3.3 IOT in Vehicle Management

Today in this rapidly changing environment safety is a major issue regarding the driving of vehicles. IOT can play a vital role in safety and proper management of vehicle with the help of GPS and other sensors. Today information regarding the status of different parts of the vehicle can be obtained to provide it with the required service when needed. Traffic in the road can also be obtained so users can take another road. Also, facilities like Global Position System (GPS) gives us the correct route to a particular place [5].

3.4 IOT in Agriculture

Applications such as drones can help in spreading the pesticides which are very efficient as normally for a human to do this is in a proper way is difficult. With the help of different sensors, we can measure the quality of soil and water. IOT can be proof of its virtue in this sector as through this we can prevent water wastage, monitor the agriculture fields, reduce human work, enhance productivity [6].

3.5 IOT in Education

IOT can be very useful in the education sector as it can be used in automatic biometric attendance, maintaining a database of each student, a smarter way of teaching with the help of projectors. Students can use the SMART Table through which student can send their views or activity to everyone in the class. School buses can be tracked so that real-time information about students can be retrieved, lights installed with sensors can also be beneficial as it will prevent unnecessary wastage of lights. To prevent any unauthorized users from entering a particular area face recognition system can be used [7].

3.6 IOT in Smart Industry

Today the growth of the industry is tremendous. So to improve the industry sector IOT can play a vital role by providing condition-based monitoring of heavy machinery. The machines developed now days work under specific temperature and condition. So IOT can use its sensors to alert us when the required condition is not met to prevent any loss. We can use IOT inventory System which alerts us with the items which are required, the present stock available, by which time we should order so that the item arrives in time and there is no loss of work, quality can also be checked, the percentage of work done. So in this way, we can prevent mishappening, reduce cost, increase efficiency [8].

4 Proposed Work

Our proposed work is a small IOT wearable device which could be carried in shoes, pocket etc. moreover location of device holder is easily traceable Device would be in dual working as pressing it will send the alert message to nearby police stations or with witch device is registered. Device would handle the mobility successfully by sending location of device holder.

- **Potential User**: Everyone who needs security could be a potential user.
- **Motivation**: Our motivation to think for such device is the significant increase in theft, kidnapping, and rape It may also let you figure out that teenaged child has went to school or roaming around.
- **Significance**: This small device is very significant as it can save a human's life by a press ing of a single button.
- **Technical Problem**: The network is an issue as this works on GSM (Global System for Mobile Communication) and GPRS (General Packet Radio Services) and GPS

(Global Positioning System). It works on battery so it will need charging. A 12-volt battery with 2 amperes current will be sufficient for a full week as it requires very less current.

- **Contribution to Society**: In highly technical and advanced world this device will surely help victim of robbery, kidnapping or for any unpleasant condition. This device will certainly contribute a lot to society.

5 Challenges in IOT

- **Connectivity**: The connectivity of IOT devices with sensors and the internet is a big challenge. For the transmission of data, they need internet connectivity all the time. This also may cause a problem as internet connectivity is unstable [18].
- **Big Data**: A lot of data is collected by the IOT devices every hour but out of the whole data, some part is important. To segregate the data, we need to analyze the huge data which was collected which possess a big problem. We should find ways through which relevant data is sent for the process of analyzing [19, 20].
- **Interoperability and Standardization**: Devices fabricated by various dealers vary in the technologies and services they render resulting in incompatibility. Since the Internet is the source of connection of these gadgets, hence the objective of standardization is required to be reformed to make devices compatible enough to communicate and exchange data among themselves within the wireless sensor networks [18].
- **Naming and Identity Management**: Once IOT is visualized to connect thousands of devices, there is a need that each of the objects is identified uniquely. This demands for a scheme that can efficiently assign unique names and identities to devices connected across the globe [21]. Presently, the implementation of the IPv6 protocol can be the solution to insufficient address space [22].
- **Security of Objects**: Since "IoT" is made up of a thousand of devices connected across the globe, access to objects by uncertified persons is required to be prohibited to safeguard them against their physical damage or malfunction [18].
- **6.6 Security & Privacy**: IOT has gradually become one of the most important elements of the future Internet. Due to this IOT applications are in danger to attacks or threat to security. Security attacks are of major concern due to the physical accessibility sensors, actuators and objects, and the openness of the system, including the fact that most devices will communicate wirelessly [20].

6 Conclusion

The paper presents an illustration of architectural overview, potential applications, and key challenges in deploying IOT infrastructure. The lower level detail of our proposed application has been excluded as its development is still in progress. Furthermore, the security is also a major concern in IOT networks. The success of IOT technology depends heavily on secure and safe handling of the user data while maintaining its

privacy; however, such illustration is beyond the scope of this paper. Therefore, the study on safety, security and privacy issues in IOT are being postponed for our future paper.

References

1. Introduction to the Internet of Things security: Standardization and research challenges
2. Sharma, S., Parashar, S.: Smart city implementation models based on IOT technology. In: Techno Site 2014–2015
3. Ahmed, M., Causevic, A., Fotouhi, H., Lindén, M.: An overview on the internet of things for health monitoring systems. In: Research Gate, Conference Paper: Malardalen University. Vasteras, Sweden (2015)
4. Mohammed, Z.K.A., Elmustafa, S.A.A.: Internet of things applications, challenges, and related future technologies. World Sci. News. **67**(2), 126–48 (2017)
5. Dhall, R., Solanki, V.K.: An IoT based predictive connected car maintenance approach. Int. J. Interact. Multimed. Artif. Intell. **4**(3), 16–22 (2017)
6. Malavade, V.N., Akulwar, P.K.: Role of IoT in agriculture. In: IOSR-JCE, pp. 56–57
7. Bagheri, M., Movahed, S.H.: The effect of the Internet of Things (IoT) on education business model. In: 12th International Conference on Signal-Image Technology and Internet-Based Systems (2016). https://doi.org/10.1109/SITIS.2016.74
8. Sheik Dawood, M., Jehosheba Margaret, M., Devika, R.: Review on applications of an internet of things (IoT)
9. Coombs, C.F., Jr.: *Electronic Instrument Handbook*, p. 5.1, Second edn. Mc Graw Hill (1994)
10. Grattam, K.T.V., Sun, T.: Fiber optic sensor technology: an overview. Sens Actuators A Phys. **82**, 40–61 (2000)
11. Coombs, C.F.: *Electronic Instrument Handbook*, Second edn., pp. 5–1. Mc Graw Hill, New York (1994)
12. Tschulena, G.R.: Market data—sensors in household appliances. Sens. Update **12**(1), 231–241 (2003)
13. Hussein Ahmad Al-Ofeishat†, Mohammad A.A.Al Rababah "Near Field Communication (NFC)"
14. An introduction to RFID technology
15. Want, R.: An introduction to RFID technology. IEEE Pervasive Comput. **5**(1), 25–33 (2006). View at PublisherView at Google ScholarView at Scopus
16. Zhu, X., Mukhopadhyay, S.K., Kurata, H.: A review of RFID technology and its managerial applications in different industries. J. Eng. Technol. Manag. **29**(1), 152–167 (2012). View at PublisherView at Google ScholarView at Scopus
17. Baronti, P., Pillai, P., Chook, V.W.C., Chessa, S., Gotta, A., Hu, Y.F.: Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards. Comput. Commun. **30**(7), 1655–1695 (2007). View at PublisherView at Google ScholarView at Scopus
18. Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future internet: the internet of things architecture, possible applications and key challenges. In: Proceedings of the 10th International Conference on Frontiers of Information Technology, 17–19 December 2012, pp. 257–260 (2012)
19. Matharu, G.S., Upadhyay, P., Chaudhary, L.: The internet of things: challenges & security issues

20. Gupta, K., Shukla, S.: Internet of things: security challenges for next-generation networks
21. Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future internet: the internet of things architecture, possible applications and key challenges. In: Proceedings of the 10th International Conference on Frontiers of Information Technology, 17–19 December 2012, pp. 257–260
22. Li, L.: Study on security architecture in the internet of things. In: International Conference on Measurement, Information, and Control (MIC), vol. 1, 18–20 May 2012, pp. 374–377 (2012)

Real Time Data Warehouse Updates Through Extraction-Transformation-Loading Process Using Change Data Capture Method

Sunaadh Thulasiram(✉) and Nagaraja Ramaiah

Information Science Department, BIT, Bangalore, India
Sunaadhtl@gmail.com, prof.rnagaraja@yahoo.com

Abstract. The world of big data becomes a Business-critical component for Enterprise resource planning system and Business Intelligence. The ERP system runs big data longer and uses resource locks, which directly blocks the users from running queries on the database. Additionally, users will require updates on real-time data changes. More computational resources are required to reduce the loading cycle creating expensive processes with complete data loads. An ETL technique with CDC is used to resolve problems, through periodic updates of changed data. A process which identifies changed records to reduce the extract volume is knows as CDC. This paper proposes a structure capable of performing CDC by means of timestamps and replication tool designed for spontaneous synchronization between two databases. The overall performance of CDC technique to ERP system is compared. This approach is employed in a real-world project has noticed a transition to near real-time data ETL and performance improvement.

Keywords: CDC (Change Data Capture) · ETL (Extract, Transform & Loading) · Incremental load · Nearly Real Time Data Warehouse (NRTDWH) · Data integration

1 Introduction

The data storage and processing have achieved new dimensions with organizations, offering administrations strongly dependent on client information. Applications depend on the analysis of big data, so as to help regular day to day data services towards end users. On the other hand, the expenses for maintaining and handling databases remain more restrictive. To overcome this issue a database with massive scalability has been developed [15].

ETL tools exist to store data into a data warehouse. Integrating data through ETL tools are of three stages: extraction that is being applied on sources of heterogeneous data type, transformation, which gives high quality of data then finally loading the data to the warehouse repository. The procedure for development of any data warehouse is to grantee that workflow processes should not affect the performance of the operational/ enterprise/ transactional data sources being used [1].

Today's data cannot be up to date with respect to traditional data warehouse since it's usually loaded from operational systems. Tactical decisions built on any out dated

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 552–560, 2020.
https://doi.org/10.1007/978-3-030-37051-0_62

data would produce incorrect results. The method that can be used to solve this problem is change data capture. Change Data Capture (CDC) remains a tactical component in the data integration framework that drastically improves efficiencies, diminishes the requests for batch window loading, deals with the increasing data dimensions, delivers information in near real-time and reduces costs. Attunity Stream provides an enterprise-class CDC solution that balances and works effortlessly with existing ETL, data integration and event processing technologies [9, 14].

One of the major obstacles anticipated for Multi - National corporations and large Business will be to acquire and analyze huge volumes of data from various source systems. Various architectures focusing mainly on the data warehouse model are presented. Transferring raw data from source to target by means of transformation and mapping into standardized form is the basis of ETL process in a nut shell. Extraction is the process of mining data from source systems to use it later downstream in an environment of the data warehouse [4].

Whenever a company acquires another company its information systems are acquired which indicates stressful technical data integration as well as vitally expensive components for constructing a data warehouse. More often than not, the data warehouse helps the historical information and evaluation, which are not able to obtain the up-to-date data [2].

Real-time data warehouse is ready to display the ETL latest outcomes given a specified time with respect to the ERP system time on a CDC method. Frequently, Data Warehouse updates are processed by means of an ETL (Extract, Transform and load) process. In order to accomplish near real time data ETL would be consequently applied on changes in data and capture them in the act. CDC is utilized to grasp any data modifications taking place in source systems then seize data to be taken for delivery at the target database system. Lowering the rate and assets related to updating a company Data warehouse is the predicament for industry or IT. Our tools furnish new changes to be transferred onto a data warehouse which would shrink cost along with resources linked for updates of a corporation Data Bank. The procedure followed for loading incremental data which keeps frequently changing in the Data warehouse is by synchronization with the changes that have occurred in the Data sources considering the previous load. Incremental reload works quicker and successfully than full reload since only the changes in data are loaded [2, 12].

2 Related Work

2.1 Existing System Current Change Data Capture Approaches

In the former research, the different techniques of CDC are brought into effective action to set up a RTDW system. The test of these techniques involves record based, trigger based, log based, Data base snapshot and refresh table which results in differences in performance for various systems [6].

After many experimental analyses the outcome of results will suggests log based since it supports Real time capture and this type of research utilizes joins and functions

and aggregation using quires to CDC by pre-calculation of data. For handling of large amount of data more efficiently different generated techniques are used [6].

In the other approaches triggers were used as CDC and to generate that triggers the algorithms were created based on the precise tables, and from the other experimental research, the trigger method made the algorithm to be considered for the utilization of CDC which is used for incremental loading process to select the data warehouse with large dimensions [6].

Other research method is of ETL transformation which includes different types of mapping like one to one, many to many, many to one. These mappings are quite complex so that ETL operations are used because of its liability, which further can helped in understanding about the data stored in data bank which leads to inappropriate results and analysis. Hence it is a critical test to check whether data stored is correctly extracted and generated into data warehouse [8].

In the other research study, Supply chain management with the business strategy for business models of two different companies are chosen to analyze the issues of an infrastructure, implementation strategy, operational efficiency and the cost. These results explain the challenges which are faced while designing and managing of supply chain [7].

3 Method/Proposed System

Combination of timestamp and Replication and last by not the least using delta views for daily updates is the method which leverages the advantages of each method for strategic use to produce better CDC results.

3.1 Timestamp

Timestamps would be applied to records for the purpose of recording the time when a record was modified as of inserted or updated. It is likely to capture deleted records with timestamps only if there is a well-defined column which would take the operations into consideration for example, Insert (I), Delete (D), Update (U) and filtering by these values can help in understand why these records undergoes through the operation. Timestamps take fairly little time to setup and they DBMS is responsible in maintaining the timestamp. Figure 1 displays a timestamp method to CDC [11].

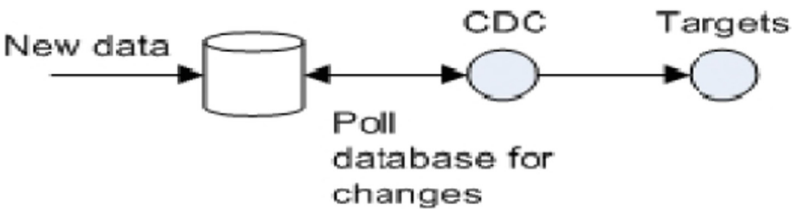


Fig. 1. CDC Timestamp: changed data will be time stamped. The CDC tool polls and extracts records which have been modified since the previous snapshot.

In this research change data capture method used is through timestamps on new records which has changed its value since the previous identified values, along with replication between two different Environments.

Data Warehousing (DW) Through ETL Process

A common occurrence for using CDC involves the practice of moving information into a Data warehouse. Conventionally, updating actions in a data warehouse is performed by using an ETL tool. ETL is a process which mines information from various sources. Transformation would perform cleansing of information before loading it in a data warehouse. The methods necessitate with the purpose of keeping ERP systems which would be off-line for a specific interval of time. The specified interval also known as "Batch Window" usually would be considered for daily and hourly loads. Meanwhile system would be full of active operations which moves the data and which is unable to perform business critical objectives. Major drawback of "bulk" loading process is the need for more processing time and more resources and since many IT companies and manufacturing factories load data on day-to-day or weekly basis it creates an obstacle for obtaining latest information. ETL tools are sometimes considered for achieving the same goal. CDC, however, produces a new alternative method to move relevant data to a data warehouse which runs flawlessly through ETL tools and replication tools [2, 13].

The Fig. 2 shows a high level functionality with respect to data warehousing and how ETL process using CDC method would be employed for a specific scenario. Operational/ERP/transactional systems would become one of the major sources of data which is replicated with an attunity tool designed to synchronize changes between two databases every few seconds and it would consider the timestamps to determine the start and end time replication. This would be utilized by the Informatica power center which is the data integration tool that uses workflows, mapping and sessions which would be designed keeping in mind business goals that needs to be integrated into IT. This allows business to be aligned with IT and through business intelligence reports the company is able to take better decisions [5].

The following combinations of methods are employed to enhance Near Real Time updates to the Data Warehouse.

3.2 Modified Date Using Timestamp

Various transaction systems collect metadata footpaths on every single line, containing creator name, id, version and the most recent modification was done by whom and what time it was generated as well as modified. CDC method of tactfully being able to back track any modifications which have occurred and runs query filters in contrast to Modified_date column, to acquire all definite change data capture rows modified from the time of the previous extraction process [6].

System processes are the following:

Complete variables are declared also initiated and StartDTime which holds last_run_time value plus RunDate which holds time of execution and date. Delete which holds erased data from source database. Complete fresh data inserts to database. Updating records which has changed with respect to previous modified time. Also updates values present in last_run_time through time of execution as well as the date.

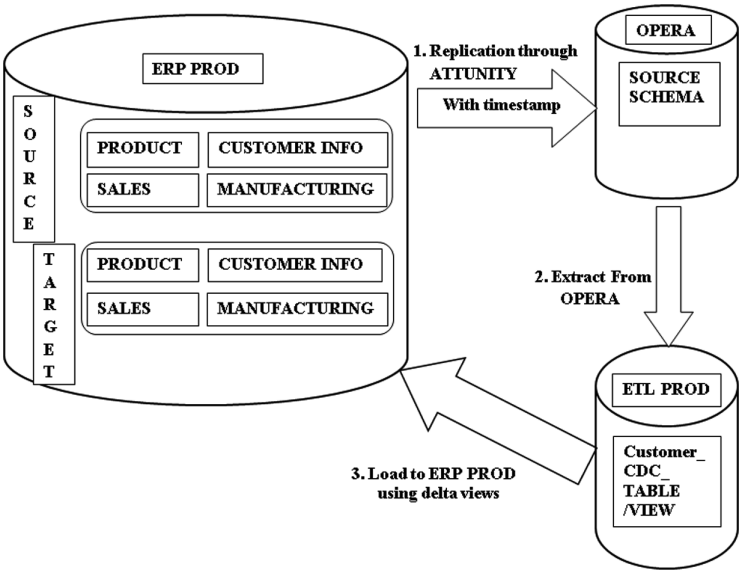


Fig. 2. CDC implementation on data warehouse

3.3 Attunity Tool Replication

The technique would guarantee constancy data among databases improving data dependability, error tolerant and availability. The technique would be typically useful for diverse Databases, naturally by means of master and slave correlation sandwiched between an original source and replica. Synchronization between data source/database and ETL database should be maintained periodically so as to achieve better data availability to provide better reports for end users and lets them to take a strategic decision to improve business for the present as well as for the future [6].

Here's a case for creating replication taking place in a Microsoft SQL Server DBMS:

Setup shared files for daily snapshots of data values. Design master and salve for data to flow. Catalog configuration is for replication, publication along with design and gathering objects. Backups on databases of master instance as well as restoring the slave instance for future retrieval of data and finally configure for replication from source to stage area.

3.4 Views Using Delta Loads

Once several records ought to be altered from source systems, data is used to update facts in addition to dimension tables of data warehouse. Fact tables are also the ones that profit most from the Loading incrementally/Delta loading style are most profitable to the fact tables as they naturally comprise a vast quantity of records. Alternatively, dimension tables remain comparatively smaller and updates are done by a truncate-reload style. Nevertheless, present-day cases also suggest presents of enormous

dimension tables, mutually in relationships with quantity of records also quantity attributes associated to the records. These dimensions are called as "monster dimensions", "whose size surpasses 100 million rows" [11].

Usually, these remain customers or client's dimensions of big organizations. These individual dimensions might yield an extensive loading time, as both record count as well as amount of attributes are huge it needs a longer time for calculation. The confidence intended on these huge dimensions, will be by building a "delta view" – a view which holds candidate keys as records which must be reported through ETL process. Despite fact schema, delta views will be inferred as of the source tables, then again from various additional tables which will be used by dimensions of ETL process. Real-life modification of any relational tables could influence many contents of a dimension [10].

Attunity Replication empowers organizations to speed up data replication, ingest and streaming through an extensive range of heterogeneous databases, data warehouses and Big Data platforms.

Here is a snowflake schema designed for data warehouse, Fig. 3 presents the schema diagram and meta-data for fact table shipment as described below. There can be direct or indirect customers for a manufacturing company who seller different products. Direct customers are those who would make e-commerce or retail store purchases of smaller quantities whereas indirect customers are those who go through distributors or wholesale stores to purchase large volumes of products in a weekly/monthly/yearly basis. The diagram depicts a relationship between these dimensions (DIM) tables and how fact table values are affected through inflation.

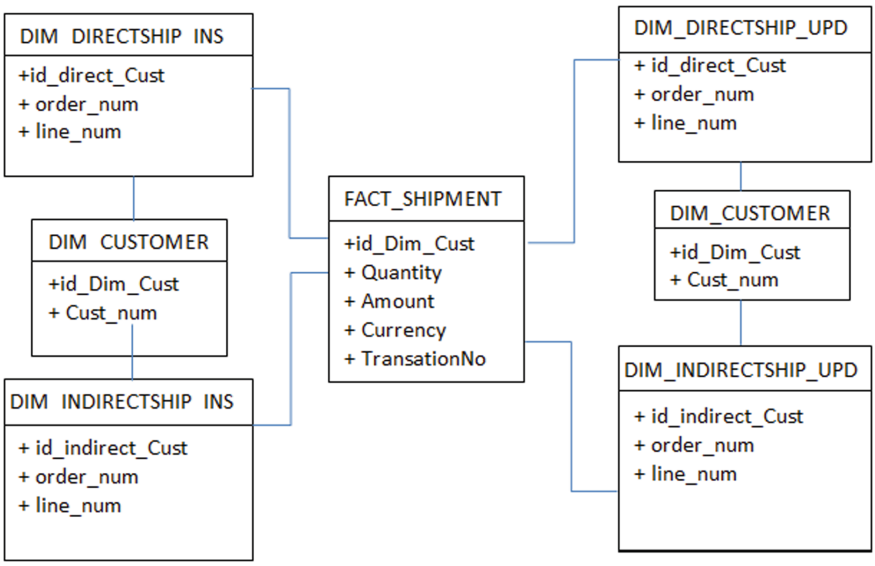


Fig. 3. Snowflake schema data warehouse

4 Experimental Results

The preliminary stage in the study was designing different models to fit the CDC approach for operations like Insert, Update and whether to have parallel or serial inserts, updates on which testing is performed on dummy data. Data would be consisting of booking, backlog, shipment and billing as the major modules of sales and manufacturing products of a product company. Various categories of data sources like flat files, CSV files, relational database (Oracle and Microsoft SQL Server) are performed on the modules. The investigation consists of numerous steps which are tested on each method. Generally, the execution of the query using informatica workflows will be the leading step. Next steps would consist of inserting data which have been modified to the staging area for ETL methods. The final stage would be the process of ETL on dimension and fact tables for operation in the order of insert-update-delete. Testing is performed on each module step by step and reconciliation results are produced in minutes of measurement of time which are calculated on the execution time of database and perform ETL processing by Informatica power center integration tool. The methods which are tested use either incremental loading process or full reload in some cases. These methods use timestamp on table rows and for files. The target system is of oracle PL/SQL database. Only the changes which are changed after the modified date would be warehoused to the database of the target system. Industrial process validating data and also producing reconciliation results is a skill which is used to manage data and scientific approaches to automatically ensure reconciliation and data validation by modifying dimensions. Reconciliation of data is a procedure that aims at measurements of errors which are a cause of random errors/ measurement noise and correcting those errors. The errors in the measurements may reduce the strength of the reconciliation results. Minimizing overall error data is needed in order to satisfy the system constraints.

Figures 4, 5 displays the reconciliation graph results that have been tested on change data capture method through ETL process. Figure 4 displays amount of price and quantity of products present in source and target for all the major modules of revenue generation of a product company. All the modules would directly service as a decision maker since these are components of sales and supply and demand for the company [3]. The general basis is that counts between source and target should be the same values to have consistency but vary only in exceptional cases.

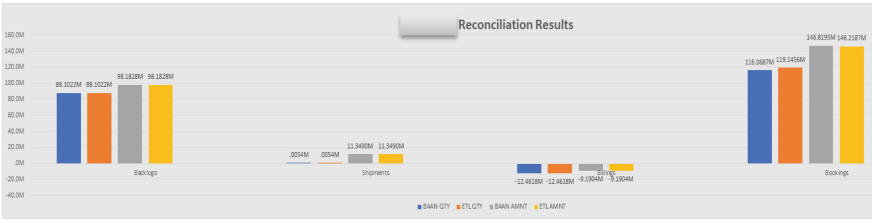


Fig. 4. Displays the reconciliation results for different modules which are integrated using CDC

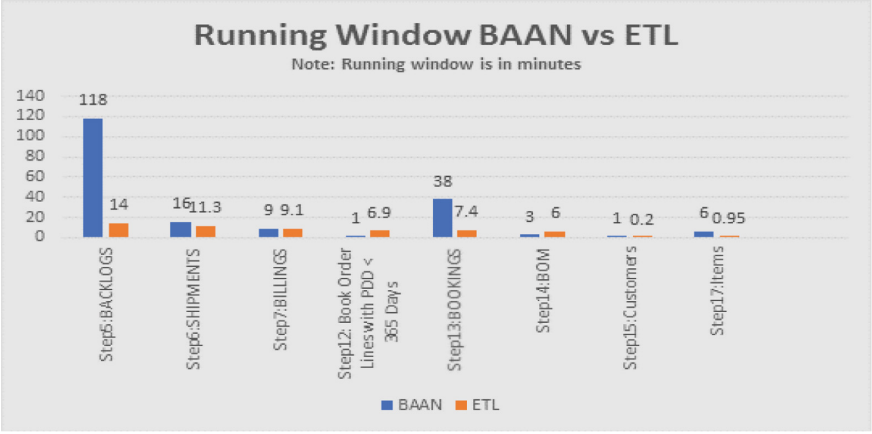


Fig. 5. Displays the performance graph for the run time window between transitional system (BAAN) and the ETL system process via CDC.

5 Conclusion & Future Work

The proposed paper explained ETL process using change data capture based on monitoring any modification of data at the source database and combining different ETL methods to optimize the Data integration process along with de-coupling the transitional system load and resource locks. Attunity tool synchronizes databases at a high-performance network. Now it is possible to process big data through CDC and ETL as the volume of data would enormously grow. The proposed paper is designed with the qualities of reliability, integrity, predictability and security in order for the business to take a firm decision at any vital situation with near real-time data.

Futures work would include further optimizing query through high-performance joins or sub-query for specific models to reduce the latency and/or backtrack any additionally queries common to end users are not used so that the number of tables/views are reduced and/or move to a HP Superdome Server when using very large datasets in the future.

References

1. Li, J., Xu, B.: ETL tool research and implementation based on drilling data warehouse. In: Seventh International Conference on Fuzzy Systems and Knowledge Discovery, pp. 2567–2569 (2010)
2. Tank, D.M., Ganatra, A., Kosta, Y.P., Bhensdadia, C.K.: Speeding ETL processing in data using high-performance joins for changed data capture (CDC). In: International Conference on Advances in Recent Technologies in Communication and Computing, pp. 365–368 (2010)

3. Woodall, P., Jess, T., Harrison, M., McFarlane, D., Shah, A., Krechel, W., Nicks, E.: A framework for detecting unnecessary industrial data in ETL processes. IEEE, pp. 472–476 (2014)
4. Pan, B., Zhang, G., Qin, X.: An overview and implementation of extraction-transformation-loading (ETL) process in data warehouse. In: 3rd International Conference on Information and Communication Technology, pp. 70–74 (2015)
5. Pan, B., Zhang, G., Qin, X.: Design and realization of an ETL method in business intelligence project. In: 3rd IEEE International Conference on Cloud Computing and Big Data Analysis, pp. 275–279 (2018)
6. Chandra, H.: Analysis of change data capture method in heterogeneous data sources to support RTDW. In: 4th International Conference on Computer and Information Sciences, pp. 1–6 (2018)
7. Al Faris, F.Z., Nugroho, A.: Development of data warehouse to improve services in IT services company. In: International Conference on Information Management and Technology, pp. 483–488 (2018)
8. Homayoun, H.: Testing extract-transform-load process in data warehouse systems. In: IEEE International Symposium on Software Reliability Engineering Workshops, pp. 158–161 (2018)
9. Efficient and Real Time Data Integration with Change Data Capture, An Attunity White Paper, pp. 1–20 (2009)
10. Mekterović, I., Brkić, L.: Delta view generation for incremental loading of large dimensions in a data warehouse. In: MIPRO 2015, 25–29 May 2015, pp. 1417–1422 (2015)
11. Ghugarkar, M.P., Borude, M.Y., Irabashetti, P.: Real-time change data capture using staging tables and delta view generation for incremental loading of large dimensions in a data warehouse. Int. J. Innov. Eng. Res.Technol. 1–5
12. Bokade, M.B., Dhande, S.S., Vyavahare, H.R.: Framework of change data capture and real time data warehouse. Int. J. Eng. Res. Technol. (IJERT) **2**(4), pp 1418–1425 (2013)
13. Atmaja, I.P.M., Saptawijaya, A., Aminah, S.: Implementation of change data capture in ETL process for data warehouse using HDFS and Apache Spark. In: Conference Paper, September 2017
14. Shi, J., Bao, Y., Leng, F., Yu, G.: Study on log-based change data capture and handling mechanism in real-time data warehouse. In: International Conference on Computer Science and Software Engineering, pp. 478–481 (2008)
15. Schmidt, F.M., Geyer, C., Schaeffer-Filho, A., DeBloch, S., Hu, Y.: Change data capture in NoSQL databases: a functional and performance comparison. In: 20th IEEE Symposium on Computers and Communication, pp. 562–567 (2015)

Predicting Stock Market Movement Based on Twitter Data and News Articles Using Sentiment Analysis and Fuzzy Logic

Roshni Pal(✉), Utkarsha Pawar, Karishma Zambare, and Varsha Hole

Bhartiya Vidya Bhavan's Sardar Patel Institute of Technology, 400058 Mumbai, India
{roshni.pal, utkarsha.pawar, karishma.zambare, varsha_hole}@spit.ac.in

Abstract. Social media has become an integral part of everyone's life. Twitter is the most prevalent social networking service where millions of users share information astronomically everyday. Aggregation of these tweets provides a reflection of public sentiment which has a notable impact on the Stock Market. The objective of the proposed method is to predict the impact of Tweets and News Articles on Stock Market and provide insights to the investors to help them decide whether or not to invest in a company. The paper proposes a method to improve the efficiency of the existing methodologies by including news articles and adding specific weights to each tweet based on authenticity, followers of the twitterer and it's retweet count for scrutinizing the public sentiment. It also considers sentiments expressed via emoticons and converts prolonged words into their normal form to increase the efficiency of sentiment analysis. Further, it uses N-gram representation for Feature Extraction and performs sentiment analysis on the collected tweets and news articles using Natural Language Processing and classifies the result into negative, positive or neutral using Naive Bayes classifier. The empirical results displayed in graphical format show that the proposed system can predict the fluctuations in the stock prices based on the sentiment analysis performed on previous day's collected tweets and news articles.

Keywords: Sentiment analysis · Polarity · Stock movement · Correlation · Nature language processing

1 Introduction

In today's era of digitization, where information technology is growing progressively, the incessant use of social media has reached miraculous levels. It has become the perfect platform for people to share their feelings and point of view. Public opinions and information is shared on a large scale daily. These opinions have a significant impact on the collective conscience of the society. Twitter, a social media platform with 275 million users worldwide is one of the most used social networking service. The information extracted from these tweets can be considered highly reliable as an investor information source. Research shows that the collective conscience created by tweets can be used effectively for predicting the company earnings and their subsequent impact on the stock prices. A study

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 561–571, 2020.
https://doi.org/10.1007/978-3-030-37051-0_63

report published in 2010 claims that the Dow Jones Industrial Average can be predicted with an accuracy of 87.6% based on the Twitter data. Studies have also shown that companies such as Tesla, Snapchat, Apple, etc. experienced evident fluctuations in their stock prices because of the tweets posted by celebrities, politicians and influencers. This effect of twitter sentiments on the stock market has been a motivation for many researchers. Many studies and experiments have been conducted that successfully predict the stock trends based on twitter data with and acceptable accuracy. In this paper we contribute to the idea of using news articles along with twitter data to increase the accuracy of the prediction [9, 12]. Sentiment Analysis is the process of recognizing the sentiments expressed in the textual data. It classifies the data as negative, neutral and positive. For sentiment analysis emoticons are considered along with text for more efficient results. Further, it also considers the authenticity of the tweets i.e. the number of followers; whether the tweet is posted from a verified account and the number of times the tweets are retweeted to improve the accuracy of the sentiment analyzer. The final results are depicted in graphical format to make it easier for the users to read and interpret the results.

2 Related Work

As introduced in introduction it can be deduced that social media reflects opinions that in turn affects the stock market. In recent years researchers and data scientists are actively working on analyzing these tweets and news articles that have an impact on stock market. Few of the research methods for analyzing such impact are described below. An author Huma Parveen has proposed a method for sentiment analysis of tweets that extends hadoop architecture to use naive bayes algorithm efficiently. It has also described the comparison of results with and without considering the emoticons where the results of emoticons are better [4]. In a conference paper published by Yahya Eru Cakra different classification models are compared based on their accuracy. The different models compared are support vector machine, naive bayes, decision tree algorithm, random forest & neural network. Linear regression is used for prediction model. According to a paper random forest classifiers gives the best accuracy and naive bayes give second highest accuracy [11]. Authors Chou and Nguyen have proposed a method in which prediction model for predicting stock market fluctuations, linear regression is used with sliding window metaheuristic optimization where past twitter data of certain days were used to predict the stock prices of observation day then this output was used in next day prediction by removing oldest data successively. It has shown that the prediction of one day ahead was more accurate and accuracy decreased as the no. of days in advance increases [5]. In a conference paper published by Pagolu where Word2vec representation of tweets was trained using a Random Forest model showed an accuracy of 70.2%, it is shown that a strong relation exists between the stock market fluctuations and the sentiments expressed on twitter related to that company [10]. Another paper by Dang and Duong sheds light on an improvised approach for determining stock market movements based on sentiment analysis of the published news articles. The authors have labeled the news articles on the basis of the delta closing price of the stocks and Support Vector Machine is used as a machine learning method to classify the financial news articles with an accuracy of 73% [7].

3 Data Acquisition

The tweets, news articles and stock market data can be collected using different APIs. The extracted data will be segregated according to the companies using data cleaning and data preprocessing techniques. This phase will have 3 subtasks.

3.1 Twitter Data Collection

Twitter data is collected using Tweepy. It is a supportive tool that gives access to twitter API. Python library called Python Twitter Tools is used for connecting to Twitter Streaming APIs. The data is obtained using this library is in JSON format. The JSON includes user details i.e. id, verified user or not, tweet created at, text etc.

3.2 Stock Market Data Collection

Stock market data is collected using Alpha Vantage API. Alpha Vantage is a real time API that provides Stock Time Series Data, Physical and Digital/Crypto Currencies (e.g., Bitcoin), Stock Technical Indicators and Sector Performances. The suite of APIs for Stock Time Series Data provides realtime and historical global equity data in 4 different temporal resolutions i.e. daily, weekly, monthly and intraday. It contains more than 20 years of historical data or even more if requested. The response is obtained in JSON format.

3.3 News Articles Data Collection

News articles are collected using News API. A request is sent by specifying the URL of News API. It returns a JSON response with key value pairs. The keys are authors, title, description, content etc. We iterate over the JSON object and store the content at one place in string format for further use.

4 Data Preprocessing

The data retrieved through different APIs is not in standard form. It contains URLs, prolonged words, punctuations, unnecessary spaces, etc. which doesn't contribute to the calculation of sentiment polarity. In order to improve the efficiency of result we should clean data by removing unwanted content. This phase has four main steps.

4.1 Separating Emoticons from Tweet

Emoticons are used now-a-days a lot in social media. Many peoples are used to append emoticons at end of text based on their emotions. So analyzing sentiment of emoticons along with text gives better results. For sentiment analysis of text and emoticons we need to separate text and emoticons from the tweet. So we are extracting emoticons from tweet before preprocessing the tweet using emoji. UNICODE_EMOJI dictionary of emoticons library.

4.2 Tokenization

The tweets are combination of multiple things like text, punctuations, emoticons, some regional language text. To remove any unnecessary part of tweets converting the text into array of single words makes computation easier. So the extracted tweets and news articles are converted into an array of words. These array are then analyzed to see if the array contains unwanted punctuations, regional language texts, emoticons, etc. Removal of these unnecessary symbols becomes easier by performing tokenization.

4.3 Pattern Matching

Usually hashtags (#) and @ are found in tweets. They are substituted by suitable characters. For example, #Nestle is replaced with Nestle and @DonaldTrumph is replaced with user. Intense emotions shown by prolonged word like 'yeaaaahhhhh!' are replaced by 'yeah!'. Using pattern extra white spaces, new line character can also be removed.

5 Sentiment Analysis

This phase involves the extraction of public sentiments from the acquired data. Sentiment analysis can be performed using NLTK library's Naive Bayes Classifier or using Textblob library that is build on top of NLTK.

The preprocessed tweets and news are passed to the sentiment analyzer where shallow parsing is performed to identify the constituent parts of sentences like verbs, nouns, adjectives, etc. Natural Language Processing is used to measure the polarity of the text. The calculated polarity is a float value that lies in the range of [−1, 1] where −1 denotes that the statement is negative while 1 represents that the statement is positive.

The sentiment analysis of emoticons along with text sentiment enhances the results [3]. For the sentiment analysis of emoticons, a dictionary is maintained containing the UNICODE values of the emoticons along with their polarity value that denotes the positivity, negativity or neutrality of the emoticon. For each emoticon in a tweet the respective polarity value is fetched from the dictionary and the total emoticon sentiment of the tweet is calculated by averaging the polarity values of all the individual tweets.

This emoticon sentiment is further added up with the tweet and news sentiments to calculate the aggregate sentiment for efficient prediction [8].

The impact of a tweet depends on various attributes. The number of followers the twitterer has plays a major role in determining the reach of a particular tweet. If the tweet is posted by a verified account, more people are likely to believe it since twitter has strict policies for getting an account verified. If an account is verified then it means that the account is managed by a valid user and the user credentials such as the identity proof and contact details have already been verified by twitter. The retweet count also affects the reach of a tweet. More times a tweet has been retweeted, more number of people are likely to read it.

Pseudocode for calculating sentiment:

For each tweet:

```
If (followers>100)
        check if (twitterer == verified user)
            sentiment = sentiment * 2;
        else if (retweet count >= 50)
            sentiment = sentiment * 2;
        else
            sentiment= sentiment ;
else
    discard tweet
```

For each tweet, attributes such as user name, number of followers, number of retweets and whether the tweet is from verified user account are extracted. Initially the number of followers of the user is checked. If the follower count is more than 100 then the tweet is considered for further processing else it is discarded. The tweets are further checked for number of retweets which expresses a strong agreement or disagreement with the tweet. If the number of retweets is more than 50 then the sentiment count is

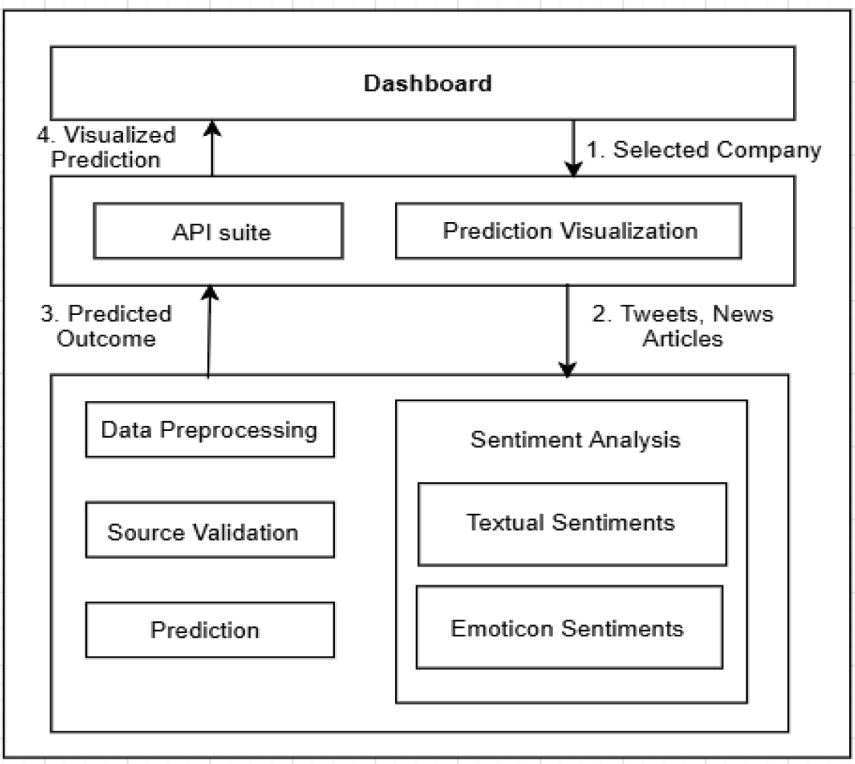


Fig. 1. Architecture diagram of proposed system

doubled. Similarly we check if the tweet is from a verified user which indicates authenticity of a tweet. If the tweet is from a verified user account, then again the sentiment count is doubled. If the tweet is neither from a verified user nor has the retweet count greater than 50, then its sentiment remains the same. In the end, the sentiment count is aggregated and percentage of positive and negative tweets about a particular topic is calculated.

Finally, the twitter sentiment results and the sentiments extracted from the news articles are aggregated for studying the impact on the stock market movements. Figure 1 shows the architecture diagram of proposed system.

6 Implementation Details

6.1 Data Acquisition

The Fig. 2 shows the collected twitter data formatted in JSON structure. The left part of the image depicts the entire data that contains tweets along with all its attributes. Whereas the right side depicts the extracted useful attributes that contribute to sentiment analysis.

The Fig. 3 shows the collected news data formatted in JSON format. The left part of the image depicts the entire data that contains news along with all its attributes. Whereas the right side depicts the extracted news content that contribute to sentiment analysis.

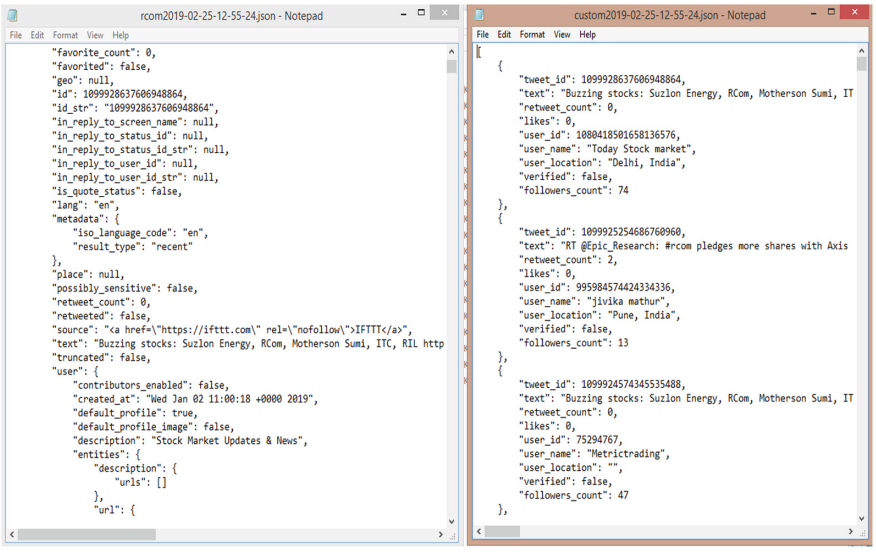


Fig. 2. Collected twitter data

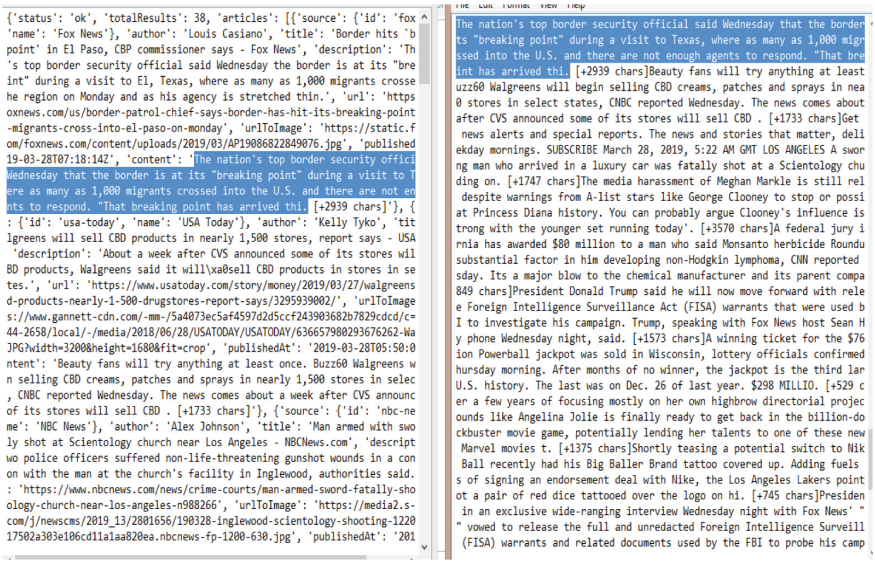


Fig. 3. Collected news data

6.2 Data Preprocessing

The Fig. 4 shows a sample of input data and results obtained after preprocessing it. The preprocessing method includes various stages such as separating emoticons from data, tokenizing the data and removing unnecessary symbols, URLs and white spaces. It also replaces prolonged words with their correct spellings. The output from these stages can be observed in the figure.

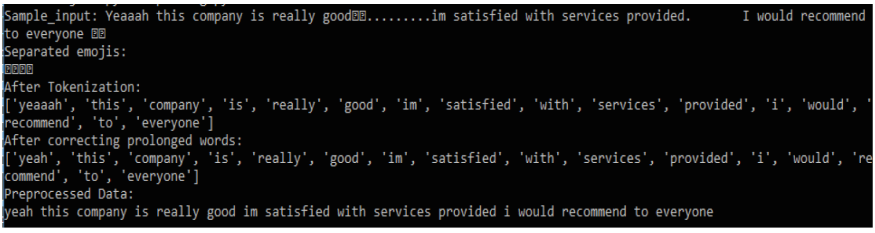


Fig. 4. Data preprocessing sample input & output

6.3 Sentiment Analysis

The Fig. 5 shows the result of the emoticon sentiment analyzer. A sample tweet "Yeaaah this company is really good.....im satisfied with services provided. I would recommend to everyone" was passed to the emoticon sentiment analyzer as input and positive sentiment was obtained from the extracted emoticons.

```
Sample_input: Yeaaah this company is really good.....im
 satisfied with services provided.       I would recommend to
 everyone
Emoticon sentiment is: positive
```

Fig. 5. Sentiment of emoticons

The Fig. 6 shows the sentiment analysis of twitter and news data on Snapchat. We can observe from the results that the positivity, negativity and neutrality of tweets related to snapchat is 38.88%, 5.55% and 55.55% respectively. Whereas, when tweets and news both are considered for calculating the aggregate sentiments, the observed values for positivity, negativity and neutrality are 63.15%, 31.5% and 5.26% respectively. Hence, it can be observed that considering news data along with the twitter data results in refined output.

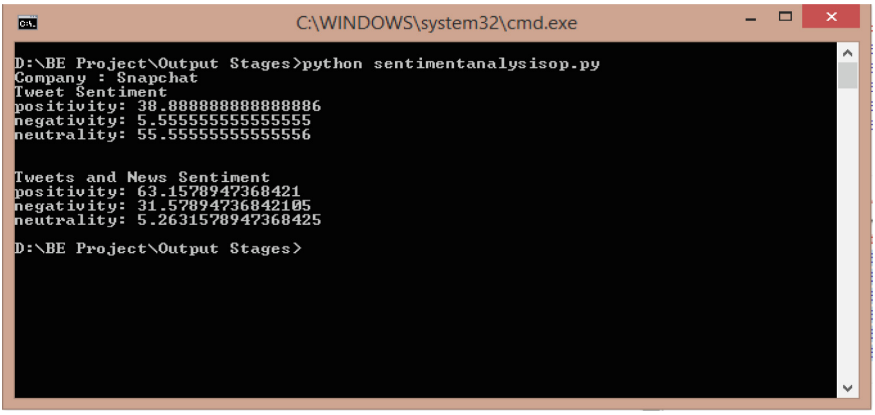


Fig. 6. Sentiment analysis result

7 Results and Discussion

Closing price of the stock for last 5 days is depicted using line graph. The sentiment analysis performed on news and tweets both are illustrated using pie charts which make it easier to understand and interpret the results. The pie charts show the positivity or negativity which can be compared with the rise or fall of the stock prices depicted in the line graph. If the pie charts show a considerable amount of positivity in the tweets and news articles, an increase in the line graph is likely to happen and vice versa.

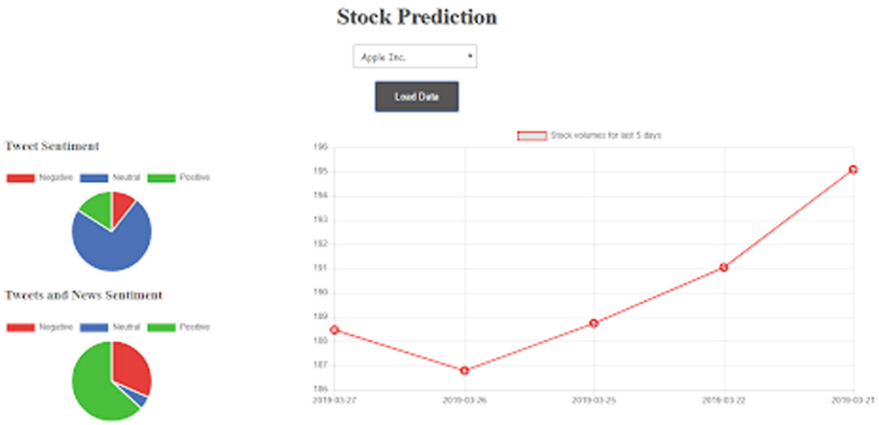


Fig. 7. Verifying predicted result with actual stock movement

The Fig. 7 shows the impact of twitter and news data on Apple Inc. stock prices. We can observe from the pie charts the arc length of the positive slice is greater than negative slice and hence rise in the stock price has been observed. We studied these result for multiple companies for 45 days and the aggregated results has been shown in the following graph.

Figure 8, shows the change in the achieved accuracy when different factors were considered. When sentiment analysis was performed on only twitter data 71% accuracy was achieved, while performing the same procedure on tweets as well as the news articles helped in achieving an accuracy of 77%. Whereas, when preprocessed data was passed to the sentiment analyzer and twitter attributes were taken into consideration, it achieved an accuracy of 73% and 81% with tweets and tweets as well as news articles respectively.

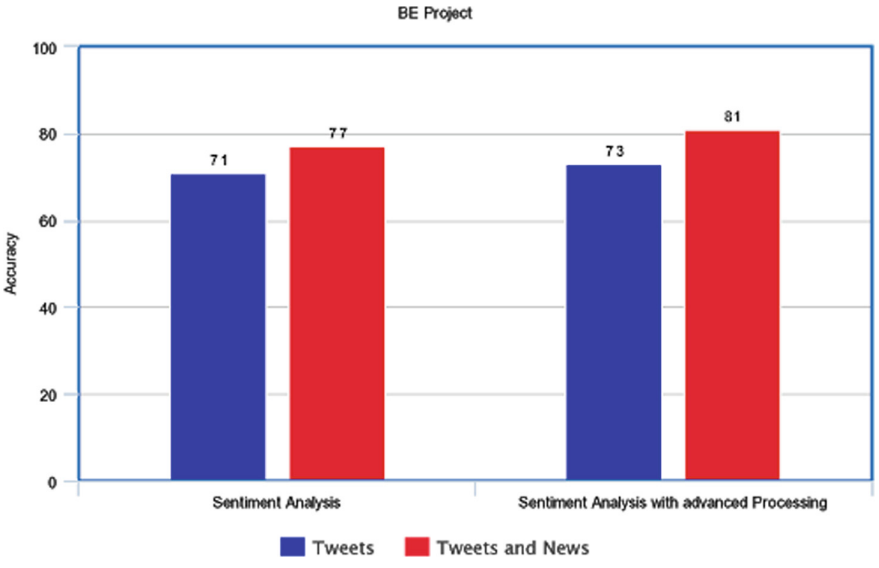


Fig. 8. Accuracy

8 Conclusion and Future Work

In this paper we have evaluated how strongly do the tweets correlate to the stock market movements by considering various twitter attributes such as follower count, authenticity etc. We calculate the percentage change in the stock based on the sentiment calculated by considering various parameters of the tweets, news articles and performance of the stock in past. Further we have used fuzzy logic to get a specific amount of movement in the stock. The prediction accuracy gets enhanced due to the consideration of news articles, enhanced filtering and assignment of weights to tweets such as retweet count, no of followers before calculating sentiment. The prediction system has achieved 81% accuracy.

Machine learning approaches such as RNN can be used for calculating the sentiments more accurately. Along with the authenticity and impact of the tweets the magnitude of news articles can also be taken into account with the use of Google trend index value [1]. The calculation of stock movement using fuzzy logic could be improved with neural networks [2, 6].

Since only a group of companies were considered for this study, the scope can be expanded by using various ticker symbol lookup APIs which will facilitate the users to use the prediction system for any given company whose twitter data is available.

References

1. Kaushal, A., Chaudhary, P.: News and events aware stock price forecasting technique (2017). https://doi.org/10.1109/BID.2017.8336565
2. Hawley, A.: Fuzzy nets: fuzzy logic and neural networks (2002). https://doi.org/10.1109/IJCNN.2001.939079
3. Wang, H., Castanon, J.A.: Sentiment expression via emoticons on social media (2015). https://doi.org/10.1109/BigData.2015.7364034
4. Parveen, H., Pandey, S.: Sentiment analysis on Twitter data-set using Naive Bayes algorithm (2016). https://doi.org/10.1109/ICATCCT.2016.7912034
5. Chou, J.S., Nguyen, T.K.: Forward forecast of stock price using sliding-window metaheuristic-optimized machine-learning regression (2018). https://doi.org/10.1109/TII.2018.2794389
6. Yap, K.S., Wong, S.Y., Tiong, S.K: Compressing and improving fuzzy rules using genetic algorithm and its application to fault detection (2013). https://doi.org/10.1109/etfa.2013.6648106
7. Dang, M., Duong, D.: Improvement methods for stock market prediction using financial news articles (2016). https://doi.org/10.1109/NICS.2016.7725636
8. Elfajr, N.M., Sarno, R.: Sentiment analysis using weighted emoticons and SentiWordNet for Indonesian language (2018). https://doi.org/10.1109/ISEMANTIC.2018.8549703
9. Im, T.L., San, P.W., On, C.K., Alfred, R., Anthony, P.: Analysing Market Sentiment in Financial News using Lexical Approach (2014). https://doi.org/10.1109/icos.2013.6735064

10. Pagolu, V.S., Reddy, K.N., Panda, G., Majhi, B.: Sentiment analysis of Twitter data for predicting stock market movements (2016). https://doi.org/10.1109/SCOPES.2016.7955659
11. Cakra, Y.E., Trisedya, B.D.: Stock price prediction using linear regression based on sentiment analysis (2015). https://doi.org/10.1109/ICACSIS.2015.7415179
12. Wang, Z., Ho, S.B., Lin, Z.: Stock market prediction analysis by incorporating social and news opinion and sentiment (2018). https://doi.org/10.1109/ICDMW.2018.00195

Distributed Storage Hash Algorithm (DSHA) for File-Based Deduplication in Cloud Computing

S. Hema(✉) and A. Kangaiammal

Government Arts College (Autonomous), 7 Salem, India
hema_mast@yahoo.co.in, indurath2002@yahoo.co.in

Abstract. Increasing volume of digital data in cloud storage demands more storage space and efficient technique to handle these data. Duplicate is unavoidable while handling huge volume of data. Data Deduplication is an efficient approach in cloud storage environment that utilizes different techniques to deal with duplicate data. Existing systems generate the hash value by using any kind of cryptographic hash algorithms such as MD5 or Secure hash algorithms to implement the De-duplication approach. These algorithms produce fixed length of 128 bit or 160 bit as output respectively in order to identify the presence of duplication. So, an additional memory space is used to store this hash value. In this paper, an efficient Distributed Storage Hash Algorithm (DSHA) has been proposed to lessen the memory space occupied by the hash value which is utilized to identify and discard redundant data in cloud. Experimental analysis shows that the proposed strategy, reduces memory utilization of hash value and improves data read/write performance.

Keywords: Deduplication · Chunking · MD5 · SHA-1 · Bloom filter

1 Introduction

Cloud computing provides a new way of internet technology that manages resources and applications using both internet and central remote servers. Many end users use this innovation with least cost as well as gain access to application without an installation. Cloud computing has some desirable qualities such as fault tolerance, high speed processing, large storage capacity and bandwidth. Moreover, it allows to access the remote information and files using the Internet [4]. The most vital and typical cloud service is information storage service. In cloud storage, duplication cannot be avoided when handling huge volume of data. Even though cloud storage space is huge; this kind of duplication greatly wastes networking resources, consumes a lot of power energy, and makes data management complicated. Deduplication has proved to achieve high space and cost savings, which can reduce up to 90–95% storage needs for backup applications [15] and up to 68% in standard file systems [7].

Data deduplication and data compression are the most prominent techniques used among the available techniques for optimal storage in cloud. Data deduplication is one of the intelligent compression techniques which eliminates duplicate data by storing

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 572–581, 2020.
https://doi.org/10.1007/978-3-030-37051-0_64

only a single copy of each file [9] or block. Duplicate data is replaced by means of a pointer to the unique copy of data. Data deduplication is a vital methodology to prevent the storage of redundant data in storage devices. The reason behind data deduplication is to extend the amount of information that can be stored on disk arrays and to improve the suitable amount of data that can be transmitted over networks. As indicated by the report of Microsoft research [1, 8] the three quarter of digital information is redundant. Data deduplication is expanding with much consideration by the analysts since it is a beneficial method to manage data reduction.

There are two main strategies used in data deduplication storage systems namely Delta-based deduplication and Hash-based or Finger Printing-based deduplication. Delta-based deduplication is a strategy that performing deduplication in view of the distinction between two files. This approach takes old and new versions of a file as an input and calculates the dissimilarity between them. Delta-based deduplication techniques are used in incremental backups. During the incremental backups, delta encoding algorithm computes the difference between the old and new versions of a file. The differences obtained are called delta value. These delta values are stored along with a pointer which points to the old version of a file [8, 18, 23].

Hash-based or Finger printing based deduplication method uses a cryptographic hashing function which generates a hash value to find and remove redundant data. Cryptographic hash functions are considered as a unique category in the field of cryptography and they are designed to exhibit one-way operations. The one-way means that it is computationally very hard to derive the original text from the hash value. Hash functions take an arbitrary length of information as input and forming a hash value (message digest) of fixed length in the range of 128–512 bits. While the same data is implemented several times in the hashing process, each time the same hash is created. Some of the hashing algorithms used in today's real-world applications are Secure Hash Algorithm 1 (SHA-1) [6] and Message-Digest Algorithm5 (MD5) [16]. Hash based de-duplication splits information into blocks or "chunks", either fixed [17] or variable size [11], and processes the "piece" with the hashing calculation to make a hash. Once the information is chunked, an index can be produced from the outcomes, and the duplicates can be found and discarded. Only a single instance of each chunk is secured. In the event that the hash does not exist, at that point the information is stored and the hash index is refreshed with the new hash. SHA-1 [12] is stronger but slower than MD5 [12]. It has very less chances of data collision occurrence. MD5 [20] is faster but less secure than SHA-1 [12]. The major challenge in deduplication systems is to identify duplicate data segments quickly. An index can be produced from the hash value which is necessary to identify the presence of duplication. Because of the hash value pattern, index access being random, result in an excessive amount of random disk IO. Moreover, it degrades whole system performance significantly.

To reduce the disk index lookups during the deduplication process, they used a Bloom filter [2, 3] as the summary data structure to test that the hash value is new to the system. It reduces disk lookups for data chunks that do not exist in the index. Nevertheless, the problem is bloom filters are probabilistic data structure, so it can be ensured that an element is NOT present in the index but cannot ensure its presence. Instead of using bloom filter, Sparse Indexing [13] can be utilized for sampling the index of hash value, which requires less than half of RAM to store index.

This approach solves the disk bottleneck problem and provides an excellent deduplication on data set. Main drawback of this approach is that it allows a few duplicate chunks to be stored.

Inspired by all these considerations, an efficient approach has been designed and the main focus of this approach is to lessen the memory space occupied by the hash value as well as improve the data read/write performance at low system cost.

The rest of this paper is designed as follows: The existing well known deduplication approaches are evaluated with the proposed approach. The related work is given in Sect. 2. Section 3 describes proposed system architecture. Section 4 shows the implementation and test analysis. At the end, conclusion of the proposed work is presented in Sect. 5.

2 Related Work

Zhu et al. [3] approach focus on the best way to execute Identical Segment Deduplication storage system with high throughput and low system cost for removing the disk bottleneck. Using the SHA-1 algorithm, the hash value is calculated to identify the segments separately. This approach employs the Bloom filter data structure and cache index fragments to reduce disk index lookups. However, the problem is that Bloom filters are probabilistic in nature, so it can be assured that an element is not in the index. But its existence cannot be confirmed.

In Lillibridge et al. [13] presented Sparse indexing technique that applied sampling and locality ideas for large-scale backup storage. In this approach, chunk-lookup disk bottleneck issue has been solved using locality principle. Sampling and sparse indexing are additionally utilized to identify similar segments. It needs just few searches for each segment, so that chunk-lookup disk bottleneck problem could be avoided; and at the same time, it improves the deduplication method hugely.

Bhagwat et al. [5] introduced a new technique for non-traditional backup workloads called Extreme Binning for Scalable and parallel deduplication System. Rather than using locality principle, Extreme Binning used file similarity principle. This approach employs chunk-based deduplication and splits chunk index into two levels. First level is put in RAM and the second level is put away in disk. Therefore, it diminishes the disk bottleneck problem and gives sensible throughput. Designed by Zhang et al. [21], the deduplication storage system is named as Droplet. This method has high throughput and scalability. It distributes data streams onto multiple storage nodes. In this manner, it limits number of data blocks stored on every node and guarantees the whole hash value index kept into RAM memory as well as provides good Input/Output performance.

Venish et al. in [19] examined various chunking algorithms and looked at its performance. According to this work, file level chunking strategy handles small size files efficiently. But it is not suitable for large size files. This paper specified the boundary shifting problem happening in fixed size chunking method may be resolved by using variable size chunking method. At last, it indicates that the content-aware chunking method provides better results for multimedia files such as video, audio, image. İt also indicates that the usage of storage is significantly reduced.

Yan et al. [22] has suggested a proxy re-encryption (PRE) plan to store encrypted data in cloud. This scheme has used three types of entities such as CSP for storage, Data owner who has the highest priority for data storage and Data holder. These three entities communicate with one another through a safe channel. The clients upload their personal data in an encrypted form to a CSP and allow it to protect these information. Further, for data holder to access any data file is only possible after showing evidence of his ownership [9]. Experimental outcome demonstrates that this plan is effective, with sound adaptability and extensibility.

3 Proposed System Architecture

This section describes the architecture of the proposed system that generate hash value by using suggested Distributed Storage Hash Algorithm (DSHA) utilized to identify and remove duplicate data in cloud. Here single server that monitors the entire system performance and maintains storage nodes in the system. More than one storage nodes handles hash value index and deduplicated file data.

3.1 System Components

In this proposed approach, the client first connects to the server and generates queries for the desired process. Initially hash value is generated for any read/write operation and compared with the associated hash index list for duplication check. The process is discarded immediately if the hash value already exists else it will be treated as new data block and stored on appropriate storage nodes.

De-duplication can be implemented by either In-Line method [10] or Post-Process [14] method. In In-Line method, deduplication takes place at the instant when the data is written to the storage device. But it would be time-consuming process. For post-processing, deduplication takes place in an idle time after the data has been written to disk; it requires a large storage space. It is usually faster than In-Line method. However, most of the researchers prefer inline process model, because the duplicate data will be deleted before the data is written to the storage device and it improves data writing performance. This paper uses inline deduplication process, since it requires less storage space than the post-process method (Fig. 1).

3.2 Client API

Proposed scheme provides good interface between client and storage server. This reduces the load of the CPU by selecting the required storage node. The sample of client code created in java is given below (Fig. 2).

3.3 Hash Value Generation

Existing systems make hash value using well-known cryptographic hash algorithms such as MD5 [16] or SHA-1 [6]. These algorithms produce fixed length of 128 bit or 160 bit as output respectively. These hash values are used only to identify file/chunk

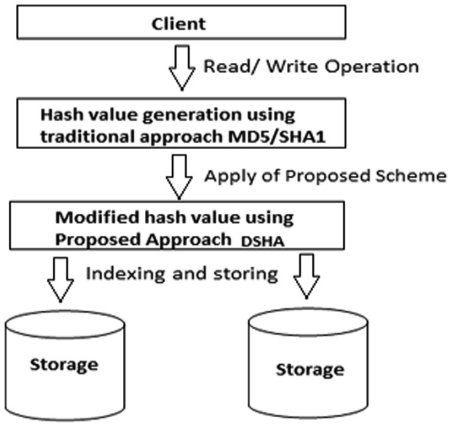


Fig. 1. Proposed system architecture

```
System.out.println();
jLabel3.setText(digits+outputString1);
Class.forName("com.mysql.jdbc.Driver");
con = DriverManager.getConnection("jdbc:mysql://localhost:3306/javamysql","root","root");
String HashValue = digits + outputString1;
String status=null;
    int result,tab=0;
```

Fig. 2. java Code: client program

uniquely and to identify the presence of duplication. In this scheme, we considered entire file as chunk that means we applied file level approach. Here, we build the hash value based on traditional approach. Our proposed hash value function, not only reduce the length of hash value but also used to identify duplicate data.

3.4 Storage Node

Storage has been created by multiple storage nodes. These nodes separately handles its associated hash value index and the file data. Each node has been recognized by its distinctive ID, and also the blocks within the node has been recognized by their offset value. To find a specific hash value, this approach selects the correct storage node and uploads only the hash value associated with this storage node in RAM. In this way, it reduces the search time of a hash value.

4 Implementation and Test Analysis

The proposed method is implemented in Java as front-end and MYSQL as backend. The performance has been evaluated. Table 1 describes the test environment. SHA1 has been selected for its collision resistant property to calculate the hash value. Moreover, different file types and size of files are utilized to execute the experiment.

Table 1. Test Environment

Hardware environment	Processor - Intel(R)Core(TM)i5-5200U CPU @ 2.20 GHz hard disk drive is 1 TB Memory: 8 GB RAM
Software environment	Operating System: 64-bit Windows 10 home version 1803 Programming Environment: Net Beans IDE 7.0.1, Java: 1.7.0; Database Server: 127.0.0.1 via TCP/IP, Software: MYSQL 5.5.27

4.1 Experimentation

Case 1: client uploads a new file named pt.txt

This method does not store the file rapidly. First generates a hash value using the SHA-1 algorithm, then following the proposed algorithm, the generated SHA-1 hash value is modified. By using this modified hash value, it identifies the corresponding storage node and checks the presence of hash value in the hash value index. As the hash value is not in the index, the file associated with the hash value is considered as a new file and uploaded. The process is depicted through Fig. 3.

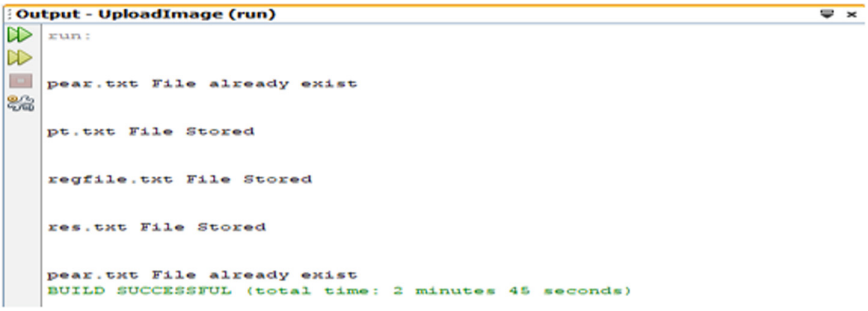


Fig. 3. New file upload and duplicate file reject process

Case 2: Client uploads duplicate file named pear.txt

As shown in Fig. 3, the client tries to upload the same file that is already stored. However, this approach confirms that the uploaded file is a duplicate and hence immediately rejects it.

4.2 Test Analysis

Test 1: Memory space usage

File level is appropriate because the files chosen for testing are smaller in size. For each uploaded file, the proposed hash value as well as the SHA-1 hash value was created.

All the examinations, the following parameters appeared in Table 2 was utilized. From the end of this test, it is revealed that the proposed hash function does not take too much time to create hash value.

Table 2. Setting environment for file upload

Parameters	Value
Total number of records	1275
Space occupied by SHA-1 hash value	25500 (byte)
Space occupied by proposed hash value	22140.5 (byte)

The hash value generated using the modified function is of varying size. However, its size is less than the size of the SHA-1 hash value. The chart in Fig. 4 depicts how the proposed hash value reduces memory space usage. From this experiment, it proves that SHA-1 occupies more memory space than the proposed algorithm.

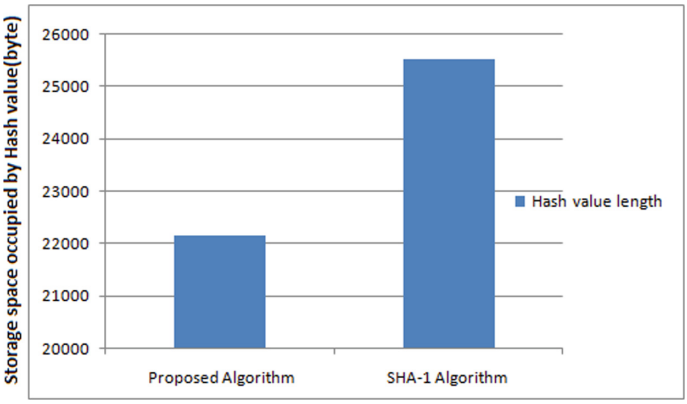


Fig. 4. Comparison of proposed algorithm and SHA-1 algorithm

Test 2: Reading performance

The aim of the following framework is to assess reading performance of storage node. Instead of using single storage, multiple storage nodes are proposed to enhance the data read/write performance (Table 3).

In this framework each storage node is identified by unique ID and also the file data is saved at the storage terminal on the basis of its hash value. Figure 5 shows that the proposed scheme takes less time than single storage. This is because the time it takes for search has been reduced by looking into only the storage terminal associated with the hash value.

Table 3. Files with different types and different sizes used to search

File name	Time taken by single storage node (s)	Time taken by multiple storage node (proposed) (s)
msg_41.txt	3.0361	1.9815
index.txt	3.0926	1.8022
msg_35.txt	3.2901	2.2642
msg_24.txt	3.6041	1.1901
webadd.docx	3.2916	1.2055
img39.jpg	3.4631	1.3373

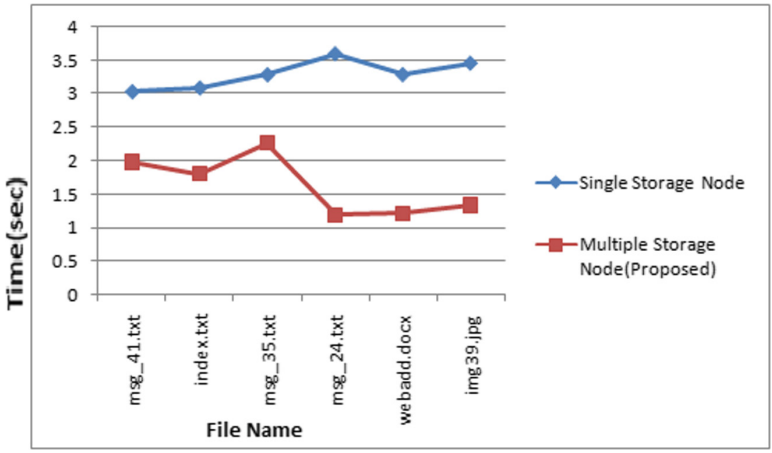


Fig. 5. Read performance of single storage node and multiple storage node.

5 Conclusion

The proposed approach DSHA generates the variable length hash value rather than the fixed length hash value generated in the existing approach. Each file with a new hash value is treated as new data block and stored on the appropriate storage nodes. Thus, generated DSHA hash value is utilized to identify and discard duplicate data in cloud At any given point of time, the hash value in the storage node is unique. Instead of using single storage node, the file data are distributed among multiple storage nodes based on its hash value; so that it reduces disk access and increases the speed of read/write operation.. Hence it proves to be an optimal algorithm for file-based deduplication in cloud computing environments. The proposed approach is designed for a client and it clearly displays effectiveness of DSHA in terms of time and space. In future, this approach could be used for multiple clients. It is evident to see from the test results that this approach would be cost effective when used for multiple clients and for huge volume of data.

References

1. El-Shimi, A., Kalach, R., Kumar, A., et al.: Primary data deduplication–large scale study and system design. In: Proceedings of the 2012 Conference on USENIX Annual Technical Conference (USENIX'12), USENIX Association, Boston, MA, USA, June 2012, pp. 1–12 (2012)
2. Bloom, B.H.: Space/time trade-offs in hash coding with allowable errors. Commun. ACM **13** (7), 422–426 (1970)
3. Zhu, B., Li, K., Patterson, R.H.: Avoiding the disk bottleneck in the data domain deduplication file system. In: Proceedings of the 6th USENIX Conference on File and Storage Technologies (FAST'08), pp. 269–282. USENIX Association, Berkeley, CA, USA (2008)
4. Yeo, C.S., Buyya, R.: Service level agreement based allocation of cluster resources: handling penalty to enhance utility. In: 7th IEEE International Conference on Cluster Computing (Cluster 2005), September 2005
5. Bhagwat, D., Eshghi, K., Long et D.D., et al.: Extreme binning: Scalable, parallel deduplication for chunk-based file backup. In: Proceedings of IEEE International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS'09), pp. 1–9. IEEE Computer Society Press, London, UK, September 2009
6. Eastlake, D.: Us secure hash algorithm 1 (sha1). http://tools.ietf.org/html/rfc3174, September 2001
7. Meyer, D., Bolosky, W.: A study of practical deduplication. In: Proceedings of the USENIX Conference on File and Storage Technologies (FAST'11), pp. 229–241. USENIX Association, San Jose, CA, USA, February 2011
8. MacDonald, J.: File system support for delta compression. Masters thesis, Department of Electrical Engineering and Computer Science, University of California at Berkeley (2000)
9. Dave, J., Faruki, P., Laxmi, V., Bezawada, B., Gaur, M.: Secure and efficient proof of ownership for deduplicated cloud storage. In: Proceedings of the 10th International Conference on Security of Information and Networks (SIN'17). ACM, New York, NY, USA, 19–26 (2017)
10. Wang, Jibin, Zhao, Zhigang, Zhaogang, Xu, Zhang, Hu, Li, Liang, Guo, Ying: I-sieve: an inline high performance deduplication system used in cloud storage. Tsinghua Sci. Technol. **20**(1), 17–27 (2015)
11. Eshghi, K., Tang, H.K.: A framework for analysing and improving content-based chunking algorithms, Technical Report HPL-2005-30(RI) (2005)
12. Kumar, Sandeep, Gupta, Er Piyush: A comparative analysis of SHA and MD5 algorithm. Int. J. Comput. Sci. Inf. Technol. **5**, 4492–4495 (2014)
13. Lillibridge, M., Eshghi, K., Bhagwat, D., et al.: Sparse indexing: Large scale, inline deduplication using sampling and locality. In: Proceedings of the 7th USENIX Conference on File and Storage Technologies (FAST'09), vol. 9. USENIX Association, San Jose, CA, February 2009, pp. 111–123
14. NetApp deduplication and compression. www.netapp.com/us/products/platform-os/dedupe.html, April 2016
15. Opendedup. http://opendedup.org/
16. Rivest, R.: The md5 message-digest algorithm, April 1992. http://tools.ietf.org/html/rfc1321
17. Quinlan, S., Dorward, S.: Venti: a new approach to archival data storage. In: Proceedings of the 1st USENIX Conference on File and Storage Technologies (2002)

18. Suel, T., Memon, N.: Algorithms for delta compression and remote file synchronization. Lossless Compression Handbook (2002)
19. Venish, A., Siva Sankar, K.: Study of chunking algorithm in data deduplication. In: Proceedings of the International Conference on Soft Computing Systems. Springer, New Delhi (2016)
20. Wang, X., Yu, H.: How to break MD5 and other hash functions. In: EUROCRYPT (2005), vol. 3494, pp. 19–35. Lecture Notes in Computer Science. Springer
21. Zhang, Y., Wu, Y., Yang, G.: Droplet: a distributed solution of data deduplication. In: 2012 ACM/IEEE 13th International Conference on Grid Computing, Beijing, pp. 114–121 (2012)
22. Yan, Z., Ding, W.X., Zhu, H.Q.: A scheme to manage encrypted data storage with deduplication in cloud. In: Proceedings of ICA3PP2015, November 2015
23. Kaur, R., Chana, I., Bhattacharya, J.: Data deduplication techniques for efficient cloud storage management: a systematic review. J. Supercomputing **74**(5), 2035–2085 (2017)

Comparative Analysis of Heart Disease Classification Algorithms Using Big Data Analytical Tool

Sinkon Nayak(✉), Mahendra Kumar Gourisaria, Manjusha Pandey, and Siddharth Swarup Rautaray

KIIT Deemed University, Bhubaneswar, India
sinkonnayak07@gmail.com, mkgourisaria2010@gmail.com, {manjushafcs, siddharthfcs}@kiit.ac.in

Abstract. Immense volume of data has been generated from unlike sources like health care, social media, business applications, manufacturing industries and many more. HealthCare plays a pivotal role in Big Data. Spotting and safeguarding of the diseases at a primitive stage are very much crucial. Heart disease specifically implies the condition of the heart that contracts or obstructs blood vessels which result in heart attack, chest pain or stroke. This paper emphasizes on the diagnosis of heart diseases at a primitive stage so that it will lead to a successful cure of the diseases. In this paper, diverse data mining classification method like Decision tree classification, Naive Bayes classification, Support Vector Machine classification, and k-NN classification are used for identification and precaution of the diseases at an early stage so that it can be curable and preventable.

Keywords: Big data · Healthcare · Heart disease · Decision tree classification · Svm classification · Naive bayes classification · K-NN classification

1 Introduction

HealthCare is the maintenance and betterment of the health by the help of diagnosis, prevention, and treatment of any kind of diseases. But a major challenge faced is to provide better care and clinical services at an affordable cost. By the help of various predictive analysis, the cost will get diminish and can get better clinical care. Cardiovascular disease refers to the trouble occur with heart. It specifically implies the condition of the heart that contracts or obstructs blood vessels which result in heart attack, chest pain or stroke. So various data mining classification techniques such as Decision tree classifier, Naive Bayes classifier, Support Vector Machine classifier, and k-NN classifier are used to spot and prevent the diseases at an primitive stage.

This paper is organized into section as follows. Section 2 summarizes heart disease. Section 3 provide a brief description of literature survey of heart related disease. The work flow steps are discussed in Sect. 4. Section 5 is all about the concise discussion of the classification techniques such as Naive Bayes, Decision tree, SVM, k-NN. Dataset collection attributes elucidation, comparison study is discussed in Sect. 6.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 582–588, 2020.
https://doi.org/10.1007/978-3-030-37051-0_65

Section 7 is all of the result analysis. Section 8 is the conclusion, summarizes a brief overview of the content.

2 Heart Disease

Any abnormality in heart results to heart disease. Heart disease affects the structure and function of the heart. There are various types of abnormality observed in the heart such as narrowing arteries, heart attack, aberrant rhythms of the heart, crushing of heart, disease related to a heart valve and heart muscle etc. The abnormal function of the heart is because of various factors such as blood sugar level, cholesterol level, blood pressure, etc. From the various study, the death rate of Cardio Vascular Diseases is 272 people per 100 000 population in India and globally it is 235 per 100 000 population. 610,000 number of people deceased because of heart-related problems in the United States every year.

3 Literature Survey

Aditya Sundar et al. describes classification techniques for prediction and evaluates the performance of Naive Bayes classification technique and WAC (Weighted Association Classifier) by using different performance measure [1]. Sellappan Palaniappan et al. describe various data mining classification algorithm Naive Bayes, Decision tree and Neural network to predict heart disease [2]. Dangare et al. in their paper describe early anticipation of heart related illness by the help of Neural network, Decision tree and Naive Bayes and determine their accuracy [3]. J Thomas et al. in their paper describes the classification techniques k-NN classification, Naive Bayes Classification, Decision tree classifier and Neural network method to predict the danger level of a diligent to have a heart-related illness or not [4]. Swathy Wilson et al. in their paper conclude that decision tree with k means clustering yield improved accuracy as compared to others [5]. A Nishara Banu et al. did the study of Association Rule Mining, Classification, and Clustering for spotting heart-related disease. They showed that the designed spotting structure is able to spot the heart attack efficiently [6]. Shabana Asmi et al. add some attributes for spotting the heart-related unwellness which results in high accuracy by the help of association rules [7]. Beant Kaur et al. used various Genetic and data mining algorithm for the spotting of heart-related illness. Their result shows that Genetic Algorithm gives an accuracy of 73.46% [8]. Sashikant Ghumbre et al. in their study used SVM classifier and Radial basis function network for heart disease diagnosis and got the result that SVM is best for identification [9].

4 Work Flow Design

Figure 1 describes the workflow and methodology for the prediction of heart disease. We have taken the dataset from UCI/Kaggle in CSV format then preprocess the data has been done which includes data transformation, data cleaning, and data integration.

After preprocessing data mining classification algorithms such as Decision Tree, SVM, Naive Bayes, k-NN are applied for the prediction and comparison of the classification techniques based on their performance.

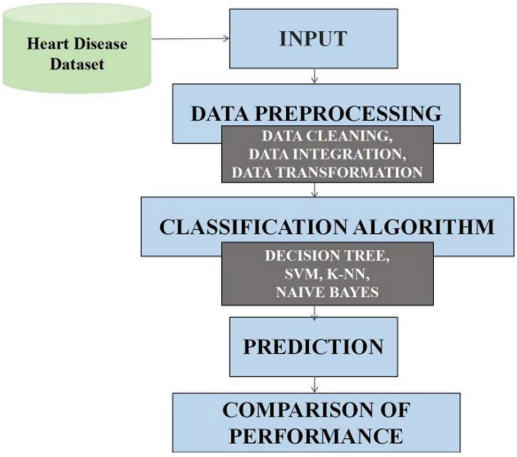


Fig. 1. Work flow for prediction of heart disease

5 Classification Algorithm

Classification belongs to a supervised learning method, which predicts a class for each object and assigns them to a target class [12]. The main goal is to prognosticate the target class for each data in a data set accurately.

5.1 Decision Tree

A decision tree is basically a tree-like structure in which branch nodes denotes attribute, terminal nodes denote class labels and branches denotes the outcome. Testing criteria are applied on the source node and branch nodes and on the basis of testing criteria result the data will follow the branch till it reaches the leaf node or class label (Table 1).

Table 1. Pros and cons of decision tree classification techniques

Pros	Cons
Fast, simple to understand and interpret	Computationally expensive to train
Robust and need less computation for classification	Overfitting and prediction of continuous variable is not suitable

5.2 Naive Bayes Classifier

Bayesian classification is based on Bayes theorem. Thus it is a classifier based on probabilities it fails in case of continuous attribute because of frequency count is not possible (Table 2).

Table 2. Pros and cons of Naive Bayes classification techniques

Pros	Cons
Simple and Easy to implement and robust	Class conditional independence thus less accuracy
Fast to train and classify as it need a single scan and space efficient also	Dependencies among attributes can not be taken into consideration

5.3 Svm

A Support Vector Machine (SVM) is based on decision planes on decision margins. A decision plane can be defined as which split up between a bunch of objects, belongs to, unlike class. SVM is used mutually for classification as well as regression analysis [9, 10] (Table 3).

Table 3. Pros and cons of SVM classification techniques

Pros	Cons
Training of dataset is easy	Need good kernel function
Scale well for high dimensional data	Sensitive to noisy data

5.4 K-NN

k-NN classifier is the most instance-based method for classifying data. In k-NN the target function may be either discrete valued or real value. k-NN stores all available records and classifies them on the basis of similarity measures (Table 4).

Table 4. Pros and cons of k-NN classification techniques

Pros	Cons
Can be applied to data of any distribution and modelling is not expensive	Computationally expensive because it need huge number of sample for accuracy calculation
Very simple and intuitive	Depends on K value and affected by irrelevant attributes
For large sample size it work good	Affected by irrelevant attributes

6 Data Set Elucidation

Heart disease dataset is collected from kaggle/UCI machine learning repository in which there are 14 attributes and 303 patients record [11] (Fig. 2).

Attribute Number	Attribute Name	Attribute Elucidation
1.	Age	Age of the patients
2.	Sex	Sex of the patients
3.	Cp	Chest pain type
4.	Resting blood pressure	Resting blood pressure level of the patients
5.	Cholesterol	Cholesterol of patients
6.	Fasting blood sugar	Blood sugar level of patients in fasting
7.	Resting ECG	ECG result
8.	Thalach	Maximum heart rate of the patients
9.	Induced Angina	If the patients experience angina as a result of exercise
10.	Old peak	ST depression induced by exercise relative to rest
11.	Slope	Slope of the peak exercise ST segment
12.	CA	Number of major vessels colour by Flouroscopy
13.	Thal	Normal, fixed or reversible defect
14.	Target	Status of the disease

Fig. 2. Detail description of dataset [11]

7 Comparison Table of Different Classification Techniques

Table 5 gives the comparison of data mining classification algorithms based on various performance measure.

Table 5. Comparison of different classifier with respect to Accuracy, Sensitivity, Specificity, PPV, NPV and AUC

Classifier	Accuracy (%)	Sensitivity (%)	Specificity (%)	PPV (%)	NPV (%)	AUC
Decision tree	84.91	36.95	61.81	44.73	53.96	0.8275
SVM	88.68	39.86	58.20	44.36	53.64	0.8848
Naive Bayes	96.23	39.13	57.57	43.54	53.07	0.9899
k-NN (Roc)	58.49	50	48.49	44.80	54.7	0.6283
k-NN (Acc)	62.26	50	49.09	45.09	54	0.6217

Confusion Matrix is exploited to compute Accuracy, Sensitivity, Specificity, Area under curve and ROC curve. Confusion Matrix for classification of heart disease is shown in Table 6.

Table 6. Confusion matrix for heart disease

Class label	Classified as present of heart disease	Classified as heart disease not present
Heart disease present	TP	FN
Heart disease not present	FP	TN

$$\text{Sensitivity} = \text{P}(+|1) = \% \text{ of True Positive} : \text{TP}/(\text{TP}+\text{FN})$$
$$\text{Specificity} = \text{P}(-|0) = \% \text{ of True Negative} : \text{TN}/(\text{TN}+\text{FP})$$
$$\text{Accuracy} = (\text{TP}+\text{TN})/(\text{TP}+\text{TN}+\text{FP}+\text{FN})$$
$$\text{PPV (Positively Predicted Value} = \text{TP}/(\text{TP}+\text{FP})$$
$$\text{NPV (Negatively Predicted Value)} = \text{TN}/(\text{TN}+\text{FN})$$

Figure 3 represents the Roc curve of different classifier.

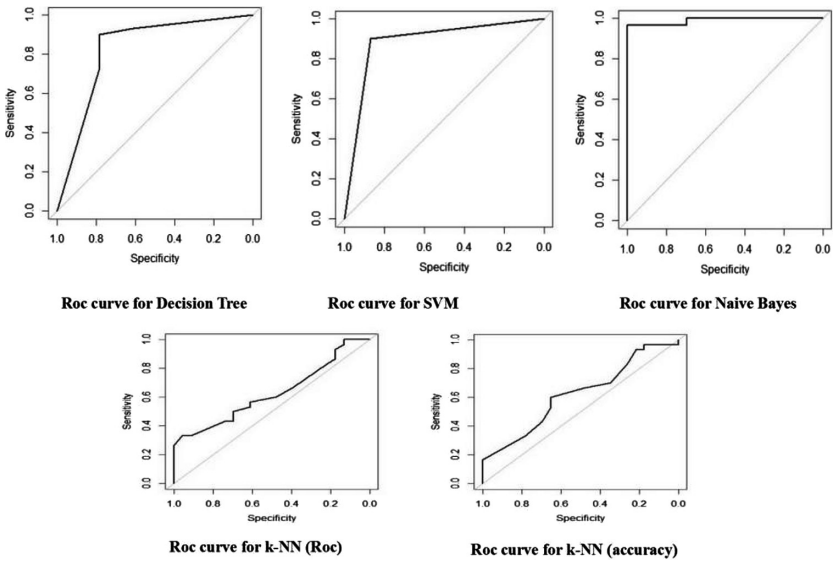


Fig. 3. ROC curve of different classifier

8 Conclusion

This paper focuses on the early detection and prevention of heart related illness by using several data mining classification method which is implemented by using data analytical tool R. For the prediction of heart disease various classifiers are used and we obtained several performance measurement parameters and observed that the performance is better for prediction in case of Naive Bayes as compared to others. Here we

also observed that the performance of classifier varies from each other and also depended upon the platform or analytical tool on which the classification techniques are implemented. In future we would try to implement other techniques in which prediction is more accurate.

References

1. Sundar, N.A., Latha, P.P., Chandra, M.R.: Performance analysis of classification data mining techniques over heart disease database. Int. J. Eng. Sci. Adv. Technol. **2**(3), 470–478 (2012)
2. Palaniappan, S., Awang, R.: Intelligent heart disease prediction system using data mining techniques. In: 2008 IEEE/ACS İnternational Conference on Computer Systems and Applications. IEEE (2008)
3. Dangare, Chaitrali S., Apte, Sulabha S.: Improved study of heart disease prediction system using data mining classification techniques. Int. J. Comput. Appl. **47**(10), 44–48 (2012)
4. Thomas, J., Theresa Princy, R.: Human heart disease prediction system using data mining techniques. In: 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE (2016)
5. Wilson, A., et al.: Data mining techniques for heart disease prediction (2014)
6. Banu, M.N., Gomathy, B.: Disease forecasting system using data mining methods. In: 2014 International Conference on İntelligent Computing Applications. IEEE (2014)
7. Waghulde, Nilakshi P., Patil, Nilima P.: Genetic neural approach for heart disease prediction. Int. J. Adv. Comput. Res. **4**(3), 778 (2014)
8. Kaur, Beant, Singh, Williamjeet: Analysis of heart attack prediction system using genetic algorithm. Int. J. Adv. Technol. Eng. Sci. **3**, 87–94 (2015)
9. Ghumbre, S., Patil, C., Ghatol, A.: Heart disease diagnosis using support vector machine. In: International Conference on Computer Science and İnformation Technology (ICCSIT') Pattaya (2011)
10. Bhatia, S., Prakash, P., Pillai, G.N.: SVM based decision support system for heart disease classification with ınteger-coded genetic algorithm to select critical features. In: Proceedings of the World Congress on Engineering and Computer Science, pp. 34–38, San Francisco, USA (2008)
11. Database. http://archive.ics.uci.edu/ml/datasets/Heart+Disease
12. Han, J., Kamber, M.: *Data Mining Concepts and Techniques*. Morgan Kaufmann Publishers (2006)

PT-GA-IRIAL: Enhanced Energy Efficient Approach to Select Migration VMs for Load Balancing in Cloud Computing Environment

V. Radhamani[1(✉)] and G. Dalin[2]

[1] Department of Computer Science, Coimbatore Institute of Technology, Coimbatore, Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India
radhamanishri@gmail.com

[2] Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India

Abstract. Cloud computing is a very well known technology for all business people, software developers, end-users, and so on. Significant researches are going on to balance the cloud load. The migration of heavily loaded Virtual Machines (VMs) into lightly loaded Physical Machines (PMs) balances the Cloud load. In Resource Intensity Aware Load Balancing (RIAL) method, based on the weight of resources under utilization, it selected the VMs from heavily loaded PMs for migration and chosen the lightly loaded PMs as destination. An Improved RIAL was proposed to consider both lightly and heavily loaded PMs as destination. Later it was enhanced in the proposed Power Consumption Aware- Traffic Aware- IRIAL (PT-IRIAL) method with the consideration of power consumption, temperature and traffic measures to select the VMs for migration and select PMs for destination. From all these, in this current paper, the crossover and mutation process of GA is utilized to optimally select the migration VMs and choose the destination PMs. Thus this GA based load optimization algorithm optimally maps the migration VMs with the destination PMs efficiently.

Keywords: Cloud computing · Load balancing · Genetic algorithm

1 Introduction

In today's world, most of the enterprises utilize the services provided by the Cloud in order to get increased performance and reduced cost. Traditional statistical analysis methods are not perfect to balance the load on servers. In most of the businesses, in order to provide faster services to their customers, they approach cloud to run their system. It increases the cloud load drastically which leads to tremendous issues in Cloud system maintenance like problems in scheduling the task, over loading of Physical Machines (PMs), increased and dynamic requirements of the customers, increased energy consumption and generation of overheat in its resource pool, etc., Migration of VMs from heavily loaded physical machines (PMs) to lightly loaded PMs was done in conventional load balancing techniques. Various algorithms like

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 589–596, 2020.
https://doi.org/10.1007/978-3-030-37051-0_66

brokering, bin packing, TOPSIS, collaborative agent, etc. were applied for scheduling and load balancing. The combination of various heuristic algorithms balances the load, and reduces the makespan time [3].

The selection of VMs for migration and the selection PMs for destination were based on the usage intensity level of resources, a Resource Intensity Aware Load balancing (RIAL) method was proposed [8]. According to the survey report, Resource Intensity Aware Load-balancing RIAL (IRIAL) was performed well in balancing the cloud load [2].

2 Literature Survey

The Improved RIAL (IRIAL) method was proposed to consider the distance between the PM of VMs chosen for migration and the PMs selected as destination. This enhanced method reduced the total number of migrations without any degradation in its performance [2]. Different attributes of Cloud data center like power consumption, temperature generation and traffic were considered in Power Consumption Aware-Traffic Aware-IRIAL (PCA-TA-IRIAL) method [5]. This method selects the migration VMs and destination PMs efficiently rather than the previous methods. In this paper, PCA-TA-IRIAL will be referred as PT-IRIAL.

Many evolutionary algorithms were evolved to find the optimal solution in both population and non-population based problems [4]. K-means clustering approach was proposed to cluster the VMs in order to reduce their execution time. It was the combination of three evolutionary algorithms named Genetic Algorithm (GA), Simulation Annealing (SA), and Particle Swarm Optimization (PSO) in load balancing to keep the makespan of the system as well as to increase the performance. The stochastic hill climbing evolution algorithm, the local optimization approach which was used in the allocation of incoming jobs into the VMs [12]. Dynamic assignment of tasks to the available hosts was proposed in State-Based Load Balancing (SBLB) algorithm [10]. Based on the threshold value, VMs load were analyzed before allocating new loads to them. It prevented the host from reaching the heavily loaded state.

To minimize the energy utilization of cloud servers, its load balancing issue should also be considered as one of the important factor. The load and temperature of hosts to map VMs with PMs for migration were also considered in Load and thermal-aware VM scheduling mechanism [11]. For load balancing in Cloud environment, an energy-aware hybrid fruit fly optimization was proposed [7]. The fruit fly did its search on two stages such as smell and vision-based search which were used to find the appropriate VMs for allocation. The proposed Improved GA (IGA) kept track of all free VMs which could be given preference for VM allocation [9]. GA was proposed to schedule VMs to physical machines by using fitness function [6] to reduce the number of VM migrations. The GA was found as the best suitable algorithm for such type of load balancing. To get optimal result, Genetic Algorithm (GA) based PT-IRIAL is proposed in this paper.

3 Proposed Methodology

Consolidation of VMs saves power by reducing the number of PMs under utilization [6]. To select optimal VMs and migrate them to the chosen optimal destination PMs, with the consideration of Euclidean distance, traffic flow, power consumption and temperature measurements, Genetic Algorithm (GA) based Power Consumption Aware-Traffic Aware-Improved Resource Intensity Aware Load balancing (PT-GA-IRIAL) method is proposed in this paper.

3.1 GA Based Selection of Overloaded VMs and Destination PMs for Migration

Genetic Algorithm (GA) provides potential solution to the population based problems [14]. Based on its simple data structure called chromosome, it uses recombination operators to preserve the critical information. The important processes involved in GA are initializing the population, calculating the fitness function, selection process, crossover process and mutation process. The population is initialized with total number of PMs in the data center, number of VMs created, and the total number of tasks to be scheduled. These individuals are called chromosomes which are used to search for the best solution. The calculated fitness values of individuals are used to reproduce and survival of next generation with improved fitness value. According to Darwin's Law, the migrating VM selection procedure is taken place. Crossover and mutation are applied on the chosen pair of parents [6].

The existing work PT-IRIAL selected the VMs which were needed to migrate from one PM to another PM. The selection of VMs were done based on MCDM method. The selection of destination PMs were done based on different measures such as expected completion time, resource intensity, VM communication rate, performance degradation, thermal power, energy consumption and bandwidth of both heavily or lightly loaded PMs. By considering these measures of heavily and lightly loaded PMs, migration process was taken place. This research work is extended by incorporating the GA policies to improve its performance.

The cost matrix of each candidate VM_{xy} in P_x is constructed for the selection of migration VMs as,

$$\text{Cost}_{xy} = \text{Min}\left(l_{xy}, \text{Pow}_{xy}, \text{Temp}_{xy}, \text{STR}_{xy}\right) \tag{1}$$

The cost matrix of each candidate PM_p from the ideal PM is constructed for the selection of destination PMs as,

$$\text{Cost}_{p,xy} = \text{Min}\left(l_{p,xy}, \text{Pow}_{p,xy}, \text{Temp}_{p,xy}, \text{STR}_{p,xy}\right) \tag{2}$$

The parent chromosomes are chosen based on low mining cost. From the selected parents, crossover process is carried out to create the new population. The mutation process allows the specific child to obtain the features which are not possessed by its

parents. Decision on choosing VMs and PMs is taken place based on the replacement process. It is repeated till to reach the maximum number of generations. Finally the selected VMs for migration are shifted to the chosen destination PMs.

Genetic algorithm based selection of Overloaded VMs for migration and choose PMs for destination

Input: n chromosomes in the population, VMs, and PMs.

Output: Optimal selection of VMs for migration and optimal selection of PMs for destination.

1. Each chromosome selects the VMs for migration and PMs for destination randomly.
2. In the population, calculate the fitness value of each chromosome by using the formulas (1) and (2).
3. According to the fitness values, select some parent chromosomes.
4. Create new population by performing the crossover and mutation processes.
5. The old population of chromosomes is replaced with new population.
6. Repeat the loop from step 2 to 5 till the maximum number of generation is reached.
7. Return the best VMs for migration and PMs for destination.
8. Finally, migrate the selected VMs to the chosen destination PMs.

4 Results and Discussion

The performance of Power Communication Aware-Traffic aware-Improved Resource Intensity Aware Load Balancing (PT-IRIAL), and Genetic Algorithm based PT-IRIAL (PT-GA-IRIAL), are evaluated based on the communication cost, total number of migrations, and performance. A CloudSim simulator is used to carry out the experiment [13].

In this resource intensity aware research work for load balancing in Cloud environment, it considers the resource utilization of each PM in Cloud data center.

4.1 Communication Cost Reduction

Communication cost is calculated based on the total number of communications between the migrating VM and destination VM in unit time period. The following Table 1 shows the communication cost reduction of PT-IRIAL, and PT-GA-IRIAL comparison values for different timings.

Table 1. Comparison of communication cost reduction

Time (hrs)	PT-IRIAL	PT-GA-IRIAL
8	180	200
16	210	250
24	240	276

The Fig. 1 diagrammatically represents the comparison of communication cost reduction between PT-IRIAL, and PT-GA-IRIAL methods on enumerated time span. 15% of communication cost is reduced by PT-GA-IRIAL rather than the PT-IRIAL method for 24 h. It keeps the frequently communicating VMs in the same PM in order to reduce bandwidth cost and follows the migration triggering algorithm for avoiding unnecessary migrations (as each migration leads to service downtime and also requires additional network bandwidth to settle down the VM in the chosen destination PM). The testing result shows that PT-GA-IRIAL method leads to considerable improvement in the reduction of communication cost.

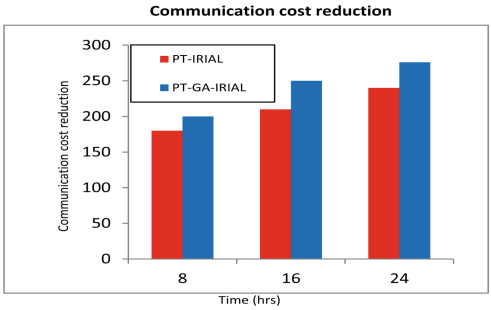


Fig. 1. Comparison of communication cost reduction

4.2 Total Number of Migrations

The comparison result of reduction in total number of migrations of PT-IRIAL and PT-GA-IRIAL is shown in Table 2.

Table 2. Comparison of reduced number of migrations

No. of VMs	PT-IRIAL	PT-GA-IRIAL
2500	0.67	0.51
3000	1.7	1.52
5000	2.1	1.9

The depicted comparison chart shown in Fig. 2 implies that there is a considerable improvement in PT-IRIAL method when applied with GA. The total number of migration using PT-GA-IRIAL is 9.52% less than PT-IRIAL among 5000 VMs.

4.3 Reduction in Performance Degradation

VMs migration plays significant role in the degradation of Cloud performance. The following Table 3 depicts the reduction in performance degradation of PT-IRIAL, and PT-GA-IRIAL methods for the different number of VMs.

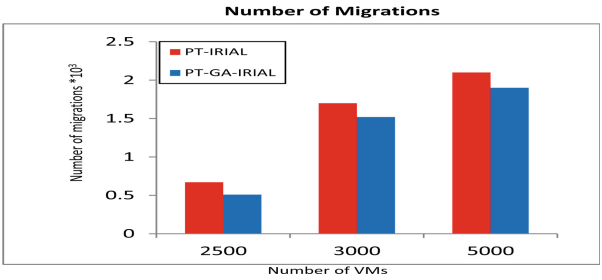


Fig. 2. Comparison of reduced number of migrations

Table 3. Comparison of reduction in performance degradation

No. of VMs	PT-IRIAL	PT-GA-IRIAL
2500	0.06	0.052
3000	0.68	0.61
5000	2.7	2.64

The reduction in performance degradation of PT-GA-IRIAL, and PT-GA-IRIAL methods are comparatively depicted in the Fig. 3 based on the number of VMs. There is 2.2% lesser performance degradation in The PT-GA-RIAL produces 2.2% of better result for 5000 number of VMs than that of PT-RIAL method.

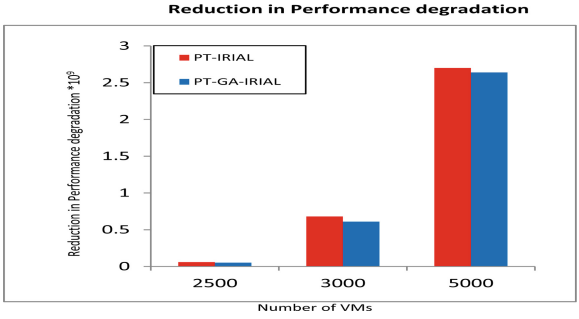


Fig. 3. Comparison of reduction in performance degradation

4.4 Overall Comparison

Based on the comparisons done for reduction in communication cost, number of migrations, and performance degradation of PT-IRIAL and PT-GA-IRIAL load balancing methods, the overall best performance results are depicted in the Table 4.

Table 4. A overall comparison table

Particulars of analysis	Unit of Measurement	Input Count	RIAL	PT-IRIAL	PT-GA-IRIAL	% of Improvement in PT-GA-IRIAL
Reduction in communication cost	Time (in Hrs)	24	175	240	276	15
Reduction in number of migrations	Number of VMs	5000	3	2.1	1.9	9.52
Reduction in performance degradation	Number of VMs	5000	5	2.7	2.64	2.22

The considerable improvement is found in PT-IRIAL load balancing method when applying Genetic Algorithm for selection of migration VMs and destination PMs. Based on the overall report, PT-GA-IRIAL reveals 10–15% of improvement from its previous load balancers.

5 Conclusion

In this proposed Genetic Algorithm (GA) based PT-IRIAL (PT-GA-IRIAL) load balancing method, crossover and mutation techniques are utilized to generate the new population. It uses replacement logic to choose the migration VMs in a strict way. Based on the simulator results, PT-GA-IRIAL provides significant improvement in Cloud load balancing task by reducing the total number of migrations, communication cost and performance degradation.

Universe is blessed with full of natural resources which are embedded with unique knowledge. Day-by-day, the researchers are inspired with the intelligence of specific resource in this world. It reveals us new swarm intelligent algorithms which can be applied in various fields of research to get fruitful improvements. In this work, PT-IRIAL is simply enhanced with the support of GA. Further, PT-GA-IRIAL may be compared with other meta-heuristic algorithms which may lead to better solutions.

References

1. Dalin, G., Radhamani, V.: Load balancing techniques in cloud: a review. JETIR Int. J. **5**(8) (2018). (ISSN:2349-5162), Unique Identifier: JEYIR1808252, EISSN:2349-5162
2. Dalin, G., Radhamani, V.: IRIAL-an improved approach for VM migrations in cloud computing. Int. J. Adv. Technol. Eng. Explor. **5**(44), 165–171 (2018)
3. Sajjan, R.S., Biradar, R.Y.: Load balancing using cluster and heuristic algorithms in cloud domain. Indian J. Sci. Technol. **11**(15) (2018). https://doi.org/10.17485/ijst/2018/v11i15/118729, ISSN (Print):0974-6846, ISSN (Online):0974-5645

4. Sajjan, R.S., Biradar, R.Y.: Task based approach towards load balancing in cloud environment. Int. J. Comput. Appl. **179**(31), 39–43 (2018). (0975–8887)
5. Radhamani, V., Dalin, G.: PCA-TA-IRIAL: Power Consumption Aware-Traffic Aware-IRIAL a novel unified approach for green and load balanced computing in cloud. In: IEEE Sponsored 3rd International Conference on Engineering and Technology (ICETECH'18), 30 & 31, August 2018
6. Sharma, H., Sekhon, G.S.: Load balancing in cloud using enhanced genetic algorithm. Int. J. Innov. Adv. Comput. Sci. IJIACS **6**(1) (2017). ISSN 2347-8616
7. Lawanyashri, M., Balusamy, B., Subha, S.: Energy-aware hybrid fruitfly optimization for load balancing in cloud environments for EHR applications. Inf. Med. Unlocked **8**, 42–50 (2017)
8. Shen, H.: RIAL: resource intensity aware load balancing in clouds. IEEE Trans. Cloud Comput. (2017)
9. Kaur, S., Sengupta, J.: Load balancing using improved genetic algorithm (IGA) in cloud computing. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **6**(8) (2017). ISSN:2278-1323
10. Naha, R.K., Othman, M.: Cost-aware service brokering and performance sentient load balancing algorithms in the cloud. J. Netw. Comput. Appl. **75**, 47–57 (2016)
11. Mhedheb, Y., Jrad, F., Tao, J., Zhao, J., Kołodziej, J., Streit, A.: Load and thermal-aware VM scheduling on the cloud. In: International Conference on Algorithms and Architectures for Parallel Processing, pp. 101–114. Springer, Cham (2013)
12. Mondal, B., Dasgupta, K., Dutta, P.: Load balancing in cloud computing using stochastic hill climbing-a soft computing approach. Proc. Technol. **4**, 783–789 (2012)
13. Calheiros, R.N., Ranjan, R., Beloglazov, A., De Rose, C.A., Buyya, R.: CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Softw. Pract. Exper. **41**(1), 23–50 (2011)
14. Ritwik, K., Deb, S.: A genetic algorithm-based approach for optimization of scheduling in job shop environment. J. Adv. Manuf. Syst. **10**(02), 223–240 (2011)

An Area Effective and High Speed SAR ADC Architecture for Wireless Communication

G. Prathiba[1(✉)] and M. Santhi[2]

[1] Department of ECE, University College of Engineering, Ariyalur, Tamil Nadu, India
gprathibasubash@gmail.com
[2] Department of ECE, Saranathan College of Engineering, Trichy, Tamil Nadu, India
santhiphd@gmail.com

Abstract. An area effective, high speed and low power 8-bit Successive Approximation Register Analog to Digital converter (SAR-ADC) using 250 nm CMOS technology introduced in this paper. Among different types of ADC successive approximation is used as it is high speed architecture, suitable packed design and has good speed to power ratio. To minimize the power a Switched Inverter Quantization (SIQ) comparator and to reduce the leakage power the Multi Phase Clocking (MPC) based D-FF shift register for SAR logic are preferred for this work. The whole circuit design is bringing out with the help of Tanner EDA Tool.

Keywords: Area effective · Low power · High speed · Speed to power ratio · Tanner tool

Abbreivations

SAR	Successive Approximation Register
ADC	Analog to Digital Converter
SIQ	Switched Inverter Quantization
MPC	Multi Phase Clocking
DAC	Digital to Analog Converter

1 Introduction

In the modern fields of wireless communication, image processing and video systems, the demand on fast and less power analog to digital converters increases as the emerging of many portable applications [1]. With the design of CMOS technology, SAR-ADC is used extensively to obtain fast and accurate performance with least power consumption. Now a day's mixed signal designing data converters are important building block [2]. ADC acts as a important link between analog and digital domain. As Digital circuits has a major advantage such as accuracy, low cost, resolution, less sensitivity, excellent in signal processing, power and good simulation results over

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 597–605, 2020.
https://doi.org/10.1007/978-3-030-37051-0_67

analog circuits. To improve the performance and area of latest electronic system a new analog to digital converter (ADC) is required [3]. Orderly to get success in high resolution and accuracy, cost efficient data converters where needed, so it was a challenge for researchers to improve and increase quality of ADC as it is employed in most of important application [4]. So SAR-ADC is mostly preferred due to the advantages compared to other ADCs. All the blocks of SAR-ADC are in digital domain except Comparator and DAC. Both Comparator and DAC need analog design and it create the structure more complicated also require external supervision [5, 6]. Hence the digital design of comparator need to avoid the above constrains. The proposed 8-bit SAR-ADC architecture has digital SIQ comparator and MPC based SAR is displayed in Fig. 1. The SAR-ADC provides a digital code equivalent to input signal using Binary search algorithm.

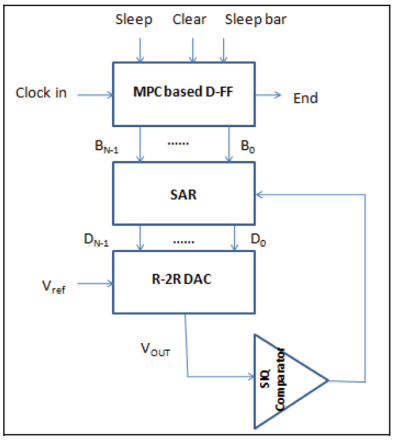


Fig. 1. Proposed SAR-ADC Architecture

Basically SAR-ADC contains three main components a comparator, a DAC and SAR block. This type of ADC is broadly used in automatic control application in factories and battery powered applications because it has good balancing between speed and Energy consumption [7]. When compared to other types this scheme offers high conversion rate. This is highly desirable feature in channel data acquisition systems [8]. In our report we make use of SIQ comparator, SAR logic with MPC based D-FF shift register and R-2R DAC. Hence this design consumes less power and area effective.

The main contributions of the paper are legion

- To minimizing the Energy consumption.
- To increase the speed of SAR-ADC by minimizing the propagation delay.
- To obtain the maximum conversion rate.
- To reduce the circuit complication by reducing the CMOS transistor count.
- To attain high reliability in SAR-ADC and also corrects the bits upto 8.

The proposed architecture of SAR-ADC having sub-blocks and are simulated using CMOS technology which consume less power and provide fast conversion time. The proposed methodology of SAR-ADC is explained in Sect. 2 and simulation results shown in Sect. 3.

2 Proposed Methadology

2.1 SIQ Comparator

Switched Inverter Quantization (SIQ) comparator technique use two inverters in cascading connection shown in Fig. 2. Reference voltage is determined by using the transistor sizes of the inverters. The Comparator's role is to compare the input voltage (V_{in}) from DAC with internal reference voltage (V_{ref}) of CMOS transistor. If V_{in} is greater than V_{ref}, the comparator produces an output which is '1', otherwise '0'.

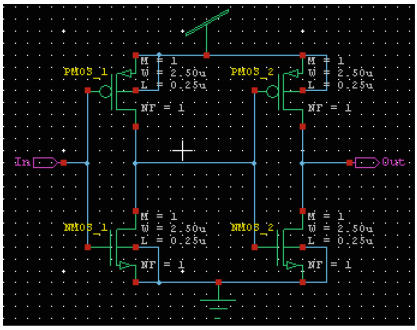


Fig. 2. Schematic of SIQ comparator

The voltage gain of the comparator is improved by the second stage of SIQ comparator and also prevents an unbalanced propagation delay [9]. V_m is referred as the inverter threshold voltage. The value of V_m is shifted depending upon the transistor width ratio. Increasing PMOS width makes V_m is highest value and increasing NMOS width makes V_m smaller value. To use CMOS inverter as voltage comparator should

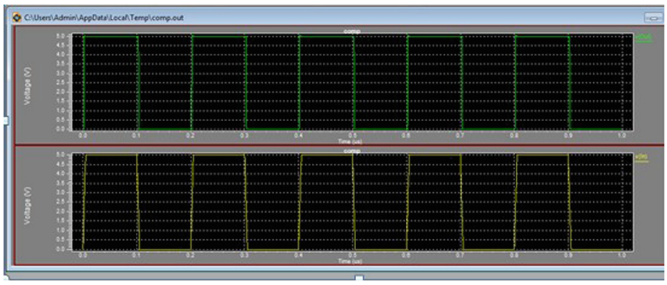


Fig. 3. Simulation result of SIQ comparator

check sensitivity of V_m to other ignored parameters such as electron and hole mobility, V_{th} of both transistors and supply voltage which does not maintain constant value [10]. This ensures perfect operation of SIQ comparator. Use of SIQ comparator in SAR-ADC does not require implementation of sample and hold circuit which further reduces power of the device.

2.2 Multi-phase Clocking (MPC) Technique

The Multi Phase Clocking (MPC) Technique is shown in Fig. 4. It is very dominant low power technique which decreases the leakage power effectively. This technique works with two modes of operations are high threshold mode and low threshold mode. Leakage power reduced in high threshold and the speed improved in low threshold mode. MPC gives better performance and consumes less power by using nap transistors in sleep mode. These nap transistors are enabled through sleep enable signals [11]. In High threshold condition transistors are used as nap transistors to reduce power consumption towards low (sleep) and in low threshold condition the nap transistors are used to increase the performance by reduce the leakage power (sleep bar).

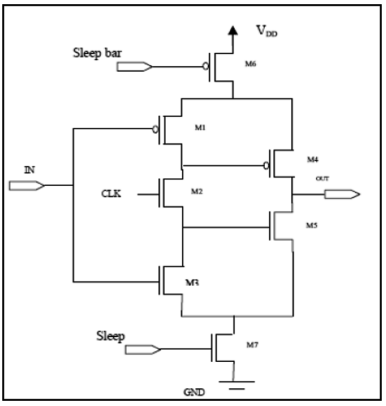


Fig. 4. MPC based D-FF

2.3 R-2R Ladder DAC

DAC principle operation is designed by various methods depends on the power requirement. Binary weighted resistor type and R-2R ladder type is simple and most desired method for DAC construction. If number of bits increases in binary weighted resistor type the required resistance also increases because of power loss and overload [12]. But this problem can be overcome by R-2R ladder type. The digital output obtained from SAR block is converted into analog signal by using R-2R DAC. The 8-bit R-2R ladder DAC structure using op-amp is shown in Fig. 5. Use of op-amp in the DAC structure produces an output voltage which is multiple times larger than the voltage difference between input terminals. The output is taken from the terminal point v2.

The stability of a DAC improved by using R-2R ladder structure compared to conventional designs.

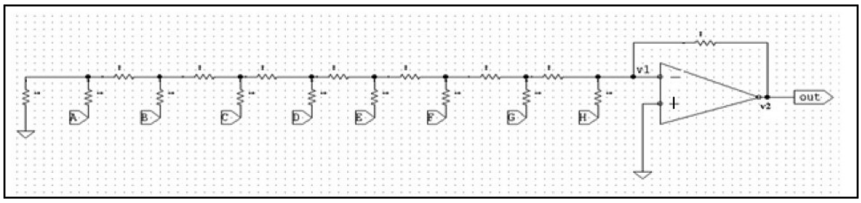


Fig. 5. R-2R resistor ladder DAC

Table 1. Transistor requirement and power consumption comparison for different comparator techniques.

Comparators techniques	Transistor required	Consumed power (μW)
Open loop comparator	8	23.70059
Improved QDC	7	15.94352
CMOS LTE comparator	6	3.328997
Proposed SIQ comparator	4	1.044111

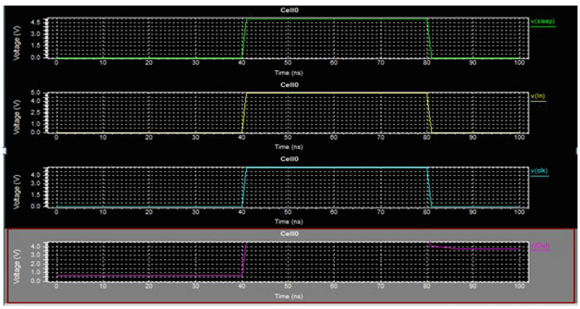


Fig. 6. Simulation result of MPC based D-FF

2.4 Successive Approximation Register

The SAR consists of shift register and a control unit. One of the sequential logic circuit is shift register used to store digital data designed using a group of flip-flops connected in a chain. So that output from one flip-flop becomes the input of next flip-flop [13]. In this SAR logic, Shift register is designed by using MPC based D-FF. True Single Phase Clocking (TSPC) D-FF turns into a Multi Phase Clocking (MPC) based D-FF, when 1 PMOS transistor and 1NMOS transistor are connected to the circuit of TSPC D-FF. In SAR logic the reciprocal output of shift register is given to one of the input to the NAND gate and the reciprocal output of the code register is given as other input to

NAND gate. The output of the NAND gate provides the output of SAR. The schematic of SAR-ADC shown in Fig. 7.

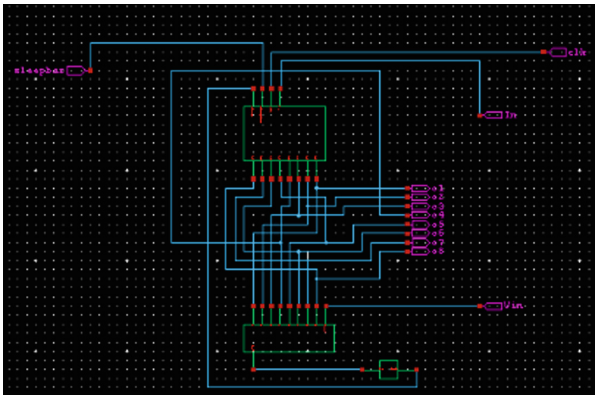


Fig. 7. Schematic of SAR–ADC

3 Results and Discussion

3.1 Simulatıon Result of SIQ Comparator

The graphical simulation output of SIQ comparator is dipicted in Fig. 3 and the different comparator structures are discussed in terms of number of transistors count and power consumption are displayed in Table 1. The power consumption of SIQ comparator is reduced to 69% and by minimizing the number of transistors to 33% when compared to the CMOS LTE comparator. The consumed power of SIQ comparator is reduced to 96%, 93%, 69% when compared to open loop comparator, modified QDC and CMOS LTE comparator is shown in Fig. 8.

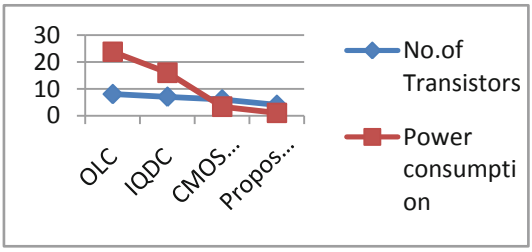


Fig. 8. Performance analysis of comparator

3.2 Simulation Result of MPC Based D-FF

Simulation result of Multi Phase Clocking (MPC) based D-FF is shown in Fig. 6. MPC based D-FF consumes 0.4 μW powers and process delay is 2.2 s.

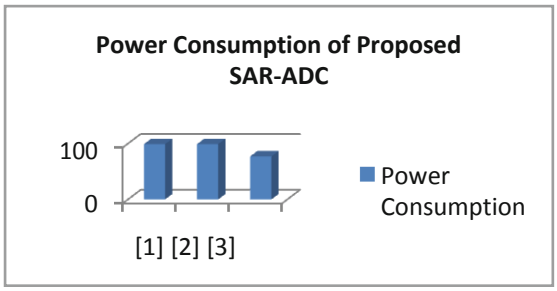


Fig. 9. Power consumption of various SAR-ADC

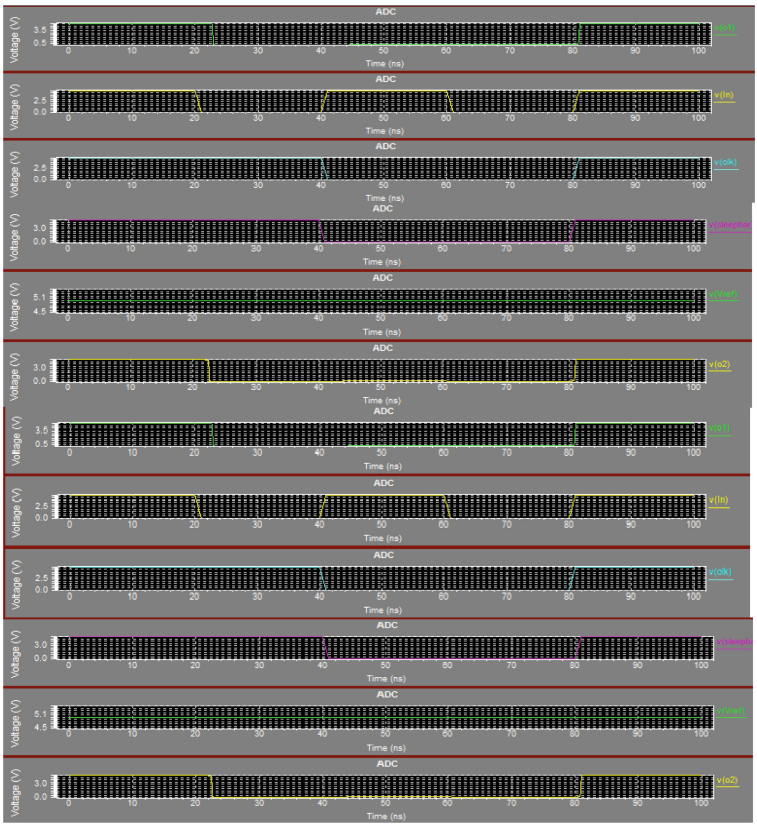


Fig. 10. Simulation result of SAR ADC

3.3 Simulation Result of SAR ADC

The supply voltage given to SIQ, DAC and PMC based D-FF SAR-ADC is 1 V and has 8-bit resolution. Proposed SAR-ADC reduces the power consumption by 99%, 99% and

77% compared to [1], [2] [3] is shown in Fig. 9. Also the proposed SAR-ADC consumes 0.0001mW power and the design is implemented by using 250 nm CMOS technology shown in Table 2. Simulation result of SAR-ADC is shown in Fig. 10.

Table 2. Comparison performance Of SAR-ADC

Specification	[1]	[2]	[3]	This work
Supply voltage (volts)	1.2	1.2	0.5	1
Resolution (bits)	12	8	12	8
Power consumption (mW)	1.32	1.2	0.00081	0.00019
Technology (nm)	130	55	90	250

4 Conclusion

An 8-bit SAR-ADC is implemented using Switched Inverter Quantization (SIQ) comparator which consumes minimum energy and offers high operating speed as compared to various types of comparator. Also an R-2R ladder DAC and MPC base D-FF shift register in SAR logic makes the design simpler which consume low power. SAR-ADC is more suitable for wireless communication applications due to the reduced power consumption and propagation delay. SAR-ADC of 8-bit is designed in this work, which can also be extended up to 16- bits.

Acknowledgments. Not applicable.

Author's Contribution. G. Prathiba and M. Santhi are developed the main idea, designed a new architecture SAR-ADC using SIQ comparator and MPC based D-FF shift register. G. Prathiba construct and simulate the SIQ comparator, MPC based D-FF and SAR-ADC. M. Santhi reviewing the schematic, simulation output and Finalizing the manuscript. Authors are stuided and approved the completed manuscript.

Funding. This work does not have any funding.
Availability of Data and Materials. Data sharing not applicable and no datasets were generated are analyzed.

References

1. Chung Y.H., Yen, C.W., Tsai, P.K., Chen. B.W.: A 12-bit 40-MS/s SAR ADC witha fast-binary-window DAC switching scheme. IEEE Trans. Very Large Scale Integr. Syst. (VLSI) **26**(10), 1989–1998 (2018)
2. Xu, D., Qiu, L., Zhang, Z., Liu, T., Liu L., Chen, K., Xu, S.: A Linearity-Improved 8-bit 320-MS/s SAR ADC with metastability immunity technique. IEEE Trans. Very Large Scale Integr. Syst. (VLSI) **26**(8), 1545–1552 (2018)
3. Hsieh, S.E., Kao, C.C., Hsieh, C.C.: A 0.5-V 12-bit SAR ADC using adaptive time-domain comparator with noise optimization. IEEE J Solid State Circuits **53**(10), 2763–2771 (2018)

4. Segura, J., Rossello, J.L., Morra, J., Sigg, H.:A variable threshold voltage inverter for CMOS programmable logic circuits. IEEE J Solid State Circuits **33**(8), 1262–1265 (1998)
5. Chan, C.H., Zhu, Y., Sin, S.W., Murmann, B., Seng-Pan, U., Martins, R. P.: Metastablility in SAR ADCs. In: IEEE Transactions on Circuits and Systems—II: Express Briefs, vol. 64, no. 2, pp. 111–115 (2017)
6. Hsu, C.W., Chang, S.J., Huang, Chang, L.J., Shyu, Y.T. Hou, C.H., Tseng, H.A., Kung, Y. C., Hu, H.j.: A 12-b 40-MS/s calibration-free SAR ADC. In: IEEE Transactions on Circuits and Systems–I: Regular Papers, vol. 65, pp. 3,881–890 (2018)
7. Praveena, A., Smys, S.: Efficient cryptographic approach for data security in wireless sensor networks using MES VU. In: Intelligent Systems and Control (ISCO), 10th International Conference(IEEE), pp. 1–6 (2016)
8. Jyothirmai, P., Raj, J.S., Smys, S.: Secured self organizing network architecture in wireless personal networks. Wirel. Pers. Commun. **96**(4) 5603–5620 (2017)
9. Choi, S., Ku, H.S., Son, H., Kim, B., Park, H.J., Sim, J.Y.: An 84.6-dB-SNDR and 98.2-dB-SFDR residue-integrated SAR ADC for low-power sensor applications. In: IEEE J. Solid State Circuits **2**, 404–417 (2018.)
10. Muhammad Ahmadi and Won Namgoong.: comparator power reduction in low-frequency SAR ADC using optimized vote allocation. IEEE Trans. Very Large Scale Integr. Syst. (VLSI) **23**(11), 2384–2394 (2015)
11. Wang, H., Wang, X., Barfidokht, A., Park, J., Wang, J., Mercier. P.P.: A battery-powered wireless ion sensing system consuming 5.5 nW of average power. IEEE J. Solid State Circuits **53**(7), 2043–2053 (2018)
12. Zahrai, S.A., Zlochisti, M., Le Dortz, N., Onabajo, M.: A low-power high-speed hybrid ADC with merged sample-and-hold and dac functions for efficient subranging time-interleaved operation. IEEE Trans. Very Large Scale Integr. Syst. (VLSI) **25**(11), 3193–3206 (2017)
13. Luo, J., Li, J., Ning, N., Liu, Y., Yu, Q.: A 0.9-V 12-bit 100-MS/s 14.6- fJ/Conversion-Step SAR ADC in 40-nm CMOS. IEEE Trans. Very Large Scale Integr. Syst. (VLSI) **26**(10), 1980–1988 (2018)

Author Biographies

G. Prathiba has received the B.E., degree in ECE from IRTT, Erode, Tamilnadu, India and received M. Tech., Degree in Applied Electronics from PRIST University, Thanjavur, Tamilnadu, India, where she is currently pursuing the Ph.D., degree in ICE(VLSI) Anna university, Chennai, Tamilnadu, India. She is currently involved in the research of low- power and high-speed SAR analog-to digital converter (ADC) and Flash-ADC for wireless communication applications.

M. Santhi has received the B.E., degree in ECE from Mookambigai College of Engineering,Trichy,Tamilnadu,India, received M.E., Degree in VLSI Systems from Regional Engineering College, Trichy, Tamilnadu, India, and received Ph.D., Degree in VLSI Systems from NIT, Trichy, Tamilnadu, India. Her current research interests include VLSI signal Processing, Wireless Communication PHY Layer, Asynchronous Techniques and Wave- Pipelining Techniques

CharityChain - Donations Using Blockchain

Rupali Hande(✉), Tarasha Agarwal, Ranjeet Monde, N. Sai Sirisha, and Richa Yadav

Bengaluru, Karnataka, India
Premakumarl976feb@gmail.com

Abstract. CharityChain is a decentralized application, built on Ethereum that provides the user with a place in the virtual ocean, where the user can find a cause that he personally can associate with and help fund it in the fairest form using Blockchain technology. Blockchain technolgy is easy to use, lesser cost and fast access in all areas. NPO s enabe the chance for donations from global donars with the help of block chain technology.

Keywords: Blockchain · Charity · Ethereum · Metamask · Transactions

1 Introduction

Currently there is a lot of corruption pertaining to charities which has increased the distrust of people in the charity system [1]. Blockchain is emerging as the easiest way to send, receive, store and currencies and secure transactions. In this paper, the Blockchain implementation to make the charity system transparent is explained in detail. Implementing this system for a community will make the donations and funds secure and people will be drawn to donate more when they see that their donations are being used completely for a particular purpose. The Ethereum platform is used to keep the transactions public. (Fig. 1)

The literature [4] reveals that in there is a dire need for a charity application to validate itself without depending on any other system or application, i.e. it should be self-righteous. For this purpose, Blockchain technology can be used as the consistency and integrity of every transaction can be verified and traced back.

The stakeholders of this application are donors, charities and auditors. The donor registers himself to the application and browses the charities according to the category of his choice. He can go through the details of the charity and transfer ether to the charity of his liking. The user can track that donation till it reaches the concerned beneficiary. Also, the information of every transaction that the charity is involved in can be seen by the donor. The major contributions of this paper are as follows:

- Remix IDE is used to build and run solidity smart contracts.
- HTML, CSS and JavaScript is used in the front end for Web Application.
- Metamak account runs in the back when any entity transfers ether to another entity.
- Power BI is used for analysis of the transactions and to generate reports and charts for the easy understanding of the user.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 606–612, 2020.
https://doi.org/10.1007/978-3-030-37051-0_68

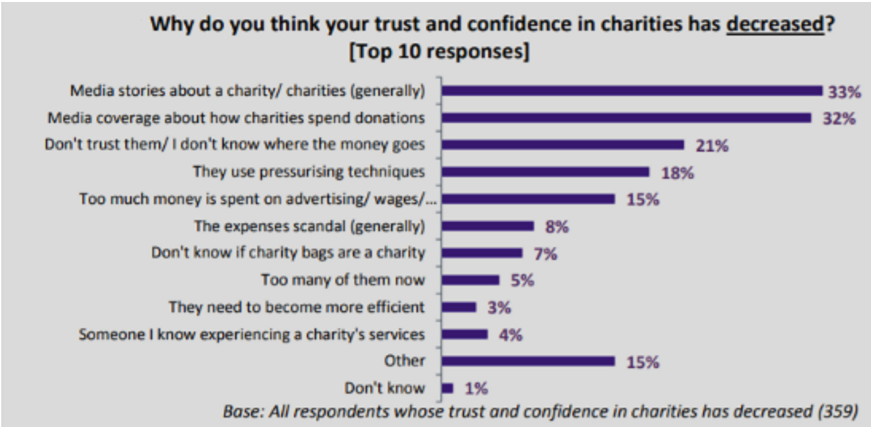


Fig. 1. Declining of trust in charities report (Source: charitycommission.blog.gov.uk/2016)

- The website is designed and hosted on the Ropsten Test Network, which can be scaled to the Ethereum Main Network easily.

2 Related Work

Blockchain is a sequence of blocks of data linked to each other with different connected nodes which forms the chain-network of blockchain. Once a new transaction is approved by consensus, it is encrypted and linked to the previous transaction. Once a piece of data is added to the chain, it cannot be deleted. If there are any modifications to be done in any created block, a new block is created stating the modifications, if this block is approved by consensus of the network, it is appended to the chain. In this way, if an impostor tries to tamper with the recorded data, he/she can never mend already created data without the consent of the network. As blockchains are transparent, decentralized and immutable, the proposed system will be best suited for the features that blockchain provides.

The literature [6] explains in detail how the China Government has utilised Blockchain technology to ensure the quality of the perishable food items. This helps in strengthening the trust between the producers, government and citizens. The application safely shares the status of the produce at each stage. The stages include manufacturing, transportation and marketing. Despite this fact that China has a large population to support, it has successfully used Blockchain to increase the trust of the people towards the government by making the production of the food resources transparent. This helps in equal distribution of the resources to the people and increases the accountability of the Government since all the transactions are recorded and can be viewed in case of disparity.

3 Methodology

We have used Agile methodology to design our proposed model. We started building our system model iteratively, improvising the product in each iteration. Before building our model, we did a subtle research about how charities in India function and also about the current charity platforms. Our motive was to make the user interface as simple as possible and the main attention was given to the blockchain backend. Hence, initially we started with building a simple graphical user interface using HTML, CSS technologies. After this stage, we moved to writing smart contacts for login of a particular user. Gradually, we increased our scope and performed transfer of ethers from Donor to Organisation. The Donor can also analyse his previous donations clearly in the system.

4 System Design

CharityChain is a blockchain platform that connects donors to charities, NGOs and other social organizations so that the donors can make donations in a transparent and secure way. The said DApp is built on Ethereum Blockchain.The smart contracts are written in Solidity. The donations are made in Ethers: token generated by Ethereum platform. In this section, we will discuss the components of the said system. These components form the requirements for realizing a design that facilitates in making the donations and tracking the transactions on the blockchain.

4.1 Testrpc

Testrpc is a Node.js-based Ethereum node used for testing and development [12]. It creates a simulation of full-node blockchain behavior and makes the production of Ethereum applications much smoother. It is written in JavaScript and is distributed like an npm package. Ethereum TestRPC is a fast and customizable blockchain emulator. It allows making calls to the blockchain without the overheads of running an actual Ethereum node.

4.2 Metamask

MetaMask is a channel that allows the user to use the distributed web of their decentralised applications [10]. It allows the user to run Ethereum dApps right in his browser without running a full Ethereum node. The main motive of Metamask is to provide Ethereum services with less hassle to worry about the complex working of a Blockchain [11]. MetaMask includes a secure identity wallet, using a specific username and password. Once the credentials are set-up, the user can request or send cryptocurrency to anyone using the address of the destination. This transaction is completed and the user is notified about the completion. Charity-Chain uses Metamask to transfer ethers from one account to another.

5 Development

Step1: **Install all the necessary software tools which are listed as follows**:

1. Visual studio code
2. Solidity smart contracts compiler (Remix IDE)
3. Geth(Go-Ethereum environment)
4. Ganache-CLI (Ethereum and js test environment)
5. Node.js and NPM
6. Metamask

Step 2 – Create Distributed Application Frontend

The building of the frontend requires the knowledge of web technologies like HTML/CSS and JavaScript. The html pages for the application's homepage, user registration, user login, user's dashboard, charity's pages are created and linked to each other. (Figs. 2, 3)

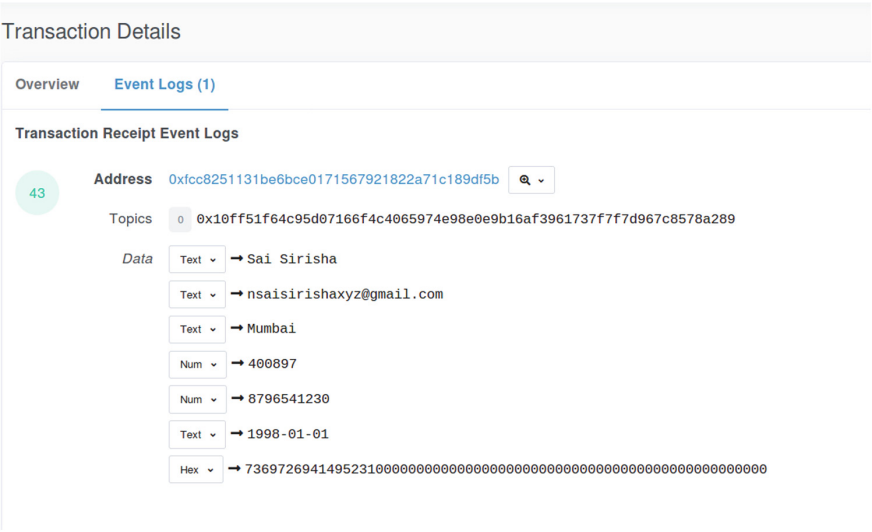


Fig. 2. Storing user's profile details on blockchain

Step 3 – Link to metamask wallet

For each transaction, a negligible amount of ethers will be used for the purpose of processing the transactions. This processing is called mining. This happens when a user registers himself to the network.

The metamask extension also provides a very user-friendly GUI for completing transactions. The user when registers to Metamask gets a public key through which he can send or receive ethers. In our case, the donor will send the ethers to the charity using the charity's public key that is mentioned in the charity's page. (Fig. 4)

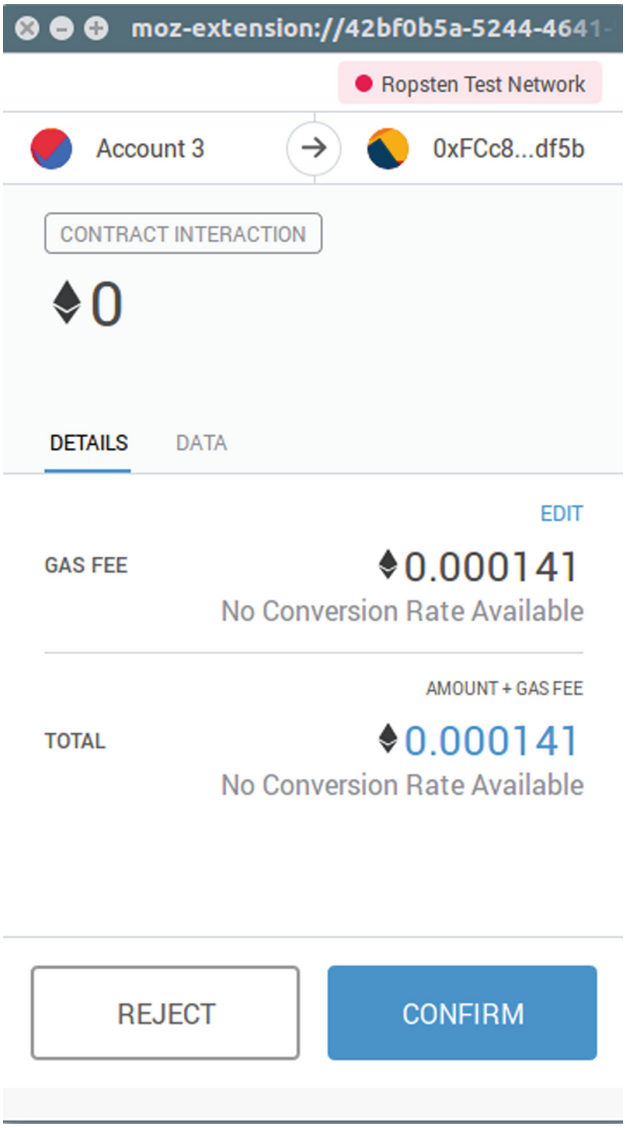


Fig. 3. Gas required for storing profile details

Step 4 – Keep track of the transactions

The transactions can be revisited and tracked using Etherscan API. Any user in the network can view all the transactions of any other user if he/she knows the corresponding public key. The data in the tabular format can be seen on the user's dashboard.

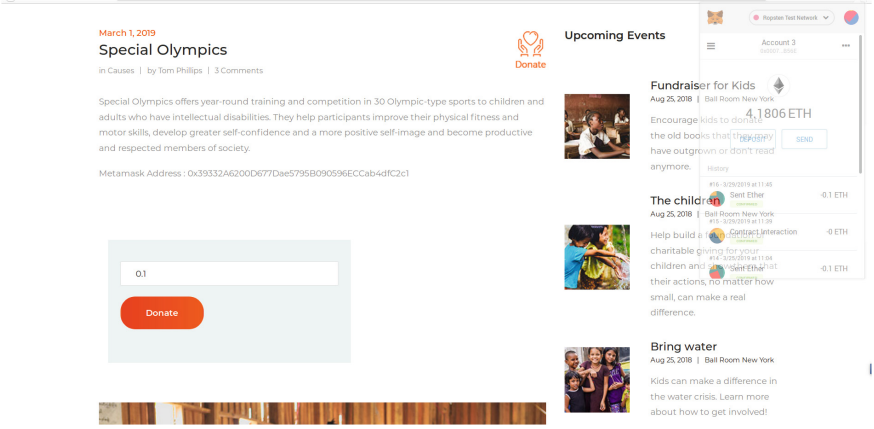


Fig. 4. Donating to charities

Step 5 - Analysis of the transactions

The user can view the charts and reports corresponding to his/her own transactions or the concerned charity through his dashboard for easier understanding. The visuals are created using the Power BI software tool.

6 Conclusion

The main reason people hesitate while donating to any charity these days is that they are unsure if the money is reaching the said charity/organization.. Blockchain is a ledger technology which can potentially remove this feeling of hesitation. Records stored over blockchain are immutable as well as visible to every node as long the ledger is public. This is the reason to use Ethereum blockchain. All the transactions occurring in the blockchain are recorded and can be viewed using the user account address. This will enable the users to keep track of their donations with the help of account address of the charity. Thus, this project will help eliminate corruption pertaining to the charities and increase the trust in donors which will encourage them to donate without any hesitation.

References

1. India today, Rs 80,000 crore has come to BJP as donation in last 5 months: Anna Hazare slams PM Modi-led govt. https://www.indiatoday.in/india/story/anna-hazare-pm-modi-rs-80000-crore-bjp-donation-5-months-india-corrupt-jan-lokpal-1111891-2017-12-15
2. Anjum A, Sporny M, Sill A.: Blockchain Standards for Compliance and Trust. 2325-6095/17/$33.00 © 2017 IEEE
3. Charity Commission, How can we rebuild public trust in charities. https://charitycommission.blog.gov.uk/2016/06/28/how-can-we-rebuild-public-trust-in-charities/

4. Why has the trust in charities been declining. https://theconversation.com/why-has-trust-in-charities-been-declining-49825
5. Tama, B.A., Kweka, B.J., Park, Y., Rhee, K.H.: A critical review of blockchain and its current applications. In: International Conference on Electrical Engineering and Computer Science (ICECOS) (2017). DOI:978-1-4799-7675-1/17/$31 .00 ©2017 IEEE
6. Hou H.: The Application of Blockchain Technology in E-government in China. 978-1-5090-2991-4/17/$31.00 ©2017 IEEE
7. Ethereum Project https://www.ethereum.org/
8. White Paper.ethereum/wiki.Wiki.GitHub, https://github.com/ethereum/wiki/wiki/White-Paper
9. Explaining Ethereum Test Networks And All Their Differences. https://medium.com/coinmonks/ethereum-test-networks-69a5463789be
10. Metamask Official Website. https://metamask.io/
11. Metamask, Medium, https://medium.com/metamask
12. Test RPC Configuration and usage. https://nethereum.readthedocs.io/en/latest/ethereum-and-clients/test-rpc/
13. Singh, S., Singh, N.: Blockchain: Future of Financial and Cyber Security. 978-1-5090-5256-1/16/$31.00 c 2016 IEEE
14. Mudliar, K., Parekh, H. Bhavathankar, P.: A Comprehensive Integration of National Identity with Blockchain Technology. 978-1-5386-2051-9/18/$31.00 ©2018 IEEE
15. Li, M., Weng, J., Yang, A., Lu, W., Zhang, Y., Hou, L., Liu, J.N., Xiang, Y., Deng, R.H.: CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourcing
16. Tasatanattakool, P., Techapanupreeda, C.: Blockchain: Challenges and Applications. 978-1-5386-2290-2/18/$31.00 ©2018 IEEE
17. Rifi, N., Rachkidi, E., Agoulmine, N. and Taher, N.C: Towards Using Blockchain Technology for eHealth Data Access Management. published in 978-1-5386-1642-0/17/$31.00 ©2017 IEEE
18. Lakshmi, S., Sankar; M., Sindhu; M., Sethumadhavan: Survey of consensus protocols on blockchain applications. published in 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS) https://doi.org/10.1109/icaccs.2017.8014672
19. Remix Documentation. https://remix.readthedocs.io/en/latest/Power BI documentation, https://docs.microsoft.com/en-us/power-bi/desktop-what-is-desktop
20. Power BI documentation. https://docs.microsoft.com/en-us/power-bi/desktop-what-is-desktop

A Survey of Wireless Communication Technologies from 1G to 5G

Jyoti Goyal(✉), Khushboo Singla(✉), Akashdeep, and Sarbjeet Singh

UIET, Panjab University, Chandigarh, India
goyalj819@gmail.com, khushboosingla09@gmail.com

Abstract. Wireless Communication services have witnessed a dramatic growth in the past few years. With Telecommunication, there has been parallel growth in usage of different applications and services like VoIP, social network, e-commerce, entertainment etc. 5G is the next generation of telecommunication technology with elaborative and twirling services that can have a profound affect on the society. It can unleash new economic opening and societal benefits giving a potential for being a conversional force for the world. This paper elucidates the evolution of mobile wireless communication technologies. It includes details of architectures, salient features like data rate, primary services etc. To deliver next generation network services, 3GPP introduces IP Multimedia Subsystem (IMS) based on Universal Mobile Telecommunication System (UMTS). This paper also covers Software Defined Network (SDN) based architecture and explains various technologies like Network Function Virtualization (NFV), Network Slicing and certain pointers to research issues related to 5G.

Keywords: LTE · 5G · IMS · NFV · Network slicing

1 Introduction

Mobile technologies have encountered incredible changes since last few decades. 1G was the first mobile phones analog technology that was used for voice calls. 2G was based on GSM and CDMA that provide services like sending pictures, text messages, user privacy, less battery consumption and many more. Enormous advancement had been made by GSM in numerous zones of media communications. This permitted framework architects to design a new system which has more capabilities than GSM and GPRS. So UMTS and WCDMA were designed under 3G technologies. 3G offers high speed data and provide services like video calling, emails etc. Wireless broadband, uninterrupted video calling, social networking application and so on are considered as the benefits provided by 3G network. After 3G, Fourth Generation (4G) was introduced. 4G technology provide services such as internet access with global roaming and full-edged support for all other multimedia applications. But the development of LTE does not finish with LTE advanced rather keeps on advancing into further releases. 5G wireless technology is expected to create a revolution in the world. 5G offers higher bandwidth, low latency, energy preserving, cost minimization, higher system capacity and tremendous device connectivity. In spite of all the advancements in mobile communication, still 5G technology has some issues that need to be addressed by the

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 613–624, 2020.
https://doi.org/10.1007/978-3-030-37051-0_69

researchers. This paper presents comparative analysis of all telecommunication technologies.

The paper describes the content as follows. Section 2 provides an overview of legacy technologies. Section 3 describes current generation networks. Section 4 provides details about technologies, advantages and research issues associated with Next Generation Networks (NGN). Section 5 gives the comparison of Mobile Communication Technologies. Section 6 presents the conclusion.

2 Telecommunication Technologies

This section presents evolution undergone by communication technologies from 1G to 3G.

2.1 Legacy Technologies

The first mobile phones introduced in 1982 were 1G mobile phones. The technology used in first generation was Advanced mobile phone system (AMPS). Second Generation (2G) was introduced in 1991 and based on Global System for Mobile Communication (GSM) and Code Division Multiple Access (CDMA). It provides services like sending pictures, Multimedia Messages (MMS) and Text messages. 2.5G refers to General Packet Radio Service (GPRS), which is considered as standard (wireless data) used on GSM networks [10]. 2.75 refers to Enhanced Data rates for GSM Evolution (EDGE), that was made to give higher information rates for packet based services with higher transmission capacity using 2G portable systems [15].

2.2 Third Generation (3G)

3G was introduced in 2000. The main objective of 3G is to provide high speed data [18]. It use wideband wireless network and provide data services like clear and continues video calling, 3D gaming, sending and receiving large emails. 3G has a bandwidth of 2 Mbps (Fig. 1).

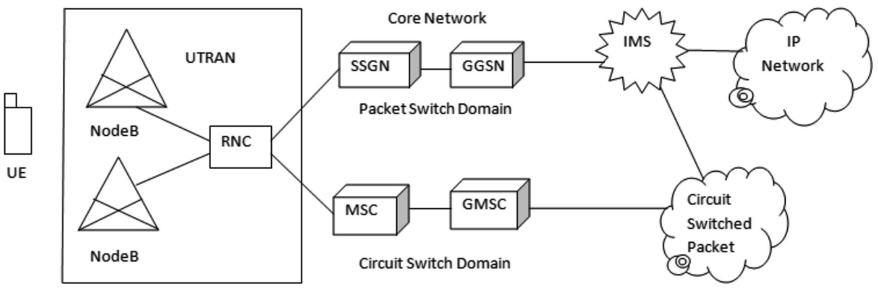


Fig. 1. Architecture of 3G

3G Architecture

The Architecture of 3G employs Universal Mobile Telecommunication System (UMTS) technology. UMTS is an upgrade version of GSM module. It is made up of 3 main elements: User Equipment (UE), UMTS Terrestrial Radio Access Network (UTRAN) and Core Network (CN).

(i) **User Equipment (UE)**

It is assigned to a single client and contains all the functions needed to access UMTS services. It contains Mobile equipment (ME) and UMTS Subscriber Identity Module (USIM).

(ii) **UMTS Terrestrial Radio Access Network (UTRAN)**

It is a hardware that binds mobile device to the public telephone network or to the internet. It contains base station i.e. NodeB and Radio Network Controller (RNC). It handles cell level mobility. NodeB helps in communicating with UE inside the cell and controls the information stream between Uu radio interface and lub interface. RNC control and manage radio resources to NodeB. For the core network RNC is viewed as a single access point of UTRAN. To route circuit switched traffic it is connected to single MSC/VLR and to route packet switched traffic it is connected to single SGSN.

(iii) **Core Network (CN)**

It is partitioned into circuit switch and packet switch domains. It contains functions for handover, gateways to different system and performs location management. It contains Home Location Register (HLR), Visitor Location Register (VLR), Mobile Switching Centre (MSC), Gateway Mobile Switching Centre (GMSC), Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN).

2.3 IP Multimedia Subsystems (IMS)

3GPP introduced IMS. It is a service delivery platform for 3G services like voice calling, messaging, video calling etc. Session initiation protocol is utilized as the signaling component in IMS. The architecture of IMS consists of Service layer and Control layer. The Service layer involves Application server. Application server is based on SIP. It Communicates with the home subscriber server to acquire the user information. The main component of control layer is Call Session Control Function (CSCF). CSCF is of three types: - Proxy-CSCF (P-CSCF), Interrogating-CSCF (I-CSCF), Serving-CSCF (S-CSCF). P-CSCF is the primary IMS node encountered when a UE (User Equipment) is attempting to build up a VoLTE call. I-CSCF first retrieve the information of user from HSS and SLF databases and then forward the SIP request to the S-CSCF. S-CSCF is middle node of the IMS control plane. It acts as the SIP registrar and SIP server. It routes SIP messages to proper application server. Home Subscriber Server (HSS) is a central database that provide user details like location, recognition information etc. Subscriber Location Function (SLF) is used to allot

appropriate HSS to user. IMS provides scalability and flexibility to the network services [1, 2] (Fig. 2).

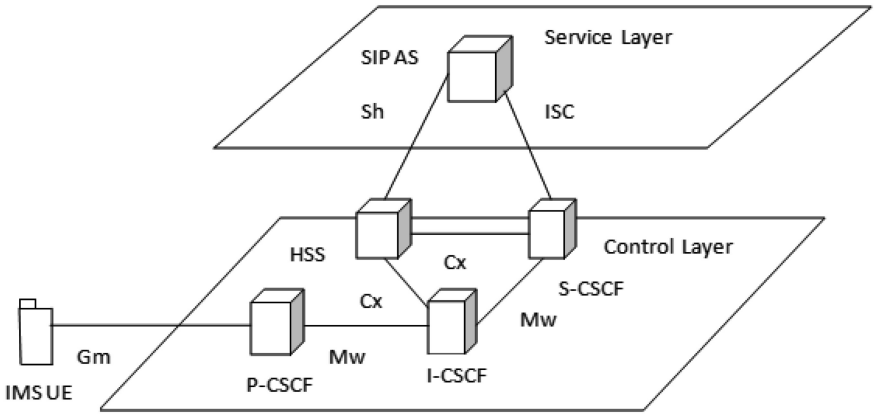


Fig. 2. Architecture of IMS

3 Fourth Generation (4G)

The advancements in mobile technology unleash the new advanced applications. These applications give rise to the All-IP based network called 4G. It provide same services as 3G as well as provide additional services like multimedia, TV programs with more clarity and sends data more faster. An abstract idea of 4G is information anywhere, anytime and in any form (Fig. 3).

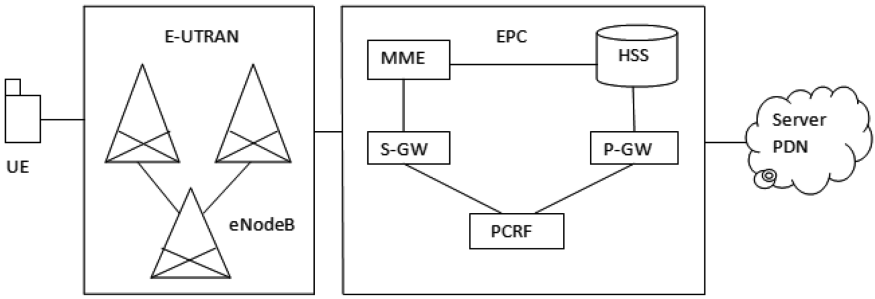


Fig. 3. Architecture of 4G

3.1 4G Architecture

The Architecture of 4G employs LTE (long Term Evolution) technology [3, 14]. LTE has three main elements that are: User Equipment (UE), Evolved UMTS Terrestrial Radio Access Network (E-UTRAN), Evolved Packet Core (EPC) [9].

(i) **User Equipment (UE)**

UE comprises of Mobile Terminal (MT), Terminal Equipment (TE), and Universal Integrated Circuit Card (UICC). MT controls all communication functions. TE terminates the data strings. UICC is also known as SIM cards for LTE equipment. Universal Subscriber Identity Module (USIM) application is operated by UICC.

(ii) **Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)**

E-UTRAN handles the radio communication between Mobile and EPC. It has one component that is eNodeB. eNodeB is a base station that handles the mobiles in cells. It comprises of Antenna, radio modules and digital modules. The eNodeB is responsible for air interface resources, load balancing, and mobility management, QoS services like latency, minimum bandwidth and maximum throughput.

(iii) **Evolved Packet Core (EPC)**

EPC exchange information with Packet Data Network (PDN) in outside world like internet, IP Multimedia System (IMS) or private corporate systems. It has following components: Home Subscriber Server (HSS), Packet Data Network Gateway (PDN-G), Serving Gateway (S-GW) and Management Entity (MME). The record of each subscriber is stored in HSS. PDN connects with outside world using SGI interface. Allocation of IP addresses to mobile device is done by PDN-GW. It has important role in roaming scenarios. PDN-GW function includes policy enforcement, packet screening, transport level packet marketing, per user based packet filtering. The function of S-GW is to manage user data tunnels between eNodeB and PDN-GW. S11 interface is used for sending the commands to S-GW. MME is responsible for managing mobiles and their session [7].

In spite of some advantages, LTE also have some issues like Handover, Expensive hardware, More battery usage etc. These issues are the key reasons that 5G will be introduced.

4 Next Generation Network (5G)

5G is the next generation of telecommunication technology having various pivot services. It supports Wireless-based web applications at higher speed [20]. It has multiple simultaneous data transfer paths with higher spectral efficiency. There are no harmful effects on human beings. All Gadgets having 5G support will work on Artificial Intelligent (AI) abilities.

4.1 SDN Based 5G Mobile Network Architecture

The architecture comprises of unified C-plane, build by three consistent controllers and fresh slate D-plane. The execution of network function can be centralized or distributed at the boundary depends on function of the supported services.

(a) **5G Control Plane**

The C-Plane manages functions in three consistent controllers: the Device Controller (DC), the Edge Controller (EC), and the Orchestration Controller (OC) [21].

(i) **Device Controller:** It is the incharge of physical layer integration to 5G network. AS function like access selection and network selection is handling by DCON. It consists of UE and Radio access application.

(ii) **The Edge Controller(1):** It executes the 5G network C-Plane, including packet routing and transfer, radio resource management functions, network access control, mobility, security, connection management and Quality of Service [4].

(iii) **Edge Controller(2):** V2V communication is one of the key use case for 5G, so it needs to support in out of coverage area, for this reason some AS/NAS functions should be situated in the cell phones. That's why the proposed architecture differentiates between Edge controller (1) and Edge controller (2).

(iv) **Orchestration Controller:** The OC is the incharge of the allocation of assets need to represent both 5G control plane and data plane. The OC consists of two modules namely, the Resource Orchestration (RO) module and the Topology Management (TM) modules. The RO is centralized and the entire cloud framework is visible to this module. The TM module controls the physical assets directly and it is formed by the Topology Management Applications (TM-A) and Topology Management Links (TM-L) (Fig. 4).

(b) **5G Data Plane**

The Data plane empowers information exchange to and from customers and control various discussions. Data plane traffic goes through routers. During system connection, an address is assigned to the gadget. Also, LHRE and NEP is related to it. From the NEP to LHRE/LHRE to NEP, a forwarding path is set up that allows the packets generated by the device to be routed.

(i) **Last Hop Routing Element (LHRE):** The device's RA point is connected to the backhaul infrastructure through LHRE. Mobility securing point is represented by the LHRE. A forwarding path from the LHRE to the NEP is built up by the FM App when a device connects to the system.

(ii) **Network Entry Point (NEP):** The NEP distinguishes bound for physical framework handled by the OC. PDN securing point is represented by the NEP. Different devices (like gateway, mobility anchoring point) may have different NEPs that depends upon the connection type [8, 21].

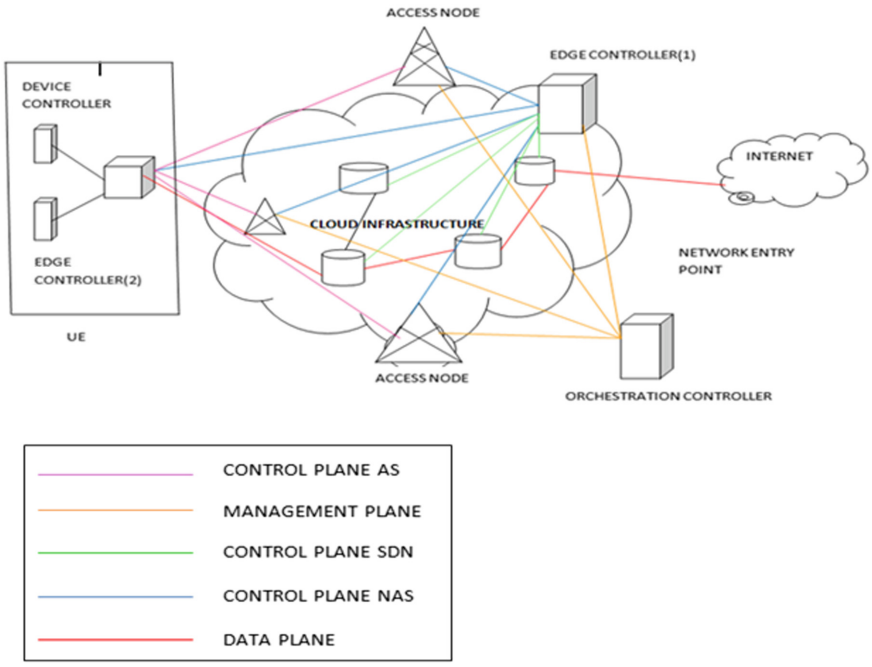


Fig. 4. SDN based 5G architecture

4.2 5G Services

(i) **Enhanced Mobile Broadband (eMBB)**

It is one of the three essential 5G New Radio (NR) use cases characterized by the 3GPP. eMBB is a characteristic development to existing 4G systems that will give quicker information rates and a better user experience.

(ii) **Massive Machine Type Communication (mmTC)**

It supports IoT (Internet of Things) in which large numbers of devices are connected. The main aim of this technology is to offer very high density of connectivity. This technology provides many applications like smart cities, smart-farms, smart power grids etc.

(iii) **Ultra-reliable and Low Latency Communications (uRLLC)**

It supports low latency transmission with high reliability from limited set of terminals which are active according to pattern specified by outside events such as alarms [6] (Fig. 5).

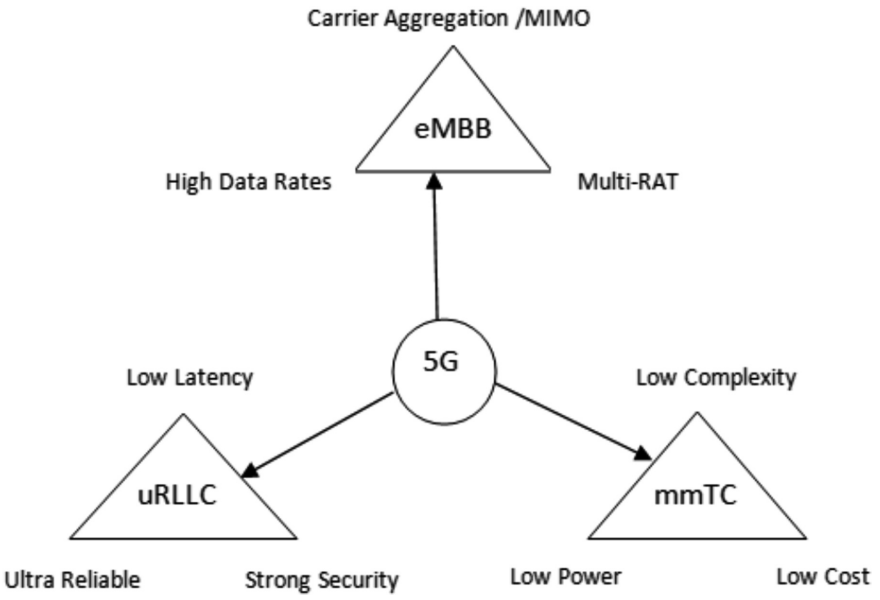


Fig. 5. 5G services

4.3 5G Enabling Technologies

(a) **Network Function Virtualization (NFV)**

The fundamental thought behind NFV is to decouple network functions which are execute in software from hardware. With NFV, service providers can send different network services, for example firewall or encryption. As for 5G, NFV will help virtualize various machines in the system. It provides many advantages like flexibility, reduced capital expenditure and energy utilization by combining network devices [5, 16].

Besides of some advantages, NFV also have some issues.

- **Interfacing:** Well defined interfaces must be delivered to service providers for communication so that they can express their needs. Interfaces between service providers and end users should be appropriate, identified and standardized.
- **Security and Privacy**: NFV gives rise to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks will influence the entire virtual network hosted on physical network.
- **Mobility Management**: In NFV Mobility Management is also one of the big issues. End users mobility from one virtual network to another and resource allocation is the biggest challenge for NFV.

(b) **Network Slicing**

It is focused on the idea of conveying different multiple logical networks with various dimensions of common isolation on the top of similar foundation [19]. It is an innovation that empowers both multi-tenancy and service tailored composition of network.

It is a key plan of action for mobile network operator to decrease arrangement operational expenses. It provides many advantages like resource utilization, improves operational efficiency, reduces expenses and capital expenditure etc. [12, 22].

There are certain issues related to network slicing.

- **Roaming**: Network Slicing provides flexibility to the operators to define the needs for individual slices. So the users hopes for the same level of service regardless of their locations.
- **Security and Privacy**: Resource Sharing and Isolation can cause various security attacks because every network slice may have different security policy needs.
- **Mobility Management**: Mobility Management is one of the biggest challenges in network slicing because every network slice may have different mobility requirements. For example mobility needs of the mobile broadband slice are dissimilar from the slice of vehicular services.

4.4 Key Advantages of 5G

- **Flexibility**: By utilizing Software Defined Mobile Network Control (SDMC), operators would have the capacity to fit the hardware to their necessities through basically reinventing the controller and therefore diminishing expenses, while having the capacity to scale all over virtual capacities.
- **Centralized Control of the Network**: By using SDN technology, operators just need to control a set of logical unified substances that run the whole system which depends on actual latency necessities.
- **Enabling new network services**: Many new services can be enabled within a few hours by making changes in the controller function.
- **Resource Sharing**: Network function Virtualization (NFV) allows resource sharing between many operators. It enables several networks to share common resources (like network infrastructure, power etc.). The advantage of Resource sharing is high performance, easier relocation to new technologies.
- **Low battery consumption**: 5G improves the battery life by harvest energy from radio signals and climatical energy sources like solar and wind energy.

4.5 Research Issues in 5G

There are various research issues in Next Generation Networks that are as follows:

- **Inter-cell obtrusion**: One of the issue in 5G is Inter-cell obtrusion, various size of large scale cells and small scale cells will be the reason behind obtrusion [4].
- **Traffic Management**: The 5G system will be a heterogeneous system. The conjunction of various systems and the fusion of their traffic information with fundamentally unique qualities will cause over-burden.
- **Infrastructure**: 5G requires large infrastructure for various services like navigation, communication etc. These services need higher availability of radio spectrum. Due to lack of fibre infrastructure, many problems arise in India like poor quality of services.

- **Spectral, power, and time variations**: 5G technology also leads to spectral, power and time variations issues. This is due to, the heterogeneous network traffic and multi-antenna techniques.
- **Security and Privacy**: Various technologies of 5G like Network Slicing and NFV leads to many security issues [11]. For instance NFV gives rise to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks [13].

5 Comparison

See Table 1.

Table 1. Includes the salient features, benefits and backlogs of all telecommunication technologies.

Technology	1G	2G	3G	4G	5G
Introduced	1982	1991	2000	2003	Probably 2020
Bandwidth	2 Kbps	14.4–64 Kbps	2 Mbps	1 Gbps	Higher than 1 Gbps
Technology	Analog	Digital	CDMA 2000, UMTS	Wi-max, LTE, LTE advanced	WWWW
Throughput	14.4 Kbps	20 Kbps	200 Kbps–3 Mbps	100–300 Mbps	1–10 Gbps or higher
Core network	PSTN	PSTN	Packet network	Internet	Internet
Multiplexing	FDMA	TDMA/CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit, Packet	Packet	All packet	All packet
Primary service	Analog phone calls	Digital phone calls and messaging	Phone calls, messaging data	All IP based network services	High speed, High capacity and provide large broadcasting of data in Gbps
Web standards	–	www	www(IPv4)	www(IPv4)	Wwww(IPv6)
Pros	First wireless communication	Improved privacy, multiple user on single channel	Better internet experience, many more features like video calling	Multimedia services with more clarity, high data rate	Increase flexibility, resource sharing, lower battery consumption
Cons	Poor spectral efficiency, security issue	Limited data rates, difficult to support demand for internet	Expensive base stations than 2G	High battery usage, handover issue, expensive hardware	Not implemented till now

6 Conclusion

This paper elucidates the architecture and features of existing and future Mobile technologies. The paper discussed that the development of LTE does not finish with LTE advanced rather keeps on advancing into further releases. This paper also covers key advantages and certain pointers to research issues related to 5G like traffic management, infrastructure, security etc. These issues need to be addressed for further improvement in 5G networks. In the near future, Fifth generation technology will unleash new economic opening and societal benefits giving a potential for being a conversional force for the world at cheaper rates.

References

1. Abu-Lebdeh, M., Sahoo, J., Glitho, R., Tchouati, C.W.: Cloudifying the 3GPP IP multimedia subsystem for 4G and beyond: a survey. IEEE Commun. Mag. **54**(1), 91–97 (2016)
2. Bertrand, G.: The ip multimedia subsystem in next generation networks. Rapp. Tech. ENST Bretagne **7** (2007)
3. Bikos, A.N., Sklavos, N.: LTE/SAE security issues on 4G wireless networks. IEEE Secur. Priv. **11**(2), 55–62 (2013)
4. Chin, W.H., Fan, Z., Haines, R.: Emerging technologies and research challenges for 5G wireless networks. IEEE Wirel. Commun. **21**(2), 106–112 (2014)
5. Chowdhury, N.M.K., Boutaba, R.: A survey of network virtualization. Comput. Netw. **54**(5), 862–876 (2010)
6. Committee, T.S.: Making India 5G Ready (2018)
7. Datta, P., Kaushal, S.: Exploration and comparison of different 4G technologies implementations: a survey. In: 2014 Recent Advances in Engineering and Computational Sciences (RAECS), pp. 1–6. IEEE (2014)
8. Goyal, R., Mahajan, N., Goyal, T., Kaushal, S., Gupta, N., Kumar, H.: Exploration of 5G technology for cellular communication: a survey. In: 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 330–334. IEEE (2018)
9. Goyal, T., Kaushal, S.: Handover optimization scheme for LTE-advance networks based on AHP-TOPSIS and Q-learning. Comput. Commun. **133**, 67–76 (2019)
10. Gupta, P.: Evolvement of mobile generations: 1G to 5G. Int. J. Technol. Res. Eng. **1**, 152–157 (2013)
11. Kabalci, Y.: 5G mobile communication systems: fundamentals, challenges, and key technologies. In: Smart Grids and Their Communication Systems, pp. 329–359. Springer (2019)
12. Li, X., Samaka, M., Chan, H.A., Bhamare, D., Gupta, L., Guo, C., Jain, R.: Network slicing for 5G: challenges and opportunities. IEEE Internet Comput. **21**(5), 20–27 (2017)
13. Moustafa, N., Hu, J.: Security and privacy in 4G/LTE network (2018)
14. Mshvidobadze, T.: Evolution mobile wireless communication and LTE networks. In: 2012 6th International Conference on Application of Information and Communication Technologies (AICT), pp. 1–7. IEEE (2012)
15. Ohmori, S., Yamao, Y., Nakajima, N.: The future generations of mobile communications based on broadband access technologies. IEEE Commun. Mag. **38**(12), 134–142 (2000)

16. Rost, P., Banchs, A., Berberana, I., Breitbach, M., Doll, M., Droste, H., Mannweiler, C., Puente, M.A., Samdanis, K., Sayadi, B.: Mobile network architecture evolution toward 5G. IEEE Commun. Mag. **54**(5), 84–91 (2016)
17. Baba, M.I., Nafees, N., Manzoor, I., Naik, K.A., Ahmed, S.: Evolution of mobile wireless communication systems from 1G to 5G: a comparative analysis. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. **4**(1), 77–147 (2018)
18. Sharma, P.: Evolution of mobile wireless communication networks-1G to 5G as well as future prospective of next generation communication network. Int. J. Comput. Sci. Mob. Comput. **2**(8), 47–53 (2013)
19. Shorov, A.: 5G testbed development for network slicing evaluation. In: 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EICon-Rus), pp. 39–44. IEEE (2019)
20. Sood, R., Garg, A.: Digital society from 1G to 5G: a comparative study digital society from 1G to 5G. Int. J. Appl. or Innov. Eng. Manag. **3**(2), 186–193 (2014)
21. Trivisonno, R., Guerzoni, R., Vaishnavi, I., Soldani, D.: SDN-based 5G mobile networks: architecture, functions, procedures and backward compatibility. Trans. Emerg. Telecommun. Technol. **26**(1), 82–92 (2015)
22. Zhang, H., Liu, N., Chu, X., Long, K., Aghvami, A.H., Leung, V.C.: Network slicing based 5G and future mobile networks: mobility, resource management, and challenges. IEEE Commun. Mag. **55**(8), 138–145 (2017)

A Virtual Assistant Chatbot for College Advising System

Hadeel Mohamed[1(✉)], Osama Badawy[1], Khaled Eskaf[1], and Mohamed Saad Zaghloul[2]

[1] Department of Computer Science, College of Computing and Information Technology, Arab Academy for Science, Technology and Maritime Transport, Alexandria, Egypt
hadeel.mohamed@windowslive.com, {obadawy,keskaf}@aast.edu

[2] Department of Electronics and Communications Engineering, College of Communication, Arab Academy for Science, Technology and Maritime Transport, Alexandria, Egypt
dr_mszaghloul@yahoo.com

Abstract. This paper proposes the merging of different Techniques for the implementation of an artificially intelligent Chatbot with which the users can interact with text or voice commands. Main objective for the Chatbot to be used as an information and advising system that helps postgraduate students in answering their different queries and respond and provide the best possible options for them. It is created using Visual C# (GUI) and SIML (Synthetic Intelligence Markup Language) as a knowledge base for the Chatbot and uses Microsoft SAPI for both speech synthesizer, and speech recognition with natural language processing abilities as well as providing a few different extra help for the students as a course list, schedule and more.

Keywords: Artificial intelligence · Chatbot · SIML · Natural language processing · STT · TTS

1 Introduction

Students face many difficulties and face many challenges with selecting the right route that interest them and this is where a problem arise with student advising systems that are available to not only undergraduates but postgraduates as well seeing as how the advising system is the key if not one of the most important aspect for the student registration.

Web based interfaces are usually used in order to help the staff that mostly newly got their jobs and lacking the sufficient experience that would help with choosing the right path for the students to register.

Many students register into fields that doesn't meet their expectations or they get shocked at how this differ from what they were expecting to specialize in as our high school system don't provide sufficient data if at all for the students to choose their path and the required info is gathered usually after they are already registered. According to

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 625–633, 2020.
https://doi.org/10.1007/978-3-030-37051-0_70

statistics compiled by ACT (American College Testing Program) 51% of four year college students in the United States graduated after five years due to the lack of academic advising. Moreover, inappropriate course selection has resulted in 58% of students graduating out of the set timeframe (Siegfried et al. 2003) [6].

This can lead to many difficulties in the future, as students feel as if they are forced into a specific path and this leads to them to perform poorly which leads to below the average grades if not failing the course and repeating a whole year or courses. Thus, there is a need for a system that automates and simplifies the process for both students and advisors.

2 Related Work

Many Research work focus on implementing and improving the recognition speech problem as speech is a very powerful form of communication. So for human computer interaction a lot of research has been developed in recent years from Google, IOS,

Table 1. Shows approach used and the related work

Approach	Works and authors
(GUI)-based expert system	Dr. Abdullah Al-Ghamdi, Sumaia Al-Ghuribi, Arwa Fadel, Fatima Al-Aswadi, Thamary AL-Ruhaili designed a (GUI)-based expert system and had been developed using JESS and java [18]
Domain specific Chatbot	Johan Rahman Implementation of ALICE as domain specific knowledge bot for BRAC U [11]. This one is the most related to our research
Natural language processing chart parsing algorithm	Agreda, Eliz Danielle B, Kristine Sarah. Fabito, Lyzel C. Prado, Ma. Hannah G. Tebelin and Benilda Eleonor V. Comendador implementation of an advisor chatbot for family-based cases [1]
Rule based system	Dina Yahia, Mahmoud Youssef, and Osama Badawy, designed A Scalable and Portable Rule-Based Expert System for Student Advising using JAVA [17]. This one is the most related to our research
GUI system	Tanvir Roushan, Dipankar Chaki, Onishim Hasdak, Md. Syeed Chowdhury, Annajiat Alim Rasel, M. Abdur Rahman, Hossain Arif designed an online-based system for course advising and registration [19]
Action agent	B Hettige and AS Karunananda designed an AIML and java based Chatbot called Octopus [14]
Dialogue systems	Sameera A. Abdul-Kader a survey and a comparison between nine papers on the techniques used to design Chatbot [13]
AIML	Sarthak V. Doshi, Suprabha B. Pawar, Akshay G. Shelar and Shraddha S. Kulkarni designed an AIML and program-o Chatbot in android [15, 19]

Android, Microsoft and more companies tries to make the best bot. A Chatbot is a software program that interacts with users using natural language.

Choosing different approaches that will work together in order to develop the Chatbot. Those chosen approaches are shown in Table 1.

3 Developed System

The main objective of this research is to develop proposed information and advising system to:

- Facilitate the advising process in university.
- Enable students to gather information and advice on courses.
- Reduce the time wasted in taking appointments with advisors, which might sometimes take more than one day.
- Building a system that's available for the students any time.

3.1 System Architecture

When the system start, the user is proceed to the dashboard. That branches to chatting with angel, term schedule, rules, events and course list. Choosing to converse with the bot in both text and speech forms then once the conversation starts, the user can add their input.

Processing the data to parse the words using Chart Parsing Algorithm, to be able to understand the meaning of the Words used, then it will fetch the suitable advice or the answer needed from the Knowledge-Base which is the bots brain as shown in details in (Fig. 1).

3.2 System Implementation

The main language used to program the Chatbot is C#.

Visual studio 2015 Bunifu Framework is used to design the Chatbot application.

SIML for the brain (knowledge base).

Sqlite for schedule and time table databases system.

Speech Engines

Speech engines are built into Windows operating systems. System. Speech in the .NET Framework provides access to Microsoft's speech recognition and speech synthesis technologies in Windows. Using a minimum of the Microsoft .NET Framework 4 to work with both speech synthesis and speech recognition.

Speech Synthesizer

UsingSystem.Speech.Synthesis;

It contains the classes required for initializing and configuring a speech synthesis engine for creating prompts, speech generation, responding to events, and for modifying voice characteristics.

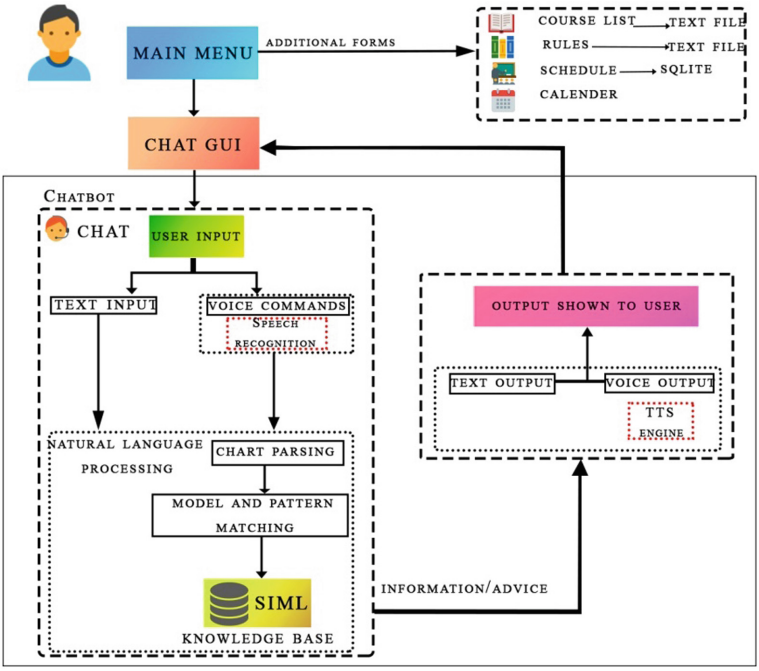


Fig. 1. System architecture

A speech synthesizer converts input text into audio. Speech synthesis is also known as text-to-speech (TTS) [2].

A simple way to generate synthesized speech is to create a SpeechSynthesizer instance, and then call the synthesizer's Speak (String) method, passing the string to be spoken as an argument. To generate speech from a string use the Speak () or the SpeakAsync() methods.

Speech Recognition

UsingSystem.Speech.Recognition;

Used by implementing speech recognition with Windows Desktop Speech technology.

A speech recognition engine takes an input audio converts it into text. The speech recognition process can be thought of as having a front end and a back end [3].

These basic operations are performed by the speech recognition app:

1. Speech recognizer Initialized.
2. Input being set for recognition.
3. Speech recognition grammar is created.
4. Load grammar.
5. Register for the recognition event notification.
6. A handler created for the recognition event.
7. Start recognition.

Choices object is used to add words. The Choices must be spoken by the user then matched to the words added as a string array (Add ([])) method argument.

- Create an Event Handler for Speech Recognition

SpeechRecognized displays the recognized word using the Result property on the SpeechRecognizedEventArgs parameter.

- Start Speech Recognition

It starts as an asynchronous operation using the RecognizeAsync() or as a synchronous operation using the Recognize().

SAPI

Speech application programming interface (SAPI) is used to reduce the code overhead required for an application to use text-to-speech and speech recognition making speech technology used more for applications.

SAPI engines have two basic types: speech recognition (STT) and text-to-speech (TTS) systems.

TTS is a synthesizer for converting text and files into spoken form using synthetic voices. Speech recognition (STT) converts speech into text and files [7].

SQLite

SQLite for Visual Studio provides access to SQLite data and objects using Microsoft Visual Studio [4].

SIML

SIML (Synthetic Intelligence Markup Language) has been developed with Speed, Simplicity and Power in Mind during the development of Syn Engine 2.0. The class library is a .NET 4.5.

SIML (Knowledge Base) is used to store and retrieve information about courses, FAQ, registration and more. Information/Advice are retrieved from the KB and are ready to process [8].

3.3 Knowledge-Base Design Methodology

The questions asked by the student define the knowledge domain given to the Chatbot. The course information, FAQ,…etc are not found easily and the need to contact the student council or a professor to gain such knowledge can be time consuming and repetitive, this is where this bot comes to work as it provide all information needed to the student acting as a replacement for providing such information [9].

Setting up the Chatbot

All the knowledge related the computer science department is included in FAQ and glossary files that make up the brain for the bot. So making a method to extract all the possible knowledge from the bot could be an important starting point for the process to generate an answer based on the available information in the knowledge base aka the Chatbot brain.

Input/Output Explanation

The Input/Output data is as follows:

FILE Course Cin:

Q <Model><question text> (input)

A <Model><answer text> (Oout)

FILE Glossary Gin:

G <Model><TERM text> (input)

D <Model><definition text> (Oout)

3.4 Chatbot Generator Algorithm

Input provided by the user {Cin, Gin,…etc}, the Oout algorithm output will be a 1.0.1 compliant SIML(XML) file. The SIML generated output can be used as the knowledge base of the question answering Chatbot, being processed by any SIML interpreter [5].

Algorithm

The algorithm has been developed in C# programming language. The main steps can be summarized as follows:

For example we will use the courses file to demonstrate he steps taken;

1. Extract the relevant answer from courses questions Cin.
2. Calculate branches.
3. Extract answers.
4. Generate output.

Step 1

This step will be used to generate the pattern matching of the words taken from the user question "Cin "with the SIML knowledge base files in order to search the right answer to the question asked.

Step 2

This step will be used to generate the SIML code by calculating the branches from a category to the different answers.

Step 3

Extract the answers from the knowledge base files.

Step 4

Return the answers generated that will be sent as the output Oout.

3.5 Results

AAST Bot is limited as it composed with approximately 1000 conversation entries to avoid the risk of not returning any responses to participants. This is done by modifying topic changing and personality related files such "course.siml, aast.siml and glossary.siml" to the context for improving the accuracy of response relating to the asked query. The AAST bot also consists of all the CCIT Courses knowledge base entries in addition with the conversational entries, glossary and FAQ (Table 2).

Table 2. Shows example of the question/response

Category	User question	Response
Greeting	Hello	Hi There
Course info	What is advanced artificial intelligence?	This course allows the introduction of material relating to current artificial intelligence …
College info	Registration requirement	Accomplished according to schedules ……
Glossary	What is fuzzy logic?	Fuzzy Logic (FL) is a method ……

Example: asking the Chatbot:

- What is Schedule?

It connects and parses the words to understand what is being said to it and calculate the time needed to retrieve the response, the output then is printed out as shown in Fig. 2.

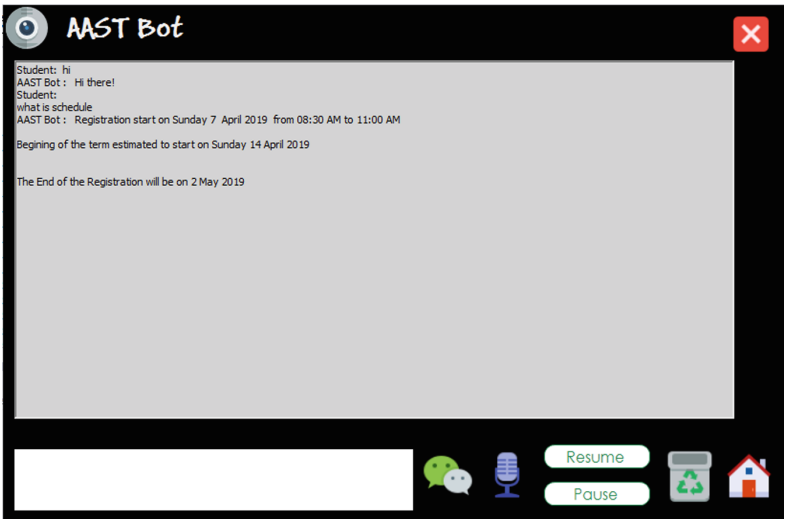


Fig. 2. Chatbot UI

Accurate responses are based on how appropriate the Chatbot responded to questions asked by the user.

The AAST Bot performed in case of text provided, results produce were 92 percent accurate with a small margin of error due to misspelling the text entered.

After testing the system response to different questions and queries from over100 test runs, the accuracy is higher than the error rates. The Likert-Scale was used to present interpretation for the computed data (Table 3) [14].

Table 3. Shows result of interacting with AAST Bot

Context of conversation	Accuracy	Error
Course info	92%	8%
College info	75%	25%
Glossary	95%	5%
FAQ	60%	40%

4 Conclusion

This paper provides scalable, cost effective and simple information and advising Chatbot system for student academic advising has been designed and developed.

Providing a simple and easy method for helping and aiding postgraduate students with information and advising by offering explanation for Courses, glossary, admission and more with the ability to respond and understand voice commands.

AAST Bot is a Chatbot that to help postgraduate students at the CCIT Department at AAST to know the courses, to facilitate the advising process and clear the ambiguity experienced by students in choosing between CS or IS.

References

1. Agreda, K.S.B., Fabito, E.D.B., Prado, L.C., Tebelin, M.H.G., BenildaEleonor, V.: ATTORNEY 209: a virtual assistant adviser for family-based cases. J. Autom. Control. Eng. **1**(3) (2013)
2. Speechsr. https://msdn.microsoft.com/en-us/library/hh362830%28v=office.14%29.aspx. Accessed 20 Mai 2017
3. Speech recognition. https://msdn.microsoft.com/en-us/library/hh378337%28v=office.14%29.aspx. Accessed 20 Mai 2017
4. MySQL for Visual Studio. https://dev.mysql.com/downloads/windows/visualstudio/. Accessed 20 Mai 2017
5. C#. https://docs.microsoft.com/en-us/dotnet/csharp/csharp. Accessed 20 July 2017
6. Siegfried, R., Wittenstein, A., and Sharma, T.: An Automated Systems for Course Selection and Scheduling. Journal of Computing Sciences in Colleges, **18**(3), 17–25 (2003).
7. SAPI. https://msdn.microsoft.com/en-us/library/ms720151%28v=vs.85%29.aspx. Accessed 19 Sept 2017
8. SIML. http://simlbot.com/. Accessed 20 Oct 2017

9. Bailes, P., Li, X., Lovell, B., Sadiq, S., and Zhuo, X., 2002. The Academic Advisor's Apprentice – An Automated Academic Advising System. CSEE Strategic Development Proposal.
10. Ahmed, I., Singh, S.: AIML based voice enabled artificial intelligent chatterbot. Int. J. u-and e-Serv. Sci. Technol. **8**(2), 375–384 (2015)
11. Rahman, J.: (11141002) Supervisor: Dr. SupratipGhose Thesis Paper. Implementation of ALICE Chatbot as domain specific knowledge bot for BRAC U (FAQ bot). BRAC University (2013)
12. Abdul-Kader, S.A., Woods, J.: Survey on chatbot design techniques in speech conversation systems. (IJACSA) Int. J. Adv. Comput. Sci. Appl. **6**(7) (2015)
13. Hettige, B., Karunananda, A.S.: Octopus: a multi agent chatbot. In: Proceedings of 8th International Research Conference. KDU. Published November 2015
14. Likert-Scale http://wpforms.com/beginners-guide-what-is-a-likert-scale-and-how-to-use- it/. Accessed 20 April 2019
15. Doshi, S.V., Pawar, S.B., Shelar, A.G., Kulkarni, S.S.: Artificial intelligence chatbot in android system using open source program-O. Department of Computer Engineering, VPKBIET, Baramati, Pune, India. Int. J. Adv. Res. Comput. Commun. Eng. **6**(4), April 2017
16. Yahia, D., Youssef, M., Badawy, O.: A scalable and portable rule-based expert system for student advising. In: The International Conference on Electrical and Computer Engineering (ICECE), Benghazi, Libya (2013)
17. Al-Ghamdi, A., Al-Ghuribi, S., Fadel, A., Al-Aswadi, F., AL-Ruhaili, T.: An expert system for advising postgraduate students. Faculty of Computer Sciences and Information Technology. King Abdulaziz University, Jeddah, KSA (2012)
18. Roushan, T., Chaki, D., Hasdak, O., Chowdhury, M.S., Rasel, A.A., Rahman, M.A., Arif, H.: University course advising: overcoming the challenges using decision support system. Department of Computer Science and Engineering. BRAC University, Dhaka, Bangladesh (2014)
19. AIML. http://www.alicebot.org/aiml.html. Accessed 28 Feb 2017

Performance Comparison of Machine Learning Algorithms in P300 Detection Using Balanced Mind-Speller Dataset

Jobin T. Philip, S. Thomas George(✉), and M. S. P. Subathra

Karunya Institute of Technology and Sciences, Coimbatore 641114, Tamil Nadu, India
jobintphilip@karunya.edu.in,
{thomasgeorge,subathra}@karunya.edu

Abstract. Visual P300 mind-speller is a brain-computer interface that offers an easy and effective approach to track human brain responses. One major challenge in the design of this system is the unbalanced nature of its dataset, which can bias the classification process. In this work two distinct methods viz. nontarget undersampling and target oversampling were used to balance the mind-speller dataset. Since the choice of classification algorithm can impact the performance of mind-speller, the effect of dataset balancing was analyzed for a set of classifiers. The error rate, accuracy, true positive and false negative rates, true negative and false positive rates, positive predictive value, Matthews correlation coefficient, F-score, G-mean, and time consumption were the metrics used in this study. Among the various evaluated classifiers, k-nearest neighbor, support vector machine, and artificial neural network demonstrated significantly improved classification performance for the balanced (by target oversampling) mind-speller dataset while the Gaussian support vector machine yielded the highest metric scores.

Keywords: P300 · Mind-speller · Brain-computer interface · Dataset balancing · Classifiers · Metrics

1 Introduction

Brain-computer interfaces (BCI) are devices that decode human brain signals using machine learning techniques, to perform some control action e.g., operate a wheelchair [8]. These advanced signal processing systems use electroencephalography (EEG) signals known as the event-related potentials (ERPs), which are generated by certain cognitive or sensory events. This work uses the data obtained from a mind-speller BCI based on an endogenous positively deflected ERP called the visual P300 (or simply P300), which occurs approximately 300 ms after a specific visual stimulus [10]. The visual P300 mind-speller (VP3S) allows its users to spell letters or symbols by gazing at the characters of its keyboard display. It employs the "oddball" paradigm to elicit P300 signals

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 634–642, 2020.
https://doi.org/10.1007/978-3-030-37051-0_71

and then uses the discriminability between target and nontarget event signals to identify the user-gazed character.

The original VP3S developed by Farwell and Donchin displayed the English alphabet and some symbols in a 6×6 matrix-like arrangement [7]. Its rows and columns were flashed repeatedly to serve as the visual stimuli for ERP generation. Scalp electrodes were placed on the VP3S user to record and process the EEG variations. During mind-spelling task, the user was instructed to gaze at a specific display character. P300 wave was evoked whenever the row or column associated with this character got flashed (i.e., target events). Other row or column flashes (i.e., nontarget events) did not evoke P300 wave and hence the indices of P300-evoked row and column were identified through signal processing, which specifies the user-gazed character.

Any subject-gazed VP3S-display character can be identified by 6 column and 6 row intensifications (together constitute a trial). Consequently, there are 2 target (i.e., with P300) and 10 nontarget signals (i.e., without P300) in a trial. The target class of the VP3S dataset has a lower number of samples compared that of the nontarget class. This class imbalance could bias the signal classification process and cause data misfits [9]. Alvarado-González et al. [3] have used the random undersampling technique to balance the VP3S dataset while Xu et al. [20] have considered the random oversampling technique for the same purpose. However, these works did not parametrically analyze the effect of dataset balancing on various VP3S classification algorithms (or classifiers). In this work, we used a set of metrics to analyze the performance of different machine learning algorithms for the unbalanced and balanced VP3S datasets.

2 Materials and Methods

2.1 Dataset and Tools

We used the VP3S training dataset obtained from the BCI Competition III database [17]. It comprises two sets of 85 character-spell experiment data recorded from two healthy users of a Farewell and Donchin based VP3S with 6×6 row-column display. The row and column flashes were 100 ms in duration, with 75 ms interstimulus interval (ISI).

For the signal processing, we used Matlab R2018a software executed on Windows platform running on Intel Core i3 CPU with 2.16 GHz clock speed.

2.2 Signal Processing

EEG signals in the dataset were sampled at 240 Hz and filtered using Chebychev type-I bandpass filter with 0.1 and 60 Hz cut-off frequencies. We used the Fz, Cz, Pz, PO7, and PO8 channels for P300 detection, based on some previous researches [13,14]. To simplify the process, all the channels were normalized to be between -1 and $+1\,\mu$V. Since the P300 wave is expected to be around 300 ms from a target stimulus onset, we segmented each channel into multiple epochs, each of which begins from target onset and lasts 800 ms.

There are 15 trials for each character spelling task and each trial contains 6 column and 6 row intensifications. Since every trial has two target and ten nontarget signals, the training data from one subject contains $12 \times 15 \times 85 = 15{,}300$ intensifications, out of which $2 \times 15 \times 85 = 2550$ are target signals and $10 \times 15 \times 85 = 12{,}750$ are nontarget signals. The large margin between the number of target and nontarget signals could cause classification bias like data overfitting [9]. We applied two methods, namely nontarget undersampling and target oversampling, to overcome this issue by balancing the dataset [2]. In nontarget undersampling, the number of nontarget signals in a trial was reduced to 6, thereby reducing the margin mentioned above. While in target oversampling, the number of target signals was increased, through repetition, to that of the nontarget signals. For every flash, the Fz, Cz, Pz, PO7, and PO8 channels were concatenated to the produce the feature vector. Principal component analysis (PCA) [1] was used to tackle the data redundancy problem by retaining only those components which reflects more than 95% of the total data variance. Finally, the selected feature vectors were fed into various classifiers for performance analysis.

3 Classifiers

In VP3S, the objective of classification algorithm is to find whether an input epoch contains the P300 signal or not. This study used the tree, discriminant analysis, logistic regression (LR), k-nearest neighbor (kNN), support vector machine (SVM) and artificial neural network (ANN) classifiers. Ten-fold cross-validation was used for the comparative performance evaluation.

Tree classifier hierarchically organizes data into distinct classes. We used the standard classification and regression trees (CART) algorithm [5] with the Gini index for tree building process and the tree was pruned to avoid data overfitting. Linear discriminant analysis (LDA) assumes uniform class covariance to classify linearly separated data [12]. Quadratic discriminant analysis (QDA) is a generalized version of the LDA that uses separate class-covariances for each data class, and it can classify nonlinear data [15]. LR is a prediction based algorithm that can handle binary classification problems [11], but is quite unstable for linearly separable data.

Linear SVM utilizes a hyperplane to distinguish between classes while kernel based SVM can separate non-linear data. In kernel SVM, a kernel function (e.g., Gaussian) is used to map the data points to a higher dimensional space where the class separation appears linear. Quadratic SVM uses a quadratic function for nonlinear data classification; thereby eliminating the need for kernel trick [6]. The kNN algorithm is a nonparametric data-driven method for classification. Its basic principle is to assign an unlabeled data point to the predominant class among its 'k' nearest labeled-neighboring points.

Artificial neural network (ANN) classifier consist of layered units called nodes (or neurons) that take inputs, process them by applying some function (usually nonlinear), and then pass the results to the next layer. This process continues till

the output layer is encountered. This classifier can tune itself by adjusting the connection weights between nodes, to provide the best outputs for new inputs. It is worthwhile to note that the ANN has consistently high EEG classification performance among the supervised classifiers [16].

4 Performance Metrics

For our binary classification problem, we defined class 1 as the set of signals 'with P300' and class 0 as that 'without P300'. Therefore in this study, class 1 is the positive class and class 0 is the negative class. The confusion matrix values viz. true positive (TP), true negative (TN), false positive (FP), and false negative (FN) of the classification results were used to compute the performance metrics like error rate, accuracy, true positive and false negative rates, true negative and false positive rates, positive predictive value, Matthews correlation coefficient, F-score, and geometric mean [18]. The definition and significance of each of these metrics are given below.

The error rate (ER) and accuracy (ACC) blueprints the performance profile of a classification system by quantifying the number of errors in detecting target signals. A high ER indicates a less accurate system and vice versa. The mathematical expressions for calculating the ER and ACC are given below.

$$ER = \frac{FP + FN}{TP + TN + FP + FN} \text{ and } ACC = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

The true positive rate (TPR; also known as sensitivity) and false negative rate (FNR) give the fractions of correctly and incorrectly predicted P300 signals, respectively. Mathematically they are defined as

$$TPR = \frac{TP}{TP + FN} \text{ and } FNR = \frac{FN}{TP + FN} \quad (2)$$

The true negative rate (TNR; also known as specificity) and false positive rate (FPR) give the fractions of correctly and incorrectly predicted non-P300 signals, respectively. Mathematically they are defined as

$$TNR = \frac{TN}{TN + FP} \text{ and } FPR = \frac{FP}{TN + FP} \quad (3)$$

The positive predictive value (PPV; also known as precision) is the fraction of correct responses among the predicted P300 signals. Mathematically it is defined as

$$PPV = \frac{TP}{TP + FP} \quad (4)$$

The Matthews correlation coefficient (MCC) considers all the positive and negative rates to generate a score a value between -1 to $+1$, in which the lower

boundary indicates the worst classification result while the higher one denotes the best result [4]. Equation (5) gives the mathematical definition of MCC.

$$MCC = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{5}$$

The F-score computation takes into account the true positive metrics, namely precision and sensitivity [19]. Mathematically it is defined as

$$F_\beta = \frac{(1 + \beta^2)(PPV * TPR)}{\beta^2 * PPV + TPR} \tag{6}$$

where the parameter β determines the weight trade-off between precision and sensitivity metrics. For $\beta < 1$, the former metric is preferred over the latter and for $\beta > 1$, this preference is reversed. To ensure a balanced evaluation, we used $\beta = 2$ in this study.

Table 1. Average performance metric scores of various classifiers for unbalanced dataset

No.	Classifier	ER	ACC	TPR	FNR	TNR	FPR	PPV	MCC	F_2	G_m	Time(s)
1	Tree	18.55	81.46	0.09	0.91	0.96	0.04	0.31	0.09	0.11	0.3	151.31
2	LDA	15.98	84.03	0.13	0.87	0.98	0.02	0.46	0.18	0.15	0.31	141.54
3	QDA	21.49	78.52	0.21	0.79	0.9	0.1	0.32	0.14	0.22	0.43	140.18
4	LR	15.94	84.06	0.14	0.87	0.98	0.02	0.5	0.2	0.16	0.33	161.05
5	kNN	27.22	72.79	0.21	0.79	0.83	0.17	0.2	0.04	0.21	0.42	360.99
6	Gaussian SVM	16.29	83.72	0.04	0.97	1	0	0.7	0.13	0.04	0.18	653.42
7	Quadratic SVM	16.32	83.69	0.15	0.86	0.98	0.03	0.52	0.21	0.17	0.37	657.5
8	ANN	2.38	97.62	0.99	0.01	0.98	0.03	0.86	0.92	0.87	0.99	718.85

Table 2. Average performance metric scores of various classifiers for balanced (by nontarget undersampling) dataset

No.	Classifier	ER	ACC	TPR	FNR	TNR	FPR	PPV	MCC	F_2	G_m	Time(s)
1	Tree	27.39	72.61	0.18	0.82	0.91	0.09	0.39	0.12	0.2	0.4	122.05
2	LDA	21.79	78.22	0.3	0.71	0.95	0.06	0.63	0.33	0.33	0.53	96.01
3	QDA	28.06	71.95	0.29	0.72	0.87	0.14	0.41	0.17	0.31	0.5	86.94
4	LR	21.9	78.1	0.31	0.7	0.94	0.06	0.62	0.32	0.34	0.54	117.58
5	kNN	36.94	63.07	0.3	0.7	0.74	0.26	0.28	0.05	0.3	0.47	135.72
6	Gaussian SVM	23.05	76.95	0.13	0.87	0.98	0.02	0.7	0.23	0.16	0.36	344.67
7	Quadratic SVM	22.73	77.27	0.29	0.72	0.94	0.07	0.59	0.29	0.32	0.51	366.1
8	ANN	2.4	97.6	0.99	0.02	0.98	0.03	0.92	0.94	0.97	0.99	477.16

Table 3. Average performance metric scores of various classifiers for balanced (by target oversampling) dataset

No.	Classifier	ER	ACC	TPR	FNR	TNR	FPR	PPV	MCC	F_2	G_m	Time(s)
1	Tree	34.08	65.93	0.72	0.28	0.6	0.4	0.64	0.32	0.7	0.66	271.07
2	LDA	29.15	70.85	0.7	0.31	0.72	0.29	0.72	0.42	0.7	0.71	222.41
3	QDA	23.09	76.91	0.75	0.26	0.8	0.21	0.79	0.54	0.76	0.77	206.89
4	LR	29.03	70.97	0.7	0.3	0.72	0.29	0.71	0.42	0.7	0.71	260.34
5	kNN	9.23	90.78	1	0	0.82	0.19	0.85	0.83	0.97	0.91	514.26
6	Linear SVM	29.13	70.87	0.7	0.3	0.72	0.28	0.72	0.42	0.71	0.71	1528.6
7	Gaussian SVM	1.6	98.41	1	0	0.97	0.03	0.97	0.97	0.99	0.99	2497.95
8	Quadratic SVM	15.04	84.97	0.92	0.09	0.78	0.22	0.81	0.71	0.9	0.85	1809.45
9	ANN	2.08	97.92	0.98	0.02	0.98	0.03	0.98	0.96	0.98	0.98	1259.89

The geometric mean (G_m) of sensitivity and specificity offers a balanced score between true positive and true-negative values. It is computed as

$$G_m = \sqrt{\frac{TP + TN}{(TP + FN)(TN + FP)}} = \sqrt{TPR * TNR} \tag{7}$$

The average time consumed (in seconds) by the classifiers, for 10-fold cross-validation of a single-user data (i.e., 15,300 flashes), is used for performance analysis.

5 Results and Discussions

We have evaluated the error rate, accuracy, true positive and false negative rates, true negative and false positive rates, positive predictive value, Matthews correlation coefficient, F-score, G-mean, and time consumption for the tree, LDA, QDA, LR, kNN, linear SVM, Gaussian SVM, quadratic SVM, and ANN classifiers. The metrics ACC, MCC, F_2, and G_m were calculated using the ER, TPR, FNR, TNR, FPR, and PPV. Thus, we have given focus to the former metrics in our analysis.

Tables 1, 2, and 3 provide the values of various performance metrics for different VP3S classifiers using unbalanced (*unbal*), balanced by nontarget undersampling (*bal1*), and balanced by target oversampling (*bal2*) datasets, respectively. Our study revealed that the linear SVM classifier fails to classify the *unbal* and *bal1* datasets. However, as shown in Table 3, it produced a valid classification result for the balanced dataset, *bal2*. This performance variation could be due to the unbalanced nature of the *unbal* and *bal1* datasets along with the large-scale overlap in the distribution of the target and nontarget responses in them.

Figure 1(a) shows the comparison of mean ACC of various classifiers for the unbal, *bal1*, and *bal2* datasets. The accuracies of all classifiers, except ANN, exhibited significant decline for the *bal1* dataset when compared to that for

the *unbal* dataset. This accuracy degradation could be due to the information loss caused by undersampling of the *bal1* dataset. Similarly, the tree, LDA and LR classifiers exhibited significant drops in accuracy for the *bal2* dataset. This accuracy reduction could be due to the classifier overfitting caused by data redundancy in the *bal2* dataset. However, the QDA, quadratic SVM, and ANN classifiers demonstrated comparable accuracies and the kNN, linear SVM, and Gaussian SVM manifested significantly increased accuracies for the *bal2* dataset compared to that for the *unbal* dataset.

The MCC, F_2, and G_m comparison charts (refer Fig. 1) show significant increases in corresponding scores for the *bal1* and *bal2* datasets compared to that for the *unbal* dataset. Also, among the two balanced datasets, the *bal1* dataset yielded the highest scores. Though the ANN classifier delivered comparable accuracies and G_m scores for all the three evaluated datasets, it's MCC and F_2 scores were improved for *bal1* and *bal2* datasets. The kNN classifier yielded the highest accuracy improvement (∼18%) for *bal2* dataset compared to that of the *unbal* dataset, which is followed by the Gaussian SVM classifier (∼15%). For all the evaluation metrics, Gaussian SVM topped in performance with an accuracy of 98.41%, MCC of 0.97, F_2 of 0.99, and G_m of 0.97. However, its time consumption is the highest and thus needs further modifications for practical VP3S implementations.

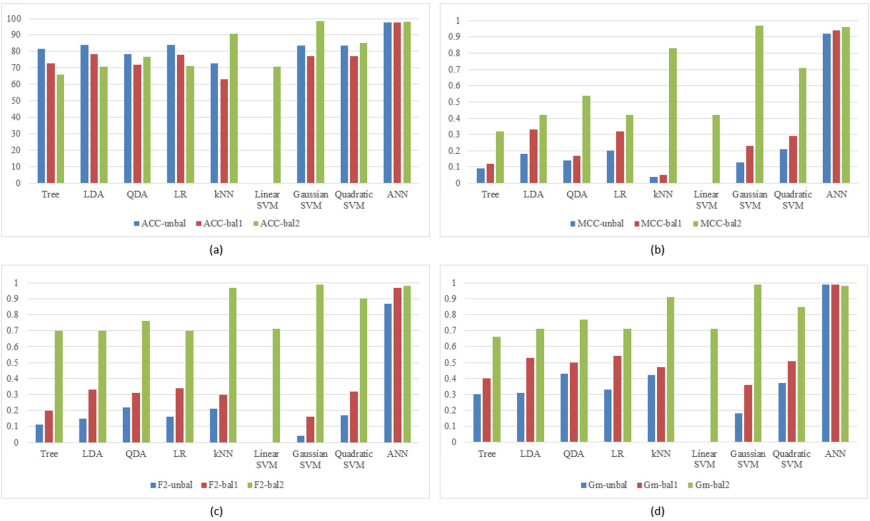


Fig. 1. Comparison of the mean (a) ACC (b) MCC (c) F_2 and (d) G_m scores for various classifiers.

6 Conclusion

In this research, we studied the impact of VP3S dataset balancing on the tree, discriminant analysis, logistic regression, k-nearest neighbor, support vector machine, and artificial neural network classifiers. The accuracy, MCC, F_2, and G_m metrics were primarily used for the analysis. All the classifiers, except ANN, produced lower accuracies for the balanced dataset based on nontarget undersampling. However, they exhibited mixed responses for the balanced dataset based on target oversampling. Balancing of mind-speller dataset significantly improved the MCC, F_2, and G_m scores for all the classifiers. Within the limits of our study, the Gaussian SVM classifier produced the best performance in all the evaluation metrics, for the balanced dataset based on target oversampling. Future researches can examine the dataset balancing methods like SMOTE, classifiers based on deep learning methods and metric-optimization techniques for the efficient P300 classification in mind-spellers.

References

1. Abdi, H., Williams, L.J.: Principal component analysis. Wiley Interdiscip. Rev.: Comput. Stat. **2**(4), 433–459 (2010). https://doi.org/10.1002/wics.101
2. Afzal, W., Torkar, R., Feldt, R.: Resampling methods in software quality classification. Int. J. Softw. Eng. Knowl. Eng. **22**(2), 203–223 (2012). https://doi.org/10.1142/S0218194012400037
3. Alvarado-González, M., Garduño, E., Bribiesca, E., Yáñez-Suárez, O., Medina-Bañuelos, V.: P300 detection based on EEG shape features. Comput. Math. Methods Med. **2016**, 1–14 (2016). https://doi.org/10.1155/2016/2029791
4. Baldi, P., Brunak, S., Chauvin, Y., Andersen, C.A.F., Nielsen, H.: Assessing the accuracy of prediction algorithms for classification: an overview. Bioinformatics **16**(5), 412–424 (2000). https://doi.org/10.1093/bioinformatics/16.5.412
5. Breiman, L., Friedman, J.H., Olshen, R.A., Stone, C.J.: Classif. Regres. Trees (2017). https://doi.org/10.1201/9781315139470
6. Dagher, I.: Quadratic kernel-free non-linear support vector machine. J. Glob. Optim. **41**(1), 15–30 (2008). https://doi.org/10.1007/s10898-007-9162-0
7. Farwell, L., Donchin, E.: Talking off the top of your head: toward a mental prosthesis utilizing event-related brain potentials. Electroencephalogr. Clin. Neurophysiol. **70**(6), 510–523 (1988). https://doi.org/10.1016/0013-4694(88)90149-6
8. Gentiletti, G., Gebhart, J., Acevedo, R., Yáñez-Suárez, O., Medina-Bañuelos, V.: Command of a simulated wheelchair on a virtual environment using a brain-computer interface. IRBM **30**(5-6), 218–225 (2009). https://doi.org/10.1016/j.irbm.2009.10.006
9. He, H., Garcia, E.: Learning from imbalanced data. IEEE Trans. Knowl. Data Eng. **21**(9), 1263–1284 (2009). https://doi.org/10.1109/TKDE.2008.239
10. Haider, A., Fazel-Rezai, R.: Application of P300 event-related potential in brain-computer interface. In: Event-Related Potentials and Evoked Potentials. InTech (2017). https://doi.org/10.5772/intechopen.69309
11. Hardle, W.K., Simar, L.: Applied Multivariate Statistical Analysis. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-17229-8

12. Kim, S., Magnani, A., Boyd, S.: Robust fisher discriminant analysis. In: Advances in Neural Information Processing Systems 18. Neural Information Processing Systems Foundation, Inc. (2005)
13. Krusienski, D., Sellers, E., McFarland, D., Vaughan, T., Wolpaw, J.: Toward enhanced P300 speller performance. J. Neurosci. Methods **167**(1), 15–21 (2008). https://doi.org/10.1016/j.jneumeth.2007.07.017
14. McCann, M.T., Thompson, D.E., Syed, Z.H., Huggins, J.E.: Electrode subset selection methods for an EEG-based P300 brain-computer interface. Disabil. Rehabil.: Assist. Technol. **10**(3), 216–220 (may 2015). https://doi.org/10.3109/17483107.2014.884174
15. Mika, S., Ratsch, G., Weston, J., Scholkopf, B., Mullers, K.: Fisher discriminant analysis with kernels. In: Neural Networks for Signal Processing IX: Proceedings of the 1999 IEEE Signal Processing Society Workshop (Cat. No.98TH8468), pp. 41–48. IEEE, Piscataway (1999). https://doi.org/10.1109/NNSP.1999.788121
16. Poulos, M., Rangoussi, N., Alexandris, M.: On the use of EEG features towards person identification via neural networks. Med. Inf. Internet Med. **26**(1), 35–48 (2001). https://doi.org/10.1080/14639230118937
17. Rakotomamonjy, A., Guigue, V.: BCI competition III: dataset II-ensemble of SVMs for BCI P300 Speller. IEEE Trans. Biomed. Eng. **55**(3), 1147–1154 (2008). https://doi.org/10.1109/TBME.2008.915728
18. Sokolova, M., Japkowicz, N., Szpakowicz, S.: Beyond accuracy, F-score and ROC: a family of discriminant measures for performance evaluation. In: AI 2006: Advances in Artificial Intelligence, pp. 1015–1021. Springer, Berlin, Heidelberg (2006). https://doi.org/10.1007/11941439_114
19. Stapor, K.: Evaluating and comparing classifiers: review, some recommendations and limitations. In: Advances in Intelligent Systems and Computing, pp. 12–21. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-59162-9_2
20. Xu, G., Shen, F., Zhao, J.: The effect of methods addressing the class imbalance problem on P300 detection. In: The 2013 International Joint Conference on Neural Networks (IJCNN), pp. 1–5. IEEE, Aug 2013. https://doi.org/10.1109/IJCNN.2013.6706890

Deep Learning Enabled Physical Layer Security to Combat Eavesdropping in Massive MIMO Networks

C. Ismayil Siyad(✉) and S. Tamilselvan

Pondicherry Engineering College, Puducherry, India
{ismayilsiyad, tamilselvan}@pec.edu

Abstract. The physical layer security is a new security paradigm based on the principles of information theory. Several methods for achieving secrecy in physical layer is proposed. This paper proposes PLS based on the deep learning architecture. In which the deep learning model will transform the channel coefficients, the beamforming based on this transformed channel coefficients can be decoded using deep learning architecture in the receiver. The secrecy rate and secrecy outage probability of proposed system is compared with the zero forcing based beamforming and superior performance is verified by the simulation using popular deep learning library TensorFlow.

Keywords: Massive MIMO · Deep learning · Physical layer security · Beamforming · 5G communication · Wireless security

1 Introduction

Wireless networks have far-flung usage in 21st century digital life. Most of the extravagant personal data are transferred through wireless medium. According to Ericsson between 2016 and 2022, the traffic generated by smartphone alone will increase by 10 times. The fifth-generation (5G) wireless mobile communication will revolutionize the data traffic further by the usage of IoT and other cloud-based services. The increased data traffic will obviously increase the concern for the improved security. Traditional cryptographic techniques used for data security, due to its established weaknesses, are not much effective to combat new security threats aroused due to broadcasting nature of wireless transmission.

To covert secret data from eavesdroppers without any deprivation in the information content, one of the major solutions under popularity in recent days is Physical Layer Security (PLS) techniques [1]. Physical layer security considers security problem in PHY layer whereas traditional cryptographic method considers in higher layers. Physical layer security techniques exploit fundamentals of the information theory principles. In literature PLS is one of the prominent security tools as compared to cryptographic methods, since it doesn't rely on computational intricacy of the equipment, which is becoming a solvable problem now. Whereas PLS will not compromise for an adversary having splendid complexity. The secrecy in PLs can be achieved by different methods. These are artificial noise injection to degrade signal to eavesdropper.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 643–650, 2020.
https://doi.org/10.1007/978-3-030-37051-0_72

Modification of signal constellation is studied in [2]. Another method is secure beamforming to nullify the reception in eavesdropper. One of the popular PLS technique is the physical layer encryption [3, 4].

Massive Multi Input Multi Output (MIMO) networks one of the backbone technology of 5G communication [6]. Massive MIMO networks make use of large number of service antennas which are arranged systematically and adaptively to achieve desired characteristics in the network. Massive MIMO networks can increase the system performance drastically in many aspects of modern digital communication. PLS in massive MIMO networks studied extensively in literature [7–11]. In all the works one intended user and one adversary is considered whereas one desired user with multiple adversaries are studied in [8] for i.i.d Rician channel model. Distributed power allocation technique for physical layer security is proposed in [10]. [12] studied robust beamforming technique for beam division multiple access (BDMA) massive MIMO system where spatial multiplexing technique is exploited for the sake of security. [9] studied the physical layer encryption method named chaotic antenna index 3D modulation and constellation points rotated. Constellation modification in OFDM networks is studied in [2]. [14, 15] studied active attack by means of pilot contamination in single cell multi user single eavesdropper for i.i.d Rayleigh.

Deep learning (DL) is one of the major breakthroughs in the arena of computer science. It is a gamechanger in almost all areas where computer algorithm serves the function. Search engines, voice recognition, voice assistant, self-driving cars and computer vision are some applications where DL is the benignant power. In wireless communication technology also, deep learning has significant contribution. In literature application of different DL models for different solutions in wireless communication networks have been proposed [16, 17]. To best of our knowledge this is the first attempt to integrate DL technique to physical layer security of massive MIMO network. In our approach DL network learns the channel matrices between the legitimate user and base station. Instead of traditional mathematical transformation of CSI in zero forcing (ZF) beamforming and singular value decomposition (SVD) beamforming the DL based approach self-identify the best transformation of CSI and successfully decode at the legitimate user. The autoencoder architecture of DL is used for achieving aforementioned security goal.

2 System Model

A single downlink massive MIMO network with N_t transmit antennas at base station and a single receiver antenna at user terminal and another single antenna adversary is considered, which is an active eavesdropper profess as a legitimate user node try to modify the secret information transmitted by the base station (BS) to legitimate user (LU) as shown in Fig. 1. The channel matrix representing channel coefficients between BS to LU is denoted as H_L.

The channel matrix representing channel coefficients between BS to eavesdropper (EU) is denoted as H_w. The system is considered to be operated using orthogonal frequency division multiplexing (OFDM) over N_c subcarriers.

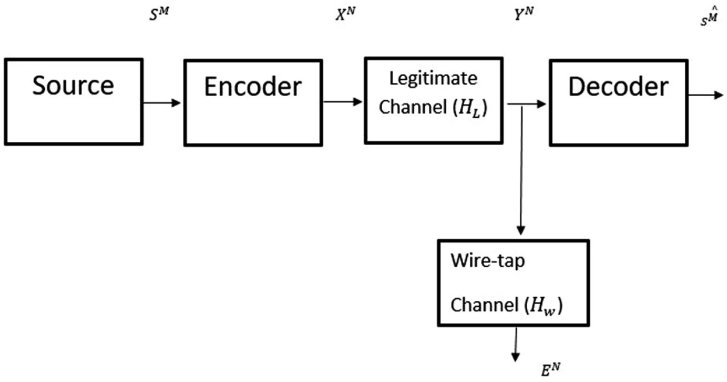


Fig. 1. Wire-tap channel model

The received signal at LU for n^{th} subcarrier can be shown as,

$$y_{Ln} = h_{LN}^{H} x_n + z_{Ln} \tag{1}$$

Where, $h_{Ln} \in C^{N_t x 1}$ is the channel vector $x_n \in C$ is the pre-coded data bearing symbol s_n in which the precoding of the data is done such that $x_n = g^{-1}(s_n)$ and $z_{Ln} \in C$ is the additive noise added.

For N_c subcarriers

$$\widetilde{H_L} = \left[\widetilde{h_{L1}} \quad \widetilde{h_{L2}} \quad \widetilde{h_{L3}} \quad \ldots \quad \widetilde{h_{N_c}} \right] \in C^{N_c x N_t} \tag{2}$$

For the wire-tap channel

$$y_L = \widetilde{H_L} x_n + z_{Ln} \tag{3}$$

$$y_L = f\left(\widetilde{U_L}\right) x_n + z_{LN} \tag{4}$$

Where the $f\left(\widetilde{U_L}\right) = \widetilde{H_L}$ is transformed CSI the transformation function is determined by the deep learning architecture.

At the receiver the inverse operation is done.

$$g(\widetilde{y_L}) = g\left(f\left(\widetilde{U_L}\right) x_n + z_{LN}\right) \tag{5}$$

$$g(\widetilde{y_L}) = g\left(f\left(\widetilde{U_L}\right)\right).g(f(x_n)) + g(z_{LN}) \tag{6}$$

$$g(\widetilde{y_L}) = g\left(f\left(\widetilde{U_L}\right)\right).g(x_n) + g(z_{LN}) \tag{7}$$

$$g(\widetilde{y_L}) = \sigma.g\left(g^{-1}(s_n)\right) + g(z_{LN}) \tag{8}$$

The DL based algorithm design is such that it will transform optimum representation of $\widetilde{H_L}$ in the form $f\left(\widetilde{U_L}\right)$ and the decomposition is such that the inverse function will cancel the effect channel coefficient such that $g\left(f\left(\widetilde{U_L}\right)\right) = \sigma$. The transformation of $\widetilde{H_L}$ to its latent space representation will make the beamforming task simpler and more precise.

$$g(\widetilde{y_L}) = \sigma.s_n + z'_{LN} \tag{9}$$

where σ is the gain of the channel and z'_{LN} is the noise at the receiver For the

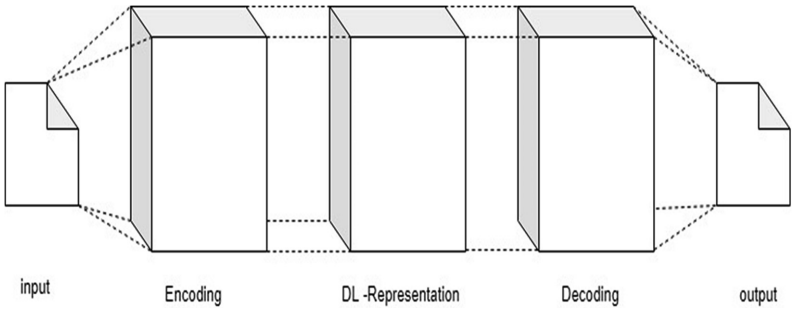


Fig. 2. DL representation of channel coefficients

Eavesdropper even though the CSI is known to the him the inverse function will not be identified and DL model will work as a virtual key. The DL modelling of the system can be represented as shown in Fig. 2.

3 Methodology

We use popular unsupervised learning based deep neural architecture named as autoencoder for the above stated objectives. The autoencoders are special class of DNN in which the input and target are the same.

The convolutional autoencoder architecture is chosen due to its ability to exploit spatial local correlation. Convolutional autoencoders make use convolution operation with suitable kernels. These networks learn to encode the input in a set of simple signals and try to reconstruct input from them. Here convolutional filters are optimized by the model itself by learning so that the reconstruction error can be reduced.

The first layer is a convolutional layer which is the input layer where the CSI values are fed to the network for learning and the activation function used is sigmoid activation function.

Where,

$$f_{sigmoid} = \frac{1}{1 + e^{-x}} \tag{10}$$

A kernel size of 3×3 is used, second layer is a dense layer which is the first hidden layer. Third layer is another convolution layer where 3×3 kernel is used fourth layer is a dense layer used for the addition of artificial noise (AN). All the remaining layers use rectified linear unit activation layer (ReLU).

$$f_{ReLU} = \max(0, x) \tag{11}$$

To overcome the dying ReLU problem layers 3 and 4 uses leaky ReLU activation function where negative values are not nullified but it is made k times y where the value of k is 0.01.

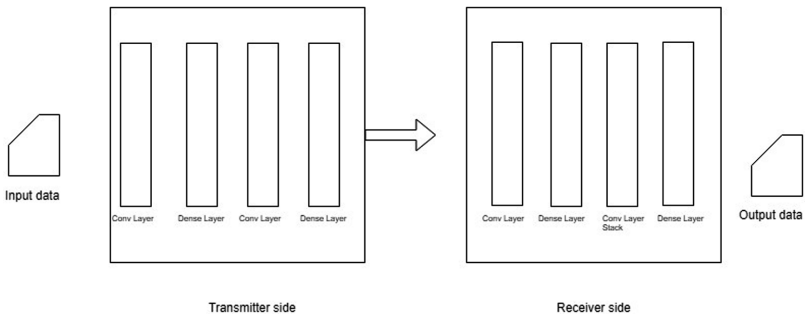


Fig. 3. DL model for training and testing

The latent space representation of the channel vectors is used for beamforming. The CNN based autoencoder network shown in Fig. 3 is used to transform the channel matrix. The beamforming is done as per zero-forcing beamforming except the fact that transformed channel features are used for precoding. In the decoder side the first layer is convolution layer where $\widetilde{y_L}$ is the input of size $N_c X N_t$. Second layer is dense layer and the third layer is a convolution layer stack having 6 convolution layers with 3×3 kernels. The output layer is dense layer.

4 Results and Discussions

The performance analysis of the proposed DL based PLS is described in this section. The popular deep learning library TensorFlow is used to model, train and validate the DNN. The simulation is done using workstation enabled with Nvidia GPU. The data

generation made use of COST 2100 and Winner2 channel models. The channel parameters are collected based on the assumptions that 5.3 GHz band is used and BS is positioned at the center of the cell whereas UEs are located randomly. Uniform linear array (ULA) with $N_t = 32$ antennas at the base station and OFDM signals with $N_c = 1024$ subcarriers are considered for the data generation. The input to the network is considered in angular domain for exploiting spatial features of CSI. Separate training, validation and testing sets are formed.

Secrecy rate and secrecy outage probability are taken as the performance parameters the performance of the proposed system with the variation of deep learning parameters batch size and learning rate are studied also the proposed system is compared with ZF based PLS and network with no enabled PL. The secrecy rate is defined as the rate difference between legitimate channel and eavesdropper channel and the secrecy outage probability is the probability that real transmission is greater than the

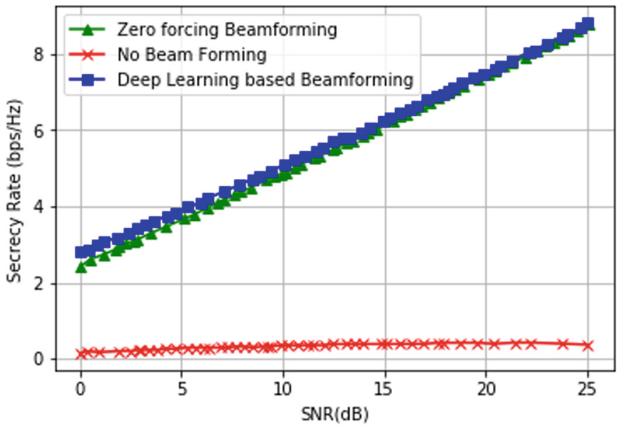


Fig. 4. Comparison of secrecy rates of proposed system with ZF and no BF

secrecy rate. Figure 4 shows the performance analysis of proposed system in terms of its secrecy rate the system shows significant improvement in secrecy rate as compared to zero forcing (ZF) based PLS. The variation is less prominent at higher SNR.

Figure 5 shows the performance analysis of proposed system in terms of secrecy outage probability where the proposed system shows clear edge over the other method. In Fig. 6 the independent variable considered is the number of antennas in the base station, as the number of antennas increases the secrecy rate is also increasing.

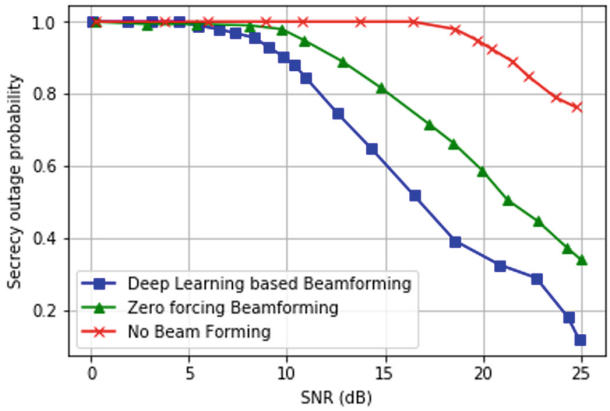


Fig. 5. Comparison of secrecy outage probability of proposed system with ZF and no BF

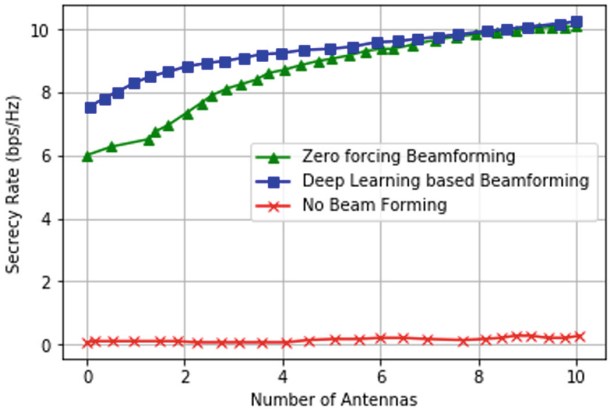


Fig. 6. Variation in secrecy rate with respect to number of antennas

5 Conclusions and Future Scopes

Beamforming based on latent features of channel instead of entire channel matrix have significant improvement over conventional techniques. The proposed deep learning based physical layer security provides secrecy rate and secrecy outage probability better than conventional physical layer security techniques. Also, the online training of the DL network improves the secrecy rate and secrecy outage probability gradually even after the deployment. The adaptive beamforming based on deep learning architecture and its performance analysis need to be studied further. Also, betterment of the network by applying more sophisticated DL architecture is another research curiosity.

References

1. Dong, L., Han, Z., Petropulu, A.P., Poor, H.V.: Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2011)
2. Neethu, V., Ismayil Siyad, C.: Performance analysis of diversity techniques for OFDM system using trellis coded OAM-QAM union modulation. In: International Conference on Intelligent Computing and Control (I2C2) (2017)
3. Rathi, V., Andersson, M., Thobaben, R., Kliewer, J., Skoglund, M.: Performance analysis and design of two edge-type LDPC codes for the BEC wiretap channel. IEEE Trans. Inf. Theory **59**(2), 1048–1064 (2013)
4. Wei, Y.-P., Ulukus, S.: Polar coding for the general wiretap channel with extensions to multiuser scenarios. IEEE J. Sel. Areas Commun. **34**(2), 278–291 (2016)
5. Andrews, J.G., et al.: What will 5G be? IEEE J. Sel. Areas Commun. **32**(6), 1065–1082 (2014)
6. Zhu, J., Schober, R., Bhargava, V.K.: Secure transmission in multi cell massive MIMO systems. IEEE Trans. Wirel. Commun. **13**(9), 4766–4781 (2014)
7. Wang, J., Lee, J., Wang, F., Querk, T.Q.S.: Jamming-aided secure communication in massive MIMO rician channels. IEEE Trans. Commun. **64**(12), 6854–6868 (2015)
8. Zhu, J., Schober, R., Bhargava, V.K.: Linear precoding of data and artificial noise in secure massive MIMO systems. IEEE Trans. Wirel. Commun. **15**(3), 2245–2261 (2016)
9. Guo, K., Guo, Y., Ascheid, G.: Security-constrained power allocation in MU-massive-MIMO with distributed antennas. IEEE Trans. Wirel. Commun. **15**(12), 8139–8153 (2016)
10. Whu, Y., Wang, J.B., Wang, J., Schobber, R., Xiao, C.: Secure transmission with large number of antennas and finite alphabet inputs. IEEE Trans. Commun. **65**(8), 3614–3628 (2017)
11. Zhu, F., Gao, F., Lin, H., Jin, S., Zhao, J., Qian, G.: Robust beamforming for physical layer security in BDMA massive MIMO. IEEE J. Sel. Areas Commun. **36**(4), 775–787 (2018)
12. Wang, S., Li, W., Lei, J.: Physical-Layer encryption in massive MIMO systems with spatial modulation. China Commun. **15**(10), 159–171 (2018)
13. Basciftci, Y.O., Koksal, C.E., Ashikhmin, A.: Physical layer security in massive MIMO (2016). https://arxiv.org/abs/1505.00396
14. Im, S., Jeon, H., Choi, J., Ha, J.: Secret key agreement with large antenna arrays under the pilot contamination attack. IEEE Trans. Wirel. Commun. **14**(12), 6579–6594 (2015)
15. Wu, Y., Schober, R., Ng, D.W.K., Xiao, C., Caire, G.: Secure massive MIMO transmission with an active eavesdropper. IEEE Trans. Inf. Theory **62**(7), 3880–3900 (2016)
16. Ye, H., Li, G.Y., Juang, B.H.: Power of deep learning for channel estimation and signal detection in OFDM systems. IEEE Wirel. Commun. Lett. **7**(1), 114–117 (2018)
17. Kato, N., et al.: The deep learning vision for heterogeneous network traffic control: proposal, challenges, and future perspective. IEEE Wirel. Commun. **24**(3), 146–153 (2017)

Microcontroller Based Low Cost Robotic Arm for Rehabilitation of Patients with Set Back in Arm Movement

M. Sivapalanirajan(✉), R. Aravindhan, M. Kartheeswaran, S. Ariharan, and N. Prasanna Venketeshan

EEE, National Engineering College, Kovilpatti, India
sivapalanirajan@gmail.com, aravindhl535@gmail.com, karthees.mskv@gmail.com, ariharansvks@gmail.com, venkateshprasannall@gmail.com

Abstract. This paper proposes a rehabilitation idea for partially paralyzed people due to neurological disorders or the ones who cannot move their arm due to an accident. Those people need aid for their routine activities which can be provided by a controllable robotic arm. This paper deals with the kinematics and dynamics of the robotic arm used for tracking and positioning the end effector within the workspace of the arm. An Arduino based low-cost robotic arm controlled by a joystick is developed. An alternate control strategy has also been developed to control the servo actuators in a wireless technique by an Android application via Bluetooth. The arm is designed to perform pick and place things which are within the designed payload. The simulation mechanism of the 4R robotic arm was designed using "RoboAnalyzer" software. The arm has been manufactured by a strong and light weighted PLA filament of 1.75 mm thickness. Parts of the arm and joints made of the servo motor casing were designed in Solidworks platform which was manufactured by FlashForge 3D printer. By this work, it is proposed to have low cost, a light weighted robotic arm which may be developed further for automatic control.

Keywords: Robotic arm · RoboAnalyzer · PLA · Arduino · Servo motor

1 Introduction

Robotic arm manipulators are required for aiding people with muscular dystrophy (MD), spinal cord injury (SCI), spinal muscular atrophy, multiple sclerosis (MS), amyotrophic lateral sclerosis, cerebral palsy (CP), rheumatoid arthritis, post-polio syndrome, locked-in syndrome, and another severe motor paralysis [1]. Specifically, upper limb hemiparesis, which occurs in approximately 26% of stroke survivors [2] has a heavy impact on bimanual tasks such as picking a tablet from its strip, holding water bottle, etc. Arm rehabilitation is the proposed solution. There are different types of rehabilitation methods such as the use of exoskeleton or using an interactive robotic arm [3]. Most of the robotic manipulators available have 7 DOF [4]. Studies have shown that providing Augmented Reality (AR) based gaming platform attached to an exoskeleton with feedback helps in rehabilitation [5]. This AR based training helps the

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 651–659, 2020.
https://doi.org/10.1007/978-3-030-37051-0_73

stroke patients in doing their Activities of Daily Living (ADL) [6]. In olden days some robotic arms have been manufactured using Nylon fabric [7]. Our arm can be operated with two fingers using a joystick or with an Android app via Bluetooth. By this, they can pick and place objects like fruits, medicine, etc. within the designed payload for their daily routine. For making such a robotic arm in low cost and custom build programming, it is required to design the kinematics of the robot for meeting the desired trajectory and the location of the end effector placed at the required position. So the design is tested in a simulation environment and would be implemented in a real system. RoboAnalyzer [8] is the platform that guides to realize the design of robots and used for making simulation study such as forward kinematics, forward dynamics, inverse dynamics and estimation of torque.

This project focuses on the people who need temporary aid for day to day activities at a low cost. It is not only restricted to a neurological disorder but also due to accidents. The objective of our project is to design a 5 DOF robotic arm. It helps the people who can't move their upper arm. The arm should not be of heavy mass as it will increase the torque of the actuators. So it is preferred to design it using lightweight materials. Poly-lactic acid (PLA) filament is a material which has high tensile strength and less weight when compared to other materials. Due to its property, the parts can be fabricated by 3D printer design using SolidWorks.

2 Robot Dynamics

A Robot consists of rigid bodies space (links) connected by joints, and the joints are driven by actuators. The actuators can be hydraulic/pneumatic/electric. It is proposed to use servo motors as actuators which are electrically controllable for position control application. As per the flexibility and reachability of the object, the number of links gets increased. The links are controlled by a servo positioning motor which places the link at the programmed location. The complexity of the robot arm depends upon the number of actuators to be controlled, and it is mentioned as "Degrees of Freedom" (DOF) of the robotic system. The DOF is defined as the number of independent variables that should be specified to locate all parts of the mechanism. The number of joints in the arm determines the degrees-of-freedom (DOF) of the manipulator. In this paper, a 5 DOF serial manipulator with a gripper as an end-effectors is considered for fabrication using 3D printing technology. The end-effector is the part of the arm that does the desired work. Generally, there are two types of joints used in a robot arm. They are Prismatic (P) and Revolute (R). A revolute joint is used for the operation of this robot arm. For calculating the position and orientation of the object in robotic arm kinematics and dynamics of the system is essential.

Kinematics is the science of an object's motion without considering the forces acting on the system. Dynamics is the science of an object's motion by examining the effects causing the changes in the mechanism. In Forward kinematics, the position and orientation of the end-effector relative to the base frame are computed. By providing the joint angles, the arm position can be predicted by neglecting the forces acting on it [9]. The joint angle is a parameter which is the angle between a joint and the reference base frame. Inverse kinematics is the reverse process of forward kinematics.

The position and the orientation of the end effectors are known in inverse kinematics. The joint angles should be calculated, to attain the position and orientation without considering the forces acting on the system. It is mandatory to understand the robot dynamics before the attempt of controlling the end effectors. Any robotic system model needs the knowledge of underlying dynamics to place the arm in the required location. It also helps to design actuators and their inputs that move the link to reach the set value with less overshoot and time consumption.

3 Proposed Methodology

3.1 Kinematic Equations

The coordinate equation of the robotic arm kinematics [10] is given as

$$X = \cos(\theta 1)[a4\cos(\theta 2+\theta 3+\theta 4)+a3\cos(\theta 2+\theta 3)+a2\cos(\theta 2)+a1]$$
$$Y = \sin(\theta 1)[a4\cos(\theta 2+\theta 3+\theta 4)+a3\cos(\theta 2+\theta 3)+d2]$$
$$Z = a4\sin(\theta 2+\theta 3+\theta 4)+a3\sin(\theta 2+\theta 3)+a2\sin(\theta 2)+d1$$
$$\delta = \theta 2+\theta 3+\theta 4$$

where, a – Link length, d – Joint Offset, θ – Joint angle, α – Twist angle

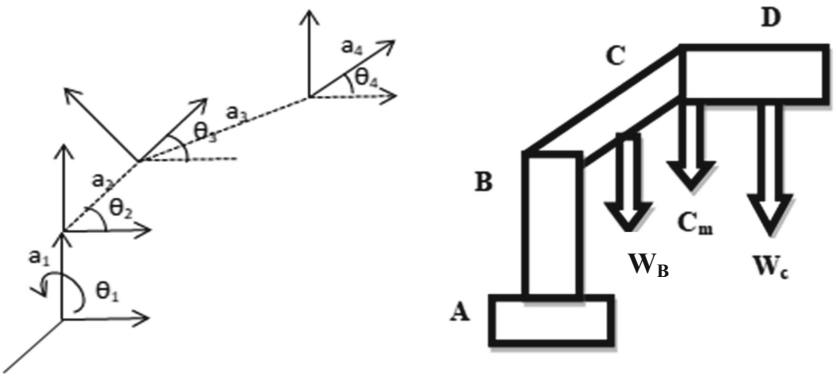


Fig. 1. Coordinate axes at each link of robotic arm and estimated force

In context to develop a 5 DOF robotic manipulator with an end effector, some important parameters are to be considered. The robotic arm can be modeled based on Link length, Joint Angle, Twist angle, Joint Offset. The forward kinematics can be calculated by using the Denavit-Hartenberg convention. The forward kinematics of the robotic arm is predicted using "RoboAnalyzer" software. Table 1 shows the dimensions and angles of various joints corresponding to the length and twist.

4R type serial manipulator is the design which has four rotary joints considering the fifth joint as an end effector. From the forward kinematics, we can find the end-effector position for a set of given joint angles. The inverse kinematics has been developed by a

Table 1. The DH parameters of the manipulator

Joint	Link length (a)	Joint offset (d)	Twist angle (α)	Joint angle (θ)
1	7 cm	1.5 cm	90°	0 to 180°
2	7 cm	1.5 cm	0°	0 to 120°
3	7 cm	1.5 cm	0°	0 to 120°
4	7 cm	1.5 cm	0°	0 to 80°

Table 2. The lookup table for inverse kinematics

S No	The joint angle from base to end effector (degree)	Position of the end effector (cm)	Joint angle δ (degree)
1	θ1 = 0	P(30.5, 0, 0)	0
	θ2 = 0		
	θ3 = 0		
	θ4 = 0		
2	θ1 = 30	P(14.1955, 1.25, 20.33)	90
	θ2 = 30		
	θ3 = 30		
	θ4 = 30		
3	θ1 = 45	P(3.4748, −4.9999, 20.5562)	135
	θ2 = 45		
	θ3 = 45		
	θ4 = 45		
4	θ1 = 60	P(−1.5, −10.825, 14.722)	180
	θ2 = 60		
	θ3 = 60		
	θ4 = 60		

look-up table, such that for a specified end-effector position, the corresponding joint angles are calculated by assuming Cartesian coordinates.

3.2 Torque Calculation

The following parameters are defined for Force Estimation as in Fig. 1.

Length of AB $(L_{AB}) = 12\,\text{cm}$
Length of BC $(L_{BC}) = 5\,\text{cm}$
Length of CD $(L_{CD}) = 10\,\text{cm}$
Weight of link B $(W_B) = 0.030\,\text{kg}$
Weight of link C $(W_C) = 0.030\,\text{kg}$
Weight of motor at C $(C_M) = 0.050\,\text{kg}$
Weight of motor at D $(D_M) = 0.050\,\text{kg}$

The force equation is derived from Fig. 1 as stated in [11],

$$\sum F_Y = (L + D_M + W_C + C_M)g - C_Y = 0$$

Substituting the equation with values as mentioned above, we get: C_Y = 6.174 N

$$\sum T_C = -(W_C * L_{CD}/2) - L(L_{CD} + L_{DE}) - D_M(L_{CD}) + T_C = 0$$

Substituting values, we get T_C = 0.0575 Nm.

$$\sum T_B = (-L)[L_{BC} + L_{CD}] - W_B[L_{BC} + L_{CD}] - D_M[L_{BC} + L_{CD}] + Wc[L_{BC} + L_{CD}/2] - C_M(L_{BC}) - W_B(L_{BC}/2) + T_B = 0$$

Substituting values we get T_B = 0.13375 Nm.

T_B & T_C is the required torque at joint B and Joint C.

4 Simulation Results

The dimensions of the 4R manipulator such as the length of the link, the mass of the link, the joint angle, twist angle, and the joint offset is provided as the input to the software. Based on the input parameters the torque at every joint has been plotted in

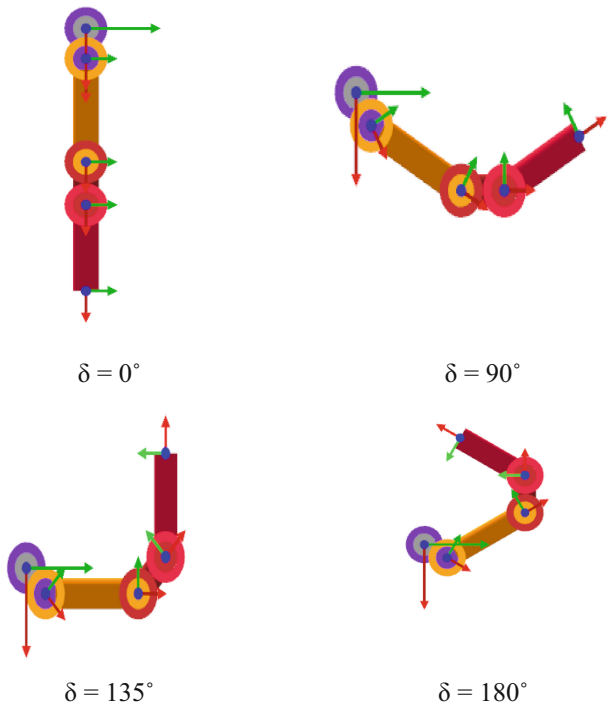


Fig. 2. Position of end effector for various δ value

Fig. 3. The actuators have been chosen based on the torque value. The software package has computed the forward kinematics, forward dynamics, and inverse dynamics. We have calculated the inverse kinematics of the system manually by mathematical modeling. The equations and the frame of reference of every link is in Fig. 1. The manual calculation of the end effector position as in Table 2 correlates with that of simulation result as in Fig. 2.

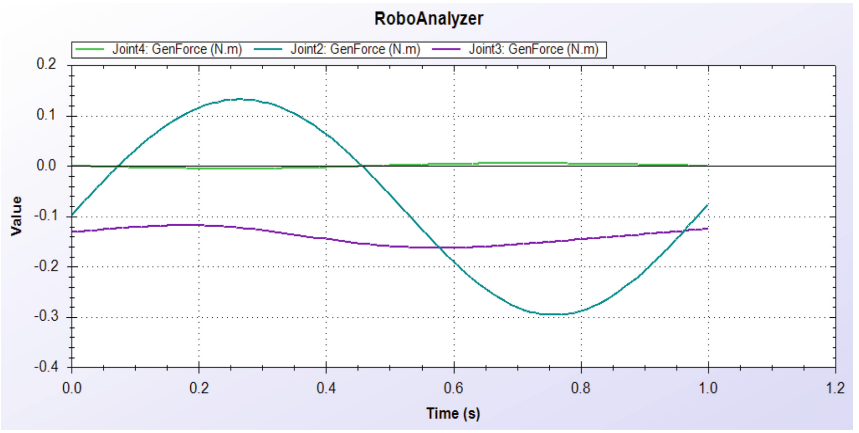


Fig. 3. Measured torque in RoboAnalyzer

The torque prevails in the processing of joints are shown in Fig. 3 that it is close to the predicted value of torque in various locations.

5 Hardware Implementation

The robotic arm design can be fabricated as light weighted and considerably strong enough to lift the load. The advantage of polymers is included in robotic arm parts fabrication. Polylactic acid (PLA) filaments are the lightweight, strong and biodegradable material which can be used in a 3D printer. PLA filaments are organic materials made from sugarcane and cornstarch. The parts of the robotic arm can be designed in Solidworks simulation environment to have various joints and provision for placing servomotor firm into the fitting [12]. Figure 4 shows the sample parts of the arm which can be fabricated using PLA in 3D printing technology.

The fabricated part by PLA filament are comparatively strong enough to withstand the payloads as compared to Acrylonitrile Butadiene Styrene (ABS) [13] shown in Table 3. PLA printed solids can be encased in plaster-like molding materials, then burned out in a furnace, so that the resulting parts can be filled with molten metal. PLA has the second largest production volume of any bioplastic as it is biodegradable. It is also less in weight as compared to steel with reasonable strength.

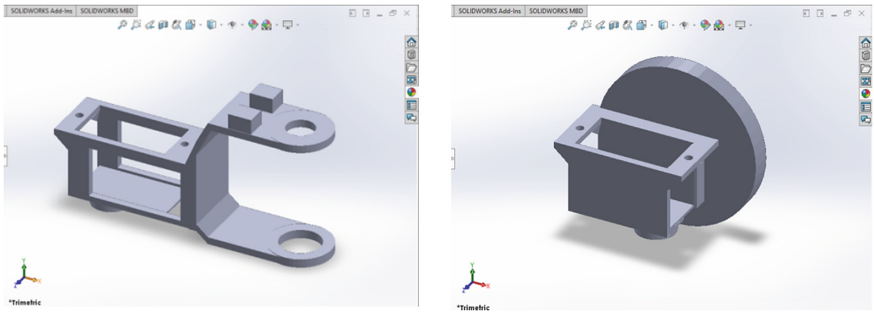


Fig. 4. Solid works design of robotic parts

Table 3. Material properties for robotic arm fabrication

Properties	ABS	PLA	STEEL
Tensile Strength	27 MPa	37 MPa	400 MPa
Elongation	3.5–50%	6%	8.0 to 55%
Flexural modulus	2.1–7.6 GPa	4 GPa	100 to 200 GPa
Density	1.0–1.4 g/cm^3	1.3 g/cm^3	7.9 g/cm^3
Melting point	Amorphous	173°	1370°
Biodegradable	No	Yes	No
Glass transition temperature	105°	60°	0°
Coefficient of thermal expansion	90 µm/m °C	68 µm/m °C	33.75 µm/m °C

Arduino Uno is chosen as the microcontroller for the control of the robotic arm as it is required to drive the four servo motors. The servos can be controlled by a joystick or by an Android app containing slider whose values are transmitted to the Arduino via an HC-05 Bluetooth module. The slider values represent the values to be sent to the potentiometer of the servo motor. From torque calculation, the arm drive torque is calculated in the joints B and C as 0.133 Nm and 0.05 Nm. In order to implement it to hardware the servomotor selection is crucial. The Stall torque of servo MG996R is 0.9218 Nm and for micro servo SG90 is 0.2452 Nm. Hence for making convincing drive 2–3 times higher torque rating is needed to meet the load requirements and withstand overload. So MG996R servo is used at joint Band micro servo SG90 is used at joint C.

The servomotor placed in the slot of the robotic arm can be programmed to operate as per the desired inputs based on the control signal given to the motor. The hardware part contains four servo motors which need to be operated simultaneously to make the end effector to reach the destination point. The Arduino programming should generate a PWM signal of 50 Hz frequency and variable duty cycle of 0–12% as per the datasheet information of SG60 [14] shown in Fig. 5. The duty cycle values for end effector positioning is in Table 4. The control signal needs to be in this range to track the desired trajectory and positioning of the end effector.

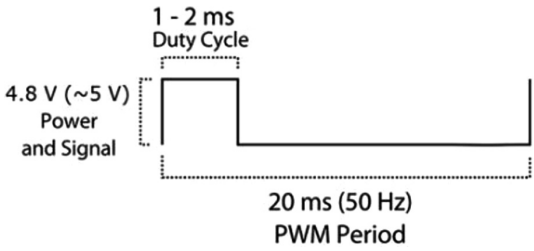


Fig. 5. Servomotor drive frequency and duty cycle

Table 4. PWM signal generation by Arduino for positioning the end effector

Position	Datasheet value	Duty cycle
0°	1 ms	3%
90°	1.5 ms	8%
180°	2 ms	10%

The complete hardware setup is in Fig. 6. It is a prototype model which is fabricated and implemented for test purpose. Each link has been designed in Solidworks platform, and 3D printed using PLA filament of 1.75 mm thickness. The power supply rating is 5 V and 2A adaptor which power the Arduino board and robotic arm. From this, the real implementation is possible by further improvisation.

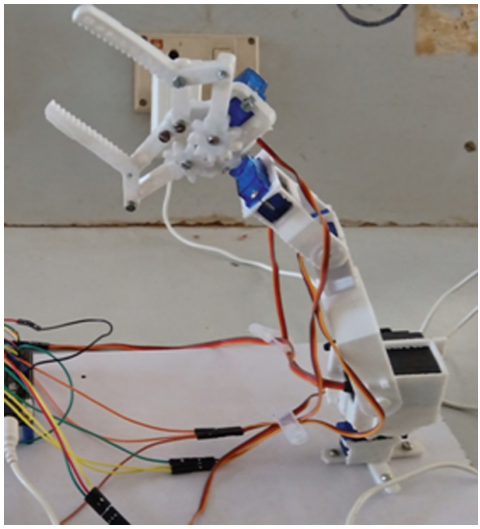


Fig. 6. A prototype model of robotic arm fabricated using PLA filament

6 Conclusion

A robotic arm is designed whose base frame is vertical axis similar to that pick and place operation of the human arm. The prototype model is having lightweight, durable and biodegradable properties by PLA material. It can be fitted in to satisfy the needy people's day to day activities. The position, orientation and motion planning of the robotic arm are performed via RoboAnalyzer software package and validated using Arduino based controller model. In future it may be extended with a realistic model of the human arm and the control may be automatic with the proper selection of sensors and signal processing.

References

1. Chung, C.-S., Wang, H., Cooper, R.A.: Functional assessment and performance evaluation for assistive robotic manipulators: literature review. In. J Spinal Cord **36**(4), 273–289 (2013)
2. Roger, V.L., Go, A.S., Lloyd-Jones, D.M., Adams, R.J., Berry, J.D., Brown, T.M., et al.: Heart disease and stroke statistics—2011 update: a report from the American Heart Association. Circulation **123**(4), e18–e209 (2011)
3. Yildiz, I.: A low-cost and lightweight alternative to rehabilitation robots: omnidirectional interactive Mobile robot for arm rehabilitation. Arab. J. Sci. Eng. **43**, 1053–1059 (2017)
4. Chen, X., Zhao, B., Wang, Y., Xu, S., Gao, X.: Control of a 7-DOF robotic arm system with an SSVEP-based BCI. Int. J. Neural Syst. **28**(8), 1850018 (2018)
5. Bouteraa, Y., Abdallah, I.B., Elmogy, M.A.: Training of hand rehabilitation using low cost exoskeleton and vision-based game interface. J. Intell. Robot. Syst. 1–17 (2019)
6. Williams, M.R.: A pilot study into reaching performance after severe to moderate stroke using upper arm support. PLoS One **13**(7), e0200787b (2018)
7. Liang, X., Cheong, H., Sun, Y., Guo, J., Chui, C.K., Yeow, C.-H.: Design, characterization, and implementation of a two-DOF fabric-based soft robotic arm. IEEE Robot. Autom. Lett. **3**, 2702–2709 (2018)
8. Raza, K., Khan, T.A., Abbas's, N.: Kinematic analysis and geometrical improvement of an industrial Robotic arm. J. King Saud Univ.-Eng. Sci. **30**, 218–223 (2018)
9. Spong, M.W., Hutchinson, S., Vidyasagar's, M.: Robot Dynamics and Control, 2nd ed. Wiley Publication (2004)
10. Feng, H., Yin, C.-B., Weng, W.-W., Ma, W., Zhou, J.-J., Jia, W.-H., Zhang, Z.-l.: Robotic excavator trajectory control using an improved GA based PID controller. Mech. Syst. Signal Process. **105**(15), 153–168 (2018)
11. Elfasakhany, A., Yanez, E., Baylon, K., Salgado's, R.: Design and development of a competitive low-cost robot arm with four degrees of freedom. Mod. Mech. Eng. **1**, 47–55 (2011)
12. https://www.thingiverse.com/thing:38875
13. https://www.3dhubs.com/knowledge-base/pla-vs-abs-whats-difference
14. http://www.ee.ic.ac.uk/pcheung/teaching/DE1_EE/stores/sg90_datasheet.pdf

IoT Based Landslide Disaster Management System

P. S. Muhammed Sajith, Vandana Nair, Venkatesh Pillai Suresh(✉), and Arun Madhu

Computer Science and Engineering, Saintgits College of Engineering, Kottayam, Kerala, India
sajith20l2ps@gmail.com, vandananairlll@gmail.com, venkateshp.suresh@gmail.com, arun.madhu@saintgits.org

Abstract. A landslide can be termed as the movement of a mass of rock, debris or earth down the slope, when the shear stress exceeds the shear strength of the material due to factors like accumulated rainfall, moisture or a wide range of ground movements. The local people who are living near the hilly areas are the ones that will be affected by this disaster as they have no time to react at all. It causes death, injury and property damage and adversely affects a variety of resources. Efforts to measure and to monitor potential landslides are required to ensure human safety and to protect civil infrastructure. Proper monitoring and awareness can help in saving lives and reduce property damage. The recent floods in Kerala, India caused numerous Landslides which lead to many deaths and major destruction in the mountain regions of the state. Kerala, India is very much vulnerable to landslide hazards. Existing methods include manual inspection using surveying equipment such as electronics distance measurement (EDM), levels, theodolites and total stations. The aim for our project is to develop a system using IoT to inform human individuals about potential landslides automatically, if any pre-failure slope deformations are identified. It uses a network of IOT that helps in updating the information about landslide on the Android App. Moisture Sensor, Vibration Sensor and Accelerometer are employed in the system that detects landslides as some critical values will be set for these sensors. If the value exceeds these critical values, then people will be notified the forthcoming landslide and huge loss can be prevented. So, this telemetry project helps to make the residents aware about the forthcoming disaster and can help to tackle the situation better. The fundamental concern of this project is to build up an early landslide warning system while using minimum resources without yielding on the efficiency of the unit.

Keywords: IoT · MQTT · Cloud computing wireless sensors

1 Introduction

Landslides are disasters that occur naturally in a short period due to the variations in environmental actions. It causes huge threat to human lives, property damage and damages to the properties of agriculture. In India, there are several places which are much prone to landslides. Usually, landslides occur during rainy season as part of other

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 660–667, 2020.
https://doi.org/10.1007/978-3-030-37051-0_74

natural disasters like earthquakes, floods and volcanic activities. So here arises the need of landslide detection and alert system. Technology based on IoT has the ability of real-time detecting of landslide losses and large-scale deployment. Network based on IoT helps to detect the slope instability or even the modest movements of ground. In a few cases, human exercises and extended improvement, for example, deforestation and changed inclines of land, can expand the events of landslide. We plan to utilize the remote wireless sensor arranges in the landslide inclined regions for evaluating the opportunity of event of landslides. Remote wireless sensors are one of the innovations with huge progressions that can rapidly react to quick changes of information and send the detected information to an information observing centre by means of cloud. Sensors are much simple for establishment, which can be situated legitimately upon the land body, or in the environment, to give ongoing information on the landslide activity. The main goal of the project is to make people aware about the forthcoming disaster and thereby enhancing the daily life which comes to a stop at whenever a landslide occurs in their place of occupation using the IoT technology. The system is capable of providing intimation to the rescue operators with proper details of the spot so that required rescue operations can be carried out without any delay which results in an efficient disaster management. It also allows decisionmakers to take measurements for the protection of the citizens.

- The goal of the project is to make people aware about the forthcoming disaster and thereby enhancing the daily life which leads to a stop whenever a landslide occurs in their place of occupation.
- Provides information to the rescue team with proper details of the area.
- Helps in efficient disaster management.

2 Related Works

Various authors have discussed and proposed several landslide detecting techniques using the modern technologies.

According to the publication [1] this research focuses on alerting the general population here various IoT sensors are used for detecting any kind of change in the ground movement. The accelerometer can easily detect horizontal as well as angular movements. It would detect small as well as the abrupt changes in the area around the sensor. The user would also be able to send a message or call the disaster management authorities in case of any kind of query and they would be able to interact with the authorities for sufficient help.

According to the publication [2] this paper makes use of a network of IoT that helps to update the information regarding landslide on the internet. Vibration sensor and Moisture Sensor are used to detect landslides based on the pre-defining the threshold values of the sensors, if the value exceeds these threshold values, then people will be notified about the forthcoming disaster and huge loss can be limited to an extent. Raspberry Pi takes the data and updates the information onto the webpage by using a MQTT protocol.

According to the publication [3] findings it is not hard to recognize the power of wireless sensor network used for real-time monitoring system. In previous work WSN is one of the surfaced-up areas which are widely being used for the expansion of real-time monitoring system. This paper discusses about advancement of a wireless sensor network to detect landslides, which combines development and design of WSN for real-time monitoring system.

In this paper three monitoring techniques are used. According to the publication, this paper proposes a disaster the board framework and departure framework for individuals, utilizing Google Maps [4]. Here the users with android device having the android application installed can register the multiple receiver or family member or friends to send SMS at a time to send notification for help. An additional feature sends the current position obtained by the GPS and including shortest path of shelter or safe zone on the map of the application.

3 Proposed System

The main purpose of the proposed framework is to build up a real-time detection of landslide factors and also to create an android application whereby users can receive the alert information on time. Whenever landslides occur, the prime issue is the delay occurred in addressing the local people residing in remote areas and the concerned departments about the forthcoming landslide alert. Manually passing the alert messages consumes a prime amount of valuable time as the information needs to be passed from one department to the other and in-between if any loop hole occurs, may lead to severe damage [5]. Hence, there is an utmost need for creating a system that can immediately detect slope deformations and send simultaneously alert notifications to everyone concerned with no man power required. To satisfy the requirement, the automatic landslide alert unit is developed. The system is designed to inform human individuals about potential landslides automatically, if any pre-failure slope deformations are identified. It uses a network of IoT that helps in updating the information about landslide on the Android App [6]. The sensor module and a transmitting unit are used for remote correspondence. The obtained information is sent to the IoT server where these values are stored. Warning sensors are installed at remote location which will get activated when sensors values exceed prescribed limit [7]. All sensor modules are connected to the Arduino Nano Controller. Vibration sensor is interfaced digitally, moisture sensor is coupled to the analogue port of the controller and the accelerometer uses I2C interface to the microcontroller [8]. The data collected from sensors are sent to the Raspberry Pi Zero-W from which the sensor values are transmitted wirelessly using the inbuilt Wi-Fi module to the IoT Cloud (Fig. 1).

From the Raspberry Pi we use MQTT protocol to send the values received directly to the Cloud. The data uploaded is then collected by the Android Application, where alert & sensor data are displayed by comparing it with the previously defined threshold values. If the values obtained from the sensors are above the particular threshold limit then an alert message is sent via the app also a text message is sent to the user [9]. We have divided the alert in two phases an Orange Alert and a Red Alert for the people to take precautions and to move to relief camps. The app also shows the exact location

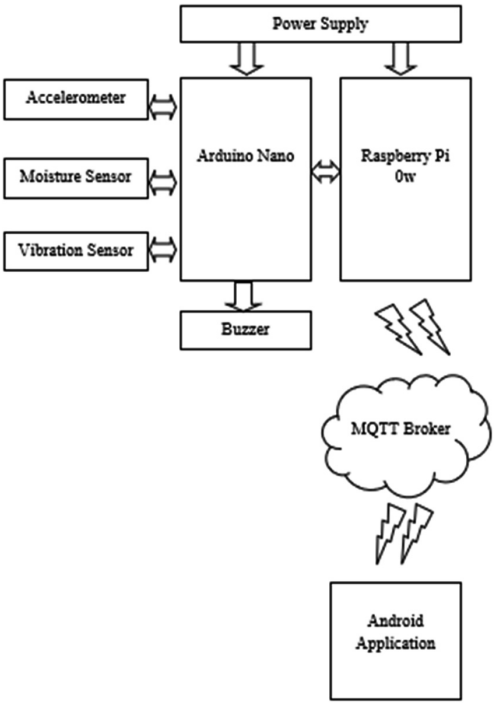


Fig. 1. System architecture

coordinates of the landslide detected area and it also features a list of helpline numbers to call in case of emergency. Also the buzzer is connected to Arduino to give a local alert to nearby people indicating occurrence of landslide by setting off an alarm.

4 Hardware Description

The major hardware requirements of the system are:

4.1 Soil Moisture Sensor

The Soil Moisture sensor includes one pair of probes that is inserted inside the soil. When current pass through the probes the level of the resistance is known. The sensor uses 2 probes that will read the resistance to get the moisture level. The output of the moisture senor is an analogue value that is joined to one of the analogues to digital port available in the microcontroller.

4.2 Accelerometer

Accelerometer MPU 6050 is implemented here. The sensor senses whether there is any movement in the angle of sensor if so, it sends the data of movement of angle to the

corresponding receiver side. The MPU-6050 devices integrate a 3-axis accelerometer and a 3-axis gyro meter on the same silicon dye. It is placed on the soil or land and if any movement occurs then the sensor detects it and transmits data so that an alert can be send via the app.

4.3 Vibration Sensor

Vibration module depends upon the vibration sensor and Comparator to detect if there is any vibration beyond the threshold set. The On-board Potentiometer is used to balance the threshold value. It occupies a 15 mA rated voltage and a 3.3 V–5 V output, digital output switching (0 and 1) a bolt sized hole for ease in installation with small board PCB having dimensions: 3.2 cm $\times$ 1.4 cm using wide voltage compactor LM393.

4.4 Arduino Nano

Arduino Nano is designed to be a compact, compete and breadboard-friendly board based on the ATmega328P. It is similar to the Arduino UNO but has a slightly different package. It makes use of a Mini-B USB cable. Input Voltage is 5 V, and consists of 14 V digital I/O pins and 8 analogue input pins.

4.5 Raspberry Pi Zero-W

Raspberry Pi Zero-W has an inbuilt WIFI module, Bluetooth hence it is ideal for IoT projects with embedded connections. It is designed to be compact and flexible with mini connectors and 40-pin GPIO. The main powerhouse on the Pi is the 1 GHz BCM2835 single-core processor with 512 MB RAM. Raspberry Pi Zero-W is 4 times efficient and faster than the original Raspberry Pi version but is only a fraction of the cost of the present RPI3.

5 Software Algorithm

The system monitors continuously for movements inside the earth and checks for any pre-failure slope deformations are identified. The sensor module detects soil movements, and variations in soil and furthermore would publish the data to the server using in-built WIFI module in the Raspberry Pi Zero-W [10]. From the Raspberry Pi we use MQTT protocol to send the values received at the transmitting end directly to the Cloud. The data uploaded is then collected by the Android Application, where alert & sensor data are displayed by comparing it with the previously defined threshold values. The system again monitors for land movements and moisture content to check whether landslide will occur [11]. If the values obtained from the sensors are above the particular threshold limit then an alert message is sent via the app & also a text message is sent to the user's cell phone. We have divided the alert in two phases an Orange Alert and a Red Alert for the people to take precautions and to move to relief camps in case of a landslide development [12]. The app also shows the exact location coordinates of

the landslide detected area and it also features a list of helpline numbers to call in case of emergency (Fig. 2).

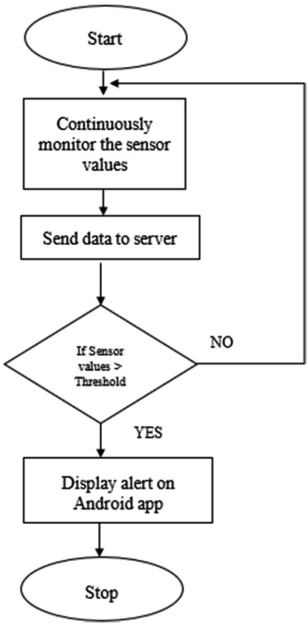


Fig. 2. Flowchart of the proposed system

6 Result and Analysis

The proposed setup of the Landslide Disaster Management is shown in Fig. 3. As soon as any pre-failure slope de-formations occurs the sensor unit of our system is triggered. When the vibrations and the soil moisture exceed the safety critical value at any time, an alert message is sent to the android application as well as a local alarm is set off. Vibration sensor is interfaced digitally, moisture sensor is connected to the analogue port of the controller and the accelerometer use I2C interface to the microcontroller. The sensor module senses soil movements and variations in the moisture content and transmits this data real time to Raspberry Pi, which then collects the data payload and publish to the MQTT host address. The information is published as a separate topic to which our Android Application is a subscriber. The information is then gathered by the Android Application, where alert and sensor information are shown by comparing it with the pre-defined threshold values. If the values obtained from the sensors are above the particular threshold limit then an alert message is sent via the app and also a text message is sent to the user's cell phone (Fig. 4).

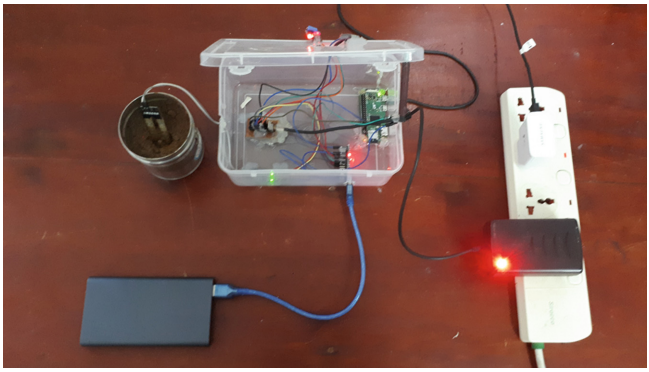


Fig. 3. Basic hardware setup

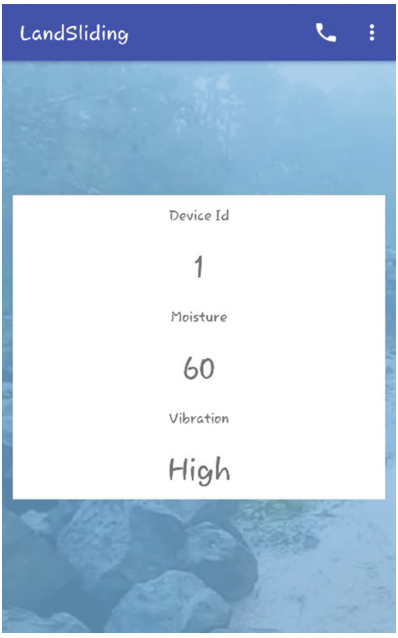


Fig. 4. Home screen of application

7 Conclusion and Future Work

In this paper, we implemented an automated landslide monitoring and warning system using minimum resources that would alert the users about the forthcoming disaster and also give proper location coordinates of the area to the proper authorities via the App. In future, we propose to further improve the method of disaster management by

including seismic activity detecting modules to predict occurrences of earthquakes that may occur and notify the people in advance.

References

1. Kapoor, S., Pahuja, H., Singh, B.: Real time monitoring & alert system for landslide. In: 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, pp. 584–589 (2016)
2. Eknath, J.K., Dashrath, N.A., Pandurang, S.V., Dinkar, R.S.: IOT based landslide detection and prevention system. Int. J. Adv. Res. Innov. Ideas Educ. **4**(2), 692–696 (2018)
3. Sofwan, A., Ridho, M., Goni, A.: Wireless sensor network design for landslide warning system in IoT architecture. In: 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, pp. 280–283 (2017)
4. Sarah, S., Dilip, M., RahulAravindh, R.: Disaster alert and notification system via android mobile phone by using Google map. Int. Res. J. Eng. Technol. (2016). 2395-0072
5. Bhandari, K.S., Tated, K.S.: Landslide monitoring system based on Wireless Sensor Network. Int. J. Mod. Trends Eng. Res. (IJMTER) **2**(7), 2349–9745 (2015)
6. Chen, Y., Chen, J., Hsieh, S., Ni, P.: The application of remote sensing technology to the interpretation of land use for rainfall-induced landslides based on genetic algorithms and artificial neural networks. IEEE J. Sel. Top. Appl. Earth Obs. Remote. Sens. **2**(2), 87–95 (2009)
7. Atzeni, C., Barla, M., Pieraccini, M., Antolini, F.: Early warning monitoring of natural and engineered slopes with ground based synthetic-aperture radar. Rock Mech. Rock Eng. **48**, 235–246 (2014). https://doi.org/10.1007/s00603-014-0554-4
8. Federico, A., Popescu, M., Fidelibus, C., Internò, G.: On the prediction of the time of occurrence of a slope failure: a review (2004). https://doi.org/10.1201/b16816-144
9. Hassan, Q.F.: A low-cost IoT framework for landslide prediction and risk communication. In: Internet of Things A to Z: Technologies and Applications. IEEE (2018)
10. Li, T., Tian, Y., Xiao, C., Zhao, W.: Slope location-based landslide vulnerability assessment. In: 2013 21st International Conference on Geoinformatics, Kaifeng, pp. 1–4 (2013)
11. Wenlong, Z., Qing, G., Baoshan, L.: Design of landslide warning system. In: 2011 Third International Conference on Measuring Technology and Mechatronics Automation, Shangshai, pp. 974–977 (2011)
12. Lira, C., et al.: Automatic detection of landslide features with remote sensing techniques: application to Madeira Island. In: 2011 IEEE International Geoscience and Remote Sensing Symposium, Vancouver, BC, pp. 1997–2000 (2011)

IOT Based School Bus Monitoring System With Child Security

Sandeep Seetaram Naik[1], T. G. Harshitha[1], H. D. Spoorthy[1], B. S. Vedashree[1], G. S. Samrin Taj[1], and P. Vetrivelan[2(✉)]

[1] Sai Vidya Institute of Technology, Bangalore, India
avva.sandeep@gmail.com, harshithatg2015@gmail.com, spoorthy228@gmail.com, vedashreebs21@gmail.com, samrinsrys67@gmail.com
[2] VIT, Chennai, India
Vetrivelan.p@vit.ac.in

Abstract. In recent days, parents are discomfit about their school going children as kidnapping cases of students has been increasing from day-to-day. It is very important for every school to have an incorruptible and reliable transport service to make sure that the students are safeguarded. Nowadays students wait for a longer time for their school bus arrival standing near roads which is unsafe for them. Even though there are some of the technologies to ensure the safety of students, they were not able to provide abundant information to parents. Without their notice, they might exit at wrong stops. To reduce parent's uneasiness about their school going children, this project presents the evolution of a school bus monitoring system which provides information about location, speed and bus arrival prediction time. It also identifies student's location within the school campus. This is done through the technology – (IoT) Internet of Things. Tracking of school bus is done by GPS (Global Positioning System) technology. The system alerts parents by notifying them. This is achieved through GSM (Global System for Mobile applications). RFID (Radio Frequency Identification) identifies unique id given to each individual. The bus track system provides solution for tracking school bus on smart phones. Also an algorithm is implemented to calculate the arrival time of the bus in addition to tracking. The information can be accessed by parents through mobile application and they can continuously monitor their child.

Keywords: IoT · RFID detector · GSM · GPS

1 Introduction

Child security is the biggest problem nowadays, school management and parents are worried about the lack of children's security. This child security system full fill all security gap and gives the better service. RFID MFRC522 reader is used to identify each student by reading the unique ID from the card and is being placed with RFID tag. Raspberry Pi can also be used, but it's been neglected in this system since it is expensive. Since HTTP connection is not encrypted this system is unsecured and is vulnerable to hacking [1]. GSM is used to send message to parents whenever student

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 668–678, 2020.
https://doi.org/10.1007/978-3-030-37051-0_75

enters and exits the bus. Parents are also alerted through short message if the school bus scheduled route is changed. The paper does the integration of both hardware and software. Hardware module includes tracking system and software module includes Kalman filtering algorithm and android application. Core part of tracking device is Arduino Mega Microcontroller which is used to control the tracking system of the school bus. This GPS (Global Positioning System) provides high accuracy and gives exact geographic coordinates anywhere on Earth. 100% accuracy is not possible using a single algorithm and it is been found that accuracy can be enhanced by using other algorithms like machine learning algorithm [2]. Even though there are many problems arising day by day, considerable attempt is not been done to overcome the existing problems. The paper presents the school bus monitoring system with local constraints and speed sensors using IoT (Internet of Things) architecture. The system has used MQTT (Message Queuing Telemetry Transport) to extend internet in order to reach sensors connected which intern helps to transmit information likes location and speed through data packets. Global communication is provided over IP from Internet of things. The format called EPC Pure Identity URI is used to identify each object in the world uniquely [3]. The model consists of different modules such as RFID module, OBD module, sensor and a mobile hotspot. Initially, the data collected i.e., temperature and humidity is fed to the microcontroller. Later OBD collects the real time data and sends to the microcontroller using an interface called RS-232 interface. OBD/CAN is directly interfaced with bus and conveys information to the server using 3G/4G connectivity and MQTT. OBD module collects real time data and transmits to microcontroller. Whenever student enters and leaves the bus arduino microcontroller captures a record with time and date [4].

To transmit huge amount of data, electronic control system and unit display is placed inside the bus. CAN (Control Area Network) is used widely in automotive internal network since it is highly stable and of low cost. Transmission is done whenever mailbox has the highest priority and transmits when CAN bus is idle. STM32 processor is responsible for exchange of data between the whole CAN (Control Area Network) and even the world outside [5]. In the period 1994–2001, 360 children were injured or killed by school transportation when travelling from and to school. Based on the workshop conducted with the experts invited, outcome resulted in choosing driver support system. The aim of this paper is to take next step towards improving school bus transport system. In order to have a safe view of school transportation from door to door, this system aimed to have a holistic approach. Holistic approach optimizes the bus route plans and can re-route if there are any traffic issues [6]. The proposed smart bus tracking system helps in estimating the arrival time of the bus by scanning QR codes (Quick Response code) placed at bus stops. By scanning this code, we can also view the current location and route of bus on the map. An algorithm called C4.5 is used to calculate bus arrival time so that waiting time of passenger's is minimized [7]. The design of transportation system for people more reliable who depend on public transportation as people will be in a hurry to reach their place. As soon as the central server receives coordinates from the GPS, bus arrival time is predicted by applying algorithm using speed pattern. Location of bus is represented by green mark and red marker indicates the location of passenger. With respect to bus stop and bus's current location, arrival time of the bus is predicted [8].

Tracking vehicle device which mainly uses the service called SMS (Short Message Service). This model sends information to mobile phones through SMS about the coordinate (location coordinate) whenever request is sent. Using the application such as Google map vehicle tracking is done by integrating both GPS (Global Positioning System) and GSM (Global System for Mobile Applications). Use of Internet (software) helps in viewing the distance travelled, exact location of the bus and the speed in which it is travelling [9]. For RFID security and work, an algorithm is implemented and is enhanced between tag and reader. The use of RFID is limited by security concerns and delay is standardized [10]. Radio nodes of low power tags and readers are introduced to catch the number plates on highways. The tag which is away from RFID reader within the range of 80 m tend to transmit the ID through channel of RF by using a scheme called novel collision avoidance scheme [11]. RFID distributed antenna array system has been demonstrated by the use of 2*2 planar antenna [12].

The system explains low cost school bus monitoring system which tracks location, speed and other information. Tracking is done by taking into account the geographic coordinates from GPS which is placed in a bus. RFID reader reads RFID tag and alerts parents by sending notification. Ublox 6M GPS is used in this paper to monitor the bus continuously and real time location, speed, route of the bus is being frequently. These emerging systems have failed to provide abundant information. Some are too expensive also. Our proposed system ensures the safety of each student by giving unique id number, once the student enters the bus RFID reader reads the id placed in each students tag and sends the information to the microcontroller. The information can be accessed by parents through mobile application and they can continuously monitor their child anywhere at any time. Message is been transmitted through GSM (Global System for Mobile application). This system not only has the feature of tracking the bus, speed, predicting arrival time of the school bus. There is also an advantage that, if parents want to know their student activity at any instant time, they can watch them with the help of CCTV which is located in the school campus. Parents will also be notified if the bus is delayed from the scheduled timing. All the information will be stored in predefined database.

2 Architecture of School Bus Monitoring System

Figure 1 shows the block diagram of school bus monitoring with RFID detector system. We have placed RFID detector in the door of the bus. This RFID detector is connected to the controller; we read the data of RFID with the help of SPI communication. Once any student with the unique ID enters the bus, RFID detector will detect the card. In this process card is a passive device, RFID detector is an active device. Continuously it will transmit the signal with the help of transmitter, if the same signal falls on the card it will be reflected back. With the help of receiver we can collect it and send it to the controller.

Power supply to the RFID detector is given with the help of controller. Once the RFID data is collected, that should be identification. For the identification, the same unique number starts comparing with the previously stored data which is placed in a database. To fetch the database data, the controller need to be given the signal through

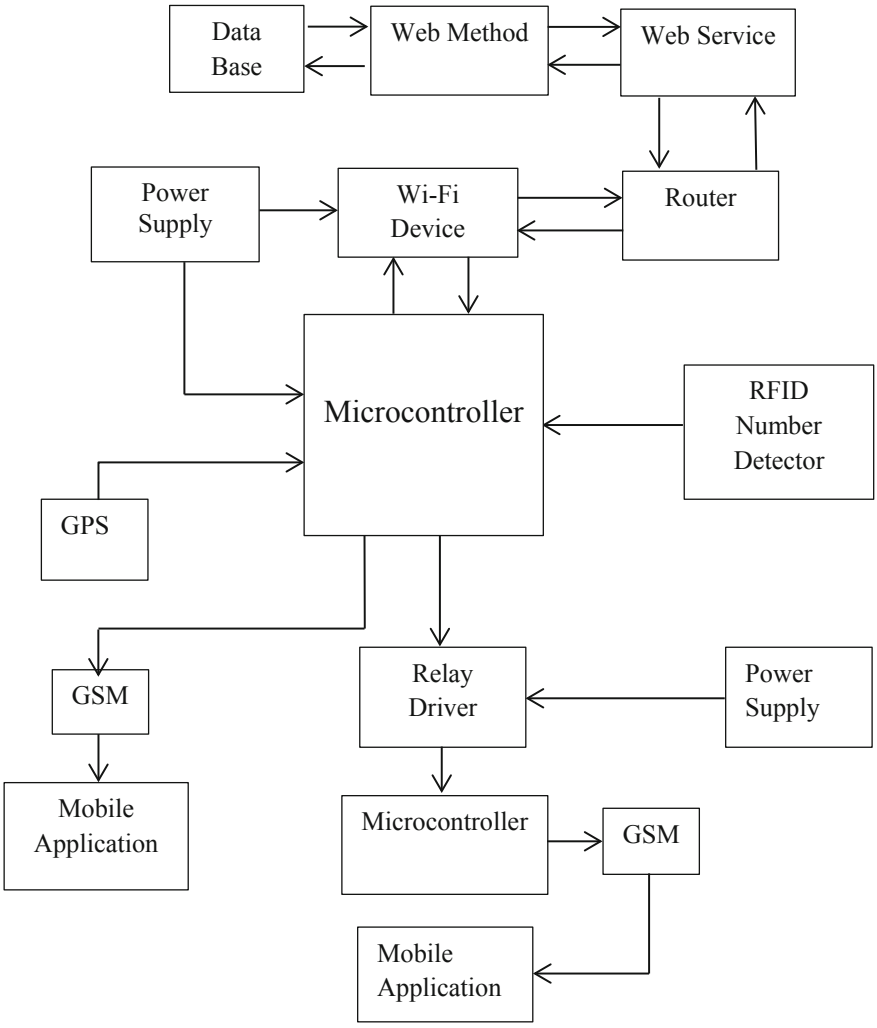


Fig. 1. School bus monitoring with RFID detector system

Wi-Fi device to the particular website which is already defined and stored in a controller. Once the website has been detected by the controller, it will ping the database with the help of web services and start fetching the data present in database.

Once any data match was found, controller can be able to recognize the unique ID which is passed through the door and it will send the message to parent with the help of GSM model. If the same unique ID is detected second time, the controller is already known that the same card is passed through the door. It will send the message to parent saying that the particular person has been de-boarded the bus. It will not only do the job of detection of RFID number, it will also do the job of detection of location with the help of Ublox 6M GPS model. Here, we have found the latitude and longitude of

particular bus with the help of GPS. With the help of latitude and longitude, we can identify where the bus is located. If the bus is 3 stop before the destination of any particular parent, GSM module sends message to parents. While doing this process, controller need to know the number of parent related to that particular place. This can be identified with the help of database. Once the location has been traced, controller will start fetching the data of parents. Once all the data of parent got fetched, then controller will send the message to particular parent number.

3 Integrated Model of Child Monitoring System

Figure 2 shows the block diagram for integrated model of live video streaming child security. This system not only helps to detect the boarding and de-boarding of the student into the bus, it also helps us to monitor student within the school premises. To do the above job camera need to be connected to the controller, we collect the data from the camera and send it to the online application for live video streaming.. ESP32 is used to provide the connection between blynk software and the controller. ESP is driven by relay switching device which intern is driven by the controller where GSM is connected. Once any parent want to see their child inside the school campus, they should go to the application which is running online and ping the nearby router with the help of student unique ID. Once ESP got pinging from any website, it will start searching for the unique ID placed near the controller. Then it will be connected to the camera nearby the student and will give live streaming to parents. If ESP is not able to find the unique ID surrounding it, it will transfer the call from first ESP to next ESP. The process will go on until the student is found in the campus. If student is not at all found, then automatic message is generated from the application and the same is sent to the guardian present in the school as well as the school principal.

4 Algorithmic Flow

4.1 RFID Detection System

Figure 3 shows the algorithm flow of RFID detection. Initially all systems are in switch off mode. Once the bus is in ON condition, it will activate the controller. Controller will come back from sleep mode to switch ON mode. It will not only switch ON the controller, it also switches ON the devices connected to the controller and power is ON with the help of GPIO pins. RFID detector is waiting for the RFID unique number present on any card. With the help of SPI it will take the data from RFID, makes string of data, compare the same data with previously stored data. If the detection is from first time, increment the detection value by one.

As the comparison got over, identify student name, unique ID and send the message to parents saying that student boarded the bus by fetching the parent information from database. If the RFID number detection is second time, do the process same as that of the previous, make RFID detection count to zero. Then send the message saying that student de-boarded the bus.

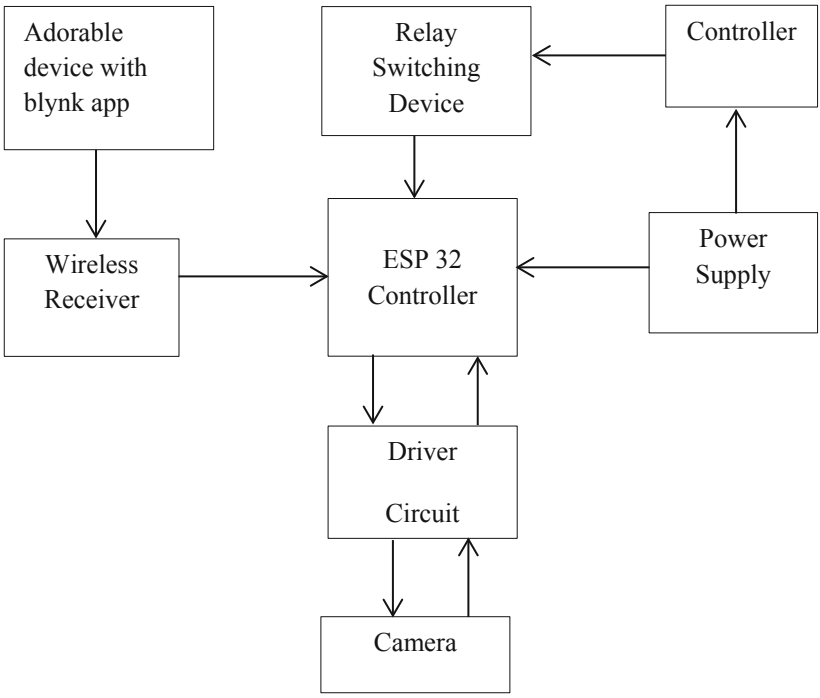


Fig. 2. Integrated model of school bus monitoring system

4.2 Bus Location Tracking System

Figure 4 shows the flow chart of algorithm flow of bus location tracking and sending the message to parents before 3 stops as we discussed in the earlier discussion once the bus is ON. When GPS gets switched ON, it will collect latitude and longitude of the bus position and the same latitude and longitude have been compared with the Google map data by fetching the information from the Google map. Once the bus location got spotted, it will start sending the message to parents with the help of GSM model before 3 stops. To send the message to parents, it needs to be known the information of the parent mobile numbers which is stored in the database. First it needs to fetch the information of the parent mobile number and send the same information to the controller. It will help to send message to parents saying that bus has been reached to the particular place and bus will reach the next 3 stage by predicted times.

5 Result and Discussion

Experimental set up has been constructed in the lab for execution and appropriate output. Initially, it needs to identify the location, for that purpose we used Ublox 6M GPS model. In this model we can accurately get the latitude and longitude of present location wherever the model is placed. For the initial setup, GPS is connected to

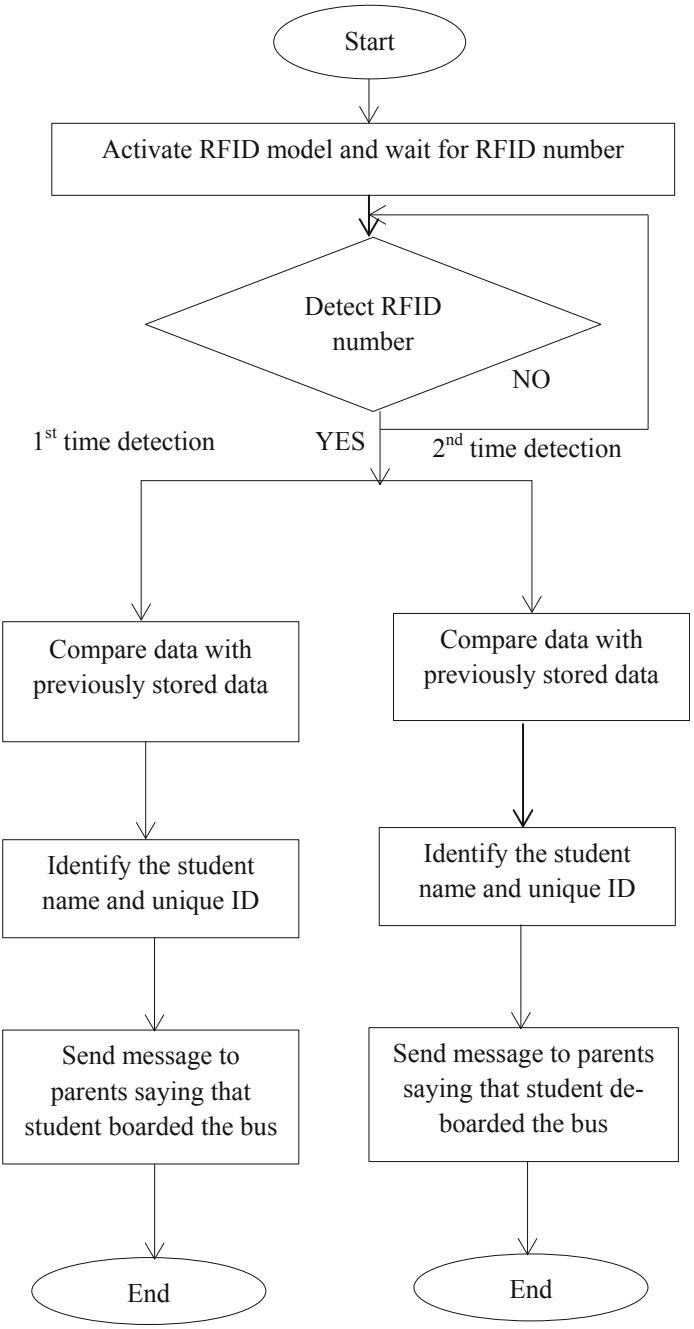


Fig. 3. RFID detection system

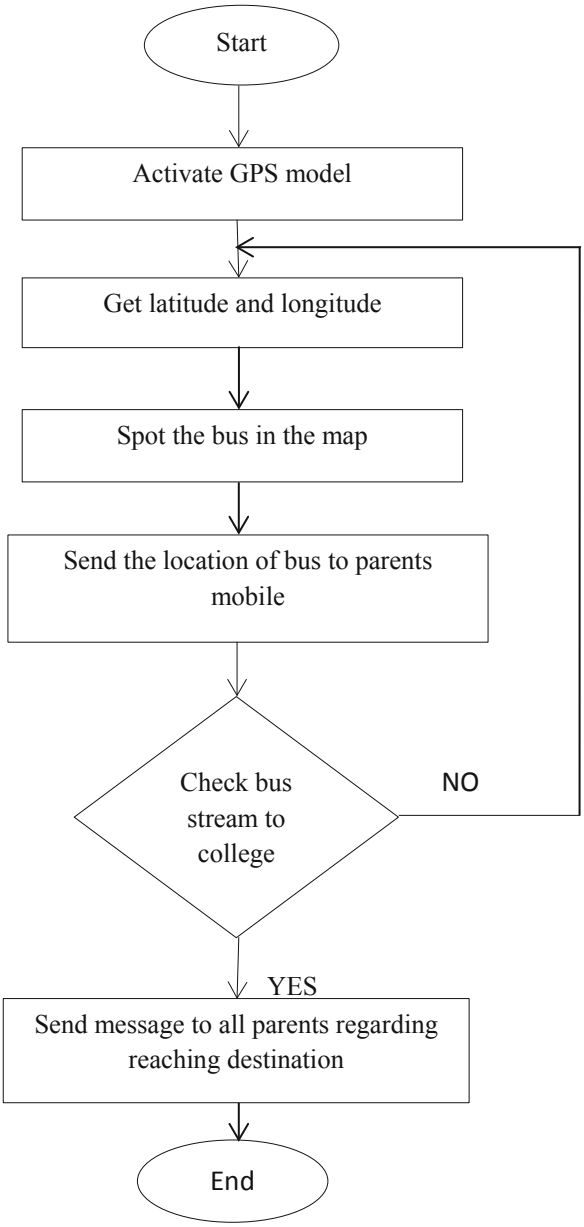


Fig. 4. Bus location tracking system

Arduino to get latitude and longitude with the help of serial UART communication method. Once we start obtaining the location with the help of latitude and longitude, GPS is integrated with the school bus and start taking the various location latitude and longitude wherever the bus path will move.

After taking the data's, we started storing the latitude and longitude details in web database so that whenever GPS will go to the same location that latitude and longitude will get ping by the present originated data. Our next job is to send the message to the concerned person. In this experimental model it is decided to send message to concerned person before 1 km to the boarding point. To do this job, initially we need to upload the mobile number of the concerned person in a same place where the latitude and longitude will be located. According to the latitude and longitude, parallel we assign the number. Now, we integrated the GSM model with the GPS model and the arduino and start testing the result. While testing, initially GSM model start sending the latitude and longitude location to the concerned mobile number which cannot be identified by the common people. To overcome this problem and simplify the application in the backend, for the particular latitude and longitude we have only assigned the location and the same will be assigned to the parent mobile number. Once after this, parents start getting the message of the exact location of the bus and they can track the bus on Google Map. Figure 5 shows one of the location obtained and placing the arrow mark on the Google integrated map with GPS and GSM model.

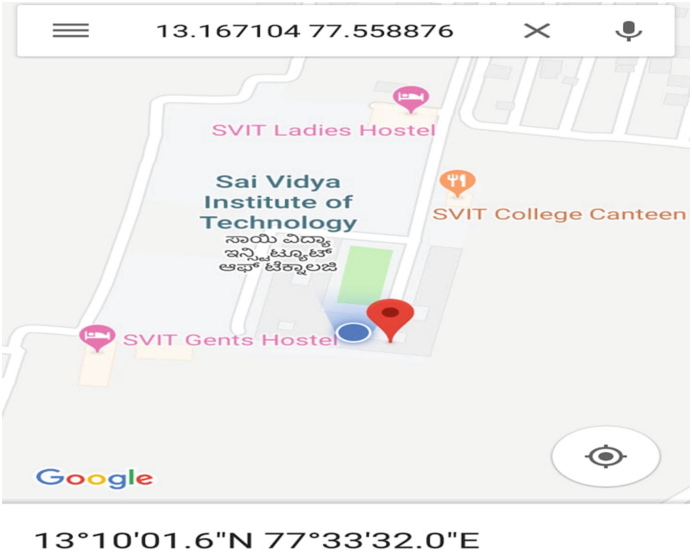


Fig. 5. Tracking location of the bus

The bus tracking as well as child monitoring system will help to increase the security but inside the campus it is not possible to track the student until and unless student identification is pin to the local web server with the help of nearest router. With the help of this system we can able to track the student inside the campus by locating the students on the map of the school structure. But this system cannot able to give the live streaming video to the parents or else to the management of school the design system we adopted the live video streaming technology to monitor students inside the

campus by the parents as well as the school management to do above process initially we use the three camera at the different places and the camera is connected to ESP32 controller.

This project integrated the blynk software for the application of live streaming. Initially we set the very high bandwidth or else the data rate for the live video streaming and sent a video call request from the parent mobile number with the help of blynk software successfully student place got identified with the help of unique RFID passive card and nearby camera automatically switched on and provided the live video streaming. Figure 6 shows the graphical representation of various protocols and the time of maintaining video streaming. To check the continuous process instead of providing high power bandwidth we reduce the bandwidth 4G sim to 3G and continued the process even with the help of 3G we got a video streaming of two minutes average and maximum up to five minute without any destruction. Next process is to change the 2G sim to 3G and check the video streaming for very low data rate the video streaming were started with lot of destruction and call has been disconnected with lesser than 15 s by this we found that we can able to get the live streaming of video using 2G and 3G sim. Next process is to check with the help of Wi-Fi by varying the bandwidth or else the data rate initially we kept the 500 Mbs data gone for the live video streaming is successful similarly for 30 Mbs, 20 Mbs and 10 Mbs data transmission has been done without any distortion.

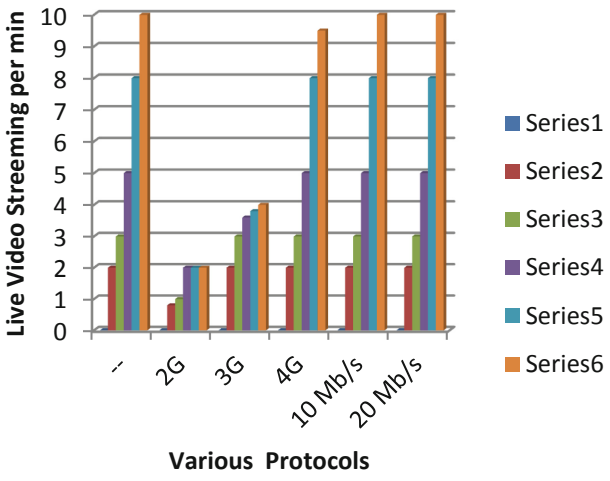


Fig. 6. Graphical representation of video

6 Conclusion

To increase the child security, the system is integrated with GSM, GPS as well as live video streaming technology. Each and every point of the bus is monitored by GPS and sends the information to the parent's mobile number with the help of GSM model.

GSM model not only sends the information regarding the bus position it also helps to send the boarding and de-boarding of the student to the bus. One of the most advanced technologies of live video streaming with very less bandwidth has been obtained and tested with 2G, 3G, 4G and Wi-Fi with different bandwidth. For the future experimental purpose, integration of two to three simultaneous live video streaming for a different number can be done.

Acknowledgement. All author states that there is no conflict of interest. We used our own data. We obtain the permission from school management. We have installed the live camera in our own institution and we got permission from the management. We would like to thank the "Sai Vidya Institute of Technology, Bangalore, India" for providing full support to do our research work.

Reference

1. Raj, J.T., Sankar, J.: IoT based smart school bus monitoring and notification system. In: IEEE Region 10 Humanitarian Technology Conference, pp. 89–92 (2017)
2. Jisha, R.C., Jyothindranath, A., Kumary, L.S.: IoT Based School Bus Tracking and Arrival Time Prediction, pp. 509–514. IEEE (2017)
3. Zambada, J., Quintero, R., Isjiara, R., Galeana, R., Santillan, L.: An IoT Based Scholar Bus Monitoring System, pp. 461–487. IEEE (2015)
4. Badawi, E., Abdulhameed, A., Elhakim, A., Zualkeran, I.A.: An IoT Based School Bus Tracking and Monitoring System. IEEE (2016)
5. Sun, H.P., Zeng, H., Guo, J.L.: Bus Data Acquisition and Remote Monitoring System Based on CAN Bus and GPRS, pp. 1094–1097. IEEE (2011)
6. Viklund, A., Appeltofft, K.: Experiences from an application for safe transport to and from school. In: International Conference on ITS Telecommunications, pp. 357–360. IEEE (2011)
7. Eken, S., Sayar, A.: A Smart Bus Tracking System Based on Location-Aware Services and QR Codes. IEEE (2014)
8. Singla, L., Bhatia, P.: GPD based bus tracking system. In: IEEE International Conference on Computer, Communications and Control (IC4-2015)
9. Ghareeb, M., Ghamlous, A., Hamdan, H., Bazzi, A., Abdul-Nabi, S.: Smart Bus: A Tracking System for School Buses. IEEE
10. Nafar, F., Shamsi, H.: Design and Implementation of an RFID-GSM based Vehicle Identification System on Highways. IEEE (2018)
11. Kannouf, N., Douzi, Y., Benabdellah, M., Azizi, A.: Security on RFID Technology. IEEE (2015)
12. Ndifon, A.M., Crisp, M.J., Penty, R.V., White, L.H.: Enhanced RFID Tag Detection Accuracy Using Distributed Antenna Arrays. IEEE (2018)

Rubik's Cube Encryption for Securing Cloud Stored Data

T. T. Anusree(✉) and K. P. Swaraj

Department of Computer Science and Engineering,
Government Engineering College, Thrissur, India
anusreethyagaraj@gmail.com, swaraj.gec@gmail.com

Abstract. Cloud storage is an efficient solution for storage needs of organizations and individuals. But the data outsourcing and data transfer using the same network makes the cloud data more sensitive for attacks. Hence providing security to the cloud data while in storage or transit requires a prime concern. The denial of access to a third party also must be ensured for the confidentiality of stored data. In this paper, Rubik's cube based encryption with data spitting technique is introduced to securely storing and transferring cloud stored medical records. And the role of the third party auditor also limited to verifying the user only. The multiple number of encryption and denial of access to the third party ensure that the data is protected in the cloud.

Keywords: Cloud computing · Rubik's cube encryption · Data analysis · Data splitting · Medical record

1 Introduction

Different varieties of new technologies are introduced in the IT field because of the growth of distributed computing and network technology. Beyond any other technologies, IT currently concentrates on big data and cloud computing. Cloud computing provides its services on-demand, which is available anywhere at any time irrespective of the geographical location. As cloud services become more popular the security of cloud stored data requires a prime concern. Because due to the hike in the number of cloud storage user's there are chances for data loss and trespasser attacks.

The cloud stored medical records requires considerable concern because these data sets contain personal and sensitive information's about patients. There is a chance that medical insurance companies or other attacker's abuse this outsourced sensitive information for their uses. The different sensitive information's that must be kept confidential in medical records are phone number, medical insurance number and disease details etc. The loss of such data's will reduce the confidentiality of the data and will break the reliability of cloud service providers and hospitals.

Our focus in this paper is to provide a secure cloud storage service for medical records. This system uses Rubik's cube encryption with a data splitting technique for secure data storage and data transfer. Also, the system limits the access of third-party auditor. The role of the third-party is defined to verifying the hospital employee only. Thus only authenticated persons are allowed to get access to cloud stored medical records.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 679–685, 2020.
https://doi.org/10.1007/978-3-030-37051-0_76

The rest of this paper is as follows: Literature survey is discussed in Sect. 2. Section 3 describes the architecture and different modules of the cloud data security system. Section 4 discusses the Dataset and result. Finally, Sect. 5 is the conclusion with brief description about the present findings and future direction.

2 Related Works

Several works are carried out for the securely storing of cloud data.

Lenka and Nayak [1] proposed a method for securing cloud proposed which implements RSA for both encryption and secure Information passing purposes, and MD5 hashing is used for key information hiding and digital signature.

Liu [2] presented a Two-factor data security system for protecting cloud storage system. This system is an Identity-based encryption system. Here to send a data which is encrypted, the sender only knows the identity of the receiver. The receiver can download the data at any time from the cloud as the sender sends the encrypted data to the cloud. First of all the user needs to have a secret key that is stored in the local computer then a personal security device which will be used to connect to the computer to decrypt the data. The cipher text cannot decrypt without any of these pieces.

Akhil et al. [3] proposed AES based security system, where there is a third party auditor. The security of data is obtained using AES encryption on the whole data. Encryption and decryption of the whole data increase the time cost.

Cheng et al. [4] presented a paper to secure cloud data. In this system, some sequenced or logical blocks of cloud data are created. These data blocks are again distributed and stored among different cloud storage service providers.

Bakibayev et al. [5] proposed a hybrid cloud architecture with Elliptic curve based data scrambling and encryption for securing the big data in an organization. Paper [6] extended this concept to n-cloud architecture.

Researchers [7–10] uses Rubik's cube based encryption for image security. Rajavel and Shantharajah [11, 12] proposed different two techniques for text data encryption based on Rubik's cube rotation. First one was based on hybridisation and cube rotation, and the other was based on random rotation type and angle.

From the above observations, in the existing systems for cloud data storage, the focus is mainly on cloud stored data, and it does not consider the security of the data during the data transfer. Also, there is a third-party auditor who has access to cloud data. Sometimes this auditor may be an intruder and gains access to all the data. Our proposed system aims at implementing organizational level security to data. Rubik's cube encryption along with a data splitting technique is used in our approach and also limits the access of third party auditor.

3 Cloud Data Security System

In a hospital huge amounts of data are getting generated through every day working. The data generated contain both sensitive data and general data. Sensitive information's are Aadhaar number, Mobile number, medical insurance number and disease details

that require more protection. The sensitive data are to be protected at any cost for ensuring its confidentiality. The other general data such as gender, profession etc. can be stored as raw data for analytic purposes.

The general architecture of the proposed system is shown in Fig. 1. The important modules of the general system architecture are Third party authentication module, Data analyzing module and Encryption module and Decryption module.

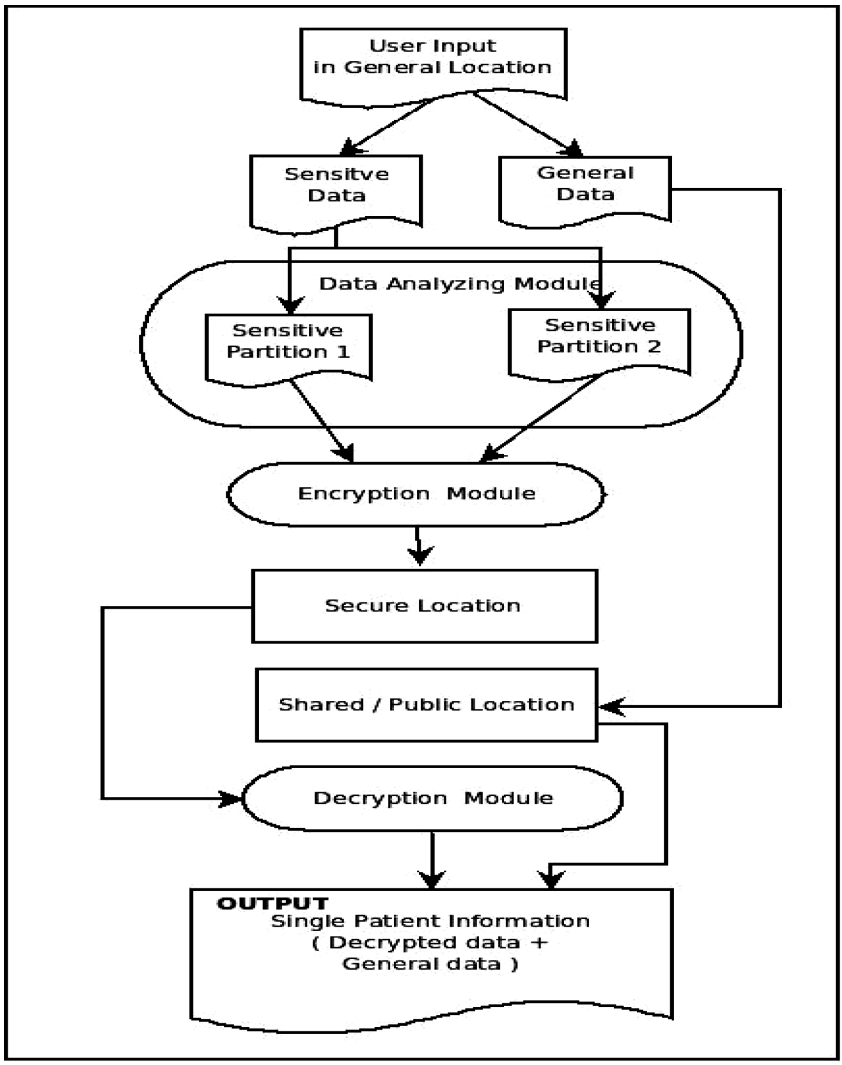


Fig. 1. System architecture

The medical records are stored at a hospital's general location. These data are analysed by the data analysing module. After analyzing the data is separated into sensitive data and general data. The sensitive data are again splits into multiple parts. The general data is stored in a shared or public location for easy access for analytic purposes. Each part of the sensitive data is encrypted based on Rubik's cube encryption method and that is store to cloud after combining them to one.

3.1 Third Party Authentication Module

The purpose of the third party authentication is to verify hospital employee only. When an employee requests for access the auditor authenticate that user. The auditor does not have the access to the cloud data. Thus any misbehaviour from the third party auditor can be prevented.

3.2 Data Analyzing Module

The medical record is analyzed using R at the organisations local location. The input consists of a mixture of sensitive and non-sensitive data. The sensitive data and general data are identified based on number of digits or characters. Then the sensitive data is again splits into two equal half's.

Algorithm 1: Algorithm for Data Analysis and splitting

Input: Sensitive data.
Output**:** Sensitive partition 1, Sensitive Partition 2.

```
Load the sensitive dataset into the R environment as a data frame.
Create two new data frames for storing sensitive partitions.
Copy the patient ID column into both the newly created data frames
for All columns in the Dataset do
    Check the value in the first field of column.
    Count the number of digits or characters in the field.
     for all the fields do
        Split value into two equal half's.
        Copy the first half into sensitive partition 1.
        Copy the remaining half into sensitive partition 2.
    end for
end for
```

3.3 Encryption Module

In this module both the partitions from the data analyzing module are encrypted using Rubik's cube encryption. Then these encrypted data are combined and stored to the cloud storage. Separate keys are generated for each customer and these keys are stored securely at hospital's local server and that is tied to hospital admin's login. Thus it requires the admin to logged in to get the key for decryption.

A 3 × 3 × 3 Rubik's cube have 6 faces with different colours in each face, when the 9 different pieces of all the six faces have same colour then the cube is solved. Cube is solved by using 18 different rotations for classical Rubik's cube.

Permutations of the original 3 × 3 × 3 Rubik's Cube is like to be 8! * 38 * (12! * 2) * 211 which is approximately forty-three quintillion. This huge number of permutations makes the Rubik's cube more complex and this is the idea to use it for encryption.

The 18 rotation types possible are 1: upper-clockwise, 2: down-clockwise, 3: upper-inverse, 4: down-inverse, 5: front-clockwise, 6: back-clockwise, 7: front-inverse, 8: back-inverse, 9: left-clockwise, 10: right-clockwise, 11: left-inverse, 12: right-inverse, 13: horizontal-clockwise, 14: horizontal-inverse, 15: middle-clockwise, 16: middle-inverse, 17: vertical-clockwise, 18: vertical-inverse.

Rotation angles are 1:90°, 2:180°, 3:270°.

Algorithm 2: Algorithm for Key generation.

Input: Number of rotations (18).
Output: Random sequence of rotation types rtp and random sequence of angles for rotation ra.

1: Generate an unrepeated random sequence for rotation Type of 18 length.
$$\text{Rotation type } [i] \in \{1, 2, 3 \ldots 18\} \text{ where } [1 \leq i \leq 18]$$
2: Generate the random sequence for rotation angle of length 18 as angle for each rotation type
$$\text{Rotation angle}[i] \in \{1, 2 \text{ and } 3\} \text{ where } [1 \leq i \leq NR]$$
3: Create an ordered dictionary (rtp[i], ra[i]). This is the key for encryption.
4: Eliminate Keys with adjacent similar rotation types.

Algorithm 3: Algorithm for Encryption.

Input: Sensitive partition1, sensitive partition 2, keys generated
Output: Rubik's cube encrypted medical record.

```
1: Define all the 18 rotation types for Rubik's cube.
2: for both the partitions do
3:    for each row in the partitions do
4:       Pad trailing 0's to the row to make it 54 length string
5:       Divide the 54 length string into six 3 x 3 matrices.
6:       Rotate the matrices based on the key.
7:       Store the cipher text.
8:    end for.
9: end for
```

3.4 Decryption Module

The purpose of decryption module is to decrypt the cloud stored information on-demand of an authenticated employee. Upon demand after retrieving the patient info back at the hospital's local location, data is decrypted using key available at the hospital local locations.

Algorithm 4: Algorithm for Decryption.

Input: Encrypted data, key
Output: Customer decrypted information.

1: Import the rotation types defined in the encryption module.
2: **for** the specified patient's row in the encrypted database **do**
3: Divide th**e** data into two 54 length strings.
4: **for** both the strings **do**
5: Divide the 54 length string into six 3 x 3 matrices.
6: Rotate the matrices based on the reversed values of key and rotations are carried out in anti-clock wise instead of clock wise and vice versa.
7: print cube's face values one by one after deleting all trailing z's to get the Original information.
8: **end for**
9: **end for**

4 Result

The medical database is the input to the system. The time to encrypt different file sizes is given in the Table 1. The time to update the database is 0.0017 ms and time to decrypt single patient information is 0.004 ms.

Table 1. Execution time for encryption.

Sl. no.	File size	Execution time
1	3 kb	0.074 ms
2	6 kb	0.148 ms
3	9 kb	0.25 ms
4	12 kb	0.32 ms
5	15 kb	0.37 ms

5 Conclusion

Cloud storage is an efficient solution for storage needs of organizations. Since the data is placed to unknown location the cloud stored data is more sensitive to attacks. This paper proposes a multilevel security system to secure cloud data at storage and in

transit. The Rubik's cube encryption and data splitting brings the security to data level. Also the access denial to the third party auditor avoids attacks from masked intruders. Thus this Rubik's cube based security system is an efficient solution for ensuring security to the cloud data.

Future extension for this work can be using multiple cloud storage servers to store different data splits for more security and implementing Map Reduce algorithms to reduce execution times.

References

1. Lenka, S.R., Nayak, B.: Enhancing data security in cloud computing using RSA encryption and MD5 algorithm **2**(3), 6064 (2014)
2. Liu, J.K., Liang, K., Susilo, W., Liu, J., Xiang, Y.: Two-factor data security protection mechanism for cloud storage. Syst. IEEE Trans. Comput. **65**(6), 1992–2004 (2016)
3. Akhil, K.M., Praveen Kumar, M., Pushpa, B.R.: Enhanced cloud data security using AES algorithm. In: 2017 IEEE International Conference on Intelligent Computing and Control (2017)
4. Cheng, H., Qian, M., Yu, S.: Securing cloud data using a pirate scheme. Chin. J. Electron. **26** (6), 1289–1296 (2017)
5. Bakibayev, N., Olteanu, D., Zavodny, J.: Big data analytics for security intelligence. In: Cloud Security Alliance Business White Paper (2013)
6. Vijayanad, K.S., Mala, T.: Ecids Elliptic curve inspired data scrambling method for securing data in hybrid cloud using N cloud architecture. Asian J. Inf. Technol. (2016)
7. Zhu, Z.-L., Wang, C., Chai, H., Yu, H.: A chaotic image encryption scheme based on magic cube transformation. In: Proceedings of the 4th International Workshop on Chaos-Fractals Theories and Applications (IWCFTA 2011) (2011)
8. Zhang, L., TiaN, X., Xia, S.: Scrambling algorithm of image encryption based on Rubik's cube rotation and logistic sequence. In: Proceedings of the International Conference on Multimedia and Signal Processing (CMSP 2011), Guilin, China, May 2011, pp. 312–315 (2011)
9. Loukhaoukha, K., Chouinard, J.-Y., Berdai, A.: A secure image encryption algorithm based on Rubik's cube principle. J. Electr. Comput. Eng. **2012**, 13 (2012). Article ID173931
10. Diaconu, A.V., Loukhaoukha, K.: An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher. Math. Probl. Eng. **2013**, 10 (2013). Article ID 848392
11. Rajavel, D., Shantharajah, S.P.: Cubical key generation and encryption algorithm based on hybrid cube's rotation. In: International Conference on Pattern Recognition, Informatics and Medical Engineering. IEEE (2012)
12. Rajavel, D., Shantharajah, S.P.: Scrambling algorithm for encryption of text using cube rotation artificial intelligence technique. Biomed. Res. (2016). Special Issue: S251-S256

Comparative Study on Face Detection by GPU, CPU and OpenCV

Sanjay Patidar(✉), Upendra Singh(✉), Ashish Patidar, Riyaz Ali Munsoori, and Jyoti Patidar

Department of Computer Engineering, Delhi Technological University, Delhi 110042, India
sanjaypatidar@dtu.ac.in, upendrasingh49@gmail.com, getashish25@gmail.com, energitiumraju@gmail.com, jyotipatidarcs@gmail.com

Abstract. Optimization of processes and functions on Software side or on Hardware side are constantly remaining under the research consideration. Optimization can decrease the average time taken by a functional element to complete a particular task. Space-Time Complexity of various algorithms has been determined. These algorithms are widely used in the real-time systems. One of the algorithms is Face detection Algorithm. This project focuses on finding the easiest way of implementing the algorithm so that it can work in real time. In this comparative study, the Viola Jones Algorithm for Face Detection is implemented in 4 forms – CPU, Multi-threaded CPU, OpenCV and GPU using CUDA may be on cloud. The Algorithm is tested over Face Detection Dataset by FDDB and the results are framed on a graph to get the comparison among the methods used. This research project also discusses the limitations, future scope and implementation of the algorithm in real-time video streaming in the most efficient way.

Keywords: Face detection · CUDA · GPU · Integral image · Open CV · Cloud

1 Introduction

Over the last two decades, computer and communication technologies have literally transformed the world we live in. Parallel processing has come out as the key enabling technology in modern computers, driven by the ever-growing demand for higher performance, lower costs and sustained productivity in real-life applications.

The main reason for parallel processing is to execute code efficiently as parallel processing saves time. As a consequence of executing code efficiently, parallel processing often scales with the problem size, and thus can solve larger problems. In general, parallel processing is an approach to provide concurrency.

Face-recognition system has emerged in the technology industry as a great tool for various functionalities such as security barriers implemented on end devices or highly secured area, filters on social apps and auto face enhancement while clicking a picture. An optimized object/algorithm for face detection was designed by Paul Viola in 2001 [1].

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 686–696, 2020.
https://doi.org/10.1007/978-3-030-37051-0_77

The concept of Parallelism can be implemented to this algorithm so that processing time is further reduced in some devices such as Smartphones, Low-end Laptops/Desktops etc.

The proposed research work is a comparative study of face detection algorithm implemented through CPU, GPU and open source library OpenCV.

Implementation of the algorithm on CPU is also done through 2 approaches:

1. Single-Threaded CPU
2. Multi-Threaded CPU.

On GPU, the algorithm is implemented using the parallel programming tool – CUDA. This tool works on NVIDIA Graphic Cards only also available on cloud.

Time Graphs are plotted for each phase of implementation. These time graphs will show the best way of implementing Viola Jones Face Detection on a system depending on the hardware support provided.

2 Related Works

2.1 Viola Jones Face Detection Algorithm

Paul Viola and Michael Jones invented a strong face location technique. The procedure use Haar highlights which are assessed quickly with the assistance of a picture portrayal. Portrayal depends on a "Fundamental Image", idea. By the utilization of Ada-Boost the boosting calculation to decrease the over-total set, it makes an immense arrangement of highlights [1]. They presented a helped classifier depends on degenerative tree which is provided fast and vivacious impedances. The identifier utilized is connected in examining style on dim scale pictures [4] (Fig. 1).

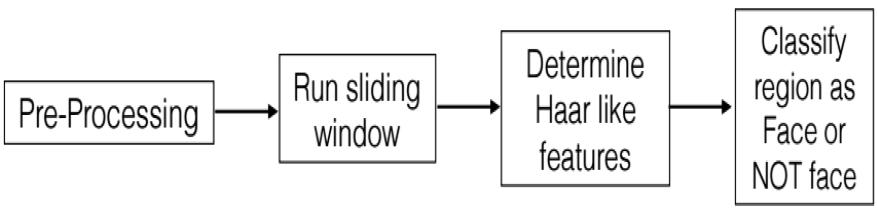


Fig. 1. Viola Jones Algorithm [1]

1. **Pre-processingstage:** In the pre-processing stage run the classifier by spot a picture. In this stage the picture is parsed, transforming it to Greyscale lastly down-examining the picture [11].
2. **Running the Sliding Window:** The sliding window is a fixed window of size 24 × 24 that movement over the picture pixel by pixel and runs certain channels on the picture region it covers. These channels reveal features which can be used later to order locale as face or not-face [11] (Fig. 2).

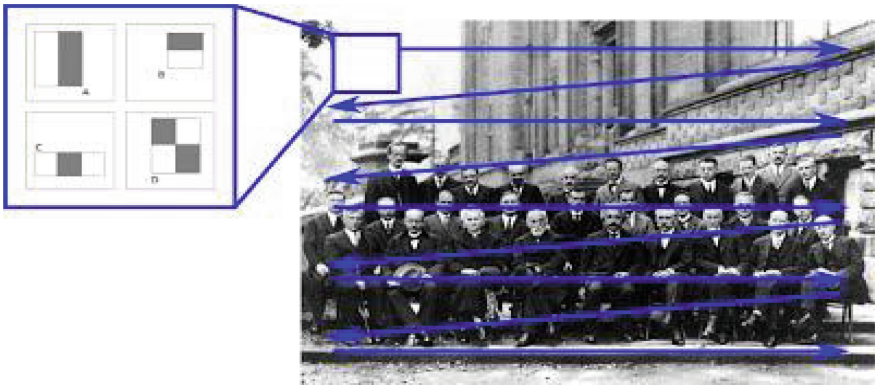


Fig. 2. The sliding window

3. **Haar Filters:** In the Haar channel there is a thought of sliding window that applies a couple of channels which are called to picture region that it limits. These channels reveal even and vertical features in picture. These Haar highlight has rectangular districts which are circumscribing at a particular region in the territory window, follows in every area pixel forces and capability is settled between these wholes. What has any kind of effect is utilized at last to sort subsections of a picture [11] (Fig. 3).

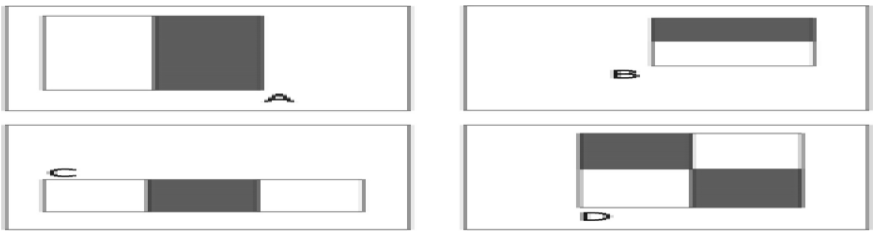


Fig. 3. Haar filters

4. **Cascade Classifier:** A course classifier comprises of a few phases of channels. Each time the sliding window moves, the new district in the sliding window will experience the course classifier organize by-arrange. On the off chance that the info district neglects to pass the limit of a phase, the course classifier will promptly dismiss the area as a face. In the event that a district passes all arranges effectively, it will be delegated a hopeful of face, which might be refined by further preparing. For the pre-prepared course classifier, there are 25 arranges, each containing various Haar channels, going from 9 to 211. Inside a phase, the picture district will experience these channels in parallel. The yield of these channels will be summed up and looked at against a for every stage edge, in light of which the choice of the identification is made [11] (Fig. 4).

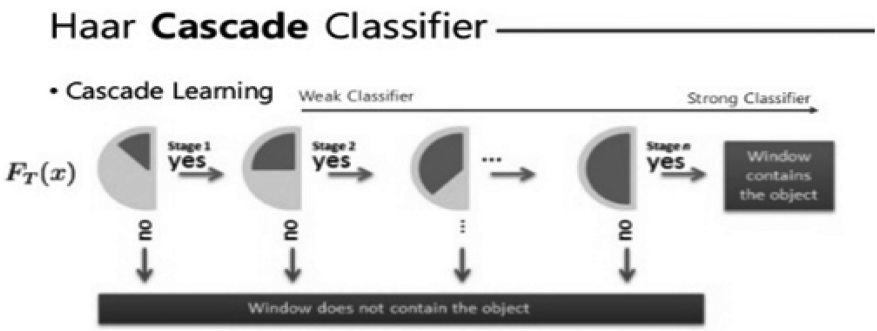


Fig. 4. The Haar Cascade classifier

2.2 CUDA

The CUDA (C-Compute, U-Unified, D-Device, A-Architecture) is model reliant on C from NVIDIA. It revealed parallel limits of GPU for headway and sending of comprehensively helpful counts straightforward [10]. On other hand CPUs have few focuses which are streamlined to perform back to back enlisting while GPUs have a colossal number of focuses which are arranged especially for parallel getting ready. Along these lines a basic speedup is cultivated by running some of the task which has no dependency on GPU while rest in CPU. Experts use GPU to enliven distinctive sensible and planning issues, for example, picture preparing, complex scientific issues and so on. Additionally, applications dependent on pixel like PC vision and picture processing and video is appropriate to innovation of broadly useful GPU [8].

The CUDA Architecture includes a couple of sections:

1. Parallel figure engines inside NVIDIA GPUs
2. OS kernel level helps for gear instatement, setup, etc.
3. Customer mode driver, which gives a device level API to engineers
4. PTX guidance set design for parallel enlisting kernel and limits (Fig. 5).

NVIDIA had imagined CUDA in 2007. This is a framework that offers designers to get the virtual direction sets and memory of parallel taking care of units in a GPU of NVIDIA.

Instead of utilizing guidelines of graphical API, a program that written in C/C++ code is coordinated to a specific equipment in the GPU and that equipment deals with the execution of that program on the GPU. The CUDA system is augmentation to the C programming language. The name of compiler is NVCC that is utilized for accumulating CUDA code [10] (Fig. 6).

3 Proposed Work

This research project is a comparative study of various implementations of Face Detection Algorithm. Implementation phase in this research work will give the idea of average time taken by processes.

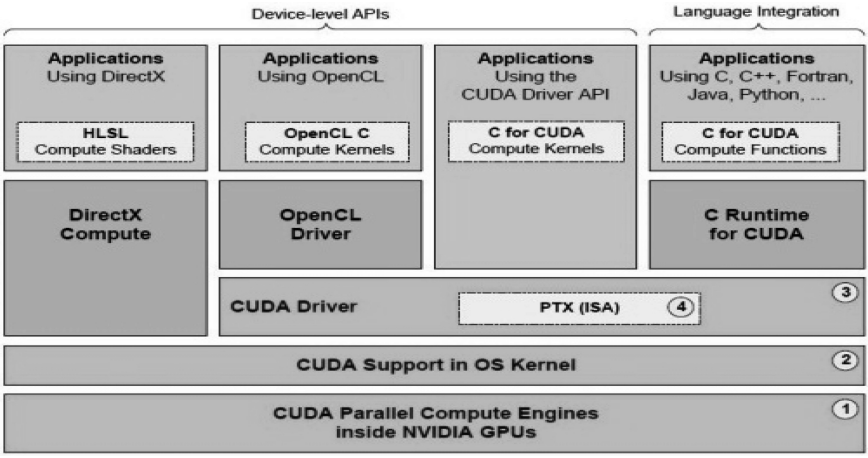


Fig. 5. Architecture of CUDA [1]

All the versions of Face Detection, written in C or C++, will be implemented on Visual Studio. GPU version of Face Detection Algorithm will be implemented using CUDA which is also written using constructs of C and C++.

The results are plotted on a graph for final comparison of various category of the Viola Jones.

3.1 Proposed Flow Chart

In Fig. 7 explain about steps between input image to output image. In step one take input image and insert image in our CCPU model for processing. In CPU model fallow 4 steps, step first start face detection second read image third apply load classifier and in last step apply image transformation. After image transformation apply next model CPU/GPU/OpenCV. In this model get form of image transformation then divided into three haar Feature 1 to 3 then in haar features we apply adaboost algorithm which generate accurate features selection then we got original face.

3.2 Algorithm

Face Detection Data Set is taken from FDDB which is proposed to consider the issues of unconstrained face revelation. This instructive accumulation contains the documentations for 6453 faces in a great deal of 3241 pictures taken from the Faces in the wild enlightening record.

Face Detection Algorithm for consecutive methodology and multi-strung methodology in CPU are taken from the assets referenced in other research ponders dependent on Face Detection.

CUDA implementation of Viola Jones Face Detection Algorithm is provided in the CUDA 8.0 toolkit. Some dependencies of external libraries of Visual Studio were

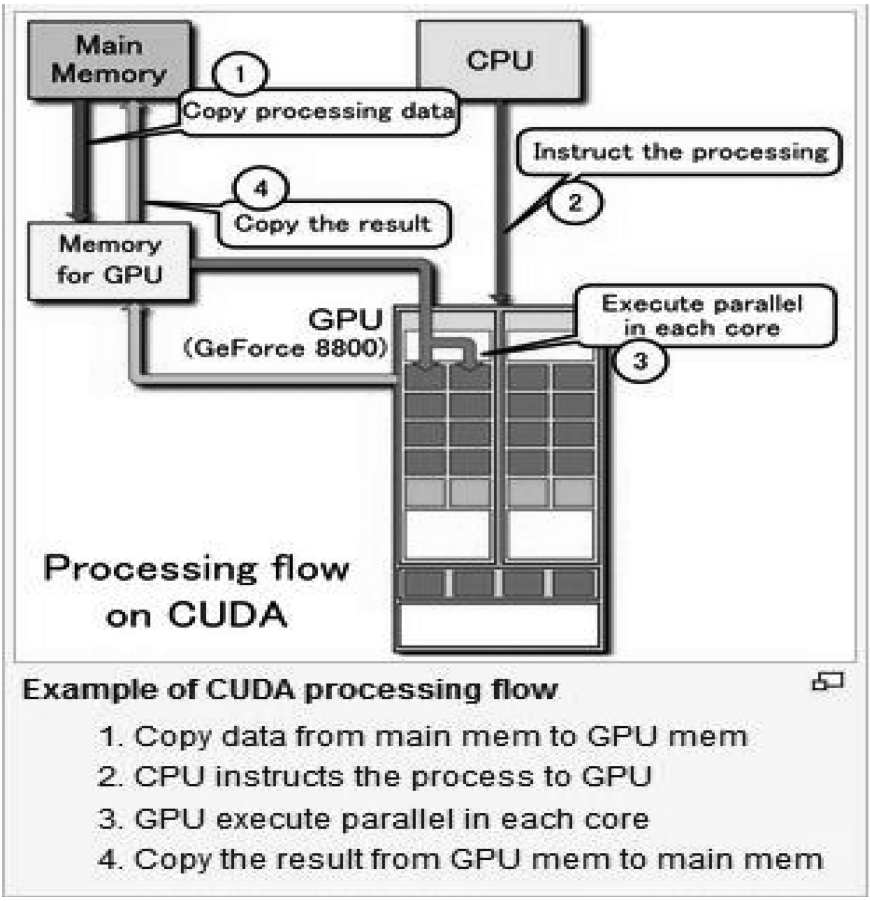


Fig. 6. CUDA processing flow

required for CUDA which were installed from credits packages on official site of Microsoft.

OpenCV implementation of the algorithm is also taken from the resources mentioned in other research projects studied during the course of this project. To implement OpenCV based algorithm, OpenCV 3.1 package is installed on the system and the path of the directories is updated in the environment variables for required dependencies.

XML files for frontal face detection are provided along with the versions.

Sample images are downloaded from internet for testing purpose as every version outputs the image, under processing, with a rectangle around the face to ensure that it has successfully detected the face.

The face identification framework that we have built up (a blend of C++ and CUDA) is tried on an Intel(R) Core i7 4210U CPU, have arrangement of 2.4 GHz having 16 GB RAM, with a NVIDIAGPU of GeForce 820M. This highlights of GPU with 4 multiprocessors, shared memory of 49152 bytes and 4 GB gadget memory.

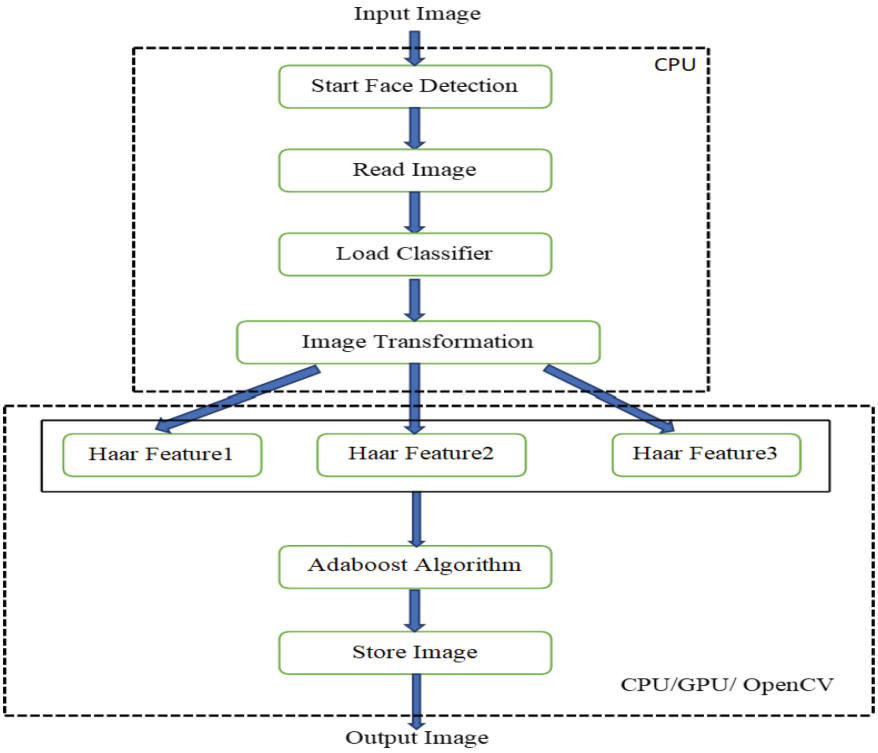


Fig. 7. Proposed flow chart

Here there can be of maximum 2048 threads per block and per multiprocessor 1536 active threads.

4 Result

The results of all the implementations done on FDDB are taken and the average time was calculated for every stage which gave the following results as shown in Figs. 8 and 9.

The total compute time for every implementation is as follows:

1. GPU – 783.4 ms
2. CPU(sequential) – 16717 ms
3. CPU(multi-threaded) – 70736 ms
4. OpenCV – 540 ms.

After using many parallelization techniques, we can say that the OpenCV GPU implementation is better. This is because:

1. The library of Open CV GPU is more optimized and as result it will perform pre-processing faster than our version.

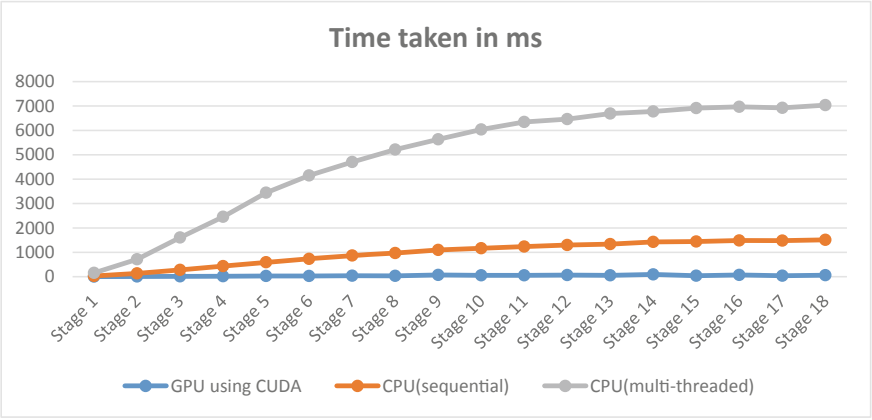


Fig. 8. Comparison b/w CPU and GPU implementations

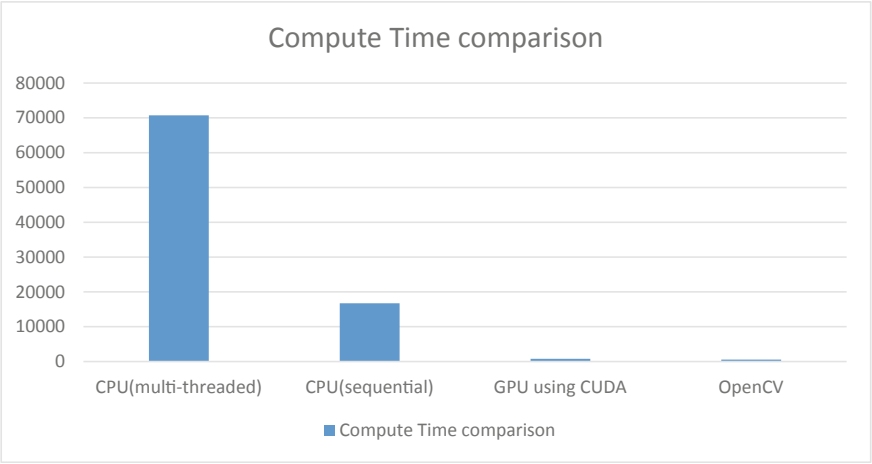


Fig. 9. Computation time comparison

2. The library of OpenCV GPU can change 2D representations of the image to 1D representation in much faster way also it use better indexing techniques han the one we used.

OpenCV is almost 100 times faster than CPU implementation of Viola – Jones Face Detection Algorithm and 1.25 times faster than GPU implementation.

CUDA implementation of GPU also performs quite fast than CPU version of the algorithm. GPU can

Also, the CPU implementations – sequential and multi-threaded are found out to be deprecated in this algorithm as many times they do not yield a result. A sample is shown in Fig. 10.

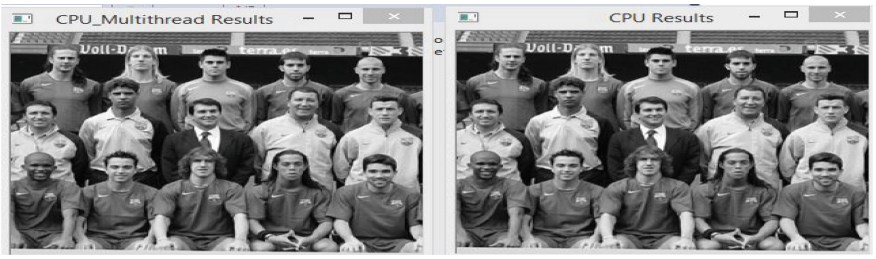


Fig. 10. CPU implementation of Face Detection Algorithm on a sample image

Also, the GPU implementation using CUDA have some errors as shown in Fig. 11 and it needs some error resolution techniques in order to make it efficient.

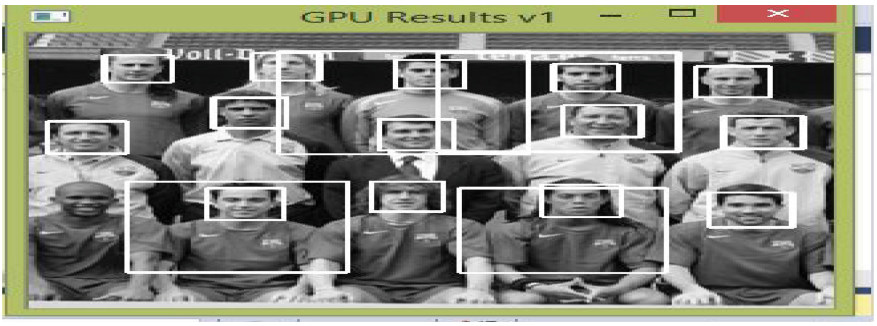


Fig. 11. GPU implementation of Face Detection Algorithm using CUDA

Errors in various versions of Viola Jones Algorithm show the Accuracy of each implementation.

1. OpenCV had highest accuracy.
2. CUDA based implementation had second highest accuracy.

CPU implementation – both single-threaded and multi-threaded had least accuracy.

5 Conclusion

Face recognition has very essential job in checking the security of frameworks. Since as we are thinking for savvy application in future it plays critical role. By presentation of GPU and programming with GPU, we can use parallelism to huge degree for processing huge assignments like face identification.

The results were not 100% accurate for all implementations. But, we got the idea that OpenCV works fastest in terms of face detection whereas CUDA based implementation was 0.75 times of that of OpenCV. CPU implementation was the slowest and least accurate.

A few limitations that were recognized are as per the following:

1. Our methodology isn't invariant revolutions. Once in a while if faces are tilted or turned the calculation may neglect to identify them. This is a consequence of utilizing the Haar channels in the course classifier that are not pivot invariant.
2. There is some heap irregularity in our CUDA execution. For example, a string with a sub window with no facial component may stop much before a string with a sub window comprising of facial highlights; the last will experience more phases of the course classifier.

This abandons us with some extent of progress which can be expressed as pursues:

1. We can improve speed by utilizing an alternate classifier. Notwithstanding amid our execution we found different classifiers like the direct twofold classifier that is essentially quicker as it has less order arranges yet is somewhat less exact.
2. Further diverse classifiers with channels or strategies that are pivot consistent would likewise enable us to get increasingly exact outcomes as it will help recognize faces that are turned or tilted.
3. Improve burden irregularity issue in CUDA execution by dedicating lazy strings to other calculation serious undertakings.

References

1. Jones, M.J., Viola, P.: Robust real-time face detection. J. Comput. Vis. **57**(2), 137–154 (2004)
2. Manjaramkar, A.K., Bhutekar, S.J.: Parallel face detection and recognition on GPU. Int. J. Comput. Sci. Inf. Technol. **5**, 2013–2018 (2014)
3. Pan, Z., He, N., Jiao, Z.: FFT used for fabric defect detection based on CUDA. In: Advanced Information Technology, Electronic and Automation Control Conference. IEEE (2017). 978-1-4673-8979-2/17/$31.00 ©2017
4. Viola, P., Jones, M.J.: Rapid object detection using a boosted cascade of simple features. In: Proceedings of the Conference on Computer Vision and Pattern Recognition, Los Alamitos, CA, USA, pp. 511–518 (2001)
5. Lienhart, R.: An extended set of Haar-like features for rapid object detection. In: Proceedings of IEEE International Conference on Image Processing (ICIP 2002), USA, pp. 900–903 (2002)
6. Wang, Y., Li, K.L., Shen, Y.N.: Research on parallel computing of FFT based on CUDA. J. Hunan Univ. **6**, 128–133 (2012)
7. Kizuna, H., Sato, H.: Accelerating facial detection for improvement of person identification accuracy in entering and exiting management system. In: International Symposium on Computing and Networking Workshop (CANDARW) (2018)
8. Sony: FeliCa contactless office security (in Japanese). https://www.sony.co.jp/Products/felica/business/solution/office.html
9. https://www.codeproject.com/Articles/85113/Efficient-Face-Detection-Algorithm-using-Viola-Jon.aspx
10. http://developer.download.nvidia.com/compute/cuda/docs/CUDA_Architecture_Overview.pdf

11. Kizuna, H., Sato, H.: The entering and exiting management system by person specification using Deep-CNN. In: 2017 Fifth International Symposium on Computing and Networking (CANDAR). IEEE (2017)
12. http://tanayvarma.github.io/Final%20Project%20Report.pdf
13. https://opencv.org/

Resource Scheduling Using Modified FCM and PSO Algorithm in Cloud Environment

A. Rudhrra Priyaa(✉), E. Rini Tonia, and N. Manikandan

Department of Computer Science and Engineering, St. Joseph's College of Engineering, Chennai, India
rudhrrapriyaa@gmail.com, rini.edward98@gmail.com, Macs2005ciet@gmail.com

Abstract. Cloud computing is a growing environment in the IT industry. Many of the users are interested to outsource their data in cloud. However, load balancing in cloud is still at risk. Resource allocation plays a major role in load balancing. In this scheduling problem, independent tasks in cloud computing can allocate resources by the use of fuzzy c means algorithm (FCM). To allocate tasks to their corresponding resources, particle swarm optimization algorithm (PSO) is used. This paper proposes a hybridization of the FCM and PSO algorithm which is called H-FCPSO algorithm. FCM uses Euclidean distances and PSO optimizes the cluster centers. FCM requires the number of clusters used in advance and thus PSO comes into action to find the number of best clusters. Hence, H-FCPSO identifies the number of clusters and enhances the load balancing. Since our proposed system selects resources based on parallel execution kit reduces the load imbalance in cloud. When compared to Genetic algorithm (GA), Ant Colony Optimization algorithm (ACO), PSO algorithm showed better results in terms of memory. Similarly, FCM was compared with k-means clustering algorithm, Hierarchial algorithm and it showed outputs with better accuracy. The proposed system evaluated data sets and proved to overcome the issues in load balancing and load scheduling which is proved by its precision in the outputs.

Keywords: Cloud computing · Optimization · Clustering · Load balancing · Resource allocation · Accuracy · Memory

1 Introduction

1.1 Cloud Computing

Cloud Computing delivers computing services like servers, storage, databases, networking, software, analytics etc. to the user over the internet. Companies that provide these services are called cloud providers and charge the customers based on their usage. The concept of cloud computing evolved around a decade ago, but already has its applications in many fields. Right from startups to established organizations, government offices to non-profit organizations use cloud computing for various purposes (Fig. 1).

- Private cloud: This infrastructure is exclusively created solely for an organization. It is not shared with other tenants. It is owned, managed and operated by the organization itself. Example: Dell EMC.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 697–704, 2020.
https://doi.org/10.1007/978-3-030-37051-0_78

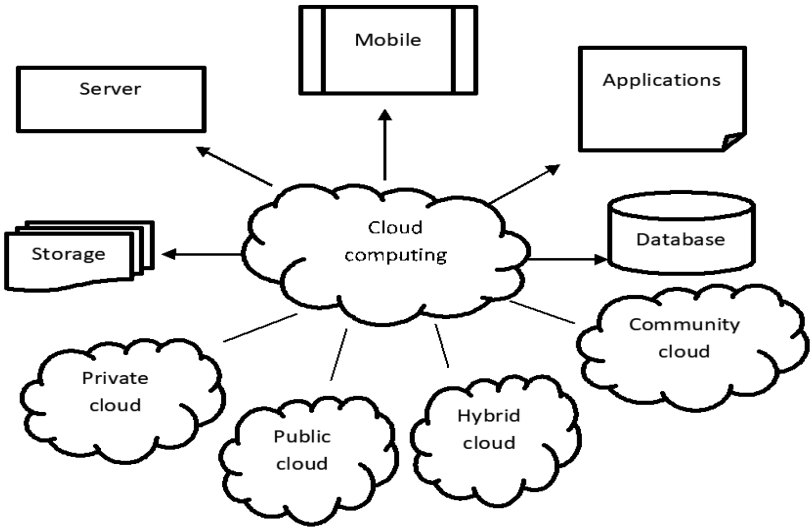


Fig. 1. Deployment models of cloud

- Public cloud: This infrastructure is open to the general public. It is the most frequent way of implementing cloud computing. It is owned, managed and operated by a business or a government organization. Example: Google.
- Hybrid cloud: It is the combination of two or more cloud infrastructures. Many companies have adopted this infrastructure to attain the benefits of both public and private clouds. It offers greater flexibility. Example: Microsoft Azure.
- Community cloud: This infrastructure provides services to a particular community within a limited number of organizations. It is owned, managed and operated by the participating organizations or a third party manager. It is often used by organizations that work on joint projects. Example: Government organizations.

Cloud services are categorized into three categories:

- Infrastructure as a Service (IaaS): External provider provides and manages the hardware. Its also called as HaaS (Hardware as a Service). It includes companies like IBM, Google and Amazon.
- Platform as a Service (PaaS): Besides the hardware the operating system layer is also managed. It maintains the platform and system upgrades and proves to be more efficient and cost effective. It includes companies like Microsoft, Salesforce and Google.
- Software as a Service (SaaS): This additionally manages the application layer besides the other two layers. The clients can use the software applications on a remote basis via an internet web browser. It includes companies like Adobe, Oracle and SAP (Fig. 2).

1.2 Load Balancing

Load balancing is dividing the amount of work that a computer has to do so that more work gets done in minimum time and, in general, all users get served faster. Load balancing can be implemented with hardware, software, or a combination of both. Load balancers help to build flexible networks and improves performance and security for

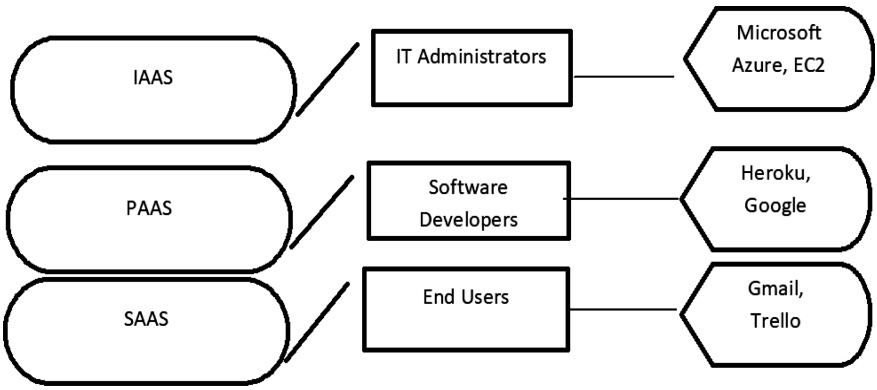


Fig. 2. Cloud services

many types of traffic and services, including applications. By efficient use of load balancers, the increased user traffic is managed and distributed among various servers and network devices.

1.3 Resource Scheduling

Resource scheduling is the delivering and allocating of various resources to a server in the cloud environment. The available resources to a tenant are in a fixed range and hence cannot be owned and reserved to a particular organization or an individual. Instead these resources are allocated to various virtual machines based on their availability using scheduling algorithms. Scheduling these resources ensures:

1. Optimum utilization of resources
2. Helps in real time applications
3. Supports multitasking
4. Maximizes throughput.

2 Contribution of Work

The requests from customers are obtained and assigned to different virtual machines (VM) dynamically by the cloud providers. They use pay-per-basis scheme. So the customers don't have to worry about the idle time. The cloud industry offers a wide range of discounts for long term customers and large requests. For example, Amazon offers 10–20% discount on $25,000–$200,000 investments by customers. This gives an opportunity for the cloud brokers to act as a bridge between customers and providers.

3 Literature Survey

Cloud Computing has been widely deployed in the IT environment due to its property of utility base computing. Utility Computing includes the concept of cloud and grid computing. MIPS rating is calculated based on various parameters like efficiency, cost, energy etc. Tasks are allocated to various virtual machines based on their MIPS rating. Besides execution time, finish time is a very important parameter taken into consideration. The tasks are prioritized based on their time or size and then clustered to gain

optimal performance. The performance of the server is calculated using the simulation technique. This is helpful in deployment of the cloud models like IaaS, PaaS, SaaS and their tasks. The results of this technique is improved using various configurations.

The data, resources, processes etc. used in cloud computing are all dynamic and heterogeneous. It means the resources can be added and removed anytime during the process. This introduces the problem of load imbalance which reduces efficiency and the utilization of resources. The process used to resolve this problem is called Interlacing peak. The working involves collection of data, sorting them and then interlacing the resource load peak. The factors needed for the efficient working of this process are average response time, load balancing, deadline violation rates and resource utilization. It now solves the problem of inefficiency and poor utilization thus proving to be better than the other standard algorithms.

Cloud computing plays a major role in the industry of technology. Many improvements and revolutions have been brought about by this concept. Services provided by the cloud are used by small scale organizations and the flexibility property of cloud is made use by large companies and organizations. There are many problems posed by cloud computing. It is solved using Computational Intelligence (CI). It mainly solves problems in multiple resource management. The problems mainly faced are holistic and cross layer optimization. CI can be combined with other approaches like machine learning, mathematical approaches etc. and have been proved efficient.

An efficient hybridization algorithm is based on a hybrid self-adaptive learning global search algorithm and firefly algorithm (HSLGSAFA). It combines two algorithms namely gravitational search algorithm (GSA) and Firefly algorithm (FA) using SL. It makes use of advantages from both the algorithms and neglects the disadvantages for optimal efficiency. It is mainly preferred by IaaS (Infrastructure as a Service) users. An important factor to be considered is the Quality of Service (QoS). An efficient algorithm with no quality would be an absolute waste. The HSLGSAFA algorithm is used to build hybridization processes and schedules tasks in DCTS problem. Thus, this algorithm proves to outstand the other traditional algorithm.

Cloud computing is mainly used for the safe storage and retrieval of data in a centralized system. Thus, a wide range of data is now stored, accessed and shared between various systems. The deployment models of cloud are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) used for this purpose. Green control algorithm used is an energy efficient algorithm in storing and retrieving of files. The main objective is to find optimal service rate and mode restriction. In return it reduces cost and increases the profit of the user. An efficient green control (EGC) algorithm solves problems related to constrained optimization. It mainly reduces the power consumption.

4 Gaps Identified in the Existing System

See Tables 1 and 2.

Table 1. Comparison of optimization algorithm

Optimization algorithms	Memory	Solve continuous problems	Easy implementation	Rapid discovery of solutions
GA	–	✓	–	–
PSO	✓	✓	✓	–
ACO	✓	–	–	✓

Table 2. Comparison of clustering algorithms

Clustering algorithms	Speed	Flexibility	Accuracy	No prior knowledge
FCM	–	✓	✓	✓
K-means	✓	–	–	–
Hierarchial	✓	–	–	✓

5 Proposed Work

5.1 Particle Swarm Optimization (PSO)

Pseudocode For PSO

The particle swarm optimization algorithm (PSO) is used to achieve objectives such as load balancing, availability and reliability in cloud environment. Cloud environment allows access of resources using pay-per-basis scheme. It uses virtual machines (VM) thereby increasing availability and scalability. The main disadvantage of particle swarm optimization algorithm is the local optima. But it can be solved by combining it with other algorithms.

```
1 Start
2           i=0
3           initialize particles R(i);
4           evaluate particles R(i);
5           while (end conditions are unsatisfied)
6           begin
7                   i=i+1;
8                   update weights
9                   select rBest for each particle
10                  select fBest from R(i-1);
11                  calculate particle velocity R(i);
12                  update particle position R(i);
13                  evaluate particles P(t);
14          end
```

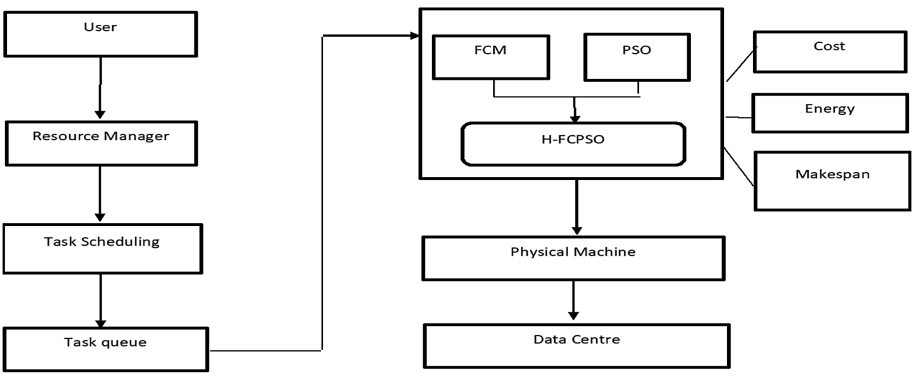
5.2 Fuzzy C Means Algorithm (FCM)

Input: θ (r,p), N

Output $P*_{FCM}$, $M*_{FCM}$

1 Initialize Partition $P^{(0)}$ randomly
2 for i=1 to n
3 for k=1 to d
4 Repeat for j=1,2,3…..
5 Update centroid $M^{(0)}$ with $P^{(i-j)}$ using (3)
6 Compute distance $B^{(j)}$ with $M^{(j)}$
7 Update partition matrix $P^{(j)}$ with $B^{(j)}$ using (5)
8 Until $\| P^{(j)} - P^{(j-1)} \| < \epsilon$
9 End
10 End
11 Return $P*_{FCM}$ <- $P^{(j)}$ and $M*_{FCM}$ <- $M^{(j)}$

6 Proposed Architecture



7 Hybridization of FCM and PSO

Initialize Partition $P^{(0)}$ randomly

for i=1 to n

Repeat for j=1,2,3…..

Update centroid $M^{(0)}$ with $P^{(i-j)}$ using (3); Compute distance $B^{(j)}$ with $M^{(j)}$

Update partition matrix $P^{(j)}$ with $B^{(j)}$ using (5)

Until $\| P^{(j)} - P^{(j-1)} \| < \epsilon$

End; Return $P*_{FCM} <- P^{(j)}$ and $M*_{FCM} <- M^{(j)}$

i=0

initialize particles R(i); evaluate particles R(i);

while (end conditions are unsatisfied)

i=i+1;

update weights; select rBest for each particle; select fBest from R(i-1);

calculate particle velocity R(i);

update particle position R(i);

evaluate particles P(t);

8 Conclusion

In this paper, we have developed an algorithm to manage load balancing and resource scheduling more efficiently. Various algorithms were studied to conclude that hybridization of FCM and PSO showed better results than other traditional algorithms. Hence, we have hybridized FCM (Fuzzy c Means) and PSO (Particle Swarm Optimization) to form H-FCPSO. Thus the properties of energy, cost and makespan have been made efficient giving larger profits to the user.

References

1. Manasrah, A.M., Ba Ali, H.: Workflow scheduling using Hybrid GA-PSO algorithm in cloud computing. Wirel. Commun. Mob. Comput. (2018)
2. Adnan, M., Razzaque, M.A., Ahmed, I., Isnin, I.F.: Bio-mimic optimization strategies in wireless sensor networks: a survey. Sensors (2013)
3. http://theallicient.blogspot.com

4. www.ijsr.net
5. https://hal.archives-ouvertes.fr
6. Rathi, S.R., Kolekar, V.K.: Trust model for computing security of cloud. In: 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA) (2018)
7. Padmakala, S., Anandha Mala, G.S., Shalini, M.: An effective content based video retrieval utilizing texture, color and optimal key frame features. In: 2011 International Conference on Image Information Processing (2011)
8. Masdari, M., Salehi, F., Jalali, M., Bidaki, M.: A survey of PSO-based scheduling algorithms in cloud computing. J. Netw. Syst. Manag. (2016)
9. Chiang, Y.J., Ouyang, Y.C., Hsu, C.H.R.: An efficient green control algorithm in cloud computing for cost optimization. IEEE Trans. Cloud Comput. (2015)
10. Liu, T.C., Wang, J.C.: A discrete particle swarm optimizer for graphic presentation of GMDH network. In: 2005 IEEE International Conference on Systems, Man and Cybernetics (2005)
11. https://apprenda.com

Network Behaviour of Open vSwitch as Per the Anticipated Functionality of Network Application Programmed Over SDN Using Pox Controller

Darekar Sachin[1,2(✉)], M. Z. Shaikh[1,2], and Harshal B. Kondke[3]

[1] Bharati Vidyappeth College of Engineering, Navi Mumbai, India
Sachindarekarl@gmail.com, mzshaikh2003@yahoo.co.in
[2] Dr. D Y Patil School of Engineering, Pune, India
[3] L. T. College of Engineering, Navi Mumbai, India
Harshalbk2017@icloud.com

Abstract. Unlike a traditional network architecture, Software Define Network (SDN) provides central control over the Network. When network visibility and network device programmability is concerned, standard documented open flow enabled physical or open vSwitch is a priority. Because of the central control over the network devices can be programed for different functionality of network application such as switches, routers, firewall and load balancer. One can program a network switch even though it is physical or virtual switch which supports standard southbound API interfacing to controller like open flow to act as hub, switch, firewall, etc. using those network application which can be interfaced with restful API to the controller platform choosen. In this paper, we study the behavior of different network functionality such as hub, switch, firewall and load balancer of open vSwitches over the SDN in linear topology. To create required virtual environment, we used mininet a network emulator tool for analysis and demonstration for network behavior of open vSwitches as hub, switch, firewall and load balancer role by running pox controller remotely outside the network of topology running machine and analyzed whether does it affect on throughput if we run our controller locally or remotely outside network boundary e.g. running on AWS cloud.

Keywords: Open vSwitch · Open flow · Network switch · Pox · And software defined network

1 Introduction

People have started implementation of SDN by replacing traditional network architecture [1] depicted in Fig. 1 (Traditional vs SDN Architecture) by means of choosing different controllers as part of control plane and running application with the ease of northbound API [1] such as Restful API to interface with the controller and the control plane itself interfacing to physical or virtual switch by standard documented protocol i.e. OPEN flow [2].

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 705–713, 2020.
https://doi.org/10.1007/978-3-030-37051-0_79

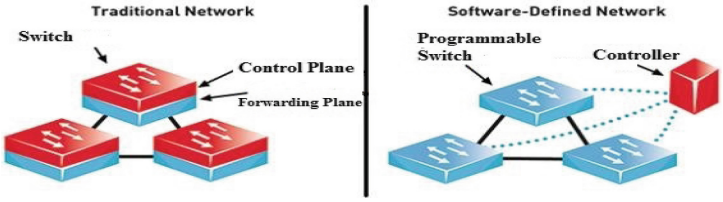


Fig. 1. Traditional vs SDN architecture

To get rid of from traditional network architecture, SDN brings more programmability and flexibility [3] in network to code hub, switch, and firewall, load balancer and many more as network application, against the vendor dominance with respect to features provided. One can choose any type of open flow based controller as controller platform depicted in Fig. 2 SDN Architecture view [3] to control forwarding layer and acting as central point.

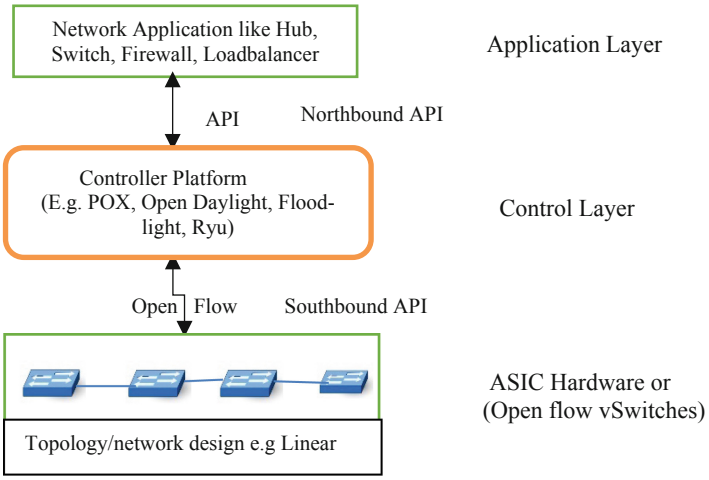


Fig. 2. SDN architecture view

As far as actual working of SDN architecture is concerned, your forwarding layer will be just like network box which will receive packets from network hosts and checks the flow table entry of open flow enabled devices according to that it acts, if no such entry present in the flow table it is send to controller running with the network application then it instructs the device to behave as per the network application programmed to take action whether to forward or drop and corresponding entry will be added to flow table at the forwarding layer for the next upcoming events to be handled. Having an eye on various SDN implementation done before by Saleh [4] who has created an switch application for the performance analysis connecting to Ryu [4] controller and also Vipin [5, 6] used firewall application over open vSwitch running

inside the mininet host. Moving further we decided to run our controller remotely on Amazon cloud having public ip and made open vSwitch behave as per the expected functional role decided by network operator with Software Defined approach.

This paper depicts following sections as follows. Section 2 provides Implementation and results by the analysis of some network behaviour as per the network functionality succeeded by Sect. 3 conclusion and future scope followed by Sect. 4 references.

2 Implementation and Results

To get start with SDN implementation, we choosed mininet [7] as network emulator to behave our open vSwitch [8] as per expected network functional role using linear topology design. To get it done to analyse behaviour we, divided it in to 4 sub sections as an analysis part as follows.

(A) Analysis of hub Behaviour
(B) Analysis of Switch Behaviour
(C) Analysis of Layer 2 Firewall Switch
(D) Analysis of Load balancer.

(A) Analysis of Hub behavior

In general, a hub enables multiple devices or connections to be connected to send and receive packets in the form of broadcasting communication from one to another and forms network of nodes connected. Here we have considered an open vSwitch [8, 9] running under mininet [7] host which is connected to the pox [10] which is an open source well documented python based controller to act as central point. For demonstrating hub based network behavior, linear topology of 4 switches and 2 hosts connected to each switch was choosen, running under mininet host which connects to pox controller running hub application on Amazon cloud having public ip depicted in Figs. 3, 4.

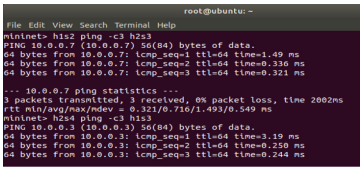


Fig. 3. ICMP check hub

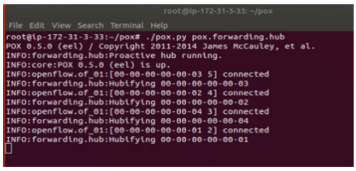


Fig. 4. Running pox controller with app on AWS cloud

Fig. 5. Node h1s1

Fig. 6. Node h2s1

Fig. 7. Node h1s2

Fig. 8. Node h2s2

Fig. 9. Node h1s3

Fig. 10. Node h2s3

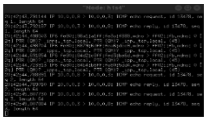


Fig. 11. Node h2s4

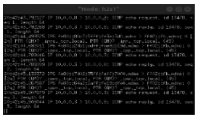


Fig. 12. Node h2s1

To check the hub behaviour 3 packets were sent using ping utility from second host of switch 4 i.e. h2s4 to first host of third switch i.e. h1s3 and analyzed that hub broadcast the packet to all ports except the one from which it is received by opening all nodes terminal and packet capturing software tcpdump running on each node shown in Figs. 5, 6, 7, 8, 9, 10, 11 and 12.

(B) **Analysis of Switch Behaviour:**

In general, switch leads as layer 2 device has its own MAC table includes MAC address with respect to specific port to forward to meet its accurate Network Interface card. Switch forwards the packet to specific port based on MAC entry associated with port number. To implement switch in SDN considering 4 switch linear topology of two host connected to each switch and topology is created by running mininet command and our pox controller connected remotely placed on AWS cloud. To show the behavior of open vSwitch in SDN after successful setup of switch scenario we had gone with random ICMP check using ping utility from host h1s1 of first host of first switch to host h2s2 which is second host of second switch present. By opening the terminal of all other hosts noticed that first packet sent was broadcasted as like hub behavior but when the next packet sent and count went on incrementing then it was only sent to specified destination by learning behavior of switch by extracting frame to add entry to MAC table as per the script l2_learning executed shown in Fig. 13 and count was more for captured packets of host h1s1, h2s2 in compare with other hosts behavior depicted in Figs. 14, 15, 16, 17, 18, 19, 20, 21.

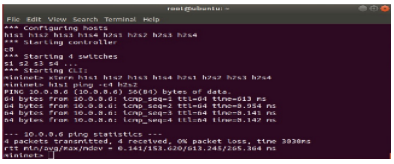


Fig. 13. Random ICMP check switch

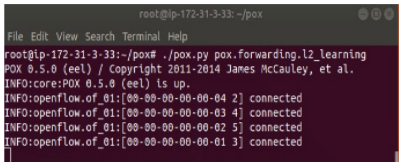


Fig. 14. Running pox controller with app on AWS cloud

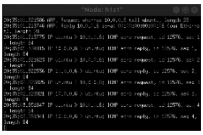


Fig. 15. Node h1s1

Fig. 16. Node h2s1

Fig. 17. Node h1s2

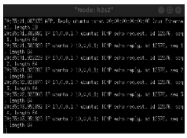


Fig. 18. Node h2s2

Fig. 19. Node h1s3

Fig. 20. Node h2s3

Fig. 21. Node h2s4

Fig. 22. Node h2s1

(C) Analysis of Layer2 Firewall

To move further with Layer 2 Firewall implementation in SDN as Firewall helps to filter out the network traffic based on policy/rule defined. In this approach same topology as like switch behaviour mentioned earlier was selected by running pox controller with Firewall switch application [11] running on AWS cloud remotely. In the forwarding directory of pox we have specified firewall code in the name of firewall-switch.py and .csv file which includes rules specified in terms MAC entry shown in Fig. 22 where first MAC entry and second MAC entry mentioned followed by space indicates that source and destination frame should be blocked and vice-versa. So by looking at the Fig. 24 ICMP checked that h1s1, h1s2, h1s2, h2s2 are not able to ping to h1s2, h1s3, h2s4, h1s4 respectively and vice-versa (Figs. 23, 24).

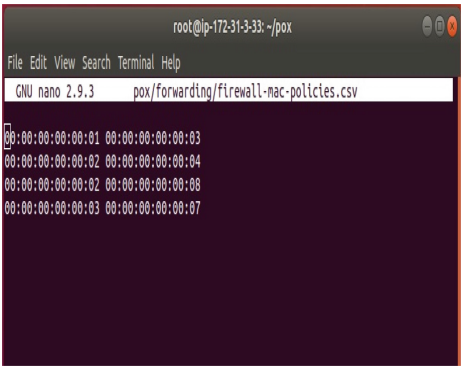


Fig. 23. Firewall-mac-policies .csv

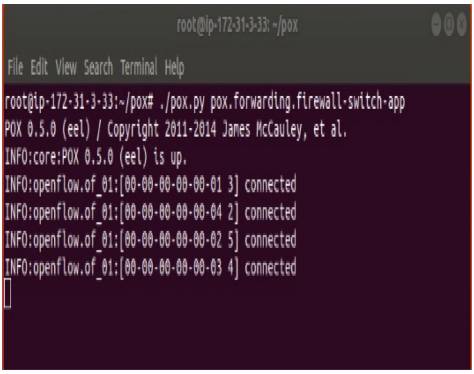


Fig. 24. Running pox controller with switch

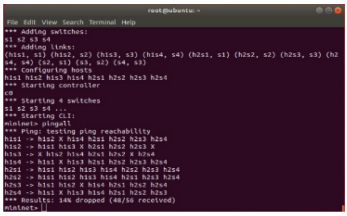


Fig. 25. ICMP check from all hosts to each host

(D) Analysis of Load Balancer

Generally, load balancer serves resources requested by equal distribution to avoid overwhelming response, so to demonstrate load balancer functionality single topology of 6 hosts choosen over open vSwitch. Out of 8 hosts running on Linear topology depicted in Fig. 25 two hosts h1, h2 are set as python based http web server as shown in Fig. 26 and http web request from all other hosts using curl [12] utility was sent to web servers running on ip address 10.0.0.1 and 10.0.0.2. Controller is set on ip i.e. 10.0.1.1 and load balancer is executed as per the following command [12].

root@ubuntu:/home# pox/pox.py log.level–DEBUG misc.ip_loadbalancer –ip = 10.0.1.1–server = 10.0.0.1,10.0.0.2.

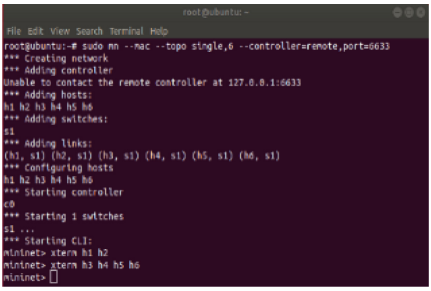


Fig. 26. Topology

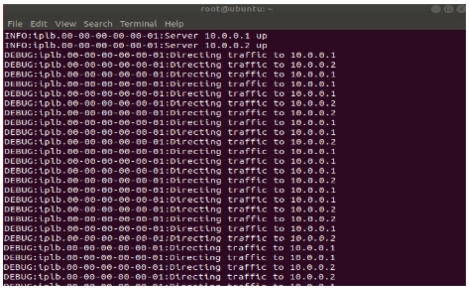


Fig. 27. Traffic distribution sent to host h1 and h2

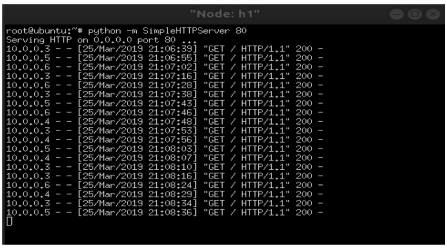


Fig. 28. Node h1 as web server

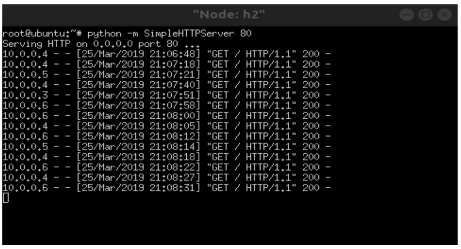


Fig. 29. Node h2 as web server

Fig. 30. Node h2

Fig. 31. Node h3

Fig. 32. Node h4

Fig. 33. Node h5

By looking at Fig. 26 observed that traffic was redirected equally to both the web servers and load balancing in terms of web request served is achieved over open vSwitch (Figs. 27, 28, 29, 30, 31, 32).

This way we have successfully demonstrated behaviour of same network switch to work as like anticipated functionality of network using software defined approach.

Now, Just to touch to throughput parameter of network, performance analysis achieved using iperf tool which says if controller is running locally within the subnet and outside the network e.g. Aws cloud there is slight variation have been obtained in case of hub and little more variation obtained in case of switch which was demonstrated for hub as well as for switch applications as shown in Figs. 33, 34, 35, 36, 37, 38, 39, 40 and 41.

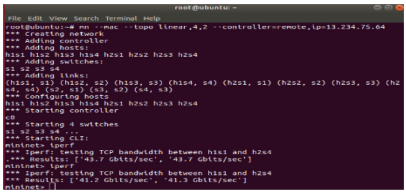


Fig. 34. Iperf results for hub running controller on AWS

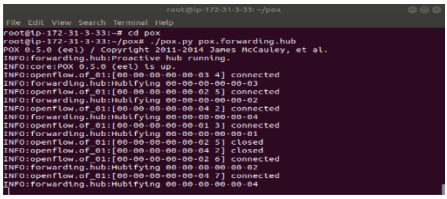


Fig. 35. Pox with hub app running on AWS

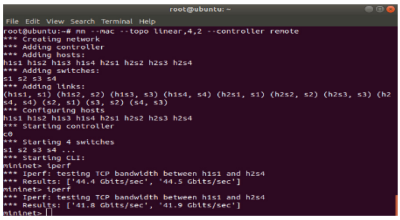


Fig. 36. Iperf results for hub running controller

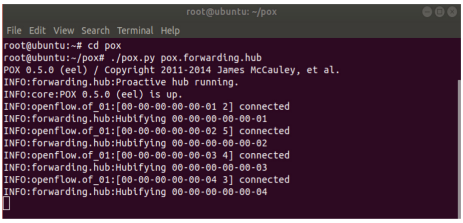


Fig. 37. Pox with hub app running on same machine locally

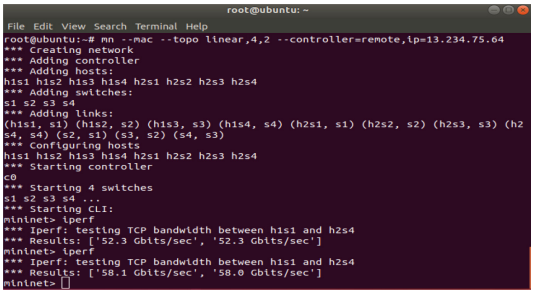


Fig. 38. Iperf results for switch running controller on AWS

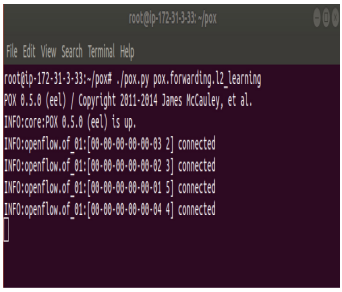


Fig. 39. Pox with switch app running on AWS

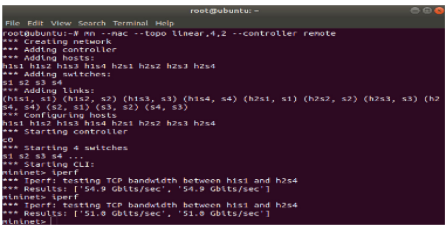


Fig. 40. Iperf results for switch running controller locally

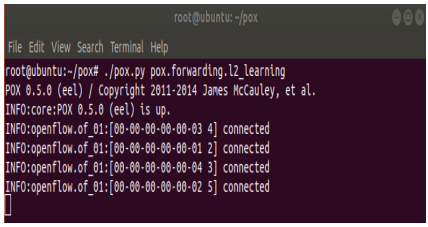


Fig. 41. Pox with switch app running locally

3 Conclusion and Future Scope

SDN is most acknowledged network architecture and has brought prosperity in network industry by allowing them to program to meet its anticipation as per functional role targeted. To get rid of from traditional and costly network boxes serves different purposes, one can make it behave by programming as per the functional role as and when required without the will and concent of the vendor. Major part is to choose right, flexible and easy to use controller, its position in the network by programming various network functions and its related features like how it tolerates the different network situation based on the various parameters of network may give call to various researchers to work upon and to provide optimized solution to leverage the life of network industry.

References

1. Prajapati, A., Sakadasariya, A., Patel, J.: Software defined network: future of networking. In: Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018) IEEE Xplore Compliant—Part Number: CFP18J06-ART, ISBN:978-1-5386-0807-4; DVD Part Number: CFP18J06 DVD, ISBN: 978-1-5386-0806-7
2. Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C.E., Azodolmolky, S., Uhlig, S.: Software-defined networking: a comprehensive survey. **103**(1). IEEE (2015)
3. Shaikh, M.Z., Darekar, S.H.: Performance anaysis of various open flow controllers by performing scalability experiment on software defined network. In: Proceedings of the International Conference on Inventive Computation Technologies (ICICT-2018) DVD Part Number: CFP18F70-DVD. ISBN:978-1-5386-4984-8
4. Asadollahi, S., Goswami, B., Sameer, M.: Ryu controller's scalability experiment on software defined networks. In: IEEE ICCTAC (2018)
5. Kaur, S., Kaur, K., Gupta, V.: Implementing openflow based distributed firewall. In: International Conference on Information Technology (InCITe). IEEE (2016). https://doi.org/10.1109/incite.2016.7857611
6. Kaur, K., Kaur, S., Gupta, V.: Software defined networking based routing firewall. In: International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). IEEE (2016). https://doi.org/10.1109/icctict.2016.7514590
7. https://mininet.org/overview. Accessed 17 March 2019

8. https://docs.openvswitch.org/. Accessed 18 March 2019
9. Pfaff, B., Davie, B.: The open vSwitch database management protocol. Internet Engineering Task Force, RFC 7047. http://www.ietf.org/rfc/rfc7047.txt (2013). Accessed 20 March 2019
10. https://noxrepo.github.io/pox-doc/html/. Accessed 19 March 2019
11. Gupta, V.: Software Defined Networking (SDN) made simple. https://www.udemy.com/sdnmadesimple/learn/v4/t/lecture/11065050?start=0 (2018). Accessed 15 March 2019
12. https://www.youtube.com/watch?v=nGV83dwfQMM. Accessed 15 March 2019

Review on Quantum Computing Tools and Algorithms

M. P. Madhu(✉) and Sunanda Dixit

Department of Information Science and Engineering,
Dayananda Sagar College of Engineering, Bangalore, India
madhump254@gmail.com, Sunanda.bms@gmail.com

Abstract. Computer performance improvement is one of the biggest challenges. The technology has moved towards increasing the performance by using Quantum computing which improves 20 times to decrypt the code compared to the classical computer. Quantum computing is computing which uses quantum mechanical phenomena. The main purpose of the quantum computing is to find algorithms which are considerably faster than the classical algorithms for solving the same problem. In this paper we are proposing the tools of quantum computing and different quantum algorithms. These ideas are first applied to classical computer and then to the quantum computer. We are also focusing on the architecture of quantum computing which is existing in literature.

Keywords: Quantum computing · Classical computing · Quantum algorithms · Superposition

1 Introduction

Scientists are planning to build a new type of computer called quantum computer as it has tremendous computing power which enables us to solve the tough mathematical problems that are holding back our progress in number of fields.

A classical computer performs calculations using the bits 0 and 1 in which 0 representing off and 1 representing on. It uses transistors to process the information in form of sequences of zeros and ones. More the transistors more will the computing power.

In classical computing bits has two possible states which are zero or one. In Quantum computing uses Qubit which is unit of quantum information. Qubit have special properties which solve the complex problem much faster than classical bits. One of the properties is superposition which states that instead of holding one value of either 0 or 1 like a classical bit, a Qubit can hold a combination of 0 and 1 simultaneously. Qubits have two possible states zero and one, but these states are superposition of zero and one. In Quantum world Qubit don't have to be one of those states. It can be any proportion of those states.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 714–719, 2020.
https://doi.org/10.1007/978-3-030-37051-0_80

2 Basics of Quantum Computing

A. Superposition of states

Quantum superposition [5] is the fundamental principle of quantum mechanics. It is much like a wave as in classical physics, in which superposing of any two or more states will result in another valid quantum state.

B. Qubits

Qubit [6] is the basic unit of quantum information. Qubit is a way of describing a quantum system of dimension two. The difference between the qubit and classical bit is that qubit can be in two states |0> and |1> or superposition of both states.

In classical bit, the bit will be in one state which is either 0 or 1.

Example: Spin of an electron in which two levels can be represented as spin up and spin down.

Raussendorf et al. [13] proposed a structure of quantum computation consisting of one-qubit measurement on a entangled state of particular class. They have described why underlying computational model is different from the quantum computing network model.

C. Quantum gates

Quantum gate is basic quantum circuit which operates on a smaller number of qubits. They act as building blocks of the quantum circuits.

D. Quantum Entanglement

Quantum entanglement [14] is a phenomenon which occurs when pair of particles or group of particles generate, interact in a way such that each particle quantum state cannot be described independently of the state of the other even if separation between the particles is large.

3 Quantum Algorithms

Feymann [1] have presented the scheme that the computation which is based on quantum physics would be much more exponentially efficient than the quantum physics. He proposed a quantum computer with his universal quantum simulator.

Deutsch [2] has showed means of quantum computing by formulating a description for quantum turing machine. He also specified the algorithm that is designed to run on quantum computer.

Shor [3] has published a quantum algorithm for integer factorization in 1994. The polynomial time is $(O(\log^3 N))$ for factoring the integer N. The Algorithm takes quantum gates of order $O(\log N)^2(\log\log N)$ $(\log\log\log N)$ using fast multiplication. The problem can be solved efficiently on a quantum computer and it is faster than the classical factoring algorithm. The Shor's algorithm efficiency is due to quantum Fourier transform which is more efficient than classical fast Fourier transform.

Grover [4] published quantum mechanical algorithm for searching an unordered database of size N. The algorithm takes $O(N^{1/2})$ steps which is faster than classical algorithm which takes (O(N)) steps. The Grover's algorithms provide quadratic acceleration whereas the other quantum algorithms which provide exponential speedup. The Grover's algorithm is probabilistic which gives correct answer when the probability is less than 1. The Grover's algorithm has a quadratic drop of complexity which has a lot of applications, namely in data retrieval.

These results are generalised and extended to related classes of problem.

4 Quantum Vs Classical

In classical computing, an electrical impulse is either represented as 1 or 0, where 1 represents the high voltage and 0 represents low voltage. In quantum computing, since state of the quantum object is not known until we observe it. Hence the superposition of all possible state happens. For example, consider the electron spin to a bit which are spin up = 0 and spin down = 1. We cannot know the exact spin of electron and thus superposition of all possible spins are created. The corresponding generated bit is called as "qubit".

In classical computer computation, if we take two bits each bit can have the value which is either 1 or 0, the possible combinations are 00, 01, 10 and 11. If we take the two electrons their possible spin can have both value 0 and 1 at the same time, hence they have much larger possible combinations when compared to number of bits allowed by classical computing.

5 Quantum Computing Architecture

5.1 Trapped Ion Architecture

Trapped ion architecture [7] uses charged atomic particles or ions to perform computation. To perform computation, the ions are confined or suspended in free space using electromagnetic fields. Using laser transitions the ions are brought to ground state which excites the electrons and they will come to lowest energy state provided some time.

The two methods of cooling using laser transitions which can be tuned to exact frequency are:

(1) Doppler cooling (2) Sideband cooling

Doppler cooling

Each atom will have a difference in energy between the ground and upper state. The two laser sources which are modulated slightly less than energy difference is kept facing each other on two sides of the atom. Due to doppler effect the atom will move towards one source or the other. The electrons will absorb additional energy difference from one of the sources and move to the first excited state. The electrons will decay from first exited state to ground state with emission of photon in different direction. The overall effect of absorption and emission of energy will reduce the momentum of

atoms. Due to this effect atoms will cool because the effect has further reduced the kinetic energy which results in cooling.

Sideband cooling

Sideband cooling is a technique to cool the atoms beyond doppler cooling limit. Along with excited state there are vibrational states. The drawback of the doppler cooling is that it will not reduce the atoms which are in their vibrational states. To excite these vibrational states and allowing them to return to their ground state we use laser tuned to difference in energy between excited state and vibrational state. This effect will allow the atoms which are in vibrational state to return to the ground state. The net effect is that we attain cooling lesser than doppler cooling (Fig. 1).

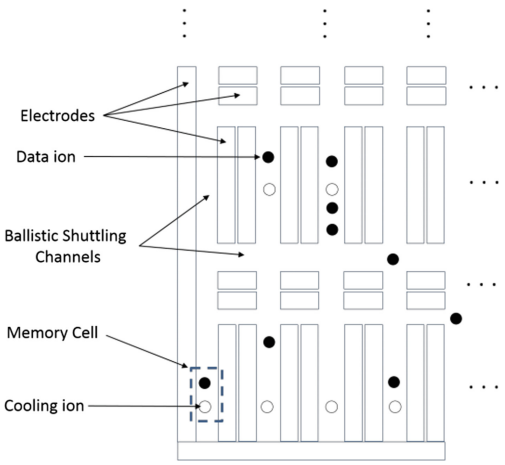


Fig. 1. Trapped ion quantum hardware

5.2 Quantum Computing Using Superconducting Qubits

Superconducting circuits [8] are the basis of the superconducting qubits. These superconducting circuits are made of quantum circuit which consist of capacitor and Josephson circuit for non-linearity and non dissipativity.

Quantum LC circuit and Josephson circuit are the basic element of superconducting quantum computer. The ladder of equal spaced states is formed by LC resonator, So the superconducting quantum circuit forms a multilevel system. But only two levels are needed among them to manipulate the qubits. Therefore, there exists a non-linear energy between the energy states in the ladder. Josephson junction is used to achieve this non-linearity.

6 Tools of Quantum Computing

6.1 IBM Quantum Experience

IBM Quantum experience [9] is the industry first initiative to build universal quantum computer for science and business. These IBM Q quantum devices are accessible by using Qiskit which is an open source programming network. At the IBM quantum experience website there are four modules which provides a short demo giving quantum computing principles and a quantum composer which allows to configure quantum gates for the qubits, a simulator for simulating their configuration, finally the access to the machine to execute the configuration and display the results.

6.2 Microsoft Quantum Development Kit

Microsoft Quantum development kit provides a new named quantum computing language called Q# [10] which is integrated with visual studio development environment. This Q# was built by Microsoft to succeed LIQUi | > and it is domain specific language which can used within Microsoft quantum development kit. It uses.NET Code SDK for easy creation, building and running quantum project using command line.

6.3 ProjectQ

ProjectQ [11] is an open source software implemented in python for quantum computing. It allows the user to execute the quantum programs in python using intuitive syntax. The structure allows testing of quantum algorithms and running them in actual quantum hardware in backend connecting to IBM quantum Experience cloud service.

6.4 Cirq

Cirq [12] is an open source Python library for writing, operating, and optimizing the Noisy Intermediate Scale Quantum (NISQ) circuits and executing them in quantum computers. It allows the researchers to write quantum algorithms for specific quantum processors.

7 Conclusion and Future Scope

Quantum computing assures to deliver new level of computational power. Quantum computing has many challenges and advantageous over classical computing. Some of the algorithms have already been implemented on small scale hardware. The paper concludes with the architecture of quantum computing. The algorithms are effective only on quantum computer, they tend to be less effective if they run on classical processor. Different algorithms of quantum computing and quantum computing tools existing in the literature has been summarised. As of today, a limited success is made in

field of quantum computing and a small number of Qubits have been designed so far. But its application will transform the field of computing. D-wave which is pioneer in the field of quantum computing is working with google in manufacturing qubits.

References

1. Feynmann, R.P.: Simulating physics with computers. Int. J. Theor. Phys. **21**, 467 (1982)
2. Deutsch, D.: Quantum theory, the church-turing principle and the universal quantum computer. Proc. R. Soc. Lond. A **400**, 97 (1985)
3. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE (1994)
4. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings 28th ACM Symposium on Theory of Computing (STOC'96), pp. 212–219 (1996)
5. Forcer, T.M., Hey A.J.G., Ross, D.A., Smith, P.G.R.: Superposition, entanglement and quantum computation, pp. 98–100
6. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press (2000)
7. Ahsan, M.: Architecture framework for trapped-ion quantum computer based on performance simulation tool, pp. 60–76 (2015)
8. Martinis, J.M., Osborne, K.: Superconducting qubits and the physics of josephson junctions, pp. 2–25
9. IBM Quantum Experience. https://www.research.ibm.com/ibm-q/
10. Ahmed, T.: Q#: a quantum programming language by Microsoft (2018)
11. Steiger, D.S., Häner, T., Troyer, M.: ProjectQ: an open source software framework for quantum computing (2018)
12. Cirq. https://ai.googleblog.com/2018/07/announcing-cirq-open-source-framework.html
13. Raussendorf, R., Browne, DE., Briegel, H.J.: Measurement-based quantum computation with cluster states, Los Alamos e-print arXiv (2003). http://arxiv.org/abs/quant-ph/0301052
14. Kranjcevic, M., Kirsek, F., Kunstek, P.: Quantum computing, pp. 2–3

Application of Cooperative Communication System in Driverless Car

Subhajit Mukherjee, Ritwick Mukherjee(✉), and Abhishek Dey

Technique Polytechnic Institute, Hooghly, West Bengal, India
mukherjee.subhajit91@gmail.com, rml1031998@gmail.com,
abhishek.dey.ece@gmail.com

Abstract. The life of human beings is getting more dynamic in this era. So, every person needs to have a safer driving feature which supports their dynamic life. Self-driving or driverless car is getting popular day by day due to its low transportation cost which can result in better accessibility of those persons belonging to economically backward classes. A driverless car can drive in an autonomous way towards the destination safely with the help of GPS based road map which can be downloaded from a GPS server in collaboration with GPS satellites. But the problem with this present system is that if the number of the driverless car increases in a city that will lead to the congestion which results in overcrowding of GPS server. So the delay in the system will increase proportionally. One solution to this problem may be the cooperative communication through which vehicular communications can improve the wireless transmission capacity and reduces the server overloading due to its distributed features. In this paper, we have proposed a next-generation vehicular technology using an ad-hoc cooperative communication system consisting of vehicles and BTSs with small database consists of surrounding destinations.

Keywords: Cooperative communication · Driverless car · Arduino microcontroller · Bluetooth transceiver · Ultrasonic sensor

1 Introduction

The drastic changes in robotic systems increase the demand for a smart robotic platform which will be autonomous and more intelligent [1]. An example of such a robotic system is an autonomous vehicle or driverless car. Lots of research work has been carried out on autonomous vehicles based on RADAR or LIDAR as sensing element [2], automatic braking and adaptive cruise control facility [3], car controller tuning through Bayesian optimization [4], collision protection and GSM based destination guiding facility [5], GPS guided driving facility [6, 7] along with obstacle detection using infrared or laser sensors [8]. In the future fifth-generation (5G) cellular networks, denser and smaller cells are expected to provide a high transmission rate for users. Different from traditional personal users, vehicles are sensitive to transmission scenarios in 5G cooperative small cell networks. Moreover, due to the mobility nature of vehicles and the related high vehicular speed, the topology of vehicular wireless networks becomes highly dynamic and prone to recurrent links intermediately [9].

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 720–727, 2020.
https://doi.org/10.1007/978-3-030-37051-0_81

Figure 1 shows the system model of 5G cooperative small cell networks which can be used for vehicular communications. The individual base station shown in this figure forms a cellular region which can be different in size based on the velocity of the vehicles. For vehicles, with lower velocity, a microcell, picocell, or femtocell can be used whereas a vehicle with higher velocity uses macrocell for communication purpose. Each cell is interconnected with their neighboring cells as well as with the backbone network to form a fully connected and robust network for vehicular communication. Since the network will be denser, therefore, the number of BTSs are required to form this type of network is also increases proportionally. So, it is expected that the base stations will be cheaper in price so as to provide the autonomous vehicle services to the peoples belonging to economically backward classes [10]. In this paper, we proposed a prototype model of driverless car which is made of using low-cost microcontroller module, sensors, and wireless transceiver modules and the base station is also made of using those low-cost devices so that it can be accessible by all category of peoples belonging to different economic classes.

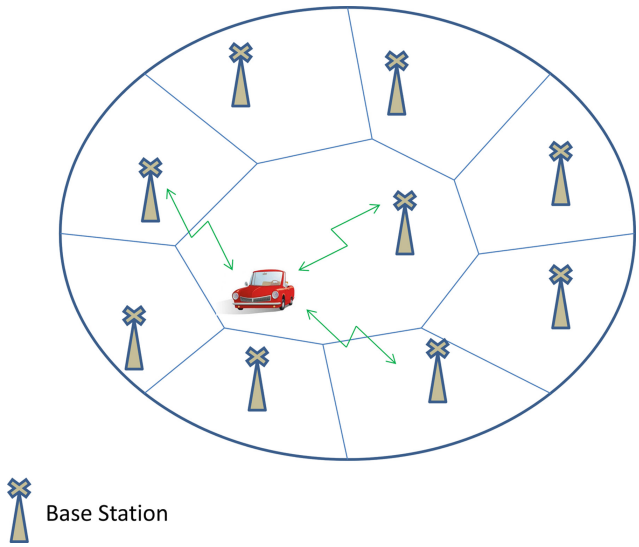


Fig. 1. System model for next generation vehicular communication system

2 Description About the Proposed System

2.1 Block Diagram

In this paper, we proposed a novel vehicular communication system where individual signaling post at any junction point of a road will perform the role of base station (BTS) which have a small database consisting of pin codes as nearby location information and a list of default route information for the prefix of those pin codes which are

not under its coverage region. When a BTS receives a destination request from a vehicle, it finds in its database about the location. If the location has been found from the database, then it sends the route information to the vehicle for the corresponding destination. There will be a central server with GPS connectivity consisting of a global database of route information about a city or a state in a country which will connect all the local BTSs residing at each junction points of roads through some backbone networks. If the local BTS fails in finding the destination route information sends by the car then it will fetch the information from the central server and forwards the information to the car. By receiving the route information the car will move towards the destination by properly utilizing all of its automatic control circuitry and sensors information about the surrounding obstruction (Figs. 2 and 3).

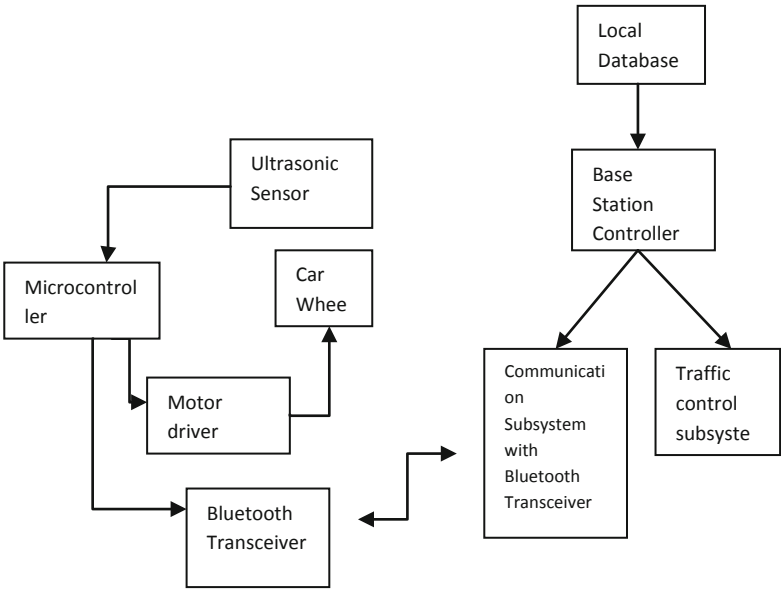


Fig. 2. Proposed model of our system

2.2 Flow Chart

In our proposed model the BTS or Base Transceiver Stations are merged with the existing traffic signaling post resides at the divider of two or more roads. The BTSs are worked with a principle such as they will have a local database consisting of the surrounding destination information. The routing of the vehicles will be performed based on the pin code of the destination address. Depending on the first few digits of the pin code the BTS can identify the destination location in terms of the country, state, city, and lane. When BTS will get a request destination message from Car then BTS first check its local database for the destination. If found, then it will send the destination information to Car using a wireless interface. If the local database has not contained destination information, then it will search the destination information

around its surrounding BTSs and if again not found then the BTS will send the request about destination address to central server which may have GPS facility or global database consisting of the route information of a city or a state in a country. The central server searches the route towards the destination with the help of its own database or GPS facility and sends the entire route information consisting the all the intermediate BTSs address towards the destination to the BTS which will again be transmitted to the

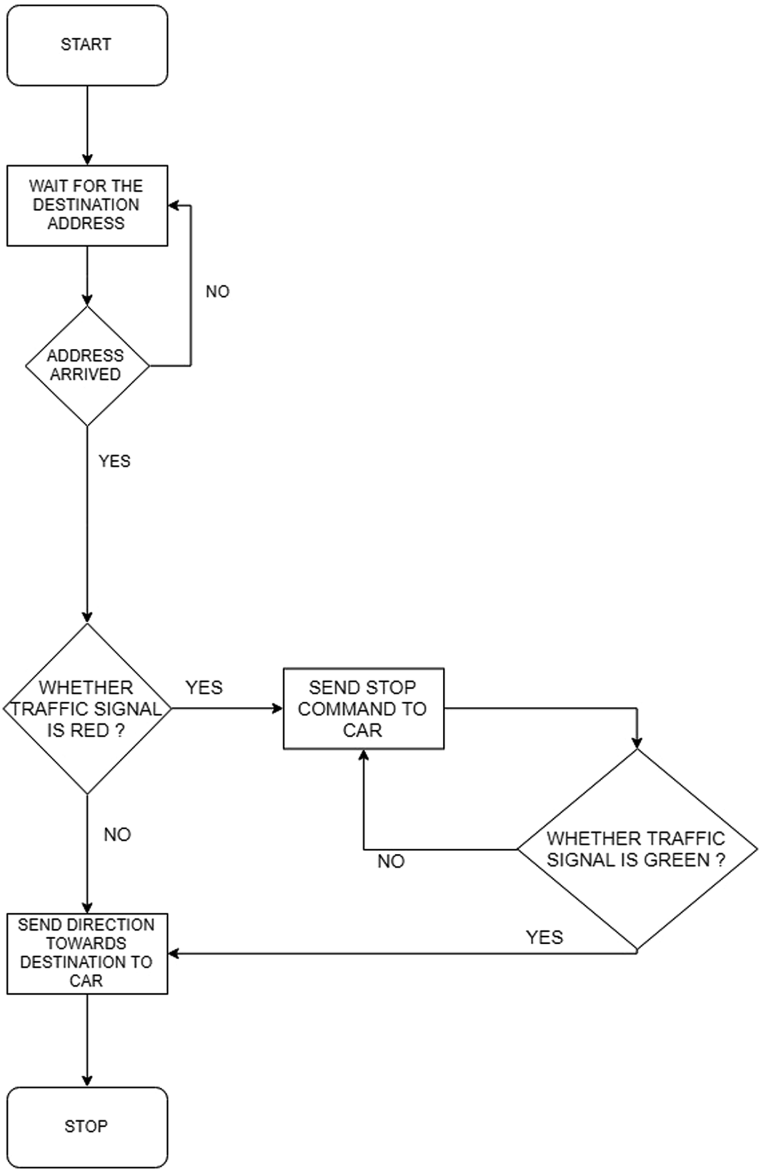


Fig. 3. Flow chart of BTS

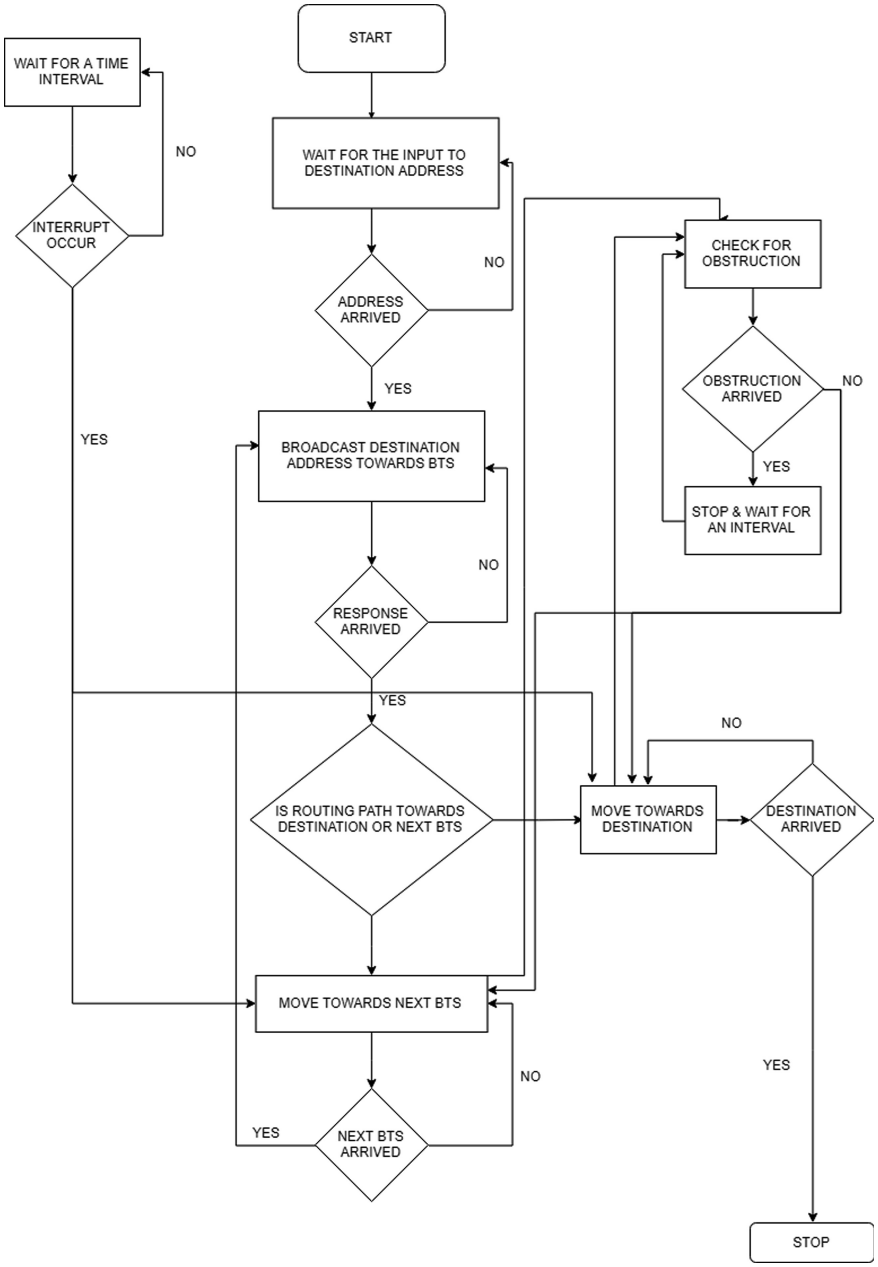


Fig. 4. Flow chart of car

Car for successfully driving to the destination. The car after getting the direction from the BTS start running towards the next BTS or destination. During the traveling of the car, an interrupt will generate in every periodic fixed time interval which will force the

car to check any obstruction towards its path in order to avoid any accidental phenomenon. The details of the flow chart about working of car and BTS is depicted in Figs. 4 and 5 respectively.

2.3 Circuit Diagram

In the circuit diagram of the prototype of the car, we used Arduino uno r3 as a microcontroller unit along with a car chassis consisting of 4 dc motors controlling by a motor driver ic and a Bluetooth transceiver module for communication with the BTS. Also, the car module consists of an ultrasonic sensor for detection and measurement of

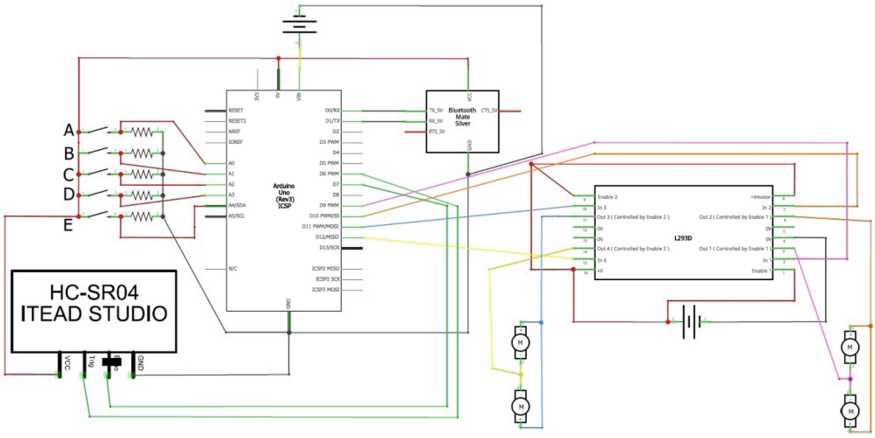


Fig. 5. Circuit diagram of car

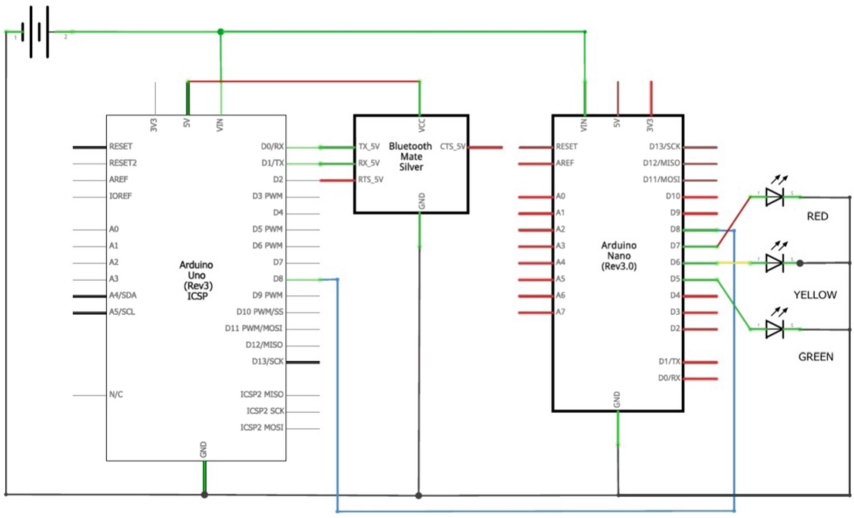


Fig. 6. Circuit diagram of BTS

any obstruction within its vicinity. The BTS module is made by one Arduino uno r3 microcontroller with a Bluetooth transceiver module for communication with vehicles and one Arduino nano microcontroller for controlling the traffic light. The details of the circuit diagram of car and BTS is shown in Figs. 5 and 6 respectively.

3 Conclusion

Also, the efficiency in detection of static and dynamic obstacles has to be addressed in future development. In this paper, the vehicular technology for driverless car has been implemented for 5G cooperative small cell networks. Based on the location information within the database of Base stations the car can be routed towards its destination. Furthermore, the collisions with environmental objects and other vehicles can be avoided with the help of ultrasonic sensor. The base stations are performed traffic controlling tasks and communication tasks with vehicles in a time shared basis. Therefore, with the help of our proposed model we can reduce the number of human interventions in driving the car which further reduces the probability of accident due to unconscious mind of driver. Our model is limited to only a small area with location information of pin codes of regions. In our future plan we will extends our model over larger area using the implementation of handoff facilities within base station, security issues in sensor networks [11, 12] and with incorporation of advanced routing algorithm.

Acknowledgements. The authors would like to express their sincere gratitude to Mr. S. N. Basu, Executive Director of Technique Polytechnic institute, Mr. Avijit Karmakar, Principal of Technique Polytechnic institute and Mr. P. S. Bhattacharya, Coordinator of Technique Polytechnic institute for their valuable comments and a fruitful discussion.

References

1. Babu, G.A., Guruvayoorappan, K., Variyar, V.S., Soman, K.P.: Design and fabrication of robotic systems: converting a conventional car to a driverless car. In: IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), September 2017
2. Rajasekhar, M.V., Jaswal, A.K.: Autonomous vehicles: the future of automobiles. In: IEEE International Transportation Electrification Conference (ITEC), August 2015
3. Bimbraw, K.: Autonomous cars: Past, present and future a review of the developments in the last century, the present scenario and the expected future of autonomous vehicle technology. In: 12th International Conference on Informatics in Control, Automation and Robotics (ICINCO), July 2015
4. Su, J., Wu, J., Cheng, P., Chen, J.: Autonomous vehicle control through the dynamics and controller learning. IEEE Trans. Veh. Technol. **67**(7) (2018)
5. Banerjee, T., Bose, S., Chakraborty, A., Samadder, T., Kumar, B., Rana, T.K.: Self driving cars: a peep into the future. In: 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), August 2017

6. Run, R.S., Yen, J.C., Tsai, C.Y.: A low cost implementation of GPS guided driverless cars. In: 5th IEEE Conference on Industrial Electronics and Applications, July 2010
7. Broggi, A., Cerri, P., Debattisti, S., Laghi, M.C., Medici, P., Molinari, D., Panciroli, M. and Prioletti, A.: PROUD—public road urban driverless-car test. IEEE Trans. Intell. Transp. Syst. **16**(6) (2015)
8. Jianmin, D., Kaihua, Z., Lixiao, S.: Road and obstacle detection based on multi-layer laser radar in driverless car. In: IEEE 34th Chinese Control Conference (CCC), September 2015
9. Ge, X., Cheng, H., Mao, G., Yang, Y., Tu, S.: Vehicular communications for 5G cooperative small-cell networks. IEEE Trans. Veh. Technol. **65**(10) (2016)
10. Bagloee, S.A., Tavana, M., Asadi, M., Oliver, T.: Autonomous vehicles: challenges, opportunities, and future implications for transportation policies. J. Modern Transp. **24**(4), 284–303 (2016)
11. Praveena, A., Smys Quot, S.: Anonymization in social networks: a survey on the issues of data privacy in social network sites. Int. J. Eng. Comput. Sci. **5**(3) (2016)
12. Praveena, A., Smys Quot, S.: Efficient cryptographic approach for data security in wireless sensor networks using MES VU. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1–6. IEEE (2016)

Check for updates

RETRACTED CHAPTER: ID Card Detection Using Histograms of Oriented Gradients

Bala Murali, Abhilash Akula(✉), Ega Jeshwanth, and Thota Kalyan Kumar

Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai 600089, Tamil Nadu, India
Balamurali_29@yahoo.co.in, abhilashakula99@gmail.com, jeshwanthega@gmail.com, kmrkalyanl998@gmail.com

Abstract. ID card location innovation assumes a significant job in the present society to recognize the data database in different areas. Histograms of Oriented Gradients is the most broadly perceived part descriptors in picture planning and PC vision and is used for article ID. High-security ID check is an extremely intense activity. Present day object distinguishing proof and acknowledgment has progressively transformed into a critical issue in various on-going applications like security frameworks and government owned reserve funds systems. The ID card can be definitely perceived by utilizing an institutionalized scanner, for example, a standardized tag scanner. The specific customer honestly takes a gander at the given information on the ID card and after that thinks about it to the information effectively given to check whether it matches. This sort of ID is used precisely to strikingly separate customers faster and is dynamically powerful to give unmistakable access control courses of action. The trial results led show that this technique can be utilized to get the careful data of an individual and the required information.

Keywords: Histograms of oriented gradients · Identification card · Barcode canner · Anti-fraud identification

RETRACTED CHAPTER

1 Introduction

In the present society character extortion is an extremely huge issue with genuine results. There have been various security issues and various arrangements have been proposed to realize the said hypothesis LBPH to reasonably get the needed results. The guideline method executed here is that the ID card is inspected utilizing an institutionalized standardized identification scanner to recognize whether the data of the individual is fake or not. A short time later, the image of the individual is researched to get the required subtleties from the database.

The original version of this chapter was retracted. The retraction note to this chapter is found at https://doi.org/10.1007/978-3-030-37051-0_109

© Springer Nature Switzerland AG 2020, corrected publication 2024
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 728–734, 2020.
https://doi.org/10.1007/978-3-030-37051-0_82

The element descriptor-Histogram of Oriented Gradients is overwhelmingly used in picture taking care of for the reason of article ID. The crucial usage of Histogram descriptor is utilized in pictures for human ID.

LBPH (Local Binary Pattern Histogram) methodology is a standout amongst the most easy counts in the field. We intend to give a figuring to effectively recognize the image and output the scanner tag (i.e.) the standardized identification scanner to get the required information for ID card acknowledgment.

LBP choices are considered here to make a part vector that recognizes a face from a non-face. Each component from the image is divided into little squares.

For recognition, the Local Binary Pattern (LBP), a calculation, is utilized that will rely upon the neighborhood double administrators. It is an outrageous [illegible] algorithmic guideline, extensively used, as a result of its ease in calculation.

Histogram of Oriented Gradients is generally used to identify the facial highlights or even the human body. To extend the adequacy of article acknowledgment, gamma and shades of the image should be institutionalized.

The item look for relies upon the recognizable proof of small pictures portrayed by sliding the identifier window that analyzes every single piece of the given info and its scaled structures. A descriptor is assigned to each pointer window.

This descriptor includes all the cell histograms for each district in the location window. This window is utilized for getting the expected information to distinguish the items. Planning and checking everything about by the utilization of this descriptor. There are various systems accessible to describe items, for example, descriptors like, neural systems, SVM (bolster vector machine, etc.

The HOG is one of the institutionalized techniques for human structure arrangement. To perceive people, stand up to area and picture affirmation may similarly be associated. In any case, the Histogram of Oriented Gradients is a not too bad descriptor for article acknowledgment and face affirmation.

We will in general investigate a basic yet a solid method to deliver string use of HOG features for face recognizable proof. So as to finish botches in facial segment disclosure because of hindrances, cause and delineation, we will in general propose HOG descriptors from a common structure. Likewise, blend of HOG descriptors at absolutely uncommon scales permits getting significant structure for face acknowledgment.

2 Related Works

There were numerous other related takes a shot at picture getting ready and item disclosure and here we select a couple of significant papers.

Fang et al. [1] This paper utilizes MATLAB stage for the task. The pre-treatment is thresholding which is finished with the assistance of OTSU calculation then the subsequent thresholding pictures utilizes high pass sifting and normal format for evacuating interface and smooth the picture.

At that point the procedure is prepared with character division which was separated into two sections line fragment and segment split. Character pictures on projection

RETRACTED CHAPTER

pivot are portioned by line division and limit esteem and determined and store by utilizing section split calculation.

Results are additionally handled to character acknowledgment. In this session the characters are standardized and diminished. At that point utilizing layout coordinate calculation is utilized for acknowledgment. At that point SVM comes to scene to get highlights and to prepare model which can be utilized to perceive.

Navneet Dalal and Bill Triggs utilized an all the more straight-forward strategy, to show frameworks of the Histogram of Oriented Gradients (HOG) descriptors through and through beat the present strategies utilized for human acknowledgment. Bolster Vector Machine (SVM) was utilized for improving the speed and the straightforwardness of this strategy. On execution of this technique, fine-scale tendencies, fine presentation binning, respectably coarse spatial binning, and splendid neighborhood separate institutionalization in covering descriptor squares are particularly significant for good results. Recognizable proof and Distinguishing human in video perception structure correspondingly expect a key employment in improving exactness and guaranteeing open property.

A framework for human recognizable proof in various appearance, obstacle, under uneven illuminations and positions has been planned. Another proposed framework for distinguishing human by improving the HOG was advanced by the author. There were some different takes a shot at acknowledgment of ID cards on secure norms.

The principle purpose behind distinguishing proof is to give an exact and safe individual data. Another examination was likewise made on verification distinguishing proof reliant on Image affirmation. Appropriate systems have been utilized for picture recognizing strategy, for instance, Machine method, Support Vector Machine (SVM) and Character recognizing confirmation. Constrained counts were utilized to botch the rate of division.

The character affirmation and the image division fall under the essential piece of the Image acknowledgment. In the process to distinguish the article, the writers gave the introduction of the component descriptor, for example Hoard (Histogram of Oriented Gradients), that is utilized to beat the confinements in the current counts face to face by walking disclosure.

RETRACTED CHAPTER

3 Local Binary Patterns

For facial appearance order Local Binary Patterns (LBP) has been seen to be a groundbreaking trademark; it's moreover been set up that once LBP is united with the Histogram of Oriented Gradients (HOG) descriptor, it upgrades the ID execution basically on some datasets.

The underlying stage in HOG acknowledgment is to parcel the source picture into squares (for example 16 × 16 pixels). Each square is additionally separated into littler parts called cells (for example 8 × 8 pixels). Usually, squares spread one another (i.e.) they cover each other, so a comparable cell is in various squares.

The flat and vertical slopes are gained for each pixel inside the cell. Histograms of edge introductions are made by the HOG algorithmic guideline from bound patches found in the photos. A fix could come back from an article, an individual, unimportant

establishment and is only some way to deal with illuminate a locale utilizing edge information.

As said before, this information will by then be used to improve an AI algorithmic rule like the help vector machines to set up a classifier prepared to remember one sort of article from another. This has the favored viewpoint that in greater scales the HOG features give a lot of world information, and give fine-grained detail in littler scales (in little sub-divisions).

The shortcoming is that the last descriptor vector increases, in this manner setting aside more effort to pull back and to plan suing the classifier which is given. In the possibility of LBP arrangement of surfaces, the occasion of LBP codes is amassed into a histogram. The facial picture is apportioned into littler areas. Autonomously these LBP surface descriptors are extricated from each locale.

This histogram suitably intertwines a depiction of the look on a completely changed elements of locale: the information of the examples on the pixel-level is contained in the histogram of the LBP, the marks are considered over a little zone to give data on a common measurement and in this manner these histograms are utilized to give a general portrayal of the face which is shown in Fig. 1.

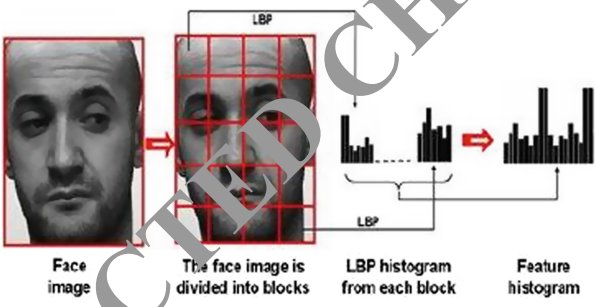


Fig. Face description with local binary patterns [7]

4 Working Principle

To beat the downsides of the past work, a structure has been proposed wherever picture taking care of and standardized tag scanner is used to find the highlights of an individual.

The strategy for Local Binary Pattern is defrauded to complete the picture handling. In an incredibly thick system the arranged picture angle introductions neighborhood histogram is assessed. this is often executed by dividing the image window into minimal spatial areas (i.e.) "cells", for every pixel of the cell storing up an adjacent 1-D histogram of tendency headings or edge introductions and that is shown in Fig. 2.

Picture preparing is done to improve the nature and nature of the digitized picture. It names the pixels of an image and the result is conveyed as a twofold territory. The standardized tag scanner is used to recognize an ID card. The information is spared in

RETRACTED CHAPTER

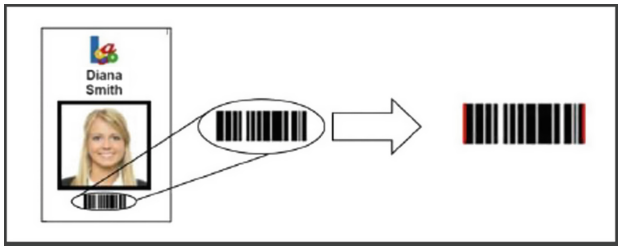


Fig. 2. Barcode verification process [3]

the database and the scanner finishes the filtering procedure. Here the LBP executions are being clarified and the finder exhibitions choices are inspected intently.

The pyzbar library is used in python to recognize and disentangle the QR and different codes. At first, it will recognize the kind of QR and standardized identification being filtered. Presently the information contained in the standardized identification will be appeared. An accumulation of focuses indicates the area of codes. There are four to signify the four corners of the QR codes. A gathering of focuses checks the start and end of word constrains in the standardized tag scanner. The ID card database will be inspected when a number is delivered and it is shown in Fig. 3.

RETRACTED CHAPTER

Fig. 3. Face detection analysis in ID card [3]

The image filtering in the ID card is finished. The face in the ID card is perceived using the LBPH and is confirmed with the image in the Identification card database. By then when the perceived face is found in the database under the number which is delivered by the scanner tag, it is checked that the ID card is a unique one. In case, if there is no counterpart for the face in the ID card under the number created by the institutionalized ID, at that point the ID card is phony which is shown in Fig. 4.

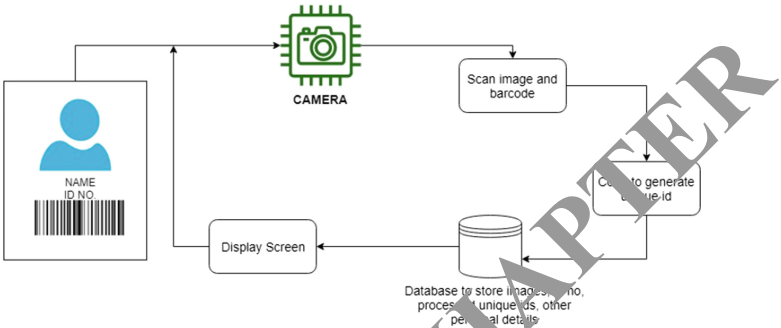


Fig. 4. Filtering approa

5 Experimental Results

The LBP logic has provoked ess tial progression in surface examination. It's comprehensively used wherever all through the globe both in examination and applications. From the execution reason for ee, we have made the area of ID card affirmation structure faster, accurate and automated which crushes every one of the issues present in the present system. It cost-amazing, capable and beneficial strategy to use.

Acknowledgeme All author states that there is conflict of interest. We used our own data. Animals/huma ar not involved in this research work.

Ref rences

1. ng, X., Fu, X., Xu, X.: ID card identification system based on image recognition library for support vector machine [EB/OL]. http://www.csie.ntu.edu.tw/∼cjlin/libsvm/, 2015 12–14, pp. 640–656
2. Bardeh, N.G., Palhang, M..: New approach for human detection in images using histograms of oriented gradients, ©2013 IEEE, pp. 753–767
3. Leibe, B., Seemann, E., Schiele, B.: Pedestrian detection in crowded scenes. In: 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2005), pp. 876–885 (2005)
4. Ladicky, L.: Global structured models towards scene understanding. Ph.D. Dissertation, Department of Engineering Sciences, Oxford Brookes University (2011)

RETRACTED CHAPTER

5. Lowe, D.G.: Distinctive image features from scale invariant key points. Int. J. CV **60**(2), 91–110 (2004)
6. Dalal, N., Triggs, B.: Histogram of oriented gradients for human detection. In: 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (2005)
7. Dalal, N. Triggs, B., Schmid, C.: Human detection using histograms of flow and appearance. In: European Conference on Computer Vision, pp. 886–893 (2006)
8. Bajpai, M., Prakash Agrawal, A.: Integration of 2D secure barcode in identity cards: a new approach. Int. J. Eng. Comp. Sci. **2**(4) (2013)
9. Kim, D., Mun, Y.: Design and performance analysis of multimedia teachware making system using 2D barcode. In: Proceedings of ICCSA 2006 on Computational Science and its Applications, pp. 195–203 (2006)
10. Chowdhury, S.A., Saki Kowsar, M.M., Deb, K.: Human detection utilizing adaptive background mixture models and improved histogram of oriented gradients. Korean Inst. Commun. Inf. Sci. (2017)

RETRACTED CHAPTER

Resolving Unfairness Issues in Cognitive Radio Networks with Collision Based Primary Users

Chaitali Chaudhari(✉), Hemlata Patil, and Sujata Kadam

Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, India
chaitalipc24@gmail.com, hema.patil08@gmail.com,
sujatakadam7890@gmail.com

Abstract. Cognitive Radio (CR) is an adaptive, intelligent radio and network technology which automatically detects available channels in a wireless spectrum and changes transmission parameters enabling communications to run at the same time as and also develops radio operating behavior. It is viewed as a novel approach for improving the utilization of a precious natural resource: the radio electromagnetic spectrum. Cognitive radio network consist of primary network and secondary network. Primary users are licensed users and secondary users are unlicensed users. Whenever the channel band is found idle secondary users can occupy it without jeopardizing the communication of primary user. Priority is to serve primary user first on the channel. But there are lot of interferences caused by both the users. Solutions proposed are not able to deal with multiple CRN's without centralized coordinator. This problem arises in coexistence heterogeneous networks. Several Markov chain models are proposed to deal with the solution which consist of decentralized MAC protocol to solve the unfairness issues. Fairness is one of the issues to solve and for this purpose probing is done. Simulation results shows how fairness is achieved and each user has got fair chance to serve on the channel.

Keywords: Cognitive radio · Primary user (PU) · Secondary user (SU)
Channel accessing · MAC protocol · Fairness · Probing

1 Introduction

As there is wide increase in applications, the number of wireless user's increases for which Radio spectrum becomes the natural and essential resource. Due to this, spectrum scarcity problems are created by number of users giving an opportunistic way for a potential technology: Cognitive Radio [1]. Cognitive radio is considered as an objective towards which a software-defined radio platform should evolve: a fully reconfigurable wireless transceiver which mechanically adapts its communication parameters to network and user demands. It is a flexible and efficient technology to solve the future spectrum management which can greatly improve spectrum utilization. Statistics of Regulatory bodies in the world (including the Federal Communications Commission's in the United States and Of com in the United Kingdom) said that temporal and geographical variations in the use of assigned spectrum range from 15% to 85% [2]. The spectrum which is unused is referred as spectrum hole or white space.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 735–744, 2020.
https://doi.org/10.1007/978-3-030-37051-0_83

In next generation technology it is a need to use this wasted spectrum in an efficient way with the help of cognitive radio. CR networks have a fascinating concept of using this spectrum when licensed band is unused.

2 Literature Survey

Spectrum is natural resource but increase in cellular communication has led to the spectrum scarcity. To solve this canonical architecture called Cognitive radio is used [1]. In this type of architecture hardware is simple and functions are software defined. It introduces new channel access modes into bands where established modes must be accommodated in bands for years. Cognitive radio wireless communication is immense hence its is referred as "disruptive but unobtrusive technology" [3]. A radio scene analysis is required which gives exact scenario of how spectrum is used and led to determination of spectrum holes. A proper spectrum sensing algorithm is required to know about spectrum depending upon various aspects of sensing talk. Challenges as well as enabling algorithms are discussed in [4, 5]. This gives better idea to use proper technique. In cognitive radio network it consist of licensed and unlicensed user. So both user faces lot of interference. First type of interference is from licensed user to unlicensed user and second one is unlicensed to licensed one. Dynamic spectrum leasing rewards the licensed user as they allow unlicensed user to operate in their licensed spectrum [6]. This gives an incentive to primary users as they gives a way to secondary user to utilize the spectral opportunities. To utilize the spectral opportunities various MAC protocols are proposed for cognitive radio network [7]. Decentralized design brings the advantages of fast deployment and flexibility. To operate in synchronized network there is need of decentralized MAC protocols [8]. It provides priority spectrum access to PU and limit the interference to PU by collecting the information from sensing the channel and managing spectrum sharing. There are challenges faced by cognitive radio network. These challenges are required to be overcome to achieve spectrum efficiency. One of the problems is to achieve fairness in cognitive radio network. FMAC-MAC protocols developed for cognitive radio network and most of them does not consider coexistence problem in this network [9]. FMAC uses a two-state spectrum-sensing model to distinguish whether a busy channel is used or idle from nearby CRN. PU uses IEEE 802.11 Distributed coordination function [10]. OC-MAC serves the secondary users by use of probing function which observes the channel for particular period of time [11]. OC-MAC has been modified to CCR MAC which is used by secondary user. The specifications of CCR MAC are same only it is used for coexistence cognitive radio networks. MAC protocols in cognitive–radio are carrier sense multiple access with collision avoidance (CR-CSMA/CA) which coordinate the channel access of secondary users and to protect primary user from interference of secondary user [12]. CR-CSMA/CA Varies users with offered traffic load of secondary users and spectrum utilization rate of primary users. CCR MAC serves good channel selection by use of probing and jamming function. This coexistence is due to PU and SU causing unfairness problems. A synchronized heterogeneous cognitive radio networks causes coexistent problems [13]. Various Markov Chains are studied

with channel models by applying probing and jamming function. Protection to primary user's traffic is also provided by enhancing fairness feature.

3 Cognitive Radio

For reconfiguration a cognitive radio looks naturally to software defined radio and for their tasks of cognitive kind it looks to signal processing and machine learning procedure. Cognitive radio cycle basically focuses on three tasks i.e. radio scene analysis, channel identification and transmit power control and dynamic spectrum management [3].

The functional aspects of cognitive radio network include spectrum sensing, spectrum management, and spectrum sharing and spectrum mobility while dealing with radio spectrum [4]. Various spectrum techniques have been evaluated for cognitive radio network. Practical challenges are still to be covered in spectrum sensing. The detection schemes include transmitter detection, cooperative detection and interference based detection [5]. This paper uses the popular solution of transmitter detection which are implemented towards sender side. Cooperative detection is a mechanism in which results are decided by a group of SU's while Interference detection schemes operates by sender and receiver in a pair.

Tradeoffs between accuracy and overhead in spectrum sensing and PU - detection mechanism must be considered. Basically SU's which originate from synchronized networks may have variable PU detection ability. Thus lack in PU detection ability may affect the system leading to unfairness problem in cognitive radio network.

This paper deals with causes of unfairness problem in coexistence synchronized networks and proposes a MAC solution. Markov Chain approach is studied which focuses to serve secondary user without affecting the primary user. MAC layer approach are designed and verified under various models. Mathematical models proposed are used in this paper for better results. All simulations are carried out in Network Simulator 2(NS2) to show the effectiveness of proposed system.

4 Issues of Cognitive Radio Network

Mostly there are three problems associated with synchronized networks which include uncoordinated spectrum unit size, uncoordinated PU-detection ability and coexistence of heterogeneous CRN's. Uncoordinated spectrum unit size problem occurs due to various spectrum sizes of secondary user and this problem is solved by using a self blocking mechanism with SU's accessing strategy. The second issue is uncoordinated PU detection ability which occurs due to variable PU detection.

Abilities of secondary users. That means SU's throughput depends upon PU's utilization on spectrum. Therefore it is necessary to identify the problems which type of user has accessed the spectrum. For this purpose MAC-layer approach which improves PU detection ability avoiding limitation of hardware capacity is proposed. The third problem can be solved with help of use of spectrum broker but in proposed scenario CRN's are not assumed to be centralized framework. Proposed scenario consist of

PU's, SU's and TSU's (an aggregate group of SU from another CRN). The user type and its priority is kept as it is in [13]. A distributed MAC protocol CCR-MAC protocol is used to solve the first two unfairness issues without a centralized coordinator avoiding harmful interference to licensed holder.

5 System Model

Consider a cognitive radio network consist of 'K' number of secondary users and 'M' primary user channels. The system model for the network is shown in Fig. 1. The main aim of cognitive radio is to sense the channel and identify the vacant channel to allocate it for transmission of data for SU. It continuously checks if PU's are transmitting on the spectrum. If no PU has been detected then it informs SU about the vacancy on radio spectrum after which if majority of SU detect the channel empty SU's broadcast message with their ID and job time on MAC layer. The secondary users will be now served on unprocessed priority. Suppose if we consider secondary users SU_1, SU_2 and SU_3. SU_1 and SU_2 had got the chance to access the spectrum. After that SU_3 and SU_1 are detected then first it is going to serve SU_3 as it has never got the chance to access the channel spectrum. Whenever the PU comes in between, the secondary systems has to stop the transmission and move towards next current available channel.

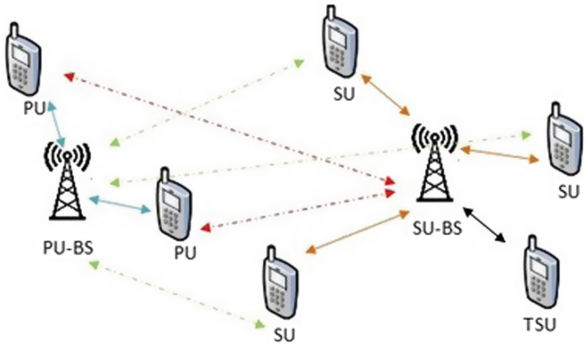


Fig. 1. Cognitive radio network

A decentralized energy efficient MAC protocol to minimize spectrum scarcity problems and to provide access to SU on the radio source is been implemented [7, 8]. This protocol combines jamming and probing for secondary users. SU is continuously observing the channel and should continue its communication without causing any harm to PU. But secondary usage of channel by SU can lead to decrease in throughput of PU. This decline in throughput is because of jamming which is an overhead of SU's secondary usage. So to control this throughput decline, use of probing function is done. MAC protocol combines with jamming and probing to solve the issues in coexistence heterogeneous CRN's.

CCR MAC inherits same characteristics as that of OC-MAC [11]. OC-MAC protocol requires less information and it is better in terms of throughput and provides better protection to PU. Similar to this CCR-MAC also requires less information which is gathered by SU [13]. Practically it is impossible to have information about the exact scenario in CR network. To avoid any harmful interference to PU probing function is combined with self blocking mechanism. Probing function can jam a channel with a probability of p, where $0 < p < 1$. Lesser is the value of p, less is advantage to TSU and high protection to PU's traffic. Jamming rate is given by p. SU has the ability to control the interference to PU just by controlling the value of p. The value of p can be found on using probing function. The channel model of single CRN has been modified with introduction of p_{win}. p_{win} is probability of transmission that SU gains the PU occupied channel resource by jamming.

The channel model in Fig. 2 consists of three states IDLE, PU and SU. Idle state is the one in which channel is found to be vacant and no user has access to the channel. Idle state is converted either to PU or SU state. PU state is when the channel is occupied by PU. After the channel is occupied by PU spaces are generated which results into generation of spectrum holes. SU's occupy spectrum holes without interfering with PU. If PU is detected in between when SU is accessing the channel, SU releases the channel and hands over traffic to PU. The generator matrix $A^{'}$ to characterize the translation of this MC model is

$$A' = \begin{pmatrix} -(\lambda_P U + \lambda_{SU}) & \lambda_{PU} & \lambda_{SU} \\ \mu_{PU} & -(\mu_{PU} + p_{win}\lambda_{SU}) & p_{win}\lambda_{SU} \\ \mu_{SU} & \lambda_{PU} & -(\lambda_{PU} + \mu_{SU}) \end{pmatrix}$$

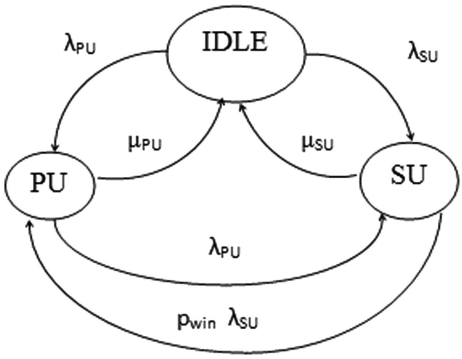


Fig. 2. Channel model of single CRN with probing [13]

The variable related to the Fig. 2 and matrix are described in Table 1. Π is the probability vector when jamming is zero ($p_{win} = 0$) and Π' is probability vector when jamming is done ($p_{win} > 0$). The probability distribution vectors in the steady state of IDLE, PU and SU states can be given by Π'_I, Π'_{PU} and Π'_{SU} respectively. Steady state probability vector Π has been modified to Π' such that $\Pi' A' = 0$ where $\Pi' = \Pi'_I + \Pi'_{PU} + \Pi'_{SU}$ and $\Pi^J_I + \Pi^J_{PU} + \Pi^J_{SU} = 1$. Comparing Π_J and Π reaches to point

Table 1. Variables related to figure

Sr. no.	Variable	Meaning
1	λPU	Traffic arrival at PU
2	λSU	Traffic arrival at SU
3	μPU	Departure rates from PU
4	μSU	Departure rates from SU
5	$pwin$	Probability of SU to gain a PU occupied channel

that PU's throughput decline level when SU gains the channel by jamming is in the probability of p_{win}. The decline level in throughput of PU can be found out with corresponding value of p_{win} of $\Pi P'\ U = 0.99 \times \Pi_{PU}$. p_{win} achieves 0.4 in extreme traffic ratios [13]. $\lambda_{P\ U}$ and μ_{PU} are assumed to be known to SU. But as SU knows Π_{PU} it can calculate λ_{PU} depending upon presumed value of μ_P by equation

$$\Pi_{PU} = \frac{\lambda_{PU}}{\lambda_{PU} + \mu_{PU}}$$

λ_{PU} is also calculated based on presumed value of μ_{PU} which may not seem to be correctly calculated. If PU is assumed to be collision based user then it may retransmit the packet after the packet collision event. That means if PU's collided packet is not transmitted then p is equal to the packet loss rate of PU. But to achieve target throughput decline level it is assume that PU does not retransmit the collided packets. But for practical scenario PU is going to retransmit the collided packet which makes PU's link stronger which means that an SU should have corresponding p, which is be quite larger than p_{win}.

PU is assumed to retransmit the collided packet after the collision event takes place otherwise SU will acquire access to the channel resource which will result in decline of PU's throughput. But after the end of maximum retransmission counter, PU stops its retransmission and SU accesses the channel with the help of jamming. To study how p_{win} changes to p there is need to study the back off model of IEEE 802.11 [10]. In this IEEE 802.11 back off model it uses DCF-carrier sense multiple access with collision avoidance (CSMA-CA) so that whenever PU retransmits the collided packet it gets transmitted [12]. This retransmission of packet can be studied from the Fig. 3.

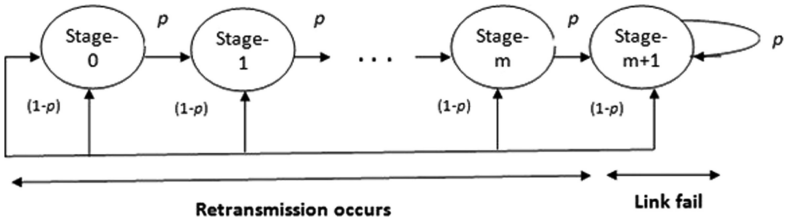


Fig. 3. Discrete-time MC of packet retransmission [13].

There are stages from *stage* 0 to *stage* $(m + 1)$ which indicates the retransmission of the packet. Each stage transits to other stage with a probability of p. m represents maximum retransmission count. i^{th} stage denotes that the collided packet has been transmitted that much times $0 \leq i \leq m$. *Stage* $(m + 1)$ denotes that the link has been failed which itself has a probability of p. Whenever the link fails it indicate that access is acquired by SU. Assume the probability distribution vector be V where $V = (V_0, V_1, V_2,, V_m, V_{m+1})$ where V_i is the probability distribution of *stage* $-i$. The probability of the link-failed state, which is V_{m+1}, is able to be prohibited by modifying p which indicates an SU can gain the channel, as indicated by $V_{m+1} = p_{win}$. As a result, the translation from V_{m+1} to p is equal to the translation from p_{win} to p. The second unfairness problem of uncoordinated spectrum unit size can be controlled with modification of p. However, modeling an MC that contains multiple-channel and multiple-system states with different spectrum unit sizes is wasteful. Therefore, the following equation is used for translating jamming rate for simplification purposes [13]:

$$1 - (1 - p_n)^n = p$$

6 Performance Evaluation

The performance of CCR MAC protocol is studied by detection of PU on channel. There are four cases where PU is detected on channel. They include:

1. PU is active at initial and final phase only.
2. PU is interrupting at specific intervals.
3. PU is present at random intervals.
4. PU is active at starting phase

Depending upon this CCR-MAC protocol deals with unfairness issues. To study how it impacts uncoordinated PU detection ability throughput results of two secondary users i.e. SU and TSU assuming TSU has better PU detection ability than SU are considered. Results are presented and verified in this section. The second problem uncoordinated spectrum unit size is studied with fairness indexes of SU's and TSU's Lastly the throughput decline of SU is studied with the probing function in section. Since fairness and throughput efficiency are always tradeoffs, the improvement of the proposed solution is shown negatively impacting the throughput performance. The system parameters are listed in Table 2.

Table 2. Simulation parameter

Sr. no.	Parameter	Size
1	SIFS period	10μs
2	DIFS period	50μs
3	Min. back off window size	32
4	Max. back off window size	1024
5	PU throughput decline ratio	0.99

6.1 Fairness Feature

By using proposed solution fairness indexes are presented to show the enhancement by applying probing function in the network. The unfairness problem of the uncoordinated PU detection ability is also addressed. Let p_S and p_T be probability of SU and TSU detection abilities of primary user's traffic. Figure 4 shows throughput results of SU and TSU when $p_S = 0$ and $p_T = 1$. As SU has less PU detection ability throughput of SU is only 4.3% and that of TSU is 95.7% due to high PU detection ability. But when $p_S = 1$ and $p_T = 1$ then both throughput performance match each other which is exactly 50%.

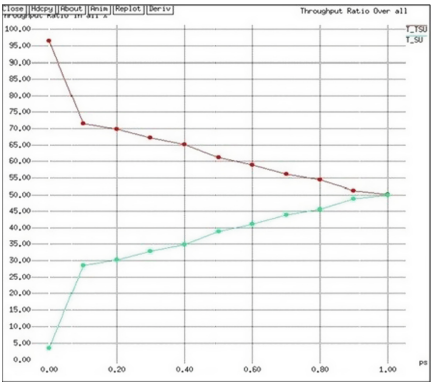


Fig. 4. Throughput ratio overall in % for secondary systems

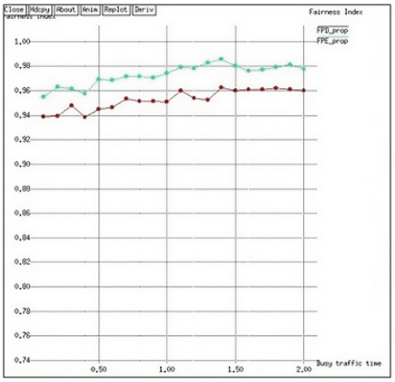


Fig. 5. Fairness index

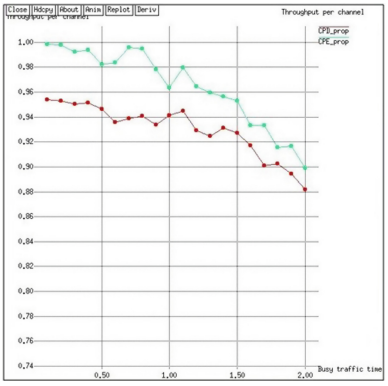


Fig. 6. Throughput per channel by probing enabling and disabling

Figure 5 shows the results of fairness index between SU and TSU in different traffic loads. Results shows enabling of probing function is efficient and provides a fair chance to users. Figure 6 shows how the throughput per channel of SU and TSU has increased

unfairness problem when traffic increases. Two lines indicated in Fig. 6 shows probing enabling and disabling to achieve fairness feature. Obviously enabling probing function enhances the throughput of users which have weak PU detection ability.

7 Conclusion

Secondary users have an opportunistic way of accessing the radio spectrum, due to this two unfairness problems are caused in coexistent heterogeneous networks. Unfairness includes uncoordinated PU detection ability and uncoordinated spectrum unit size. A MAC protocol for distributed systems i.e. CCR-MAC protocol combines probing function to work in CRN networks. This MAC layer approach solves both the unfairness problems with MC models proposed for coexistent heterogeneous CRN. Scheduling of SU done at the MAC layer is generally First in First Out (FIFO) so in order to serve SU's in a fair way without causing any harm to PU, SU are served on basis of unprocessed priority. The simulation results show that how this protocol is advantageous to CR networks thus removing unfairness feature. In future secondary systems can be served in number of ways to check whether it gets a fair chance without affecting the throughput of primary systems.

References

1. Mitola, Joe: The software radio architecture. IEEE Commun. Mag. **33**(5), 26–38 (1995). https://doi.org/10.1109/35.393001
2. FCC: Spectrum policy task force report. In: Proceedings of the Federal Communicate ions Commission (FCC 2002), Washington, DC, USA (Nov 2002)
3. Haykin, Simon: Cognitive radio: brain empowered wireless communication. IEEE J. Sel. Area Commun. **23**(2), 201–220 (2005). https://doi.org/10.1109/JSAC.2004.839380
4. Zen, Y., Liang, Y.C., Hoang, A.T., Zhang, R.: A review on spectrum sensing for cognitive radio: challenges and solutions. EURASIP J. Adv. Signal Process. **2010**(2), Article ID-381465 (2009)
5. Wang, B., Ray Liu, K.J.: Advances in cognitive radio networks: a survey. IEEE J. Sel. Top. Signal Process. **5**(1) (2011). https://doi.org/10.1109/jstsp.2010.2093210
6. Jayaweera, Sudharman K., Li, Tianming: Dynamic spectrum leasing in cognitive radio networks via primary-secondary user power control games. IEEE Trans. Wireless Commun. **8**(6), 3300–3310 (2009). https://doi.org/10.1109/TWC.2009.081230
7. Cormio, C., Chowdhury, K.: A survey on MAC protocols for cognitive radio network. Adhoc Netw. J. **7,** 1315–1329 (2009). https://doi.org/10.1016/j.adhoc.2009.01.002
8. Kaabouch, N., Fihri, W.F., Salahdine, F., El Ghazi, H.: A survey on decentralized random access MAC protocols for cognitive radio networks. In: International Conference on Advanced Communications Systems and Information Security (ACOSIS) (2016)
9. Song, M., Xin, C.S., Zhao, Y.: FMAC: A fair MAC protocol for coexisting cognitive radio networks. In: IEEE INFOCOM Proceeding, pp 1474–1482 (2013). https://doi.org/10.1109/infcom.2013.6566942
10. Bianchi, G.: Performance analysis of the IEEE 802.11 distributed co-ordination function. IEEE J. Sel. Area Commun. **18**(3) (2000). https://doi.org/10.1109/49.840210

11. Cheng, Y.-C., Wu, E.H., Hung, S.-Y., Chen, G.-H.: An oppurtunistic cognitive MAC protocol for coexistence with WLAN. In: 2008 IEEE International Conference on Communications, pp. 4063–4069. IEEE (2008)
12. Chen, Q., Wong, W.-C., Motani, M., Liang, Y.-C.: MAC protocol design and performance analysis for random access cognitive radio Networks. IEEE J. Sel. Area Commun. **31**(11) (2013). https://doi.org/10.1109/jsac.2013.131121
13. Cheng, Y.-C., Wu, E.H., Chen, G.-H.: A decentralized MAC protocol for unfairness problems in coexistent heterogeneous cognitive radio networks scenarios with collision-based primary users. IEEE Sys. J. **10**(1) (2016). https://doi.org/10.1109/jsyst.2015.2431715

New Adaptive Resonance Theory Based Intrusion Detection System

Purnesh Tiwari, Prakash Mishra, Upendra Singh(✉), and Ravikant Itare

Patel College of Science and Technology, Indore, India
purnesht.appleid@gmail.com, Mishra.prakash32@gmail.com, Upendrasingh49@gmail.com, ravikantjeclll@gmail.com

Abstract. As the beginning of twenty-first century, PC framework describes the improving Updation in the form of network efficiency, several hand holders & kind of operations that achieve on the system. As accompanied by latest generation comfortable machines for ex: Internet mobile, tabs, smart instruments i.e. updated machines & software also several calculating devices, no. connected hand holders progressing most & most. Therefore, safety on connection has been the key process which support complete hand holders. Intrusion detection has been the procedure in protecting intrusion. An intrusion detection technique may predict the complete upcoming & on- going intrusion at a structure. Intrusion detection technique may investigate complete priority under safety procedure with the help of managing the infrastructure movement. As Intrusion detection system (IDS) emerges as the obvious class under safety layout, it may manage capacity with support to determine the safety points in a framework. Several system supports under intrusion detection. Primary objective of this research work is representing i.e. With support to hybrid document opening approaches, it may minimize the duration difficulty in process as compared with mono approach. Particular structures were certified with support to kdd'99 document pair. An observational outcome remains significantly describing in nature i.e. hybrid approaches with support to k-means & Projective Adaptive Resonance Theory may uniquely minimize structure practicing duration of the framework & balances the perfectness of detections.

Keywords: Intrusion detection system · KDD CUP'99 dataset · K-means Projective adaptive resonance theory

1 Introduction

Establishment of generation to generation internet of things under computer infrastructure connection & simulation software technique are improving regularly; public still remains unable to prevent self resources through theft either attackers. As several methods were given through a term as interruption certification & interference procedure for stopping committee to that types of assault, while on the other hand several safety space in each committee [1]. Therefore hand holders attempting several path for safety his proprietary rights & too discovered several simulation tool for safety his

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 745–754, 2020.
https://doi.org/10.1007/978-3-030-37051-0_84

proprietary rights. No any safe procedure under whole country as we mandatorily applying & given safety more & more as researchers may [2]. Interruption detection approach has been path of managing programmers continuing on the infrastructure & studying prior assaults. Under interruption detection approach, document opening process has been latest Updation for finding out interruption. Documents categorization having key benefits & his achievement under great amounts of documents pair are beneficial for interruptions [3]. Primary aims under document opening with support to interruption detection are to support man-made issues with support of electronification. For getting electronification, documents opening support through drawing out system with the help of document & study approach form instrument with support to upcoming applications. This procedure given to documents for categorizing interruption & un-interruption nature, also helpful in several areas which needed document study. Several types of unique documents opening procedures they are categorization, grouping, & layout detections [4].

Formula –build interruptions detections are much as compared with alternative process of signature-build & anomaly-build interruption detection. Under this procedure, well-founded situations build on future incident-experimental analysis are described. Formula –build interruptions detections are primarily much significant as on comparing with signature-build interruption detection as it happens at numbers of variables for ex: programming build at signatures, set of rules, study, & task detection identifiers etc… Particular article publishers by support of k-means & Projective Adaptive Resonance Theory formula build code used with support to find out predict interruption under system document pair. Short representation of Projective Adaptive Resonance Theory has been PART.

2 Literature Survey

Particular research objective provides analysis of continuing interruption detection framework with support to hybrid approach i.e. document opening accompanied by flexible evaluating procedure. Numbers of several system applied under interruption found out procedure however every procedure are unable to become fully unique. Given published researches revised some published article related to the concept of interruption detection framework, procedures, & best fuzzy categorizers with support to hereditary code & document processing approaches that provides medium with support to the issues regarding interruption detection framework [5]. Additionally, a conversation on future information creativity & several approaches that assurance for progressing efficiency for computer framework in predicting interruptions are proffer [6, 7].

Given research describing observational outcomes under altogether approaches for ex: release, super charging & on analyzing the achievement accompanied by stdd. J-forty eight categorization code build under the categorization of ten % document pair. Benefits under altogether are analyzed accompanied by earn outputs [8].

Given articles also describes profits with support to anomaly detection recommend accompanied by exploitation found out procedure under finding unspecified interruption infrastructure. Under exploitation find out approaches, 4 dissimilar categorizers (Formula induction, baye, judgment tree & closest acquaintance) which support for find out acknowledged assaults. Although that codes got unsuccess in finding out unspecified interruptions [9].

Main aim of published research has been primarily choose 10 categorization codes build according to his capacities for ex: velocity, build under the observational analysis, complete better outcomes under perfectness & F-score were collected by Random tree code, however large find out speed & below wrong signaling device speed was collected through formulation-One R, J48 & Random Forest codes [10].

Device studying approaches are process with support to interruption detection. Under previous years, many procedure build for device studying codes which support to interruption detection framework although it is powerless under find out perfectness & duration also gap difficulty for continuation also with support to implemented application which choose a sub pair for categorizing that minimize duration difficulty & mind necessities. His approaches presenting up to 98% perfect & detection extent [11]. Given research with support to k-means & baye to find out interruption [18, 19].

3 Intrusion Detection System

The Intrusion detection system (IDS) can be a basic review trail process or sifting process utilizing traffic control system, for example, switch separating, parcel channels, firewalls, and so forth. A few people use IDS to mean an order utility. At the point when individuals utilize a switch based access list, or a working system screen, they can follow the intrusions by utilizing IDS. For instance, the record systems in a system situation contain an assortment of information documents and programming. Unpredicted changes in registries and records, particularly those to which get to is typically confined, might be a side effect that an intrusion has happened. Changes may incorporate evolving, making, or erasing registries and documents. What rolls out such an improvement capricious may relies upon who transforms it and where, when, and how the progressions are made. IDS is a PC based data system went for social affair data about pernicious exercises in a progression of focused IT assets, breaking down data, and reacting to the predetermined security arrangement [3]. Intrusion can be characterized as a progression of activities that endeavor to bargain the trustworthiness, classification, or accessibility of system assets. Intrusion could be in numerous structures, for example, malevolent projects, unapproved individual, and approved individual endeavoring to increase extra benefits [4]. Intrusion detection system can be comprehensively arranged dependent on two parameters as appeared in Fig. 1 [4, 5]:

- By Analysis technique, Misuse IDS and Anomaly IDS can be characterized
- By Source of information, Host based IDS and Network based IDS can be characterized

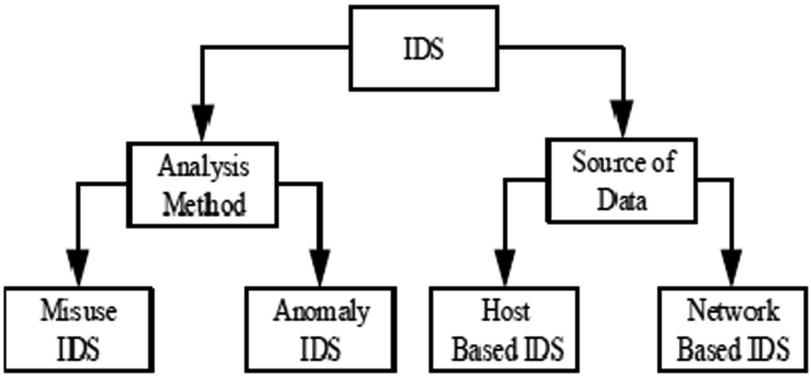


Fig. 1. Taxonomy of IDS

4 Overview of K-Means and Projective Adaptive Resonance Theory

K-means calculation is a standout amongst the most prevalent strategies for bunch investigation, which intends to contract with "n" in the information "k" bunch for the segment in which every datum object having a place with gathering the mean estimations of other. It utilizes the Euclidean measurement as a proportion of likeness. The fundamental highlights of the K-means calculation that is successful in handling substantial arrangements of information that just takes a shot at numerical qualities. The PART calculation sets governs by over and over settling on incomplete choice trees, consequently fusing two key ideal models for basic leadership, for example, a standard based choice guideline and a different strategy for learning and goals systems. After an incomplete tree is shaped, a rule is created from that point and thus the PART calculation maintains a strategic distance from post preparing. PART calculation is the mix of the gap and-vanquish procedure with independent and-overcome system of principle learning. The working stream of the PART calculation is as following [1, 2]

1. Build a fractional choice tree on the present arrangement of cases
2. Create a standard from the choice tree
   The leaf with the largest coverage is made into a rule
3. Discarded the choice tree
4. Remove the occasions secured by the standard Go to stage one.

5 Proposed System Architecture of Intrusion Detection System

The proposed system design of this paper can be seen in Fig. 2. In the figure, we utilize two ways to deal with arrange 10% KDD CUP 99 dataset occasions. Furthermore, compare the grouped consequences of two methodologies. The exploratory consequences of two methodologies can be found in segment VI.

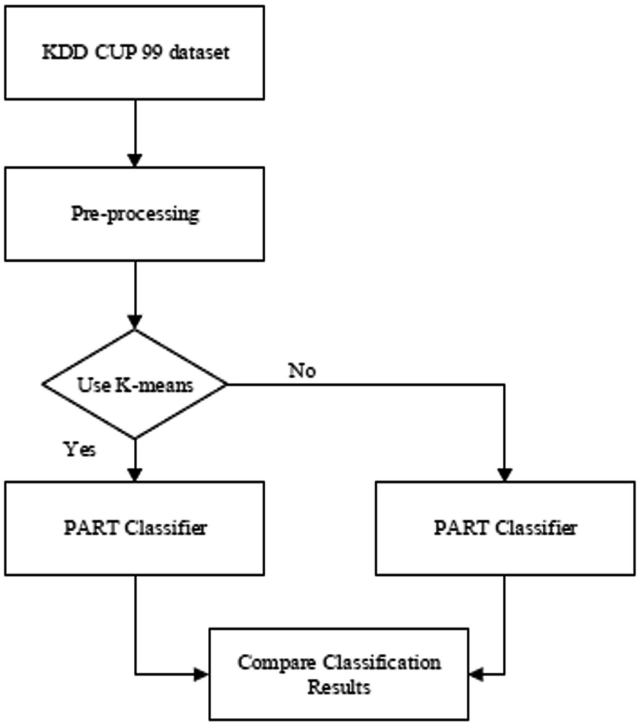
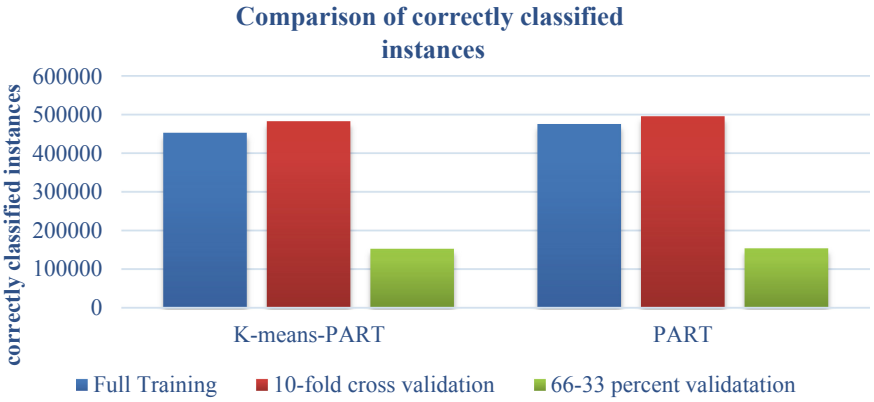


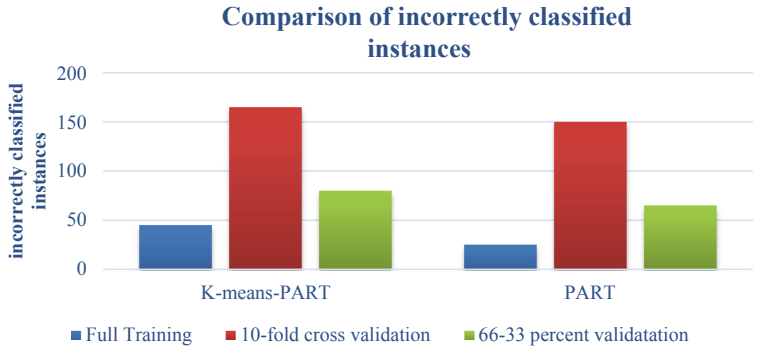
Fig. 2. Proposed system architecture of intrusion detection system

6 Dataset Selection and Experimental Results

To encourage the examinations, we utilized obscuration java and R apparatus to actualize the calculations on a PC with 64-bit window 10 working system, 8 GB RAM and a CPU of Intel center i3-4010U CPU with 2.4 GHz. Information originate from MIT Lincoln lab of KDDCup99 informational index. We select 10% informational collection which contains 494021 Connection records, each record has aggregate of 41 qualities, 7 representative field and 34 numeric fields to test on the grounds that the informational indexes are extremely tremendous. This informational index contains four kinds of intrusions: DoS, Probe, U2R and R2L and furthermore contain ordinary examples. Research exercises in IDS are as yet utilizing the KDD Cup 99 dataset for



Graph 1. Comparison results for correctly classified instances based on two approaches



Graph 2. Comparison results for incorrectly classified instances based on two approaches

examining and investigating new methodologies for better IDS. We utilize 10% informational index of KDD CUP 99 and test with two ways to deal with accurately group the ordinary and intrusions in the informational index. The examinations of two methodologies are appeared Tables 1, 2, 3, 4, 5 and 6.

Examinations of two methodologies demonstrate that approaches dependent on K-means and PART calculation is less model preparing time than just PART calculation in full preparing dataset, 10 overlay cross approval and 66-33 rate approval. Time distinction between two methodologies is impressively multiple times. In any case, accurately grouped instances (ordinary + intrusions) in view of K-means and PART calculations is less than the methodology dependent on just PART calculation. And furthermore the quantity of erroneously grouped examples (ordinary + intrusions) in view of K-means and PART is more than the methodology dependent on just PART calculation. Be that as it may, the distinctions of effectively arranged occasions and mistakenly characterized examples dependent on two methodologies is about the equivalent as indicated by the informational index volume. Furthermore, today

Table 1. Testing results for full training dataset

Dataset	K-mean	PART	Correctly classified instances	Correct instances percentages	Incorrectly classified instances	Incorrect instances percentage
10% P1	Y	Y	108838	99.9936	7	0.0064
10% P2	Y	Y	23520	99.966	8	23528
10% P3	Y	Y	280798	100	0	280798
10% P4	Y	Y	78737	99.9746	20	78757
10% P5	Y	Y	2086	99.6656	7	2093
10% kdd	N	N	493987	99.9931	34	494021

Table 2. Testing results for full training dataset with time complexity

Dataset	K-mean	RF	Total instances	Time to build model (sec)
10% P1	Y	Y	108845	1030.56
10% P2	Y	Y	23528	46.44
10% P3	Y	Y	230798	2573.76
10% P4	Y	Y	78757	855.36
10% P5	Y	Y	2093	0.2
10% kdd	N	N	494021	8451.55

Table 3. Testing results for 10 fold cross validation

Dataset	K-mean	PART	Correctly classified instances	Correct instances percentages	Incorrectly classified instances	Incorrect instances percentage
10% PI	Y	Y	108827	99.9835	18	0.0165
10% P2	Y	Y	23492	99.847	36	0.153
10% P3	Y	Y	280798	100	0	0
10% P4	Y	Y	78678	99.8997	79	0.1003
10% P5	Y	Y	1064	98.6144	29	1.3856
10% kdd	N	N	493865	99.9684	156	0.0316

organize informational index world, the volume of information measure is increasingly increasing step by step. So time multifaceted nature is additionally essential now and again. When we underline time multifaceted nature of the intrusion detection system, the trial consequences of the two methodologies can support to some broadens. The time intricacy of the two methodologies can be found in Graph 3. The effectively and inaccurately arranged occurrences (ordinary + intrusions) can likewise be found in Graph 1 and Graph 2.

Table 4. Testing results for 10 fold cross validation with time complexity

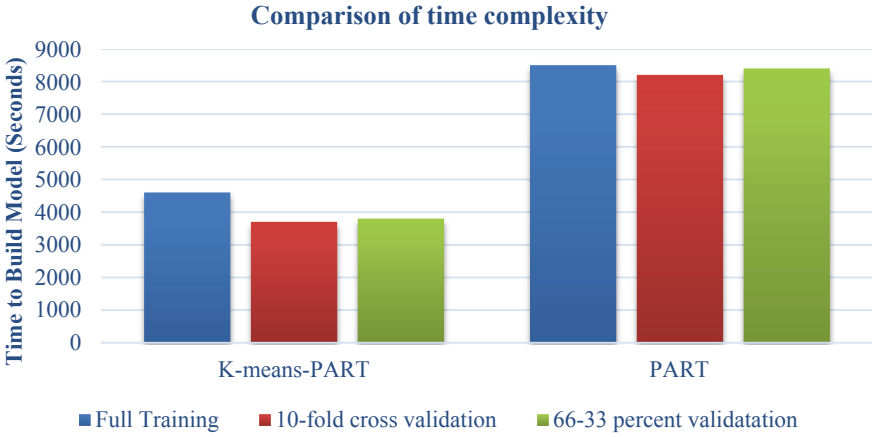
Dataset	K-mean	RF	Total instances	Time to build model (sec)
10% P1	Y	Y	108845	991.18
10% P2	Y	Y	23528	44.65
10% P3	Y	Y	280798	1863.51
10% P4	Y	Y	78757	701.78
10% P5	Y	Y	2093	0.2
10% kdd	N	N	494021	8139.05

Table 5. Testing results for 66-34 percentage validation

Dataset	K-mean	PART	Correctly classified instances	Correct instances percentages	Incorrectly classified instances	Incorrect instances percentage
10% P1	Y	Y	37000	99.9811	7	0.0189
10% P2	Y	Y	7984	99.8	16	0.2
10% P3	Y	Y	95471	100	0	0
10% P4	Y	Y	26728	99.817	49	0.183
10% P5	Y	Y	703	98.736	9	1.264
10% kdd	N	N	167898	99.9589	69	0.0411

Table VI. Testing results for 66-34 percentage validation with time complexity

Dataset	K-mean	RF	Total instances	Time to build model (sec)
10% P1	Y	Y	37007	1072.57
10% P2	Y	Y	8000	46.65
10% P3	Y	Y	95471	1851.5
10% P4	Y	Y	26777	737.86
10% P5	Y	Y	712	0.47
10% kdd	N	N	167967	8142.43



Graph 3. Comparison results for time complexity based on two approaches

7 Conclusion

As the intrusion recognition learning has started picking up security in the network, a few techniques have thought about fulfilling the issue. The intrusion detection system differs in the assets they use to get the accurate information and strategies they use to investigate this information. Every methodology has its relative benefits and impediments. Flawless following like impeccable security, isn't a reachable objective given the intricacy and advancement of a modernized system. The exploration displayed in this paper is to examine the job of information mining calculations in an Intrusion Detection System. Test results demonstrate that the participation intrusion recognition is dependent on K-means and PART is better than the identification system with a solitary PART in terms of time in a multifaceted nature.

References

1. Data Mining Rule-based Classifiers, Section 5.1 of course book
2. Kotsiantis, S.B.: Supervised machine learning: a review of classification techniques. Informatics **31**, 249–268 249 (2007)
3. Raggad, B.G.: Intrusion Detection System. Information Systems Department, Pace University, Pleasantville, NY, 10570, USA.K. Elissa, "Title of paper if known," unpublished
4. Rajan, S.S., Cherukuri, V.K.: An Overview of Intrusion Detection Systems
5. Brown, D.J., Suckow, B., Wang, T.: A Survey of Intrusion Detection Systems. Department of Computer Science, University of Califonia, San Diego, CA 92093, USA
6. Beigh, B.M., Bashir, U., Chachoo, M.: Intrusion detection and prevention system: issues and challenges. Int. J. Comput. Appl. (0975–8887) **76**(17), August 2013
7. Rath, P.S., Barpanda, N., Panda, S.: Intrusion detection system built around hybrid technology: a review. Int. Adv. Res. J. Sci., Engineering and Technology **3**(4), April 2016
8. Kulkarni, R.D.: Using ensemble methods for improving classification of the KDD CUP '99 data set. IOSR J. Comput. Eng. (IOSR-JCE) **16**(5), and e-ISSN: 2278-0661, p-ISSN: 2278–8727, pp. 57–61, (Sep–Oct. 2014)
9. Syarif, I., Bennett, A.P., Wills, G.: Unsupervised clustering approach for network anomaly detection. School Electr. Comput. Sci., University of Southampton, UK
10. Aggarwal, P., Sharma, S.K.: An empirical comparison of classifiers to analyze intrusion detection
11. Albalawi, U., Suh, S.C., Kim, J.: Incorporating multiple supervised learning algorithms for effective intrusion detection. World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng. **8**(2) (2014)
12. Choudhury, S., Bhowal, A.: Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection. In: International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), pp. 89–95 (2015)
13. Rath, P.S., Hohanty, M., Acharya, S., Aich, M.: Optimization of IDS algorithms using data mining technique. In: Proceeding of 53rd IRF International Conference, Pune, India (2016), ISBN: 978-93-86083-01-2
14. Murugan, K., Varalakshmi, P., Kumar, R.N., Boobalan, S.: Data mining using integration of clustering and decision tree. ISSN (Online) **1**(2), 2347–2812 (2013)

15. Rath, P.S., Mohanty, M., Acharya, S., Aich, M.: Optimization of IDS algorithms using data mining techniques. In: Proceeding of 53rd IRF International Conference, Pune, India, ISBN: 978-93-86083-01-2 (24th April 2016)
16. Malviya, V., Jain, A. (HOD): An efficient network intrusion detection based on decision tree classifier & simple K-mean clustering using dimensionality reduction – a review. Int. J. Recent Innov. Trends Comput. Commun. **3**(2), ISSN: 2321–8169 (February 2015)
17. Rao, V.: A clustering algorithm for intrusion detection using hybrid data mining technique. Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng. **3**(1) (April 2015)
18. Singha, P., Lakkadwala, R., Sheth, A., Gaikwad, A., Kadam, M.V.: Improving efficiency of hybrid intrusion detection system using Kmeans and Naïve Bayes. Int. J. Eng. Comput. Sci. **4**(3), 10842–10845, ISSN: 2319- 7242 (March 2015)
19. Richhariya, V., Rana, J.L., Pandey, R.K., Jain, R.C.: An efficient classification mechanism using machine learning techniques for attack detection from large dataset. Int. J. Innov. Res. Sci. Eng. Technol. **1**(2), (December 2012)
20. Rajasekhar, K., Babu, B.S., Prasanna, P.L., Lavanya, D.R., Krishna, T.V.: An overview of intrusion detection system strategies and issues. Int. J. Comput. Sci. Technol. **2**(4), ISSN: 0976-8491 (Online), ISSN: 2229-4333(Print), (Oct–Dec. 2011)

RDD-Eclat: Approaches to Parallelize Eclat Algorithm on Spark RDD Framework

Pankaj Singh[1], Sudhakar Singh[2(✉)], P. K. Mishra[1], and Rakhi Garg[3]

[1] Department of Computer Science, Banaras Hindu University, Varanasi, India
{psingh.edu,mishra}@bhu.ac.in
[2] Department of Electronics and Communication, University of Allahabad, Allahabad, India
sudhakar@allduniv.ac.in
[3] Mahila Maha Vidyalaya, Banaras Hindu University, Varanasi, India
rgarg@bhu.ac.in

Abstract. Initially, a number of frequent itemset mining (FIM) algorithms have been designed on the Hadoop MapReduce, a distributed big data processing framework. But, due to heavy disk I/O, MapReduce is found to be inefficient for such highly iterative algorithms. Therefore, Spark, a more efficient distributed data processing framework, has been developed with in-memory computation and resilient distributed dataset (RDD) features to support the iterative algorithms. On the Spark RDD framework, Apriori and FP-Growth based FIM algorithms have been designed, but Eclat-based algorithm has not been explored yet. In this paper, RDD-Eclat, a parallel Eclat algorithm on the Spark RDD framework is proposed with its five variants. The proposed algorithms are evaluated on the various benchmark datasets, which shows that RDD-Eclat outperforms the Spark-based Apriori by many times. Also, the experimental results show the scalability of the proposed algorithms on increasing the number of cores and size of the dataset.

Keywords: Parallel and distributed algorithms · Frequent itemset mining · Eclat · Spark · Big data analytics

1 Introduction

Frequent itemset and association rule mining [1] are the techniques of data mining employed to discover the interesting correlations among data objects of the database. These algorithms need to be re-desinged on big data processing platforms like Hadoop [2, 3] and Spark [4, 5] when it comes to deal with the big data. Spark is 100 times faster in memory and 10 times faster on disk than Hadoop MapReduce [4]. Many authors have designed different frequent itemset mining (FIM) algorithms on the Spark RDD framework [6–11], in which most of the algorithms follow Apriori [1] as the base algorithm. Parallelization of Eclat-based algorithm on Spark has not been explored yet to the best of our knowledge. In this paper, we consider Eclat [12], a more efficient algorithm than Apriori. Eclat reduces I/O cost due to a small number of database scan, and computation cost due to vertical data format and lattice traversal scheme.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 755–768, 2020.
https://doi.org/10.1007/978-3-030-37051-0_85

This paper proposes some approaches to parallelize Eclat algorithm on the Spark RDD framework. The name RDD-Eclat represents Spark-based Eclat algorithm, and its five variants are named in short as EclatV1, EclatV2, EclatV3, EclatV4, and EclatV5. EclatV1 is the first version of the algorithm, and each subsequent version results from the further modifications on the preceding version to achieve better performance. Algorithm EclatV1 first generate frequent items and a vertical dataset. From vertical dataset, it constructs equivalence classes based on common 1-length prefix. A default partitioner partitions the equivalence classes into (*n-1*) independent partitions, where n is the number of frequent items. Equivalence classes in each partition are processed in parallel by applying the bottom-up search recursively on each equivalence class to enumerate the frequent itemsets. EclatV2 applies all operations of algorithm on the filtered transactions which contain transactions with only frequent items. Transaction filtering is adopted from the efficient implementation of Apriori and Eclat by Borgelt [13]. EclatV3 is slightly different from EclatV2, and the difference is the use of accumulator, a kind of shared variable in Spark. Algorithms EclatV4 and EclatV5 are similar to EclatV3 except the partitioner used to partition the equivalence classes. These two algorithms use two different types of hash partitioner to partition the equivalence classes into p independent partitions, where p is the user defined value. The performance of our proposed algorithms is compared with the Spark-based Apriori algorithm on both synthetic and real life datasets, and they significantly outperform the Spark-based Apriori in terms of execution time. Further, the performance of all proposed RDD-Eclat algorithms is compared with each other in terms of speed and scalability to study the effect of various strategies applied on these algorithms.

The rest of the paper is organized as follows. Section 2 presents preliminaries for RDD-Eclat, which is a brief description of frequent itemset mining, Eclat algorithm, and Apache Spark. Section 3 discusses the related work. In Sect. 4, the proposed algorithms are described in detail. Experimental results and analysis are presented in Sect. 5. Finally, Sect. 6 concludes the paper with future directions.

2 Preliminaries

2.1 Frequent Itemset Mining and Eclat Algorithm

Frequent itemset mining is the computation of all frequent itemsets in a given database [1]. The generation of all frequent itemsets is a computationally as well as memory, and disk I/O intensive task [14]. Eclat algorithm [12] uses a vertical tidset database format, equivalence class clustering, and bottom-up lattice traversal; which reduces these costs. Eclat converts horizontal database into vertical database, i.e. from itemset format $< TID_i, i_1, i_2, \ldots, i_k >$ to tidset format $< i_k, TID_1, TID_2, \ldots, TID_k >$. In horizontal database, each transaction T_i comprise of an unique transaction identifier TID_i and an itemset, i.e. in the form of $< TID_i, i_1, i_2, \ldots, i_k >$. A vertical tidset database consists of a list of items followed by respective tidsets. The tidset of an item or itemset X is the set of all transaction identifiers containing X, and is denoted as $tidset(X) = \{T_i.TID \mid T_i \in D, X \subseteq T_i\}$. The support of an item or itemset X is the number of elements in $tidset(X)$ i.e. $\sigma(X) = |tideset(X)|$ [15]. An itemset X is said to be frequent if $\sigma(X) \geq min\_sup$,

where *min_sup* is a user-specified minimum support threshold. The tidset approach reduces the cost of support counting. The support of a candidate k-itemset is computed by the intersection of tidsets of its two (k-1)-subsets. The vertical database is more compact than horizontal and contains all relevant information, which reduces memory requirements and scanning of the whole database. Further, as the length of itemsets increases, their tidset decrease, that consequently reduces the cost of intersection operations. The computation of frequent 2-itemsets is costlier with vertical format in comparison to the horizontal format. So a triangular matrix is used to update the counts of candidate 2-itemsets [12, 14].

Algorithm 1. Bottom-Up recursive function of Eclat

Input: $EC_k = \{A_1, A_2, ..., A_n\}$, equivalence class of k-itemsets consists of atoms A_i.
Output: Frequent itemsets $\in EC_k$

```
1:  Bottom-Up(EC_k)
2:  {
3:      for(i = 1; i <= |EC_k|; i++)
4:      {
5:          EC_{k+1} = ϕ;
6:          for(j = i + 1; j <= |EC_k|; j++)
7:          {
8:              A_ij = A_i U A_j;
9:              tidset(A_ij) = tidset(A_i) ∩ tidset(A_j);
10:             if( |tidset(A_ij)| >= min_sup)
11:             {
12:                 EC_{k+1} = EC_{k+1} ∪ A_ij;
13:                 L_ECk = L_ECk ∪ A_ij;
14:             }
15:         }
16:         if(EC_{k+1} != ϕ)
17:             Bottom-Up(EC_{k+1});
18:     }
19:     return L_ECk;
20: }
```

The set of items *I* of the database forms a power-set lattice *ρ(I)*. The set of atoms of this lattice corresponds to the set of items [12]. The power-set lattice is the search space that contains all the potential frequent itemsets. To enumerate all the frequent itemsets, lattice must be traversed along with intersection operations on tidsets to obtain support count of itemsets. The equivalence class clustering partitions the lattice into smaller independent sub-lattices enabling parallel computation of frequent itemsets. It also overcomes the limited memory constraint when the complete lattice could not fit in memory due to the large intermediate tidsets. The equivalence class clustering partitions the itemsets of lattice into *equivalence classes* based on the common prefixes of itemsets. Suppose, the set of frequent k-itemsets L_k is lexicographically sorted, then its itemsets can be partitioned into equivalence classes based on their common *(k-1)* length prefixes. All the classes can be processed independently and parallely, and if a class is large enough to be solved in main memory, it can be decomposed to the next level. Eclat uses a bottom-up lattice traversal scheme [12] that processes each equivalence

class by recursively decomposing into smaller classes to enumerate all frequent itemsets. The pseudo code in the Algorithm 1 shows the recursive procedure of this bottom-up search technique, originally given by Zaki [12]. Here, L_{ECk} represents the set of frequent itemsets generated by the equivalence class EC_k. A detailed and illustrative explaination of Eclat algorithm and searching technique can be found in the base paper [12], and is not duplicated here.

2.2 Apache Spark

Apache Spark [4] is a fast and general cluster computing system for large-scale batch and streaming data processing, originally developed at AMPLab of UC Berkeley [5, 16]. Spark was developed to overcome the inefficiency of Hadoop MapReduce [3, 17] for iterative jobs and interactive analytics. It retains the good properties of MapReduce like scalability and fault tolerance. The backbone of Spark is a distributed memory abstraction called Resilient Distributed Datasets (RDDs) [16], which is a collection of immutable data objects partitioned across the nodes of Spark cluster. Spark achieves fault tolerance through a lineage chain that keeps record of set of dependencies on parent RDDs i.e. how an RDD derived from another RDD. A lost partition of RDD can be rebuilt quickly through the lineage chain. The more about RDD and its various operations, Spark application, and architecture of Spark cluster can be found in [5, 16, 18, 19].

3 Related Work

With the evolution of big data, re-designing of traditional data mining algorithms on Hadoop and Spark have been started to provide the scalability. With the introduction of Hadoop, researchers have proposed several FIM algorithms on Hadoop MapReduce framework based on the central algorithms Apriori [1], Eclat [12], and FP-Growth [20]. The well known Apriori-based algorithms are SPC, FPC, and DPC [21]. More formal and optimized versions of these algorithms are proposed by Singh et al. [22]. Recently, Chon and Kim [23] proposed BIGMiner, an Apriori-based frequent itemset mining algorithm on MapReduce. Two distributed versions of Eclat algorithms on MapReduce have been proposed by Moens et al. [24]. The algorithms are named as Dist-Eclat and BigFIM. Dist-Eclat partitions the search space on Mappers rather than data space. BigFIM is a hybrid of Apriori and Eclat approaches. Liu et al. [15] have incorporated three improvements in Eclat algorithm and proposed Peclat (Parallel Eclat) algorithm that parallelizes this improved algorithm on MapReduce framework. PFP (Parallel FP-Growth) [25] is a MapReduce-based FP-Growth algorithm. It breaks the FP-Tree into smaller independent FP-Trees, which are processed by different Mappers to generate frequent itemsets. FiDoop [26], a parallel frequent itemset mining algorithm on MapReduce uses an FIU-Tree (frequent items ultrametric tree) in the place of FP-Tree.

The development of Spark has shifted the research focus from Hadoop MapReduce-based algorithms to the Spark-based algorithms. MapReduce does not fit in with the iterative nature of data mining algorithms. Each time, for a new iteration, one needs to launch a new MapReduce job that takes a significant amount of time.

Further, the costly read/write operations on HDFS are required for the intermediate result of jobs. Spark keeps the good features of MapReduce, resolves the problems with MapReduce, and adds a number of additional features.

During the recent years, many Spark-based FIM algorithms have been proposed. Qiu et al. [6] have proposed a Spark-based Apriori algorithm named YAFIM (Yet Another Frequent Itemset Mining). YAFIM is modularized into two phases. The first phase produces frequent items, whereas the second phase generates frequent (k + 1)-itemsets from frequent k-itemsets for $k \geq 2$. YAFIM outperformed the MapReduce-based Apriori around 25 times. Rathee et al. [7] proposed R-Apriori (Reduced-Apriori), a parallel Apriori-based algorithm on the Spark RDD framework. R-Apriori is similar to YAFIM with an additional phase that reduces the computation to generate 2-itemsets. Adaptive-Miner [8] is an improvement over the R-Apriori, which dynamically selects a conventional or reduced approach of candidate generation, based on the number of frequent itemsets in recent iteration. DFIMA (Distributed Frequent Itemset Mining Algorithm) [9] is also an Apriori-based algorithm on Spark. It uses a matrix-based pruning approach to reduce the number of candidate itemsets. In the first step, it creates a Boolean vector for each frequent item, and then 2-itemset matrix from Boolean vectors. In the second step, it generates all frequent (k + 1)-itemsets from frequent k-itemsets, for $k \geq 2$. HFIM (Hybrid Frequent Itemset Mining) [10] exploits the vertical format of the dataset with Apriori algorithm. The smaller size of vertical dataset reduces the cost of dataset scanning. The first phase of the algorithm produces vertical dataset that contains only frequent items. Also, a revised horizontal dataset is obtained by removing infrequent items from the original dataset. Horizontal dataset is distributed on all worker nodes while vertical dataset is shared. Shi et al. [11] proposed DFPS (Distributed FP-growth Algorithm based on Spark) algorithm. The first step of the algorithm calculates frequent items from RDD of transactions. The second step repartitions the conditional pattern base, and the third step generates frequent itemsets in parallel from the independent partitions.

4 RDD-Eclat Algorithms

We parallelize Eclat algorithm on Spark RDD framework and named it as RDD-Eclat. We propose five different variants of RDD-Eclat by successively applying different strategies and heuristics. EclatV1 is the first implementation, and its successors EclatV2, EclatV3, EclatV4, and EclatV5 are resulted after applying the changes in their respective preceding algorithm. All proposed algorithms are modularized into three to four phases. Each phase comprises of transformations, actions, and other operations [19].

4.1 EclatV1

EclatV1 is divided into three phases described as pseudo codes in Algorithm 2, 3, and 4 respectively. Phase-1 (Algorithm 2) takes input as horizontal database and produces output as frequent items with support count, the number of frequent items, and the database in a vertical format for the subsequent use. It first creates an RDD,

transactions from the database. Here, the database is not partitioned in order to assign a unique transaction identifier, when it is not present in the database. The *flatMapToPair ()* transformation maps each transaction to a *(item, tid)* pairs, and creates a paired RDD containing the *(key, value)* pairs. The *groupByKey()* transformation groups all pairs with the same key. The *filter()* transformation removes the items having support count less than *min_sup*. The paired RDD, *freqItemCounts* contains *(item, count)* pairs, where count is the support count of item. Here, *(itemTid._1, itemTid._2)* is a *(key, value)* pair of a Tuple2 [19] type object, *itemTid.* Finally, the action, *collect()* returns the entire content of RDD, *freqItemTids* to the driver program where it is sorted in the ascending order of support and stored in a list.

Algorithm 2. Phase-1 of EclatV1

```
1:  RDD transactions = sc.textFile("database", 1);
2:  PairRDD itemTids = transactions.flatMapToPair(t -> {
3:     tid = 1;
4:     for each item of t.split(" ")
5:        pairList.add((item, tid));
6:     tid++;
7:     return pairList;
8:  }).groupByKey(s);
9:  PairRDD freqItemTids = itemTids.filter(itemTid -> itemTid._2.size () >= min_sup);
10: PairRDD freqItemCounts =
                        freqItemTids.mapToPair(itemTid -> (itemTid._1, itemTid._2.size(s)));
11: freqItemCounts.saveAsTextFile("frequentItems");
12: freqItemTidsList = sort(freqItemTids.collect());
13: n = freqItemTidsList.size(s);
```

Phase-2 of EclatV1 (Algorithm 3) computes support count of all 2-itemsets using an upper triangular matrix from the horizontal database, as recommended by Zaki in [12]. It is computed in parallel on the different partitions of the database. The database is partitioned as per the default parallelism which is equal to the number of cores on all machines of the Spark cluster. The triangular matrix is shared as an accumulator variable, *accMatrix* among all the executors to add support count of 2-itemsets in parallel. The transformation, *flatMap()* updates the accumulated matrix for all 2-itemset combination of each transaction.

Algorithm 3. Phase-2 of EclatV1

```
1:  transactions = transactions.repartition(sc.defaultParallelism());
2:  if(triMatrixMode)
3:  {
4:     create a triangular matrix, triMatrix[ ][ ]
5:     pass triMatrix as accumulator variable, accMatrix
6:     transactions.flatMap(t -> {
7:        for each 2-itemset combination, itemIitemJ of items of t.split(" ")
8:           accMatrix.update(itemIitemJ);
9:     });
10:    triMatrix = accMatrix.value();
11: }
```

Phase-3 of EclatV1 (Algorithm 4) takes the input as *freqItemTidsList*, the vertical dataset, and produces frequent k-itemsets, k $\geq$ 2. It first generates *ECList*, a list of pairs of equivalence classes for 2-itemsets and tidset of members of the class. A paired RDD, *ECs* is created by parallelizing the *ECList*, and partitioned into default *(n-1)* partitions, where *n* is the number of frequent items. The triangular matrix containing the support count of 2-itemsets is used here to avoid the costly intersection operations for infrequent 2-itemsets. The transformation, *flatMap()* processes each partition of the equivalence classes *ECs* in parallel. It applies the *Bottom-Up()* recursive function of Eclat (Algorithm 1) on each equivalence class *EC* in a partition. The source code of *Bottom-Up()* method has been taken from the SPMF Open-Source Data Mining Library [27].

Algorithm 4. Phase-3 of EclatV1

```
1:  for(i = 0; i < freqItemTidsList.size() - 1; i++)
2:  {
3:      itemI = freqItemTidsList.get(i)._1;
4:      tidsetI = freqItemTidsList.get(i)._2;
5:      for(j = i + 1; j < freqItemTidsList.size(); j++)
6:      {
7:          itemJ = freqItemTidsList.get(j)._1;
8:          if(triMatrixMode)
9:              if(triMatrix.getSupport(itemI, itemJ) < min_sup)
10:                 continue;
11:         tidsetJ = freqItemTidsList.get(j)._2;
12:         tidsetIJ = tidsetI ∩ tidsetJ;
13:         prefixIList.add((itemJ, tidsetIJ));
14:     }
15:     ECList.add(itemI, prefixIList);
16: }
17: PairRDD ECs = sc.parallelize(ECList);
18: ECs = ECs.partitionBy(new defaultPartitioner(n - 1)).cache(s);
19: RDD freqItemsets = ECs.flatMap(EC -> Bottom-Up(EC));
20: freqItemsets.saveAsTextFile("frequentItemsets");
```

4.2 EclatV2

EclatV2 comprises of four phases, the pseudo codes of first three phases are described in Algorithms 5, 6, and 7, whereas Phase-4 is same as the Phase-3 of EclatV1 (Algorithm 4). Phase-1 simply saves the frequent items and their support, and produces a list of frequent items in alphanumeric order.

Algorithm 5. Phase-1 of EclatV2

```
1:  RDD transactions = sc.textFile ("database");
2:  RDD items = transactions.flatMap(t -> List(t.split(" ")));
3:  PairRDD itemPairs = items.mapToPair(item -> (item, 1));
4:  PairRDD itemCounts = itemPairs.reduceByKey((v1, v2) -> v1 + v2);
5:  PairRDD freqItemCounts =
                        itemCounts.filter(itemCount -> itemCount._2 >= min_sup);
6:  freqItemCounts.saveAsTextFile("frequentItems");
7:  freqItemList = sort(freqItemCounts.keys().collect());
8:  n = freqItemList.size();
```

Phase-2 of EclatV2 (Algorithm 6) is similar to the Phase-2 of EclatV1 except the addition of transaction filtering [13]. The frequent items, $trieL_1$ stored in a prefix tree, must be broadcasted to all executors using the broadcast variable, before applying the transformation. The support counting of 2-itemsets is performed applying the same triangular matrix method of EclatV1, but on the filtered transactions.

Algorithm 6. Phase-2 of EclatV2

```
1:  store frequent items in trie, trieL1;
2:  RDD filteredTransactions = transactions.map(t -> filterTransaction(t.split(" "), trieL1));
3:  if(triMatrixMode)
4:  {
5:      create a triangular matrix, triMatrix[ ][ ]
6:      pass triMatrix as accumulator variable, accMatrix
7:      filteredTransactions.flatMap(t -> {
8:          for each 2-itemset combination, itemIitemJ of items of t.split(" ")
9:              accMatrix.update(itemIitemJ);
10:     });
11:     triMatrix = accMatrix.value();
12: }
```

Phase-3 of EclatV2 (Algorithm 7) generates the vertical dataset from filtered horizontal dataset. It first reduces all partitions of transactions into one partition in order to generate unique transaction identifier. The action *collect()* returns the list of *(item, tidset)* pairs, that is sorted by the total order of increasing support count and stored in a list. Phase-4 of EclatV2 is exactly same as the Algorithm 4, where equivalence classes are created and partitioned for parallel computation of the frequent itemsets.

Algorithm 7. Phase-3 of EclatV2

```
1:  filteredTransactions = filteredTransactions.coalesce(1);
2:  PairRDD freqItemTids = filteredTransactions.flatMapToPair(t -> {
3:      tid = 1;
4:      for each item of t.split(" ")
5:          pairList.add((item, tid));
6:      tid++;
7:      return pairList;
8:  }).groupByKey( );
9:  freqItemTidsList = sort(freqItemTids.collect( ));
```

4.3 EclatV3

EclatV3 comprises of four phases in which first two phases, Phase-1 and Phase-2 are exactly same as those of EclatV2. The purpose of Phase-3 of both algorithms EclatV2 and EclatV3 is same i.e. both generate vertical dataset. The difference is that EclatV3 uses a hashmap data structure to store (*item, tidset*) pairs of vertical dataset. This hashmap is accumulated across all executors, and updated by the *flatMapToPair()* transformation. The updated hashmap is used to sort the list of frequent items of Phase-1, by total order of increasing support count. Phase-4 of EclatV3 is similar to the

Algorithm 4, the only difference is the data structure used to store the pairs of item and tidset. Here, the items and corresponding tidsets are fetched from a hashmap instead of a list, and the rest of process is the same.

4.4 EclatV4 and EclatV5

Algorithms EclatV4 and EclatV5 apply the heuristics on EclatV3 to partition the equivalence classes into p partitions, where p has the value supplied by the user. Heuristics are applied to balance the partitions of equivalence classes. Only the Phase-4 of these two algorithms is different from EclatV3, and first three phases are the same to those of EclatV3. Further, Phase-4 is different only with respect to the partitioning of equivalence classes which is done at line no. 18 (e.g. in Algorithm 4). EclatV4 and EclatV5 respectively use *hashPartitioner* and *reverseHashPartitioner* in their Phase-4 instead of *defaultPartitioner* as in Algorithm 4.

The hash partitioner of EclatV4 applies a hash function on the values corresponding to the prefix of equivalence classes, and returns the remainder as a partition ID. Whereas, EclatV5 returns the partition ID in reverse order when the unique value assigned to the 1-length prefix of equivalence class is greater than or equal to p. The partitioners with hashing and reverse hashing are used to investigate the workload balance among partitions. The workload is measured in terms of the members in equivalence classes. An equivalence class having more members leads to the generation of more candidate itemsets as well as the intersection of their tidsets.

5 Experimental Results

The Experiments are conducted on a workstation machine installed with Spark-2.1.1, Hadoop-2.6.0, and Scala-2.11.8. The workstation is equipped with Intel Xenon CPU E5-2620@2.10 GHz with 24 cores, 16 GB memory and 1 TB disk, and running 64 bit Ubuntu 14.04. HDFS is used as storage for the input datasets and generated frequent itemsets. Source codes of all algorithms are written in Java-7. Table 1 summarizes datasets used in experiments with their properties. BMS_WebView_1 (BMS1) and BMS_WebView_2 (BMS2) are the click-stream data taken from [27] while T10I4D100 K and T40I10D100K are generated by IBM Generator available at [28].

Table 1. Datasets used in experiments with their properties

Dataset	Type of dataset	Transactions	Items	Average transaction width
BMS_WebView_1	Real-life	59602	497	2.5
BMS_WebView_2	Real-life	77512	3340	5
T10I4D100K	Synthetic	100,000	870	10
T40I10D100K	Synthetic	100,000	1000	40

The proposed algorithms EclatV1, EclatV2, EclatV3, EclatV4, and EclatV5 require two parameters, *triMatrixMode* and *p* to be set before the execution. The triangular matrix optimization can be enabled or disabled by providing the true or false value to *triMatrixMode*. It is true for all datasets except BMS1 and BMS2. The size of triangular matrix depends on the maximum integer value of all items in the dataset, and it is very large in BMS1 and BMS2. The very large size of the matrix may cause out of memory problem, so the value of *triMatrixMode* is false for these two datasets. Further, algorithms EclatV4 and EclatV5 partition the equivalence classes into *p* partitions, which is set as 10 for all datasets.

5.1 Execution Time on Varying Value of Minimum Support

Figures 1(a), 2(a), 3(a) and 4(a) compare the execution time of the proposed algorithms against the Apriori algorithm whereas Fig. 1(b), 2(b), 3(b) and 4(b) compare the execution time of the proposed algorithms EclatV1, EclatV2, EclatV3, EclatV4, and EclatV5. On all datasets, RDD-Eclat outperforms the RDD-Apriori (Figs. 1(a), 2(a), 3 (a) and 4(a)), and the execution time difference between them becomes wider with the decreasing value of minimum support.

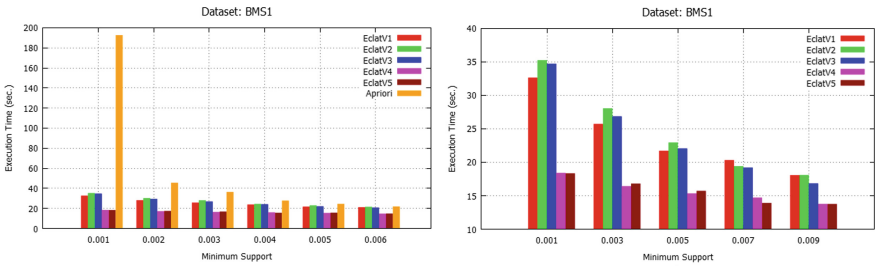


Fig. 1. Execution time of algorithms (a) Eclat variants and Apriori (b) Only Eclat variants for varying minimum support on dataset BMS_WebView_1

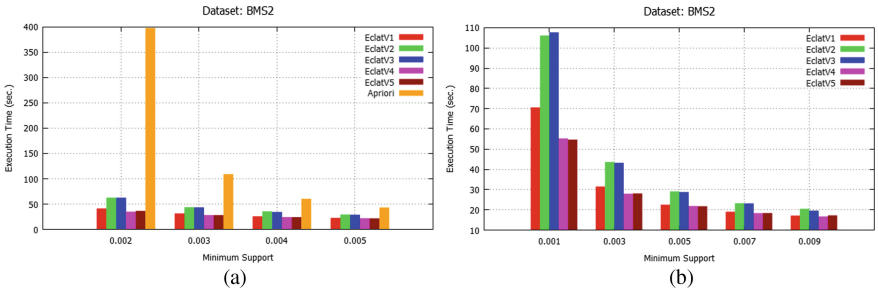


Fig. 2. Execution time of algorithms (a) Eclat variants and Apriori (b) Only Eclat variants for varying minimum support on dataset BMS_WebView_2

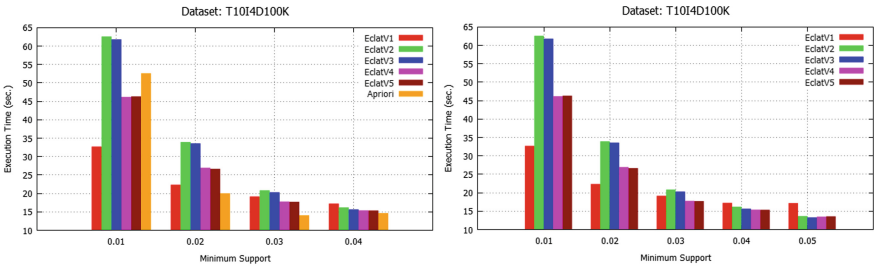


Fig. 3. Execution time of algorithms (a) Eclat variants and Apriori (b) Only Eclat variants for varying minimum support on dataset T10I4D100K

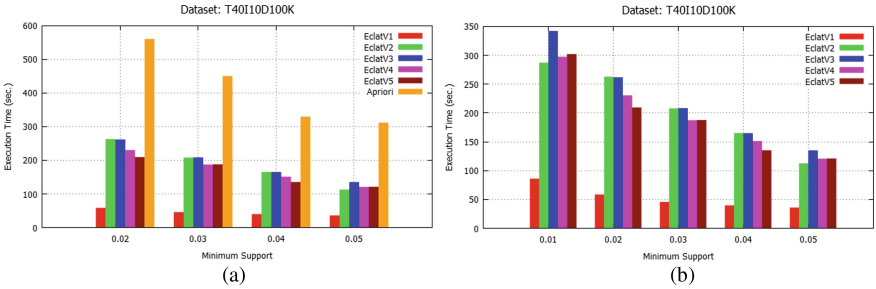


Fig. 4. Execution time of algorithms (a) Eclat variants and Apriori (b) Only Eclat variants for varying minimum support on dataset T40I10D100K

Since, the Apriori algorithm is outperformed by all the proposed algorithms, all the subsequent observations are considered only for the proposed algorithms. Figures 1(b), 2(b), 3(b) and 4(b) closely compare the execution time of the proposed algorithms EclatV1, EclatV2, EclatV3, EclatV4, and EclatV5. The major algorithmic difference between EclatV1 and EclatV2, EclatV3 is the use of filtered transaction technique in EclatV2 and EclatV3; and the difference between EclatV2, EclatV3 and EclatV4, EclatV5 is the use of hash partitioners for the equivalence class partitioning. EclatV2 and EclatV3 perform worse than EclatV1 (Figs. 1(b), 2(b), 3(b), and 4(b)). Algorithms EclatV2 and EclatV3 can only improve the performance when they significantly reduce the size of the original transactions after applying the filtered transaction technique. If the size of filtered transactions is still near to that of the original transactions, then it only adds overhead, and increases the overall execution time of the algorithms. Adoption of the filtered transaction technique may improve the performance on a dataset of larger scale where the filtered dataset is reduced significantly. Further, it can be seen that algorithms EclatV4 and EclatV5 significantly improve the performance in comparison to EclatV2 and EclatV3 on all datasets (Figs. 1(b), 2(b), 3(b) and 4(b)). It proves the effectiveness of equivalence class partitioners used in EclatV4 and EclatV5.

5.2 Execution Time on Increasing Number of Executor Cores

The behavior of the proposed algorithms is investigated on the different datasets for the increasing number of executor cores, as shown in Fig. 5(a–b). Execution time has been measured using 2, 4, 6, 8, and 10 executor cores for the two datasets. With the increasing number of cores, execution time of the algorithms decreases. The decline is more apparent in case of BMS2 dataset. It indicates that execution time can be reduced or maintained by allocating more cores or by adding more nodes.

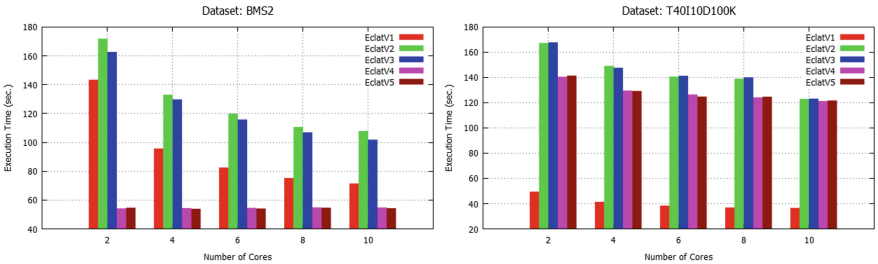


Fig. 5. Execution time on varying number of executor cores for two datasets (a) Dataset BMS_WebView_2 at min_sup = 0.001 (b) Dataset T40I10D100K at min_sup = 0.01

5.3 Scalability on Increasing Size of Dataset

Scalability test is carried out for the proposed algorithms on the increasing size of dataset T10I4D100K at a fixed value of minimum support, 0.05. To get the larger dataset size, it is doubled each time from its previous dataset, so it ranges from 100K transactions to 1600 K transactions as shown in Fig. 6. It can be seen that with the increasing dataset size, execution time of all algorithms increases linearly. It shows the ability of the algorithm to to handle the growing size of datasets at the fixed resources. Efficiency can be maintained by adding more resources.

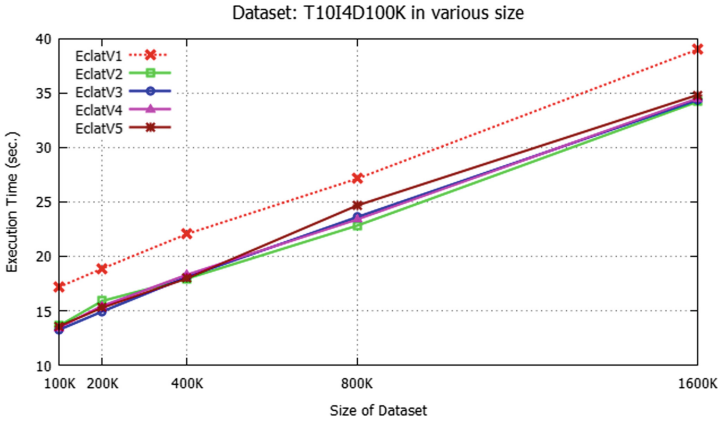


Fig. 6. Execution time on increasing size of dataset T10I4D100K at min_sup = 0.05

6 Conclusions and Future Directions

The re-designing of Eclat algorithm in the distributed computing environment of Spark has been explored in this paper. The key contribution here is a parallel Eclat algorithm on the Spark RDD framework, named as RDD-Eclat along with the implementation of its five variants. The first variant is EclatV1, and the subsequent variants are EclatV2, EclatV3, EclatV4, and EclatV5. Each variant is resulted from applying some different approach and heuristic on the previous variant. The filtered transaction technique is applied after EclatV1, and the heuristics for equivalence class partitioning are applied in EclatV4 and EclatV5. Experimental results on the both synthetic and real life datasets, shows that all proposed algorithms outperform the YAFIM, a Spark-based Apriori algorithm, by many times, in terms of execution time. As the minimum support threshold decreases, the proposed algorithms perform better in comparison to Spark-based Apriori. Further, the proposed algorithms are closely compared in order to investigate the effect of various heuristics applied on the latter variants. It has been observed that the filtered transaction technique improves the performance when it significantly reduces the size of the original dataset. Further, the heuristics applied in equivalence class partitioning significantly reduce the execution time. Also, the algorithms exhibit scalability when executed on increasing the number of cores and the size of dataset.

Moreover, a more optimized and fine-tuned RDD-Eclat algorithm can be designed in future by efficiently assembling the different modules from the different variants. For example, the heuristic of equivalence class partitioning is not applied in EclatV1 but in EclatV4 and EclatV5 along with the filtered transaction technique. This paper only considers 1-length prefix based equivalence classes, the results can be explored for the k-length prefixes where $k \geq 2$. Also, the heuristic for equivalence class partitioning can be improved further to get a more balanced distribution of equivalence classes.

References

1. Agrawal, R., Srikant, R.: Fast algorithms for mining association rules in large databases. In: 20th International Conference on Very Large Databases, VLDB 1215, pp. 487–499 (1994)
2. Apache Hadoop, http://hadoop.apache.org
3. Dean, J., Ghemawat, S.: MapReduce: simplified data processing on large clusters. ACM Commun. **51**, 107–113 (2008)
4. Apache Spark, http://spark.apache.org
5. Zaharia, M., Chowdhury, M., Franklin, M. J., Shenker, S., Stoica, I.: Spark: cluster computing with working sets. In: 2nd USENIX Conference on Hot Topics in Cloud Computing, HotCloud 10 (2010)
6. Qiu, H., Gu, R., Yuan, C., Huang, Y.: YAFIM: a parallel frequent itemset mining algorithm with spark. In: IEEE International Parallel & Distributed Processing Symposium Workshops (IPDPSW), pp. 1664–1671. IEEE Press (2014)
7. Rathee, S., Kaul, M., Kashyap, A.: R-Apriori: an efficient apriori based algorithm on spark, In: 8th Ph. D. Workshop in Information and Knowledge Management, pp. 27–34. ACM (2015)

8. Rathee, S., Kashyap, A.: Adaptive-Miner: an efficient distributed association rule mining algorithm on Spark. J. Big Data **5**(1), 6 (2018)
9. Zhang, F., Liu, M., Gui, F., Shen, W., Shami, A., Ma, Y.: A distributed frequent itemset mining algorithm using Spark for Big Data analytics. Cluster Comput. **18**(4), 1493–1501 (2015)
10. Sethi, K.K., Ramesh, D.: HFIM: a Spark-based hybrid frequent itemset mining algorithm for big data processing. J. Supercomput. **73**(8), 3652–3668 (2017)
11. Shi, X., Chen, S., Yang, H.: DFPS: Distributed FP-growth algorithm based on Spark. In: 2nd IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pp. 1725–1731. Chongqing (2017)
12. Zaki, M.J.: Scalable algorithms for association mining. IEEE Trans. Knowl. Data Eng. **12**(3), 372–390 (2000)
13. Borgelt, C.: Efficient implementations of apriori and éclat. In: IEEE ICDM Workshop on Frequent itemset mining Implementations (FIMI'03) (2003)
14. Zaki, M.J., Parthasarathy, S., Ogihara, M., Li, W.: Parallel algorithms for discovery of association rules. Data Min. Knowl. Disc. **1**, 343–373 (1997)
15. Liu, J., Wu, Y., Zhou, Q., Fung, B.C.M., Chen, F., Yu, B.: Parallel eclat for opportunistic mining of frequent itemsets. In: Database and Expert Systems Applications, LNCS, vol. 9261, pp. 401–415. Springer (2015)
16. Zaharia, M., Chowdhury, M., Das, T., Dave, A., Ma, J., McChauley, M., Franklin, M. J., Shenker, S., Stoica, I.: Resilient distributed datasets: a fault-tolerant abstraction for in-memory cluster computing. In: 9th USENIX Conference on Networked Systems Design and Implementation, p. 2, USENIX Association (2012)
17. Apache Hadoop, http://hadoop.apache.org
18. Cluster Overview, https://spark.apache.org/docs/latest/cluster-overview.html
19. RDD Programming Guide, https://spark.apache.org/docs/latest/rdd-programming-guide.html
20. Han, J., Pei, J., Yin, Y.: Mining frequent patterns without candidate generation. ACM SIGMOD Record **29**(2), 1–12 (2000)
21. Lin, M-Y., Lee, P-Y., Hsueh, S-C.: Apriori-based Frequent Itemset Mining Algorithms on MapReduce. In: 6th International Conference on Ubiquitous Information Management and Communication (ICUIMC '12), Article 76, ACM, New York (2012)
22. Singh, S., Garg, R., Mishra, P.K.: Performance optimization of MapReduce-based Apriori algorithm on Hadoop cluster. Comput. Electr. Eng. **67**, 348–364 (2018)
23. Chon, K.W., Kim, M.S.: BIGMiner: a fast and scalable distributed frequent pattern miner for big data. Cluster Computing **21**(3), 1507–1520 (2018)
24. Moens, S., Aksehirli, E., Goethals, B.: Frequent itemset mining for big data. In: IEEE International Conference on Big Data, pp. 111–118. IEEE Press (2013)
25. Li, H., Wang, Y., Zhang, D., Zhang, M., Chang, E. Y.: PFP: Parallel FP-growth for query recommendation. In: ACM Conference on Recommender System, pp. 107–114. ACM (2008)
26. Xun, Y., Zhang, J., Qin, X.: FiDoop: Parallel Mining of Frequent Itemsets Using MapReduce. IEEE Trans. Syst. Man Cybern.: Syst. **46**(3), 313–325 (2016)
27. Fournier-Viger, P., Lin, C.W., Gomariz, A., Gueniche, T., Soltani, A., Deng, Z., Lam, H. T.: The SPMF open-source data mining library version 2. In: 19th European Conference on Principles of Data Mining and Knowledge Discovery (PKDD 2016) Part III, LNCS 9853, pp. 36–40. Springer (2016)
28. Frequent Itemset Mining Dataset Repository, http://fimi.ua.ac.be/data

An Effective Paradigm on Self-regulating Cautious Strategy

Malathy Subramanium(✉), S. Jaipriya, G. Anitha, V. S. Janani, and V. Bharathipriya

Sri Krishna College of Technology, Coimbatore, India
{malathy.s, s.jaipriya, g.anitha, l5tuece055, l5tuece029}@skct.edu.in

Abstract. The number of accidents in the world is increasing day by day and most of these accidents are effectuated due to Driving While Intoxicated (DWI). Therefore, since the death due to the Drunken-Driving or Driving Under the Influence (DUI) of alcohol has assumed proportion larger (60%) than one can visualize. In order to combat such life-risking problems, we have designed a mock-up. This safety serious system is actualized using ARDUINO and the main unit of this project is alcohol detecting sensor. Here alcohol sensor (MQ3) is used in a steering wheel and also in the passenger seat to sense the alcohol molecules present inside the vehicle. When sensor equipped in a steering wheel senses the alcohol content (i.e)., when the level of alcohol of driver crosses a permissible limit, fails the attempt of the driver to start the engine irrespective of the passenger. To thwart the accidents due to immediate engine failure, a timer is proposed in the exemplary. This framework is also embodied with widely used GSM MODEM and it will automatically send the distress message to the owner of the vehicle or to the family member.

Keywords: Alcohol sensor (MQ3) · Short messaging service (SMS) · Safety Serious System (SSS) · Global system for mobile communication (GSM) Timer · Automatic engine locking

1 Introduction

Drunk driving is a major life-threatening problem around the world. In an analysis, over 10,000 traffic fatalities were directly associated with drivers who had Blood Alcohol Content (BAC) or Blood Alcohol Concentration above 0.08 mg/dl. The legal limit of BAC is 0.05% or 5 mg per 100 ml or 1 dl. Drivers demand complete attention, spontaneous action, self-control, and quick decision-making abilities to avoid any unanticipated incidents while driving a vehicle. But drunken drivers will not be in a stable condition. When BAC crosses 0.08%, alcohol in the blood seizes the human brain working and it results in a lack of concentration, difficulties in controlling the speed, drowsiness, slow reaction time, loss of self-control [10]. States that the above mentioned factors result in rash driving. Hence it is an inconvenience for the other road users and a question of life. Body Area Network (BAN) an under-developing technology, which can be able to provide mobility for person with Wearable or Implantable

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 769–778, 2020.
https://doi.org/10.1007/978-3-030-37051-0_86

devices in and around the body, who are wandering within the coverage region of monitoring system. BAN or WBAN plays a pivotal role in Human Healthcare. By integrating the concepts of WBAN and WSN, the proposed automotive alcohol detection system caters an efficacious solution for the safety of the people inside the car, pedestrians and other motorists. This framework detects the alcohol molecules in human breath, provides the corresponding analog resistive output to the arduino to control the vehicle ignition with low power consumption. The system encompassed with the timer to avert immediate engine failure after alcohol detected inside the vehicle. To report accidents occurring in real time the alert system is implemented by deploying GSM. This system also enables the inter-city transport companies to effectively track their vehicles.

2 Literature Survey

According to the World Health Organization (WHO) Report on September 2018: The deaths that occur on India's roads is almost 1 lakh, which are indirectly related to driving vehicles under the influence of alcohol. In [3], reveals about approximately 336 people/day die in Road accident, but as of WHO report 2018, the number increased to 400 deaths/day which impelling India to take car safety seriously. Model [6] admits around million children killed due to over-speeding. For a 1% increase in mean speed culminates in a 4% increase in the road fatalities. To curtail accident rate due to over speeding, model [5] uses GSM and GPS to send the message when speed of the vehicle and amount of tilting exceeds. System [2] exemplifies the traffic mechanism for speed control, SONAR in this system supports to determine the distance of surrounding vehicles. Once when an obstacle is captured, vehicle stopped. Psychological state of the driver such as Drowsiness & Distraction acting as a root to endorse night accidents. More than 80% of accidents due to drunken driving accidents take place between 1 am to 4 am. To safeguard the drowsiness and drunk drivers, [8] embodies Eye-blink sensors to find the driver drowsiness and Alcohol sensor for detecting the drunken state of the driver. It adopts GSM to send an SMS when the driver is caught in inebriated condition. It also focuses on obstacle detection mechanism using proximity sensor. In [12], depending on the alcohol concentration and Eye blinking rate, Speed of the vehicle varies. This system triggers alarm, activation of auto pilot. Smart-Helmet mechanism for Two-Wheeler Accident prevention elucidated in [7], which senses alcohol content and sends data to Smartphone via Bluetooth Module when an Accident is detected. Using Vibration Sensor, [9] reduces the action time after Accident. This clearly depicts that Driving While Intoxicated (DWI) and Rash Driving are the major sources of Road accidents across the world. These accidents will also have adverse impacts on Pedestrians, Elderly Citizens and School children who are crossing the road at that time. Survivors from these Road Accidents will lead a Traumatized life.

3 SSS Model

In an existing system, automatic engine locking process was done in an unprotected way, i.e when the alcohol is detected by the sensor the motor is turned off immediately. This immediate engine breakdown may cause unexpected accidents. Thus in the proposed model, this limitation is overcome by using a timer system. A block diagram of the SSS (Safety Serious System) Model is represented in Fig. 3. This system is divided into three sections:

- Sensing
- Processing
- Actuating network.

Sensing part consists of Infrared (IR) and Alcohol (MQ3) Sensor. Infrared Sensor in the system is used for efficacious power usage. It initiates the whole process only when a person is detected inside the vehicle. The motor will be ON only when a non-alcoholic breath is detected. Alcohol Sensor continuously monitors the driver's breath and produces an analog resistive output. Processing part has a Microcontroller. Using MQ3 Sensor, microcontroller sways the whole system. Arduino which is the heart of the system reads the data from MQ3 Sensor. Analog to Digital Converter (ADC) in Arduino converts the analog data from the sensor to corresponding digital data. In response to the detected alcohol percentage, Microcontroller controls the actuating element (DC Motor) and sends a warning message to the concerned person (Fig. 1).

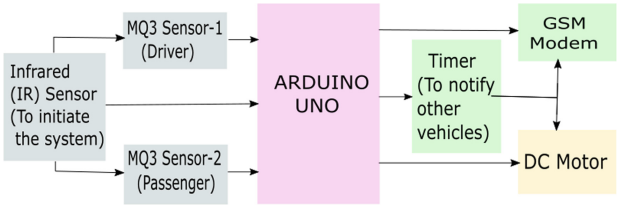


Fig. 1. SSS model block diagram

Consider a scenario of a car equipped with SSS model as shown in Fig. 4 by the owner of the vehicle. When the driver gets inside the car the SSS model activates in a jiffy. The model activation is done by the IR sensor used in the circuit. The system will be in 'ON' state only when the IR sensor output is high (i.e. IR = 1). Effectively saying when the person sits inside the vehicle is sensed by the IR sensor and sends the output to the controller to initiate the system, until the circuit remains in 'OFF' state or in 'Sleep' mode (Fig. 2).

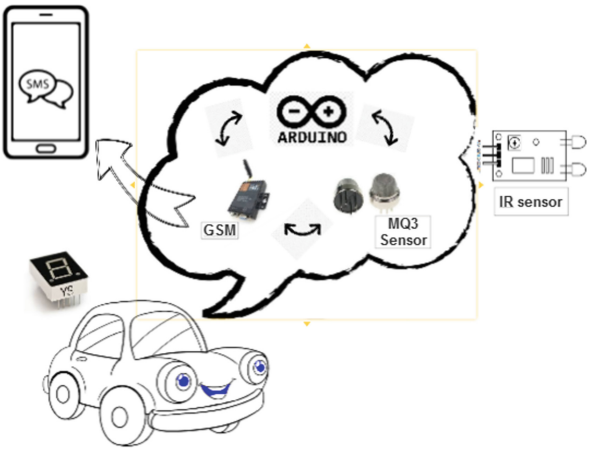


Fig. 2. SSS equipped car

Once the system turns 'ON' state, the onboard alcohol sensor will detect the alcohol content in the driver's breath and sent its value to the controller board (Arduino). The purpose of the sensor module is to provide a technique to compare alcohol source with a reference or an acceptable level and when the source exaggerates, it is capable to set an alarm limit. It acts similar to a common breathalyzer circuit. Since the sensor has gas sensitive material to sense alcohol, it has high sensitivity to small value. From the MQ3 sensitivity graph shown in Fig. 5, its sensitivity towards hexane, CH4, and CO is less

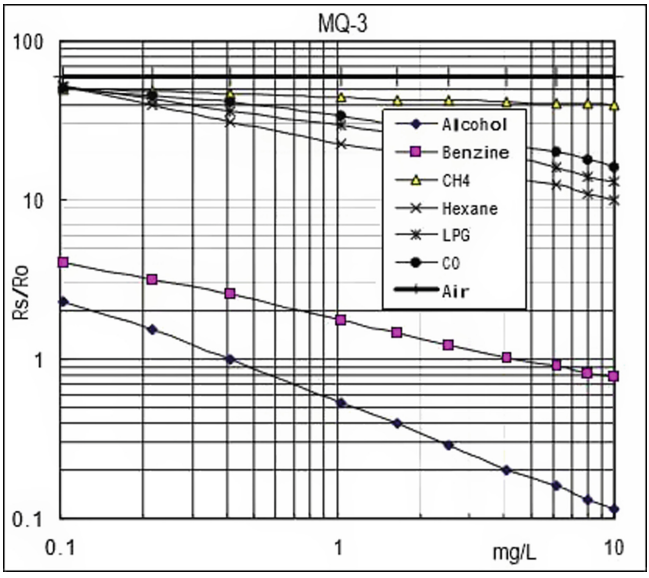


Fig. 3. MQ3 sensor sensitivity graph

when compared to alcohol which is very high. To obtain a meticulous measurement, the sensor's alarm circuit has to be fixed by considering the temperature and humidity influence.

As the result of alcohol detection the controlling process is done by the core part of this prototype (Arduino board). This board mastery the engine and turns it down as soon as the alcohol is detected. The next stage before the engine fiasco is the notification provided by the timer to alert other road users. It is a specialized type of clock which is used to sync operation time with a system clock. With extension, the alert note is sent to the vehicle holder by the low power GSM modem which uses a protocol based on the Hayes AT-Command set as shown in Fig. 6 to setup and control the transmission and reception of data (Table 1).

Table 1. AT command

Command	Description
AT	Check if serial interface and GSM modem is working
ATE0	Turn echo off, less traffic on serial line
AT + CNMI	Displays new incoming SMS
AT + CPMS	Selection of SMS memory
AT + CMGF	SMS string format, how they are compressed
AT + CMGR	Read new message from a given memory location
AT + CMGS	Send message to a given recipient
AT + CMGD	Delete a message

4 Process Control

Whenever a person sits inside the vehicle, IR sensor initiates the system. For effectual power consumption, IR sensor is used over here.

4.1 Driver Consumed Alcohol

The MQ3 Sensor in the steering wheel checks whether the person consumed alcohol or not. If a drunken driver sits in the driver seat, it works on two cases:

1. When the vehicle is not moving, then the alcohol sensor detects the alcohol content based on the breath of the driver and it fails the foray of the driver to start the engine.
2. If the driver consumes alcohol during driving, then the MQ3 sensor sends a digital HIGH output to ARDUINO. Then it turns ON the Timer to notify other vehicles such that the vehicle is going to stop instantly and this prevents the accidents that will occur due to immediate engine failure. Once the counter value reaches zero, the speed of the vehicle gradually diminishes.

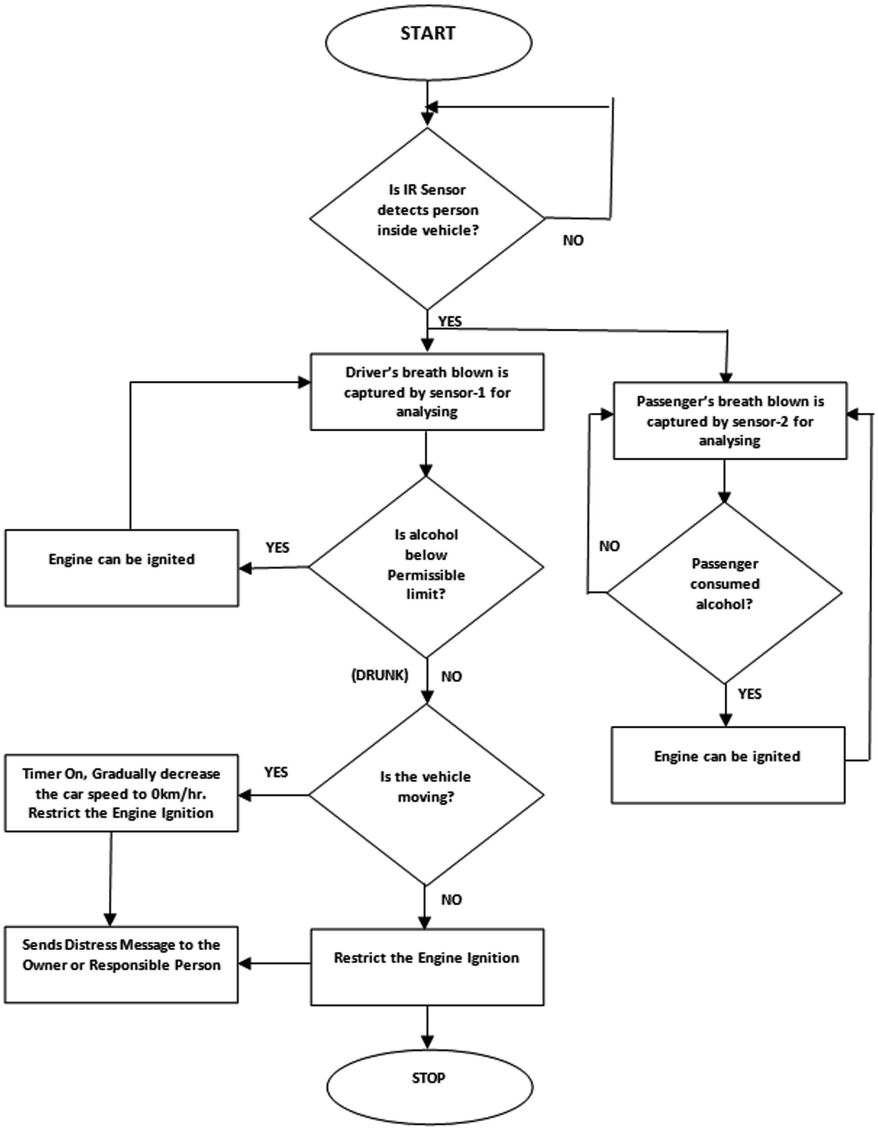


Fig. 4. Process control of SSS model

4.2 Passenger Consumed Alcohol

To avoid interrupting the system with alcohol molecules from the breath of the passenger, here MQ3 Sensor is also placed in the passenger seat. Hence this system works based on the alcohol consumption of driver irrespective of the passenger.

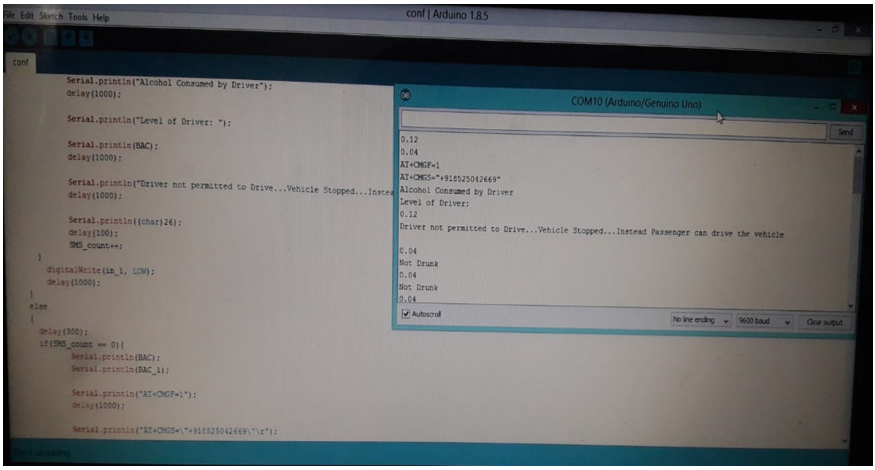


Fig. 5. Software simulation window

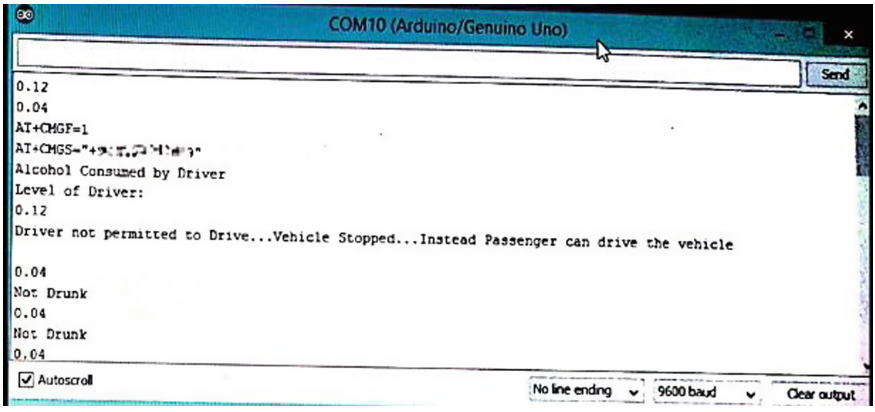


Fig. 6. Safety serious system output window

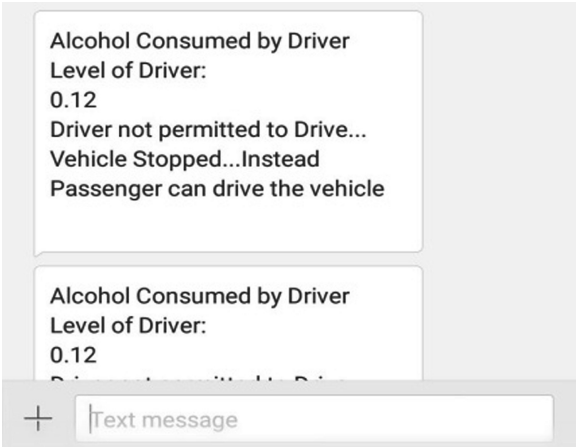


Fig. 7. Alert note from GSM

5 Results and Discussion

From Fig. 5 it is absorbed that MQ3 Sensor is Heat-Driven Device. It takes some time to sense precisely. The moment the sensor detects the alcohol molecules, it locks the ignition system and sends a distress message to the concerned persons. From Fig. 6 it is inferred that, when the alcohol is detected, an acknowledgment about the alcohol level of the driver and the vehicle condition is sent by the Arduino. Figure 7 ensures the successful conveyance of SMS to the registered number of the authorized person from the system modem. The driver does not consent to Drunk Driving or Driving Under the Influence (DUI) of Alcohol.

6 Conclusion

Fire and ice can still make a pair, but drinking and riding can never get assort. When it goes together, the result will be incorrigible. Hence the SS system helps to find and preclude accidents before it happens. This device provides well-advanced facilities and has a great pertinence in today's world as it can curtail alcohol-related road fatalities and mortalities.

7 Future Work

The paper can be extended to an improved version for obviating drunken drivers from getting on the road with a new concept using various digitized alcohol detection sensors. In future instead of using MQ3 sensor, wearable sweat sensors can be used to check the alcohol content level in the blood from the sweat. Using sweat sensor will be more accurate when compared to MQ3 sensor. This can be accompanied by an RFID

sensor to prevent the fraudulent. This system can be enhanced using Accelerometer to identify Potholes in Roads. One can also encompass GPS Module [2, 3] that might provide additional functionality to track the vehicle efficaciously. Hence a system with wearable sweat sensor supported with identification mechanism for authorized and unauthorized car owner along with location tracking can cumulatively contribute to absolute safe driving.

References

1. Shahad, A.-Y., Musab, A.M., Ali, M.N.: Mohammed. Alcohol Detection For Car Locking System. ©2018 IEEE
2. Jaipriya, S., Malathy, S., Srinivasan, K., Priyanka, B., Charliene Karunya, L.: A framework for energy optimization in wireless sensor nodes at Ad-Hoc network. In: 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE (2018)
3. Divya, K., Jaipriya, S., Anitha, G., Malathy, S., Maheswar, R.: An energy efficient technique for time sensitive application using MC-WSN. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC), IEEE (2018)
4. Taieba Taher, R.U.A., Haider, M.A., Das, S., Yasmin, M.N.: Nurasdul Mamun, Accident prevention smart zone sensing system. In: 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) 21–23 Dec 2017, Dhaka, Bangladesh, ©2017 IEEE
5. Pughazendi, N., Sathishkumar, R., Balaji, S., Sathyavenkateshwaren, S., Subash Chander, S., Surendar, V.: Heart attack and alcohol detection sensor monitoring in smart transportation system using internet of things. In: International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017), ©2017 IEEE
6. Selvathi, D., Pavithra, P., Preethi, T.: Intelligent transportation system for accident prevention and detection. In: International Conference on Intelligent Computing and Control Systems (ICICCS), ©2017 IEEE
7. Sadad Mahamud, Md., Monsur, M., Saniat Rahman Zishan, Md.: An Arduino based accident prevention and identification system for vehicles. In: 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) 21–23 Dec 2017, Dhaka, Bangladesh, ©2017 IEEE
8. Seelam, K., Lakshmi, C.J.: An Arduino based embedded system in passenger car for road safety. In: 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), ©2017 IEEE
9. Malathi, Ms.M., Sujitha, Ms.R., Revathy, Ms.M.R.: Alcohol detection and seat belt control system using Arduino. In: 2017 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS), ©2017 IEEE
10. Das, A., Ray, A., Ghosh, A., Bhattacharyya, S., Mukherjee, D., Rana, T.K.: Vehicle accident prevent cum location monitoring system. In: 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), ©2017 IEEE
11. Tushara, D.B., Vardhini, P.A.H.: Wireless vehicle alert and collision prevention system design using Atmel microcontroller. In: 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), ©2016 IEEE
12. Kaplan, S., Amac Guvensan, M.: Member, IEEE, Ali Gokhan Yavuz, and Yasin Karalurt, "Driver Behavior Analysis for Safe Driving: A Survey", IEEE Trans. Intell. Transp. Syst. **16** (6), December 2015, ©2015 IEEE

13. Raja Raghavan, M., Bhuvaneswari, N.S.: Intelligent safety and security systems in automobiles. In: 2015 IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR), ©2015 IEEE
14. Sahabiswas, S., Saha, S., Mitra, P., Chatterjee, R., Ray, R., Saha, P., Biswas, B.A.: Drunken driving detection and prevention models using Internet of Things. In: 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), ©2016 IEEE

A Smart System for Detection, Restoration, Optimization and Preservation of Fresh Water

Aswin S. Sekhar(✉), V. P. Bassam, Amrutha P. Asokan, Joice Anna Cherian, and Jubilant J. Kizhakkethottam

Computer Science and Engineering, Saintgits College of Engineering, Kottayam, Kerala, India
aswinsekhar38@gmail.com

Abstract. Fresh water availability, conservation, and management are intense areas that need consideration. The paper focuses on automated mechanism to find effective solution to certain problems like, leakage detection when there occurs a break in the pipelines, water wastage due to overflow of water from buckets and storage tanks, no facility to check the quantity and quality of water in storage tank, use of water pipelines without the knowledge of the household owner and user needs to check manually the condition of lid of the storage tank. The system comprises of Raspberry Pi, pH value detector probe, ultrasonic sensor, solenoid operated valve, PIR sensor, light sensor, water flow meter, and a push button switch. The work also aims to notify the user of their water usage for each activity by monitoring the quantity of water used at each pipe and analyzing the consumption rate.

Keywords: Internet of things · Automation · Water conservation · Water management · User interactive app · React native

1 Introduction

Water [8] scarcity is a major problem that prevails in the present world. The issues faced related to the water consumption exists in household as well as in public water system. One of the major reason for this is the poor water management system existing in the society. An efficient and effective method for proper water management is necessary in this situation. The paper brings out a well-designed approach for proper water management, a method for Detection, Restoration, Optimization and Preservation of fresh water – DROP. DROP is implemented using IoT and a react native user-friendly app.

The proposed system comprises of a set of sensors to control, monitor and analyse the water usage and its status on a live basis. The system notifies the user about the water usage and quality of the water being used. All this information is passed to the user via app where each user has their own account and the user can control the water flow at their home by themselves. As an extension of its application, the system can be implemented on public and community water systems [10].

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 779–786, 2020.
https://doi.org/10.1007/978-3-030-37051-0_87

2 Literature Review

2.1 The Real Time Monitoring of Water Quality in IoT Environment

M.B. Kalpana discussed on "Online Monitoring Of Water Quality Using Raspberry Pi3 Model", in which it was mentioned that there exists a low-cost system for real time monitoring of the water quality in IoT. The system consists of several sensors such as conductivity, turbidity and dissolved oxygen of water and pH sensor. The measured values from the sensors can be processed by raspberry PI 3 model which is used as a core controller. Finally, the sensor data can be viewed on internet using cloud computing [1]. Similarly, N Vijayakumar and R Ramya proposed a system in which raspberry PI B + model was used as micro controller [4]. A novel approach was proposed by Prashant Salunke, et al. to design smart sensor interface for water quality monitoring in IoT environment. Different sensors are available for water quality monitoring which are used to check the quality. IoT provide interface to monitor and operate remotely from anywhere and anytime. Intel Galileo Gen 2 board is used as interfacing device in the proposed system [7].

Brinda Das et al. analysed on "Real-time water quality monitoring system using Internet of Things" in which water quality measuring system checks the quality of water in real time using various sensors to measure the quality of water. There is a ZigBee module in the system that transfers data collected by the sensors to the microcontroller wirelessly, and a GSM module which transfers wirelessly the data further from the microcontroller to the smart phone/PC [5, 12].

2.2 Leak Detection

R F Rahmat, et al. reviewed on "Water Pipeline Monitoring and Leak Detection using Flow Liquid Meter Sensor" in which a solution to detect and to determine the location of the damage when there is a leak. The detection of the leak location will use fluid mechanics and kinematics physics based on harness water flow rate data obtained using flow liquid meter sensor and Arduino UNO as a microcontroller [3].

Jihoon Choi, et al. studied leakage detection techniques in which a new method for leak detection and location based on vibration sensors and generalised cross-correlation techniques was proposed [2].

2.3 Water Level Controlling System

Siddartha Shankar and Dr M. Dakshayini proposed a system for Smart Water Level Controlling which was developed based on IoT and Mobile. This effectively reduces the wastage of water by monitoring the level of water in the storage tank and intimating the user to turn on or turn off the motor using their mobile phone. The water level sensor is deployed in the storage tank and connected to the Arduino Board. The Arduino updates the database in the server with the level of water in the tank. This information stored in the server is displayed in the mobile phone [6]. Water level monitoring as well as controlling with IoT and android application is also an existing system [11]. Tech giant IBM has partnered Indian Institute of Information Technology

and Management, Kerala (IIITM-K) to develop a system that will monitor quality and presence of metals in water in real-time [10].

3 Proposed Model

An introduction of smart automated water management system can be done to solve the above defined problems. Here this can be solved by gathering up the issues at each point in the water transmission lines. Considering the water storage tanks, problems like lack of proper monitoring of water quality, improper alert system for the user on low water level in the storage tank, insufficient facility for controlling the water meter, inadequate system for monitoring the overall water usage, absence of a system to check whether the storage tank is protected or not i.e. whether the lid is closed or not exists. These issues can be solved by taking the tank as a module. So the master module in the Sect. 4.1 deals with how it can be solved. Another major problem is the water leakage. The solution for the same is discussed in the outlet control module (Sect. 4.2). Other functionalities adding up to this system is the controlling the taps used in households and in industries. This function gives the user the power to control the pipes, the usage status of water at each pipes and this is examined in the tap control module. Overflow control module is introduced to prevent overflow of water from buckets even in the absence of user. Considering the literature survey undertaken, the system is planned to implement the system module wise. Connecting all the modules after completing each of them gives the solution for all problems that have mentioned above. These four modules bring up a solution to the existing water problems. The overall design of the proposed system is as shown in Fig. 1.

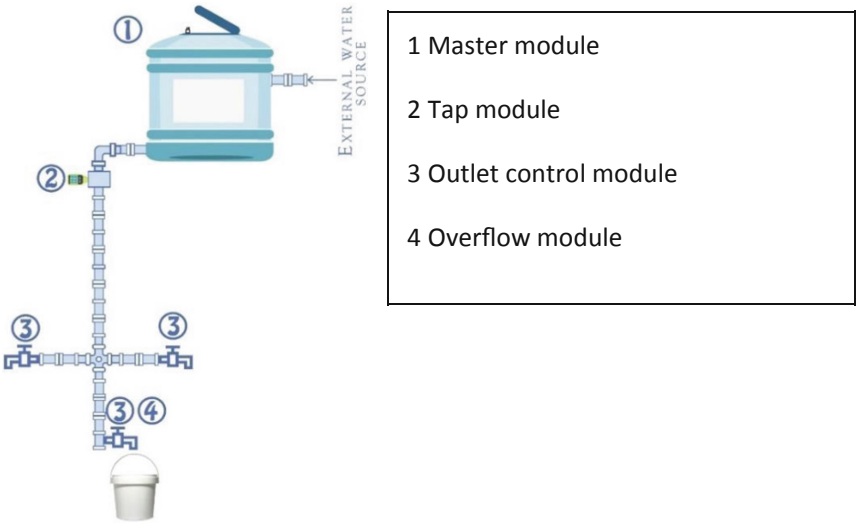


Fig. 1. Overview of module design

4 Design and Methodology

The proposed system is implemented module wise. Each module performs specific functionalities to contribute to the overall water management system. These modules are later interconnected to implement for forming the complete water management system. The system can be implemented in the household, industries as well as in public water system.

The modules that are introduced in the system are.

4.1 Master Module

This module performs the functions that must be performed at the water storage tank level that are stated in proposed system. The master module is assigned with the tasks of checking the water quality in storage tanks, to give the user a live status of the water level in the tank, to ensure the protection of storage tank. In order to accomplish these tasks, the module includes push button switch and a light sensor to ensure the lid of the water storage tank is closed or not, ultra-sonic sensor to measure the water level, water quality sensor to test the quality of the water and solenoid valve is placed at the main outlet of the tank to control the water flow from the tank to other water consuming

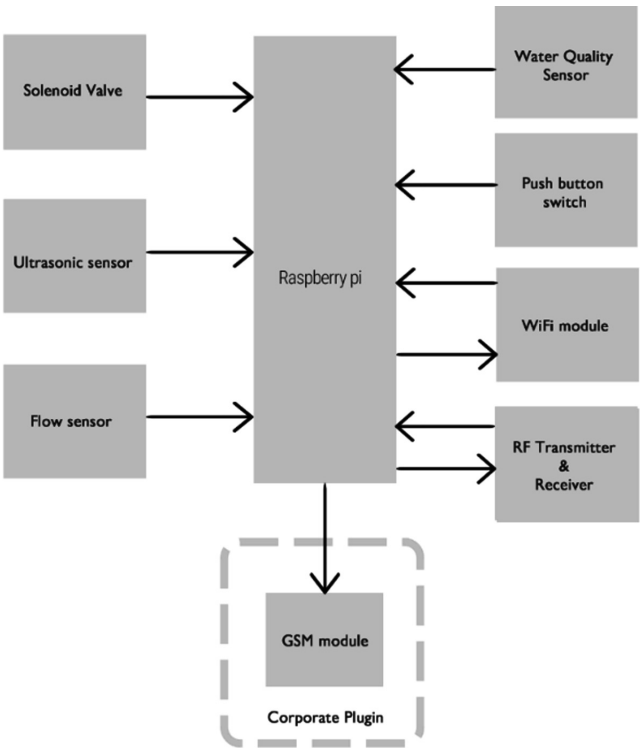


Fig. 2. Master module architecture [9]

points. For the analysis of water consumption, a flow sensor is used to measure the water flow to the other pipelines consuming the water from the storage tank. All these sensors are connected to the raspberry pi board as shown in Fig. 2 and the data from the sensors are uploaded to the server. This data is retrieved to the app and is monitored and controlled by the user.

4.2 Outlet Control Module

In order to control the water flow to each pipe and for performing leakage detection test the outlet control module shown in Fig. 3 is introduced. The module is placed at every junction in the pipelines and it consists of water flow sensors and solenoid valves. The leakage in the pipe line is detected by measuring the quantity of water which is passed from different points in the pipelines. The flow sensor in the module is used for easing up this process. Solenoid valve in the module is used to control the water flow to the different water consumption points from the junction. The leakage detection can be done on a timely basis or with a manual instruction from the user through the app.

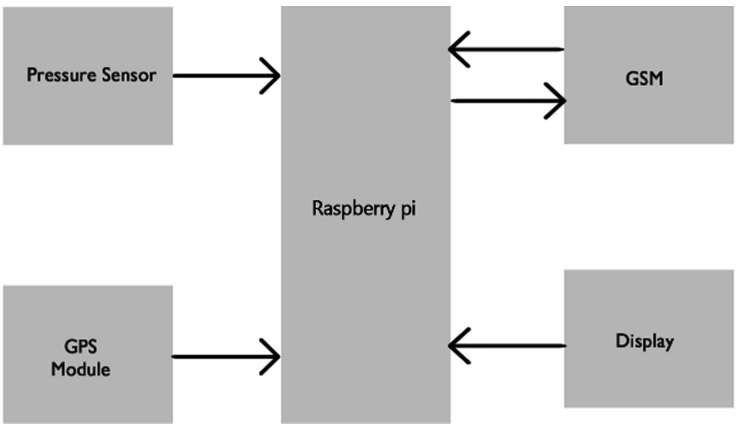


Fig. 3. Outlet control module architecture [9]

4.3 Tap Control

For controlling and analysing the water being used for different puposes tap control module is used. The tap control module (Fig. 4) consists of solenoid valve, waterflow sensor Passive Infra-Red sensor. The PIR sensor lets the user turn ON and OFF by gesturing. The water flow sensor analyses the water being used at the outlet. The obtained data of usage is uploaded to the server which is retrieved by the app and displayed to the user, it helps to give the live status of water usage analysis which is very useful for the consumers to look at their water consumption rate.

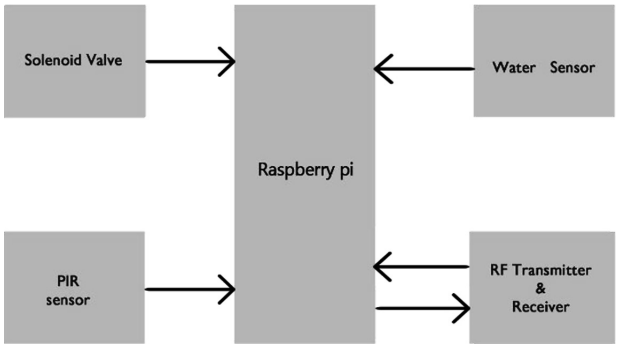


Fig. 4. Tap control module architecture [9]

4.4 Overflow Control

For solving the bucket overflow problem, the overflow control module is placed. The module is implanted at every outlet where there is a chance that buckets or any other containers may be used for water collection. The module consists of solenoid valve, PIR sensor, ultrasonic sensor and a water flow sensor. The module is like the tap control module apart from an extra sensor for checking water overflow. PIR and solenoid valves are used to turn the tap ON and OFF and the water flow sensor is used to monitor and analyse the water being used at the outlet. An extra ultrasonic sensor is added in the overflow control module for checking the water level in the water collecting container placed beneath the tap. Once the container is filled and starts overflowing the ultrasonic sensor senses that there is no rising in the water level in the container. This information signals the solenoid valve to cut off the water supply. Thus, with a slight tolerance amount of water loss the bucket overflow problem is solved without any manual intervention (Fig. 5).

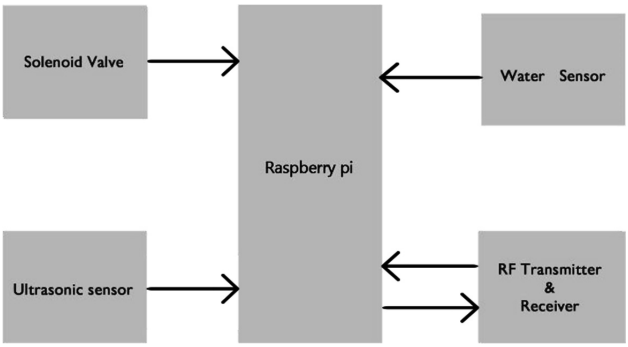


Fig. 5. Overflow control module architecture [9]

5 Conclusion

Water conservation and its proper management are important. Though there exist conventional methods for leakage detection, water quality and quantity check and to prevent water wastage due to overflow, there is no proper and cheap automated system which solves all these problems together. Each of the existing conventional methods have its own drawbacks. The proposed system preserves water from being wasted by detecting leakage and controlling overflows, and aware users about water quantity used at each consumption point. The system promotes water conservation strategies and makes awareness of conservation of freshwater among society.

As a future scope of the project, it can be extensively implemented over cities and villages. Especially this technique can be implemented in hostels, flats and hotels to monitor the water consumption rate of each occupants individually. Hence the system will be convenient for the owner to deal with the water bills. One of the functions that can be applied in our public water system as an extra functionality of the project is providing timing information about the water arrival at the pipeline connected to the user's house. This function will be beneficial for the Kerala Government's Rural Water Supply and Sanitation Project 'JALANIDHI'. Since the app provide the guidelines about the water conservation, the instructions can be passed to the client in association with the Kerala water authority. This will help to spread the announcements from the authority in a very fast and easy manner. The system can be set up not just in Kerala but also in other state's water authorities.

References

1. Kalpana, M.B.: Online monitoring of water quality using raspberry Pi3 model B. In: IJITR (2016)
2. Choi, J., Shin, J., Song, C., Han, S., Park, D.: Leak detection and location of water pipes using vibration sensors and modified ML prefilter. In: MDPI (2017)
3. Rahmat, R.F., Satria, I.S., Siregar, B., Budiarto, R.: Water Pipeline Monitoring and Leak Detection using Flow Liquid Meter Sensor" in IAES International Conference on Electrical Engineering, Computer Science and Informatics (2017)
4. Vijayakumar, N., Ramya, R.: The real time monitoring of water quality in IoT environment. In: International Conference on Circuit, Power and Computing Technologies (2015)
5. Das, B., Jain, P.C.: Real-time water quality monitoring system using Internet of Things in 2017 International Conference on Computer, Communications and Electronics https://ieeexplore.ieee.org/document/8003942
6. Shankar, S., Dakshayini, M.: IoT-mobile enabled smart water level controlling system to regulate water: 978-1-5386-5314-2/18/$31.00 ©2018 IEEE
7. Salunke, P., Kate, J.: Advanced smart sensor interface in internet of things for water quality monitoring. In: 2017 International Conference on Data Management, Analytics and Innovation (ICDMAI)
8. Brito, H., Gomes, A., e Jorge Bernardino, A.S.: Script in mobile applications: react native vs native script vs native development. In: Iberian Conference on Information Systems and Technologies (CISTI) (2018)

9. Bassam, V.P., Asokan, A.P., Sekhar, A.S., Cherian, J.A., Kizhakkethottam, J.J.: Automated fresh water wastage prevention mechanism with quality management. In: Households And Industry in Kerala state Technological Conference (2019)
10. A real-time water quality management system - 'Swatchpaani' developed by Indian Institute of Information Technology and Management –Kerala (IIITM-K) and IBM
11. Shah, P.P., Patil, A.A., Ingleshwar, S.S.: Iot based smart water tank with android application. In: 2017 International conference on I-SMAC (IoT in Social, Mo-bile, Analytics and Cloud)
12. Yadav, V., Borate, S., Devar, S., Gaikwad, R., Gavali, A.B.: Smart home automation using virtue of IoT. In: 2017 2nd International Conference for Convergence in Technology (I2CT), pp. 313–317. IEEE (2017)

Variants of Cuckoo Search with Levy Flight and Dynamic Strategy Based Cuckoo Search (DSBCS)

Akhilesh Kumbhkar(✉), Deepak Garg, Sarita Lamba, and Mahaveer Pingolia

National Institute of Technology, Kurukshetra, Haryana, India
akhileshkumargoal@gmail.com, pv3019996@gmail.com

Abstract. Cuckoo algorithm which is inspired from the breeding strategy of cuckoo bird is a type of meta-heuristics, which is widely used in solving NP-hard problems. Furthermore, CS has only one input parameter i.e., discovery probability. So, it is generally applicable to vast set of problems as compared to other multi parameter algorithms. Moreover, Cuckoo search uses Levy flight which is supposed to be global random walk as compared to other distribution schemes. In this paper, we have deeply studied Cuckoo Search Algorithm and Levy flight with important variants of both. We reviewed and compared Binary cuckoo search, Improved (Dynamic)cuckoo search, as variants of CS while Mantegna, Gaussian, and Cauchy distribution as variants of Levy walk. Furthermore, on the behalf of this we have proposed Dynamic Strategy based cuckoo search (DSBCS) which is supposed to give better results due to dynamic discovery probability, best global walk, good neighbor strategy after discovery and solution preserving strategy for replacement.

Keywords: Binary CSA · Cuckoo search · Improved CSA · Levy flight · Meta-heuristic approach · Nature inspired strategies · Random walk

1 Introduction of CS

Yang and Deb discovered an Algorithm named as Cuckoo Search for optimization. This is to solve the certain emcee bird optimization issues, this can catch the immediate problems of appropriate Cuckoos which is inspired by nature's behavior [1–5]. Obligate brood Parasitism is a feature in which some Cuckoo's drop their eggs in the host nest of another species, birds for better or good growth and wealth because of which it is said to be based on nature inspired algorithm. Taking, the emcee bird find that the egg is not its own, then it abandons that unwanted egg or leave the nest simply by making an another nest. The cuckoo birds specially broad parasitic abate have emitting in a pattern, as the mimic of voice and the colors of the opted host bird species by the Cuckoo's. Cuckoo birds claim for the Optimization problems as they enhance such reproductive acts [6–10]. The first act of the cuckoo chicks after appear in live, is to make the emcee bird eggs or chicks by forcing them to get out of the nest. This behavior of cuckoo decreases the splitting of eatables collected by the host parent birds [10–12].

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 787–796, 2020.
https://doi.org/10.1007/978-3-030-37051-0_88

1.1 Some Important Aspects of Cuckoo Search Algorithm [1, 2]

1. Each & every egg within the nest consists of a solution, and that egg of Cuckoo Species depicts a contemporary solution.
2. In the Algorithm, we obtain the best and prospective solutions by replacing the good-for nothing eggs out of the nest.
3. We apply this algorithm for only one bird per host nest because it is the best appearances in this mode.
4. This algorithm is also applied with multiple eggs in a nest for composite problems to constitute a set of solutions.

1.2 CS Algorithm, in Three Assumptions

1. By selecting a emcee bird nests from the total number of nests with the help of levy flight, each Cuckoo lay one Cuckoo egg per nest.
2. Nest having better quality eggs, which are carried onto the next round
3. The number is fixed and the quality of the nest is static and is not alterable.

Algorithm Name: Cuckoo Search Algorithm

Algorithm 1CS Algorithm

1. P_k where, (k = 1, 2,3,4,5, ..., n) Get the start population of n nests(host).
2. While(G>Max generation) or (stop-condition)
3. Get a cuckoo randomly by Levy flight
4. Evaluate its fitness function Z_k
5. Choose a nest among n (say, s) randomly
6. If (Z_k > Zs),
7. Replace Z_s by the fresh cuckoo solution or egg;
8. end
9. Abandon or discover nest with p_a probability by host bird and create new nest
10. Hold up the best solutions
11. Solutions is ranked and search the current best solution
12. end while
13. Post results
14. end

2 Levy Flight Algorithms

Levy flight algorithm is handles a group of molecules at every generation. Start with best available location, creates all new breed(generation) at distances are aimlessly allot by Levy [4, 9]. Then the best/fresh one is estimated and selected from the fresh or new generation. The operation is repeated until the close condition is reached. Only the

finest featured solution is chosen. Levy Equation which is used to generate fresh solution $y^{(s+1)}$ for a bird (cuckoo i)

$$y_j^{(s+1)} = y_j^{(s)} + \alpha \oplus levy(\beta) \tag{1}$$

Where,

A = Step size ($\alpha > 0$), in most cases we use $\alpha = 1$ and $1 < \beta \leq 3$.

Here the random step length is chosen by the levy distribution which is as follows.

$$Levy \sim v = s^{-\beta} \tag{2}$$

With the help of this levy equation some new solutions are generated which revolve around the current best solution and make the local search work faster then normal.

Algorithm 2 LFA (Random Walk)

```
1 Process  LF Optimization()
2 Start-state();
3 Current-value = objective-function();
4 best-value = Current-value;
5 best-State= present-state();
6 while(close-condition-not-meet)
7       while (jump-number-not-reach-maximum)
8             flight-length = Levy-flight(base-length ,beta(  β));
9             jump-random-at- the distance(flight-length);
10            present-value  = objective-function();
11            if(present-value<best-value)
12                best-value  = Current-value;
13                best-state= Current-state();
14            end if
15      end while
16      output : "reached-to-best-known-state()" ;
17 end while
18 end procedure
```

A symmetric Levy distribution, denoted as lα(c,g) is a PDF with a characteristic function:

$$l_\alpha(c, g) = e^{-c|g|^\alpha} \tag{3}$$

Note that this can only be a valid characteristic function for $0 < \alpha < 2$ because the variance of lα(c, g) does not exist (i.e. = 0) for $\alpha > 2$.

We have already seen some examples of Levy distributions. The Gaussian distribution is $l_2(\sigma 2\ /2,g)$:

$$p(g) = e^{-\frac{\sigma^2 g^2}{2}} \qquad \rightarrow p(g) = \frac{e^{-\frac{x^2}{2\sigma^2}}}{\sqrt{2\pi\sigma^2}} \tag{4}$$

And the Cauchy distribution is $l_1(c,x)$:

$$p(g) = e^{-c|k|} \quad \rightarrow \quad p(g) = \frac{c}{\pi(c^2 + x^2)} \tag{5}$$

3 Variants of Cuckoo Search

3.1 Binary Cuckoo Search

As we know that, CS Algorithm is applied in Continuous searching and as output gives real values which is inappropriate to apply in discrete search space, because of which Binary Cuckoo search came into existence as an improved version/variant of CSA [6]. A set of bits as a problem solution is given by the binary CSA, which is said an extension to the CSA. Levy flight random walk and Binary search representation are the two major steps of Binary CSA. After completing these two steps a Sigmoid function is used to get the BCS. A new cuckoo is selected with the help of levy flight operation. Secondly, for every Cuckoo the flipping chance is calculated with the help of a sigmoid function. After calculating the flipping chances for every cuckoo it will be used to find the binary value of cuckoo's. Handling of Binary optimization problems is the main objective of BCS Algorithm. A binary representation z_k' is obtained, to convert z_k from real to binary solution which is the main feature of BCS algorithm.

Algorithm 3. Binary Search Representation Algorithm
insert: z_k Real solution representation
return: $s(z_k)$

1. For (k = 1 to (problem size)) {
2. $S(z_k) = \frac{1}{(1+e^{-z_k})}$;
3. If (random number $\gamma < S(z_k)$)
4. $z_k^{'} = 1$;
5. otherwise
6. $Z_k^{'} = 0$; }

Where $S(z_k)$ = bit's (z_k) 'Flipping Chance. $z_k^{'}$ takes the value 1 shows the probability of bit.

From interval [0,1] a random number is created for dimension of the solution z (D_k) & with the flipping chance $S(z_k)$, to get the binary solution z_k.

If $\gamma < S(z_k)$, R$\in$ [0, 1] then
$Z_k = 1$;
else
$X_k = 0$;

Algorithm 4. Binary Cuckoo Search Algorithm [6]

1. Objective function f(z), z = (z_1, …, z_d^v);
2. Initialization of population of R host nest z_k where, (k = 1, 2,3,4, …, R);
3. while (v < Maximum Generation) or (close-criterion){
4. Using Levy flight for random cuckoo generation (which is k);
5. BSR algorithm is used to get the binary representation;
6. Evaluate its quality/fitness H_k; //(where H = fitness)
7. select a nest among R (which is r) randomly; //(With the help of BSR)
8. Estimate its quality/fitness H_r;
9. if ($H_k > H_r$){
10. Fresh solution replaces r; //(Fresh solution quality estimated by BSR)}
11. Worse nests fraction(p_a) is abandoned;
12. With the help of levy flight random walk, new nest is created at new location;
13. store the best output solutions;
14. Get the best current & order the solute.

3.2 Improved Cuckoo Search

As we know that original Cuckoo Search use fix value of p_a and α. This values are set at initial level and cannot be altered for new generations. To find optimal solution in number of iterations, this search shows most of the flaws. If α is large and p_a is small then increases in number of iterations and poor performance. Speed of convergence is good but not able to get best solution if p_a is high and α is small. The best and important difference between CS and ICS is to adjust p_a and α. To resolve the CS flaws, variable p_a and α are used at start generation. Algorithm increases the divergence of output vector. To obtain better fine-tuning of output vector at final generation the values should be decreased. The values of both the parameters are changed dynamically with number of generations [8].

Algorithm 5. Improved CS Algorithm

1. $P_a(cn) = P_a ma - \frac{cn}{NI}(P_a ma - P_a mi)$
2. $\alpha(cn) = \alpha_{ma} \exp(c.cn)$

$$C = \frac{1}{NI} \ln\left(\frac{\alpha_{mi}}{\alpha_{ma}}\right)$$

Where,

NI = Number of total iteration
Cn = Current iteration
P_a ma = Maximum value of Pa
P_a mi = Minimum value of Pa

4 Variants of Levy Flight (Random Walk)

4.1 Mantegna Algorithm (Equation)

The first Algorithm is the Mantegna Algorithm, which produces random numbers by Symmetric levy distribution. The distribution parameters p∈[0.3,1.99] (Standard value set), p > 0, number of iterations n, and the number of points which are to be generated. If the points are not specified it by default generates only one point [4, 12].

$$V = \frac{s}{|t|^{1/\alpha}} \tag{6}$$

where s and t are random variables. But s will be calculated by $s\sigma_s$and t by $t\sigma_t$ –

$$\sigma_s(\alpha) = \left[\left\{\frac{\Gamma(\alpha+1)\sin\frac{\pi\alpha}{2}}{\alpha\Gamma((\alpha+1)/2).2^{((\alpha-1)/2)}}\right\}\right]^{(1/\alpha)}, \sigma_t = 1 \tag{7}$$

4.2 Cauchy Random Distribution

The **Cauchy random walk** relates to the curves of normal distribution which is continuous probability distribution. As because comparability is available, normal curve has a shorter peak value than the Cauchy. Normal distribution is distinct, because of which it's fat tail decays much slower than other distributions [9].

The Cauchy has two important attributes: a scale specification (λ) and a location specification (x_0).

- Where the peak is given by the locate specification (x_0).
- The PDF will be at half of the max height when the scale specification is width's half.

The locate specification $_{x0}$ turns the graph along the x-axis and the scale specification λ results in a height (short/long) graph. The smaller the scale specification, the taller and thinner the curve. PDF for Cauchy random distribution

$$\mathrm{F(x)} = f(x) = \left\{\frac{1}{\lambda\pi\left(1+\frac{x-x_0}{\lambda}\right)^2}(-\infty < x < \infty); \right. \tag{8}$$

Where $\boldsymbol{x_0}$ ***is*** the locate specification and λ is the scale specification. Standard Cauchy distribution will reach when $\boldsymbol{x_0} = 0$ and λ = 1. Standard Cauchy random distribution changes to Eq. (10) after the value being set to standard-

$$f(x) = \frac{1}{\pi(1+x^2)} \tag{9}$$

However, the standard Cauchy random distribution can be obtained from the general formula with a specific value set.

4.3 Gaussian Distribution

Gaussian Distribution is also called bell shaped curve/ normal distribution is a continuous distribution. Because of central limit theorem, the Gauss distribution is useful. If large number of random variables being summed up together, under some conditions the sum will be approx normal by CLT statement. In the real life there are many random variables which are shown as the sum of the large numbers of random variables as with the help of Gaussian distribution we can debate that the sum will be of gauss pattern by CLT [4, 9].

PDF of the Gaussian random variable distribution/normal distribution:

A continuous random variable Z is said to be a standard normal (standard Gaussian) random variable, shown as $Z \sim N(0,1)$ if its PDF is given by

$$f(z|\mu, \sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{10}$$

The area is equal to one is confirmed by $1/\sqrt{2}\pi$,

This PDF will be seen if $Z \sim n(0,1)$, then Z a continuous random variable is said to be the Normal random variable (Standard Gaussian).

5 Comparison Among Variants of Cuckoo Search & Levy Flights

On the behalf of the deep research as covered in Sects. 3 and 4 regarding cuckoo search and levy flights variants, comparison has been made among these as tabulated in Tables 1 and 2 [4, 9, 12].

Table 1. Comparison on Cuckoo search variants

#	Cuckoo search	Binary cuckoo search	Improved cuckoo search
Input parameter	$\mathbf{P_a}$ = Discovery probability **n** = Population size	$\mathbf{P_a}$ = discovery probability **n** = Population sigmoid function	$\mathbf{P_a}$ = Dynamic discovery probability and $\boldsymbol{\alpha}$ = Dynamic step size
Output	Population of improved ones	Population of improved ones	Population of dynamically improved ones
Step-Size	Step size ($\boldsymbol{\alpha}$) >>> **0**, commonly used is $\boldsymbol{\alpha}$ = **0.01**	Step size ($\boldsymbol{\alpha}$) >>> **0**, commonly used is $\boldsymbol{\alpha}$ = **0.01**	Dynamic Step size is $\boldsymbol{\alpha} > \mathbf{0}$
Range	$\mathbf{P_a}$ = **[0,1]**, commonly $\mathbf{p_a}$ = **0.25** **n** = **[15,50]**, commonly **n** = **15**	$\mathbf{P_a}$ = **[0,1]**, commonly $\mathbf{p_a}$ = **0.25** **n** = **[15,50]**, commonly **n** = **15**	Range will change dynamically with the number of generations. $\mathbf{P_a}$ **(min)** = **0.005**, $\mathbf{P_a}$**(max)** = **0.5** $\boldsymbol{\alpha}$ **(min)** = **0.01** and $\boldsymbol{\alpha}$**(max)** = **0.5**

(*continued*)

Table 1. (*continued*)

#	Cuckoo search	Binary cuckoo search	Improved cuckoo search
Step length	Random walk process obeys the heavy-tailed power law step length distribution	Random walk process obeys the heavy-tailed power law step length distribution	Step lengths is given by heavy probability distribution
Modification	Uses levy flight as global search and find the best over all the nest present	Used to transform real solution into binary by using a sigmoid function for all binary values provided by BSR	As the improvement in Cuckoo search it uses variable value of $\mathbf{P_a}$ and **n** to deduce the number of iterations and high up the convergence rate
Application	There are many NP-Hard problems, Mining and clustering, Image processing issues, and power and energy problems in which CSA gives optimum solution	Gives better solution for 0-1 Knapsack problem and traveling salesman problem as compared with other optimization algorithm	Planer graph coloring issue

Table 2. Mantegna v/s Cauchy v/s Gaussian distribution

#	Mantegna algorithm	Cauchy distribution	Gaussian distribution
Number of parameter	Distribution Specification $p \in$ [0.3,1.99]	Location(x_0) and Scale(λ) Specification	Location Specification (μ) is mean & Scale specification ($\sigma^2 > 0$) is variance
Range	$-\infty$ to $+\infty$	$-\infty$ to $+\infty$	$-\infty$ to $+\infty$
Variance	Finite variance	Undefined	Finite variance
Application	Local and global searching in many optimization problems	Extreme events such as annual maximum one-day rainfalls	To fit data in best fit for minimizing error of least square problems

6 Proposed DSBCS (Dynamic Strategy Based Cuckoo Search)

On the behalf of comparisons we have come to know that performance of CS lacks due to constant discovery, non strategical replacement, non strategical neighbor searching and only use of Mantegna as levy flight.

Algorithm DSBCS (DD, BW, NSS, SPS)

*Input-DD: Dynamic Discovery (Current / total)*Pa*
BW: Best Walk (out of Mantegna, Gauss, Cauchy)
NSS: Neighbor Search Strategy (used after discovery)
SPS: Solution preserving Strategy (Keeping the bad moves with some probability)
1. Initialization of Population
2. Fitness Evaluation
3. While (stopping criterion not true)
4. Generation of cuckoo eggs using ***BW(Mantegna, Gauss, Cauchy)***
5. Comparison & Keep good one out of Cuckoo egg and Host egg
6. If (Rand > ***DD***) //Dynamic discovery
7. Host bird create new nest through **NSS(neighbor search strategy)**
8. end
9. Replace by ***SPS (Solution preserving Strategy)***
10. end

7 Conclusion

In this paper we have successfully deeply studied cuckoo search and levy flight including their various important variants proposed so far by other researchers. Binary CS dealt population dimension in binary rather than real number while Improved CS removed constant parameters by making them corresponding to iterations. In cuckoo search levy flight played important role so deeply discussed variants of levy flight such as Mantegna algorithm, Gaussian, Cauchy. Comparison has been done among variants of levy flight and variants of cuckoo search. Furthermore, on the behalf of this we have proposed Dynamic Strategy based cuckoo search (DSBCS) which is supposed to give better results due to dynamic discovery probability, best global walk. Future scope involves use of practical implementation of this dynamic parameters and strategies in other metaheuristic to extend the performance.

References

1. Yang, X.-S., Deb, S.: Cuckoo search via Levy flights. In: 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC). IEEE (2009)
2. Rakesh, S., Mahesh, S.: A comprehensive overview on variants of CUCKOO search algorithm and applications. In: 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT). IEEE (2017)
3. Shehab, M., TajudinKhader, A., Azmi Al-Betar, M.: A survey on applications and variants of the cuckoo search algorithm. Appl. Soft Comput. **61**, 1041–1059 (2017)
4. Reynolds, A.M., Rhodes, C.J.: The Lévy flight paradigm: random search patterns and mechanisms. Ecology **90**(4), 877–887 (2009)
5. Umenai, Y., et al.: A modified cuckoo search algorithm for dynamic optimization problems. In: 2016 IEEE Congress on evolutionary computation (CEC). IEEE (2016)

6. Medjahed, S.A,, et al.: Binary cuckoo search algorithm for band selection in hyperspectral image classification. IAENG Int. J. Comput. Sci **42**(3), 183–191 (2015)
7. Walton, S., et al.: Modified cuckoo search: a new gradient free optimization algorithm. Chaos, Solitons Fractals **44**(9), 710–718 (2011)
8. Valian, E., Mohanna, S., Tavakoli, S.: Improved cuckoo search algorithm for global optimization. Int. J. Commun. Inf. Technol **1**(1), 31–44 (2011)
9. Roy, S., Sinha Chaudhuri, S.: Cuckoo search algorithm using Levy flight: a review. Int. J. Modern Educ. Comput. Sci. **5**(12), 10 (2013)
10. Shehab, M., Tajudin Khader, A., Al-Betar, M.A.: A survey on applications and variants of the cuckoo search algorithm. Appl. Soft Comput. **61**, 1041–1059 (2017)
11. Gherboudj, A., Layeb, A., Chikhi, S.: Solving 0–1 knapsack problems by a discrete binary version of cuckoo search algorithm. Int. J. Bio-Inspir. Comput. **4**(4), 229–236 (2012)
12. Garg, D., Kumar, P.: A Survey on Metaheuristic approaches and its evaluation for load balancing in cloud computing. In: International Conference on Advanced Informatics for Computing Research. Springer, Singapore (2018)

RETRACTED CHAPTER: Secure IoT Systems Using Raspberry Pi Machine Learning Artificial Intelligence

R. Ganesh Babu[1(✉)], P. Karthika[2], and V. Aravinda Rajan[3]

[1] Department of Electronics and Communication Engineering, Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India
ganeshbaburajendran@gmail.com
[2] Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnan Koil, Tamil Nadu, India
karthikasivamr@gmail.com
[3] Department of Electronics and Instrumentation Engineering, K.L.N. College of Engineering, Madurai, Tamil Nadu, India
aravind_rajan2k7@yahoo.com

Abstract. The Internet of Things (IoT) ML and AI is an enormous gathering of gadgets containing sensors or actuators associated together over wired or remote systems. With a gauge of more than 25 billion gadgets associated together by 2020, IoT using ML and AI has been quickly becoming over the previous decade. Amid the development, security has been distinguished as one of the weakest territories in ML IoT. While actualizing security inside an IoT using AI arrange, there are a few difficulties including heterogeneity inside the framework just as the amount of gadgets that should be tended to. To approach the difficulties in verifying IoT gadgets in ML, we propose utilizing AI inside an IoT door to help secure the framework. We explore utilizing Artificial Neural Networks in a portal to distinguish oddities in the information sent from the edge gadgets. We are persuaded that this methodology can improve the security of IoT frameworks.

Keywords: Internet of things · Security · Artificial intelligence · Machine learning

RETRACTED CHAPTER

Introduction

The Internet of Things (IoT) is a monstrous gathering of gadgets containing sensors or actuators associated together over wired or then again remote networks [1]. IoT has been quickly becoming over the previous decade and, amid the development, security has been recognized as one of the weakest regions in IoT. There are finished six billion evaluated gadgets as of now associated with the Internet what's more, a gauge of more

The original version of this chapter was retracted. The retraction note to this chapter is found at https://doi.org/10.1007/978-3-030-37051-0_109

© Springer Nature Switzerland AG 2020, corrected publication 2024
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 797–805, 2020.
https://doi.org/10.1007/978-3-030-37051-0_89

than 25 billion associated by 2020. IoT gadgets can be separated into two essential gatherings: edge gadgets and portal gadgets. An edge gadget is a low-control, low-asset [2] gadget containing sensors as well as actuators. Edge gadgets typically have a solitary reason, for instance, gathering temperature information and detailing it to a portal. Entrywaygadgets normally have more assets contrasted with edge gadgets. A portal gadget is in charge of associating the edge gadgets to the Internet and conglomerating information from edge gadgets. With the broad amount of gadgets, measure of information that movements between the gadgets, and the effect these gadgets will have in our regular day to day existences, security is a need. There are a few difficulties with actualizing security inside an IoT arrange [5]. In the first place, IoT frameworks are heterogeneous. There are diverse sorts of gadgets, techniques [8] for correspondence, kinds of information being exchanged and shared, different asset dimensions of gadgets, and framework setups. Each unmistakable component adds to the test of viably secure IoT. A second test inheres in the quantity of gadgets that are associated together. Billions of gadgets associated together gives another examination region of center when thinking about ostensible capacity, flexibility and security also.

To address the difficulties in verifying IoT gadgets, we propose utilizing AI inside an IoT passage to helpsecure the framework. AI is a zone of Artificial Knowledge (AI) in which PC programs are empowered to gain as a matter of fact, models, and analogies [3]. Aslearning happens, the abilities inside the program become progressively clever and the program winds up fit for making educated choices. Inside AI, two of the most famous methodologies are counterfeit neural systems (ANN) and hereditary calculations. ANNs emulate the neurons and neurotransmitters inside the mind to exchange information for correspondence, learning, what's more, basic leadership [4]. ANNs are utilized inside IoT frameworks to screen the territory of IoT gadgets and to make educated choices [6]. We propose the utilization of ANN to get familiar with the sound condition of a framework and associated gadgets. The rest of this paper is composed as pursues. Area gives a review of the territory of IoT Security what's more, the utilization of AI inside security. The portrays our way to deal with calculator learning inside an IoT passage. Segment discusses our experimentation what's more, results incorporating achievement and disappointments in calculator learning inside the gateway. The Empowering the Internet of Trusted Things can resemble opening Pandora's Box. We are putting forth one of the business sole IoT security arrangement stages to use the individual identities of IoT gadgets to give precise perceivability and assurance of an association's IoT resources in Fig. 1.

Our stage use AI to find IoT gadgets, survey chance, pattern ordinary conduct, distinguish strange exercises, and give constant remediation over an association's whole IoT impression. The Conventional security arrangements depend on acknowledgment of working frameworks [11], modules, and introduced applications to group and give gadget settings. Lamentably, setting for IoT gadgets are not surely known. Recognizing X-beam machines, mechanical robotization frameworks, or purpose of-offer gadgets just as Windows-based gadgets offers little knowledge into how best to oversee and verify these gadgets.

RETRACTED CHAPTER

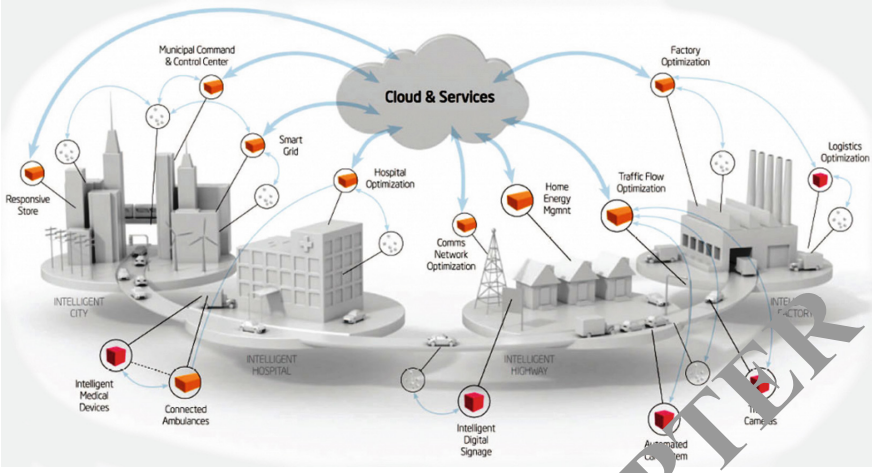


Fig. 1. IoT identification & security –machine learning artificial intelligence approach

The dangers of a gadget, as indicated by customary security arrangements, are frequently determined by looking at the gadget practices against the ordinary/confided in practices of a common client. Such examples are frequently used to distinguish infections. Sadly, this methodology can't be connected to IoT gadgets. To precisely survey hazard to IoT gadgets, the security arrangement must have full learning of the gadget including its trusted and planned practices. Without such subtleties, numerous associations are depending on wrong hazard appraisals of their IoT resources. Customary security arrangements depend on apparatuses, for example, Enterprise System Management (EMS) for PCs and Mobile Device Management (MDM) for cell phones to oversee and update end-point gadgets. These arrangements guarantee that the most recent fix and best practice setups are authorized. Sadly, this methodology isn't appropriate to IoT gadgets. IoT gadgets are reason assembled and not intended to be workable by end-clients. Any endeavor to overhaul their product or even block their correspondence can prompt unusual practices.

2 Analytical Methodology

2.1 Performance Analytics

In the initial move toward scientific estimation of framework execution, we create Gaussian Models (GM) of the biometric information, that around copy the conduct of information. Different highlights can be separated from the biometric information, and combined to shape a nD include vector.

RETRACTED CHAPTER

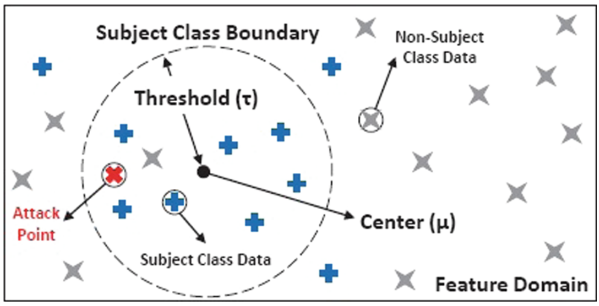


Fig. 2. The mechanism of centroid-based object classifiers

Training Phase: Feature vectors, x = (x_1, x_2… x_n), separated from preparing information is demonstrated utilizing multivariate [10] Gaussian dissemination ($N(x|\mu^{trn}_{sub\,sub}, \sum^{trn}_{sub})$) where, μ is a nD vector containing the mean estimation of each component, and Σ is an n × n covariance lattice of x. Equation (1) is the Probability Density Capacity (PDF) of a multivariate Gaussian dissemination.

$$\int(x) = \frac{1}{\sqrt{2\pi \sum}} e^{-\frac{1}{2}(x-\mu)^T (x-\mu)\sum^{-1}(x-\mu)} \tag{1}$$

where superscripts T and −1 show the network transpose what's more, reversal activities, individually, and |Σ| is the determinant of the covariance framework. A limit (τ) around the μ_{sub}, shapes a n-dimensional hypersphere that demonstrates the subject class limit. The classifier acknowledges includes as subject class information, in the event that they exist in the hypersphere focused at μ_{sub}, that fulfills the disparity appeared in Eq. (2):

$$(x_1 - \mu^{trn(1)}_{sub})^2 + \ldots + (x_n - \mu^{trn(n)}_{sub})^2 < \tau^2. \tag{2}$$

More noteworthy limit builds the sweep of the hypersphere, what's more, its region which implies higher acknowledgment rate, while lower edge is proportional to higher dismissal rate.

Testing Phase: K segments (set tentatively) Gaussian Mixture Model (GMM) can gauge the test information as:

$$\int(x|\wedge) = \sum_{i=1}^{k} w_i \varphi N(x_i|\mu, \Sigma) \tag{3}$$

RETRACTED CHAPTER

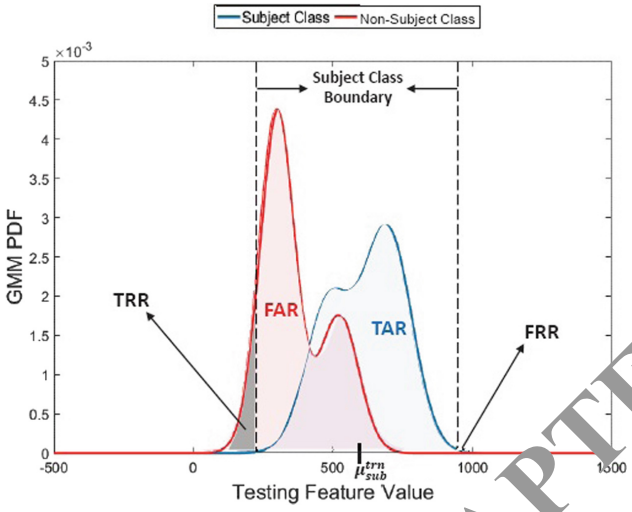


Fig. 3. Test data model

Figures 2 and 3 represent testing information model for one and two measurements, separately. In view of the PDF of subject and non-subject testing information, FRR and FAR can be determined by reconciliation over the class limit (for example hyper-sphere), utilizing Total Distribution Function (CDF) of GMM (Eq. (4)):

$$\int (x|\lambda) \sum_{i=1}^{k} w_i \varphi N(x_i|\mu_i, \Sigma_i) \tag{4}$$

where Φ signifies standard Gaussian conveyance with zero mean and unit fluctuation, and accordingly, Eq. (5) is inferred:

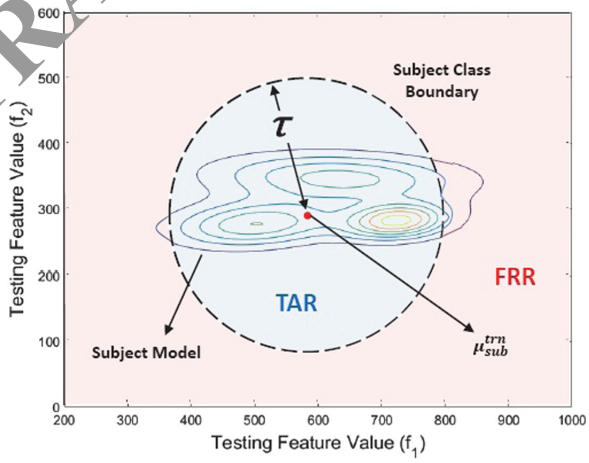


Fig. 4. Test data model for object classification

RETRACTED CHAPTER

$$\int (x|\wedge) = \sum_{i=1}^{k} w_i \varphi N\left(\frac{x_{1i}-\mu_{1i}}{\sigma_{1i}} \cdots, \frac{x_{ni}-\mu_{ni}}{\sigma_{ni}}\right) \tag{5}$$

It indicates the area infinite of hypersphere (center: μ_{sub}^{trn} and radius: τ).

2.2 Security Strength Analytics

The normal number of conjectures utilizing geometrical examination of the component space considering the classifier limits [8]. In this sense, as found in Fig. 4, the achievement likelihood of the enemy in speculating a component point inside cubi is given by Eq. (6):

$$\mathrm{P_{accept}} = \mathrm{V_{subi}}/\mathrm{V_{total}} \tag{6}$$

where V_{total} is the volume of the entire element area, and V_{subi} is the volume of the subject class c_{subi}. What's more, the aggregate ill-disposed exertion is given in Eq. (7):

$$\kappa = \log_2\left(1/\mathrm{P_{accept}}\right) \tag{7}$$

In CBC, Vsub is a n-circle around the item preparing information, with volume found in Eq. (8):

$$\mathrm{V}_n(\tau) = \frac{\pi^{n/2}}{\Gamma(n/2+1)} \mathrm{r}^n \tag{8}$$

where n is the measurement, and Γ is Euler's gamma work. For figuring V_{total}, we accept the component area is in a type of a hypercube. The focal point of the n-dimensional hypercube is situated at the mean of the entire subjects preparing information highlights. Additionally, each side of the hypercube has length equivalent to multiple times of the most extreme standard deviation of the entire preparing information among all measurements (for example 20 × max(σ1, σ2,…, σn)). This space covers almost all conceivable highlights with high likelihood (>99.99%). For assessing the exchange off among execution ands ecurity quality.

3 Experimental Results

A framework to effectively recognize as of now known weakness with the fixrecord data in double code crosswise over two working frameworks. Amid the arrangement stage, two code bases of known powerlessness works and comparing fixed capacities are examined furthermore, their numeric highlights and SimHash are put away. Whenever a new powerlessness and its relating patch are distributed, we generally can't know the detail data about them. One exceptional issue is about the dataset.

In the event that the helplessness program has an obscure weakness type, our device can't distinguish it or commit an error result. Furthermore, the arrange task stages are most certainly not enough, and we can't recognize other stages'

RETRACTED CHAPTER

vulnerabilities however they are a similar kind. In this way, in the future, we will gather greater weakness capacities and their comparing patch to our informational collection.

Table 1. The final result

$\int(x)$**.Fun**	$\int(x\|\wedge)$**.Fun**	P_{accept}	$V_n(\tau)$
sub_401177	sub_401117	Double_Free	Double_Free
sub_401013	sub_4010db	Double_Free	Double_Free
sub_4012a0	sub_4010a0	Double_Free	Double_Free
sub_400fc9	sub_4010a0	Double_Free	Double_Free

Another issue Table 1 happens when we test the machine learning classifier. The highlights extricated from the advanced extractor may have distinctive sorts to coordinate them, which implies the advanced component can't speak to the capacity very well. Later on, we will attempt more alternatives to get the highlights to decrease the scope of the potential set. At that point, amid the procedure of the parallel examination, we find that we need to apply each capacity sets with likeness over 80% to the following stage. In spite of the fact that they have a little range, regardless we need to utilize the certain vulnerability patch pair to decrease the expense of existence. In this way, in the future, we will improve the twofold examination strategy.

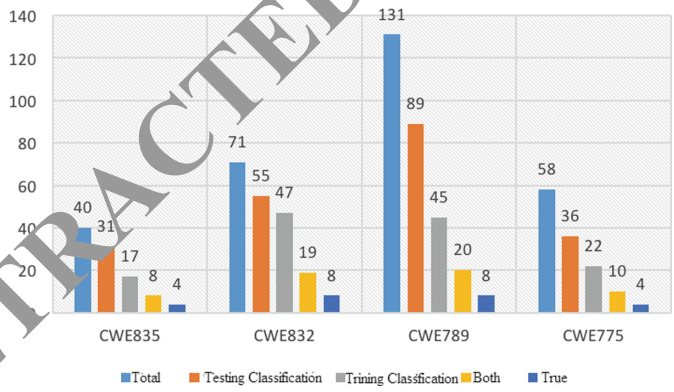


Fig. 5. The comparison between testing and training classification data set

To take with the program CWE415 and its fixed document as the info separately in the KNN classifier. At that point we can get a rundown of results that are function vulnerability sets. As Table 1defenseless program has 68 works absolutely, and the classifier returns 30 works that might be the potential weakness work. In any case, just 4 capacities have a weakness. A portion of the 30 capacities are the framework capacities, as Paccept = Vsubi/Vtotal, etc., which are clearly sheltered capacities. Additionally, there are 70 works in the fix record with 4 relating fixed capacities, be

RETRACTED CHAPTER

that as it may, 23 capacities are come back from the classifier including the same [9] framework capacities, as Paccept = Vsubi/Vtotal thuson. By watching the information, we find that there are nine framework works totally same which are Paccept = Vsubi/Vtotal etc. They take an excessive amount of vitality for us, be that as it may, they are not the helpless capacities. (i) It lessens the scope of applicant set of helpless capacities. It returns 30 and 23 potential defenseless works through the single approval. In any case, it just returns 10 potential [7] capacities by the twofold approval. It effectively disposes of the safe capacities: Paccept = Vsubi/Vtotal etc. (ii) It lessens the scope of each capacity's potential defenselessness type. Much the same as the capacity pair, sub_4010db sub_401013, which return two defenselessness type separately. In any case, through the crossing point of the outcome, it just returns one right helplessness type. The results are appeared in Fig. 5. We can see that twofold approval is superior to the single approval since it scales back the scope of competitors and decreases the bogus positive rate. The result came back from the twofold approval is nearer to the genuine circumstance.

4 Conclusion

In this paper to introduced a review of the extraordinary AI calculations used to verify and IoT. Table 1 outlines the diverse AI approaches used to verify IoT and ML. While numerous approaches result in high exactness, SVM is less mind boggling than KNN in order. There are as yet numerous difficulties in verifying IoT and ML in light of the fact that AI ought to bargain between an abnormal state of security and a low computational multifaceted nature to be appropriate for the resource limited IoT and ML gadgets. The future work to Breaking down Biometric-based Security Systems (BSS) that apply increasingly complex classifiers such as help vector machines or profound neural systems. This methodology can likewise help us to plan new sorts of highlight extraction calculations or classifiers for improving execution and security quality together.

RETRACTED CHAPTER

References

1. Esmaeili, M.M., Fatourechi, M., Ward, R.K.: A robust and fast video copy detection system using content-based finger printing. IEEE Trans. Inf. Fore. Secu. **6**, 213–226 (2011)
2. Garrido, J.M., Bustos, B.: Competitive content-based video copy detection using global descriptors. Multi. Tool. Appl. **62** (2011)
3. Ganesh Babu, R., Amudha, V.: Resource Allocation in QoS Scheduling for IEEE 802.16 Systems. Int. J. Sci. Inno. Eng. Tech., 50–55 (2016)
4. Haitsma, J., Kalke, T.: A highly robust audio fingerprinting system. In: International Symposium on Music Information Retrieval, pp. 107–115 (2012)
5. Jiang, M., Tian, Y., Huang, T.: Video copy detection using a soft cascade of multimodal features. In: IEEE International Conference on Multimedia and Expo. pp. 374–379 (2012)
6. Karthika, P., Vidhya Saraswathi, P.: A survey of content based video copy detection using big data **3**, 114–118 (2017)

7. Lei, Y., Luo, W., Wang, Y., Huang, J.: Video sequence matching based on the invariance of color correlation. IEEE Trans. Circu. Syst. Video Tech. **22**, 1332–1343 (2012)
8. Ganesh Babu, R., Amudha, V.: Dynamic spectrum access techniques in cognitive radio networks. Int. J. Emerg. Tech. Comp. Sci. **22**, 508–512 (2016)
9. Liu, L., Lu, H., Xue, X.: A segmentation and graph-based video sequence matching method for video copy detection. IEEE Trans. Knowl. Data Eng. **25**, 1706–1718 (2013)
10. Song, J., Yang, Y., Huang, Z., Shen, H.T., Hong, R.: Effective Multiple feature hashing for large scale near-duplicate video retrieval. IEEE Trans. Mult. **15**, 1997–2008 (2013)
11. Karthika, P., Vidhya Saraswathi, P.: Digital video copy detection using steganography frame based fusion techniques. In: International Conference on ISMAC in Computational Vision and Bio-Engineering, pp. 61–68 (2019)

RETRACTED CHAPTER

IDS: Signature Based Peer-to-Peer Intrusion Detection System for Novice Users

Wasim Abbas Joyo[1], Joshua Samual[1], Sangeetha Elango[1], Mohamed Ismail[1], Zainudin Johari[1], and Daniel Stephen[2(✉)]

[1] FTMS College, School of Computing Science and Engineering, Cyberjaya, Malaysia
joyowaseem@gmail.com, josaml982@gmail.com, csgeetha80@gmail.com, smileftms@gmail.com, zzj2004@gmail.com

[2] Quest Global, Techno Park, Thiruvananthapuram, Kerala, India
stephendaniel734@gmail.com

Abstract. In recent years, intrusion becomes one of the greatest problems which affect the community network. In Windows, firewall takes action on the bases of rules defined in it and there is no such software which has multi-faceted features i.e. against attacks, viruses and location tracking. This system is easy to understand and use by novice users as they cannot do the same with big Intrusion Prevention System like Snort, Suricata, etc. It is a user-friendly graphical interface system that provides all basic networks and system securities just on one click. It will provide secured environment in term of detection against intrusions in personal computers by hackers. The system is tested over Windows operating system, based on the signature method for the novice users in a community network. The system will scan the port and track the location of the attacker. If any suspicious IP is found, then those IP will be automatically blocked by the system. The system will have its own database which maintains the activity log.

Keywords: Intrusion detection · Port scanning · Location tracking · Signature-based detection · Anomaly-based detection · Intrusion prevention · Packet sniffer

1 Introduction

Network and communication technology form its advent plays a key important role in the society. The latest developments in the area of network and communication technologies have attracted billions of users that provide various connectivity's to large range of devices [1, 2]. Every single user in the society carries network services such as Social Networking, E-Mail and E- Business in their hand [3, 4]. However, on one side network and communication technology has made the life of people very flexible but on the other hand the issue related to the security in a network is a growing worry of every user [5]. Every system on a network ranging from industries to home are vulnerable to various types of attack in which intrusion is dominating security issue. CERT statistics report shows that the number of intrusion done by the intruders are rapidly growing very year

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 806–815, 2020.
https://doi.org/10.1007/978-3-030-37051-0_90

and any intrusion done on the network system causes a serious disaster on an organization [6]. To prevent such type of attack every organization practice various type of intrusion detection system (IDS) application to monitor and control the malicious activity done by the intruders who violates the network security policy [7].

In this present era the network facilities were not only limited up to the industries but it is also availed and enjoyed by the home users through community network. A very important point to note here is that the community network is also vulnerable to attack and all the home users in the society are neither a network security analyst nor ICT literate people and these users are called as novice users. Here by the term novice users mean those users who do not have any knowledge of intrusion and doesn't know how to use the IDS application. The major problem is that most of the IDS such as Suricata, Snort, N-Map and WireShark are an industrial standard system and designed to use by the network security analyst. These IDS applications are very high end application and one need to be trained and well qualified to use these IDS applications, but it is very difficult by the novice users to use this IDS applications in a community network and more over these IDS application are not users friendly.

The main objective of this research is to develop a user friendly intrusion detection system for the novice users through which they can protect their personal system from the intruders. Developing such type of system is a key challenge in this research, because here it is very important to identify what are the key features does this IDS application should need to make it more user friendly for the novice users.

Further this paper is organized in a following manner. Section 2 of this paper contains various studies which are done related to this research. Section 3 contains architecture design of the proposed work. The implementation and the results are discussed in Sect. 4. Finally, the conclusion and the future enhancement would be discussed in Sect. 5.

2 Related Studies

The first network intrusion detection system was developed in 1990 by Heberlein [8]. Intrusion detection system discovery is the way toward watching the activities in a network and breaking down them for sign of an intrusion. Intrusion detecting can be approached as anomaly detection and signature detection [9–12] In a signature based detection a predetermined attack patterns is in the form of signatures [13]. In anomaly detection techniques, it signals all anomalies as intrusions, false alarms are expected when anomalies are caused by behavioral irregularity instead of intrusions. Packet sniffing is the process of gathering traffic from a network by capturing the data as they pass and store them for later analysis [14]. Packet Sniffer especially captures the data while the communication is done between hosts for specific network [15]. A penetration test is designed to evaluate an information system's defense and discover weaknesses in the network and its resources.

There are number of open source IDS available, but these three are most popular Snort, Suricata and Bro etc., Snort-intrusion detection system perform protocol analysis, content searching, and content matching which was developed by Martin Roesh in 1998 [16]. Snort checks the packets coming against the rules written by the user and generates alerts if there are any matches found. Suricata –Network Security Monitoring

Engine can be used as IDS or as IPS. It is compatible for many operating systems like Mac, UNIX, Linux, Free BSD, and Windows. Snort use single threaded engine and the Suricata use multithreaded engine [17]. Specification of several L7 protocols on top of the L3 protocols are supported by Snort, http, ftp, tls, smb and dns in Suricata [18]. Suricata uses similar rules like Snort and is compatible. The rule structure is same for both Snort and Suricata. The difference between the two is in the keywords and protocols that can be specified.

Bro IDS focus on network security. It gives additional feature for network traffic analysis. It detects anomalies while analysing network traffic. It is primarily not rule-driven [19]. Bro is conceptually divided into an "event engine" that reduces a stream of filtered packets to a stream of higher-level network events, and an interpreter for a specialized language that is used to express a site's security policy [20]. Proposed an integrated security system were the Antivirus and the virtual private network is integrated for the home users. But this system is only implemented in windows operating system. It will not support in other operating systems like Linux, Mac [21]. Proposed a Snort based smart and swift intrusion detection system which works only a relevant or specific attack. Here supervised learning neural network is used to detect the intruders. Users are putting away their sensitive data and since they have no more control over the services or their stored information, there is need to implement strong security strategies that will prevent unauthorized access to the system functionalities and users information [22].

3 Architecture Design

The research is aimed to protect the computers from various, DoS Attack, threats launched by intruders, attacks from suspicious IP, and viruses. The function of IDS is not only to detect the interruption of the services by an attacker, but also to take preventative action. The system act as an intermediator between the Admin and the hacker as shown in Fig. 1.

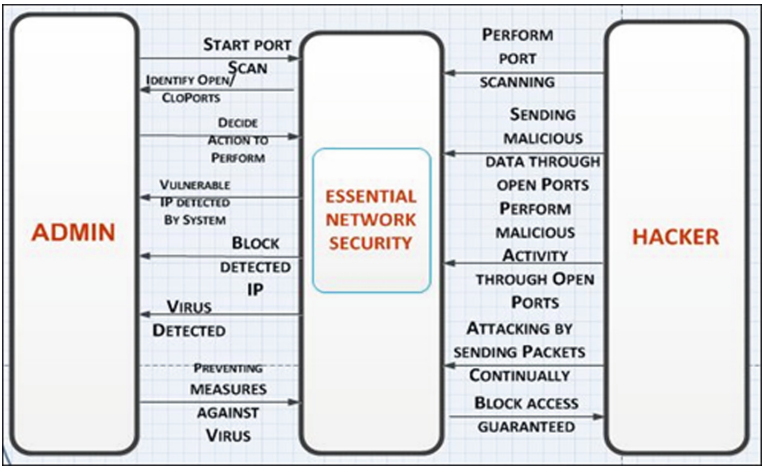


Fig. 1. System design

When the hacker sends malicious data through open ports, the IDS identify the ports, decode the action, detect the IP and take the prevention action. IDS is securing the network by analysing the network traffic as, If same IP is trying to connect to our system repeatedly will be blocked, If the format of an IP is vulnerable will be blocked and If someone is port scanning will be blocked.

The workflow of the system is detailed in Fig. 2. When the admin host the IDS, it performs port scanning, detects open and close ports and sends it to the event processor, it forwards the processed data to the event detector to check the attack signature, attack recognition will be done when the signature matches the IP with the IP's in the database and create a response towards the attacker. The system sniffs the packets and excludes the basic details of the packets, like their destination, Source and other information. If internet is not present then packets between IPv4 and router and local interfaces are sniffed. The system saved the information in the database for future use. When the suspicious IP has been detected, system perform prevention measures, in case of virus/DoS attack, prevention measures are concertina the virus, or delete the virus or block the virus.

The main features in the system are Maintain System Log, Port Scanning, Detection, and Prevention. The system has graphic interface and will provide all basic network and system security just on one click, including features like packet sniffer, packet logger and network intrusion detection system. It will not require any special training or certification due to its simple design.

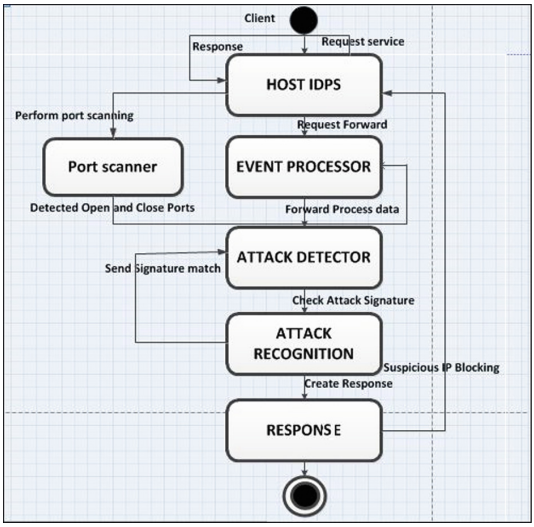


Fig. 2. Workflow diagram

4 Implementation and Results

The software requirements are Windows OS, C# visual.net and Frame work 3.5. System libraries, System.Net.Sockets, Collections, Diagnostics classes, user defined packages like, packet sniffers, port scanning, Dos Detect Algo, Resolve IP were used in building the application.

The following are the major and sub modules of the system that is used in the implementation.

Major Modules.

- Port Scanning.
- Suspicious IP Blocking
- Preventing DOS Attacks.
- Virus Protection
- Location Tracing

Sub Modules

- DNS Resolver
- Active Connections
- Active Processes
- Packet Sniffer

The main form of the system contains the functions viz., view network traffic, active connections, active services, get location, anti-virus and parental control while running the application.

4.1 Essential Packet Sniffers

This is the home page and the user can see the complete detail of incoming and outgoing packets along with time. In View Network Statistics the user can view the TCP Listener Only, Active Connections and UDP Listeners, as in Fig. 3.

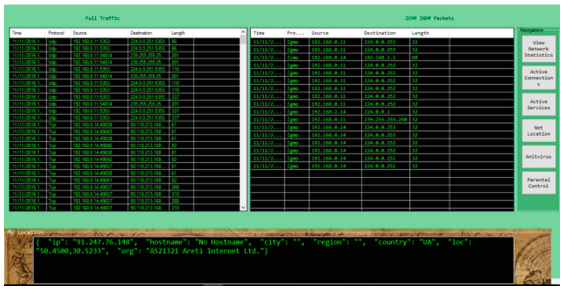


Fig. 3. Network statistics

4.2 Active Connection

When user clicked on Active Connection, the new window of TCP active connections will be open. In this new window user can see detailed view of TCP active connections included protocols, local address, remote address, states and PID's as in Fig. 4.

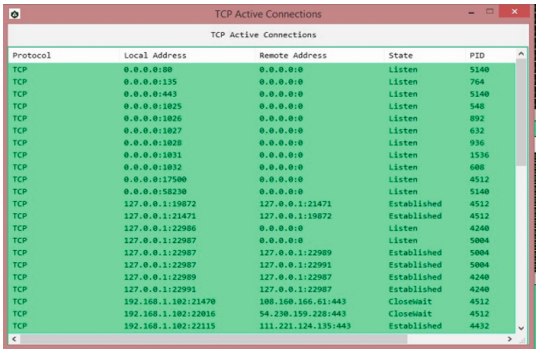


Fig. 4. Active connection

4.3 Active Services

When user click on Active Services, the new window of Active Processes will be open, it will show the ID, session ID, Process name along with start time as in Fig. 5.

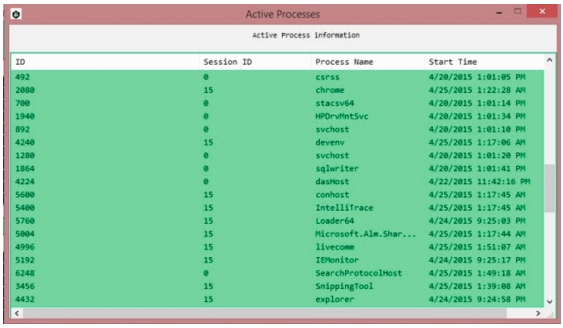


Fig. 5. Active processes

4.4 Get Location

When user enter IP address and click on find location the user can see the information of that given IP address as in Fig. 6.

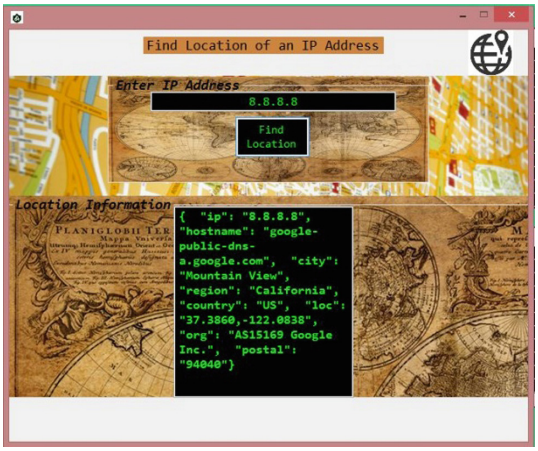


Fig. 6. Get IP location

4.5 Port Range

When user wants to check multiple ports, the user will enter the port range for checking open and closed ports. It will display all the open and closed ports as in Fig. 7.

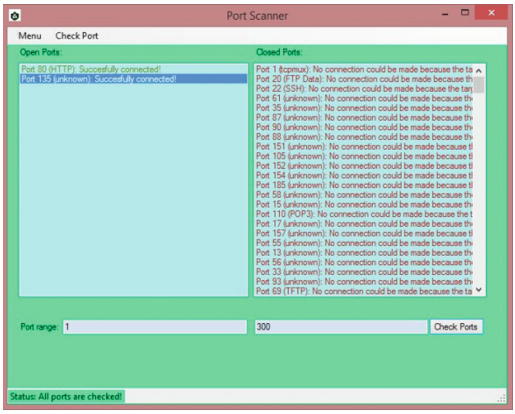


Fig. 7. Port scanner

4.6 Check Port

The user can check any individual port by entering IP address and Port number. The dialogue box will be appearing to show the complete detail about given IP and Port as in Fig. 8. Here 127.0.0.1 is the IP address used for checking.

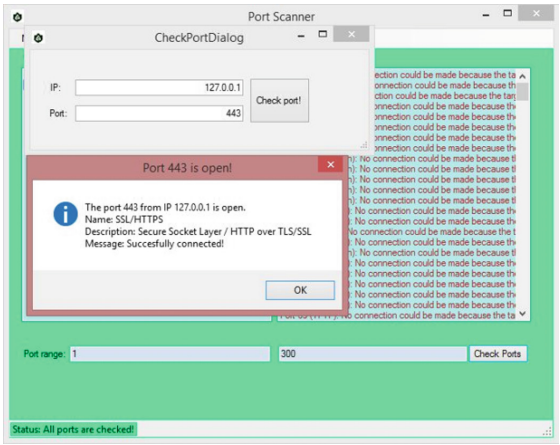


Fig. 8. Port dialogue

4.7 DNS Resolver Dialogue

By using DNS Resolver the user can get information about the external IP by entering the web address as in Fig. 9.

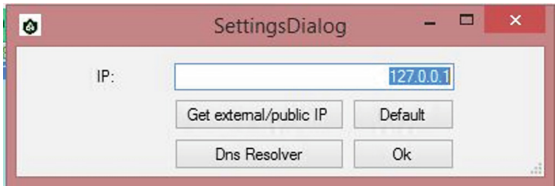


Fig. 9. Setting external IP

An Intrusion detection system was designed. The implementation and testing were done in Windows OS with C# visual.net and Frame works 3.5. The testing results clearly showed the system is a user-friendly, resolves the basic security issues of users in real time. The system received positive reviews from the user in the end user evaluation. Based on the reviews 90% of the users were satisfied with the new IDPS system. In future enhancements, Protocol analysis function will be added with the IDPS which allows users to analyze the behavior of protocols and ensure that the users are communicating with each other accordingly. It will help users to identify a range of attacks particularly DoS attacks are able to identify in terms of anomalous protocol activities.

5 Conclusions

This research was carried out in order to make novice users not to worry of intrusion and threating. The network security considers being a critical issue for the users who connect their personal computer with a community network. The intrusion may steal and/or damage the existing data and personal data irrespective of the security provided by the OS. The user friendly and interactive system was designed to detect DoS Attack, threats launched by intruders, attacks from suspicious IP, and viruses and to provide preventive action against the intrusion. The system acts intermediately between the Admin and the hacker who attempts to intrude to the system. It uses the signature based intrusion detection method which could detect the intrusion based upon certain traces. The developed system was tested for its usability and accuracy. It is found that the system functions very well in finding the intruders and taking the preventive action against them.

References

1. Penya, K.Y., Bringas, P.G.: Experiences on Designing an Integral Intrusion Detection System. In: 19th IEEE International Conference on Database and Expert Systems Application, pp. 675–679 (2018). https://doi.org/10.1109/dexa.2008.54
2. Sohi, S.M., Ganji, F., Seifert, J.P.: Recurrent neural networks for enhancement of signature-based network intrusion detection systems, pp. 1–12 (2018)
3. Chibuzor, J.U., Bennet, E.O.: An intrusion detection systems using machine learning algorithm. Int. J. Comput. Sci. Math. Theory **4**(1), 39–47 (2018). ISSN: 2545-5699
4. Syed Ali, R.S., Issac, B.: Performance comparison of intrusion detection systems and application of machine learning to snort system. Future Generation Computer Systems (2018). DOI: 10.1016
5. Huaqing, L., Zheng, Y., Chen, Y., Lifang, Z.: A survey on network security-related data collection technologies, special section on internet of things big datatrust management. In: IEEE Access, vol. 6, pp. 18345–18365 (2018). ISSN: 2169- 3536
6. Hung–Jen, L., Chun-Hung, R.L., Ying-Chih, L., Kuang–Yuan, T.: Intrusion detection system: a comprehensive review. J. Netw. Comput. Appl. 6–24 (2013). Elsevier, ISSN: 1084-8045, DOI: 10.1016
7. Theobald De. R.: Design, development and implementation of a network intrusion detection tool for air traffic management systems. In: 48th Annual IEEE/IFIP International Conference on Dependable Systems and Network Workshops, pp. 2325–6664 (2018). DOI: 10.1109, pp. 96–99
8. Ghafir, I., Prenosil, V., Svoboda, J., Hammoudeh, M.: A survey on network security monitoring systems. In: IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, 2016, pp. 77–82 (2016). https://doi.org/10.1109/w-ficloud.2016.30
9. Shijoe, J., Malathi, D., Bharath, R., Dorathi, J.: A survey on anomaly based host intrusion detection systems. In: National Conference on Mathematical Techniques and its Applications, pp. 1–10 (2018). DOI: 10. 1088
10. Nabeela, A., Waqar, A., Rehan, A.: A comparative study of data mining algorithms for high detection rate in intrusion detection systems. Ann. Emerg. Technol. Comput. **2**(1), 49–57 (2018). DOI: 10.331661

11. Vinod, K., Om Prakash, S.: Signature based intrusion detection system using SNORT. Int. J. Comput. Appl. Inf. Technol. **I**(III), 2012. ISSN: 2278-7720
12. Deepak, K.S., Jitendra, K.G.: An approach for anomaly based intrusion detection system using SNORT. Int. J. Sci. Eng. Res. **4**(9), (2013). ISSN: 2229-5518
13. Shadi, A., Monther, A., Muneer, B.Y.: Anomaly-based intrusion detection systems through feature selection analysis and building hybrid efficient model. J. Comput. Sci. 1–9 (2017). Elsevier, ISSN: 1877-7503, DOI: 10.1016
14. Krutz, R.L., Vines, R.D. The CEH™ prep guide: the comprehensive guide to certified ethical hacking. Wiley Publishing (2007)
15. Tabu, S.K., Leonard, J.M.: Penetration testing with banner grabbers and packet sniffers. J. Emerg. Trends Comput. Inf. Sci. **5**(4) (2014). ISSN: 2079-8407
16. Rishabh, G., Soumya, S., Shubham, V., Swasti, S.: Intrusion detection system using SNORT. Int. Res. J. Eng. Technol. (IRJET). e-ISSN: 2395 -0056
17. Suricata rules. https://redmine.openinfosecfoundation.org/projects/suricata/wiki/SuricataRules. Accessed 12 Jan 2019
18. Ghafir, I., Prenosil, V., Svoboda, J., Hammoudeh, M.: A survey on network security monitoring systems. In: IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, pp. 77–82 (2016). https://doi.org/10.1109/w-ficloud.2016.30
19. Paxson, V.: Bro: a system for detecting network intruders in real-time. Comput. Netw. **31** (23), 2435–2463 (1999)
20. Syed, S.A.N., Joshua, S.: Integration of antivirus with virtual private network for personal systems security. Int. J. Inf. Syst. Eng. **5**(2), 1–12 (2017). ISSN: 2289-7615, DOI: 10.24924
21. Rashidah, F.O., Islam Khan, B.U., Athaur Rahman, N., Ku Nor, A.K.Z., Sabahat, H.: Snort-based smart and swift intrusion detection system. Indian J. Sci. Technol. **11**(4), 1–9 (2018). ISSN: 0974-5645, DOI: 10. 17485
22. Ismail, M., Badamasi, Y.: Ensuring data storage security in cloud computing with advanced encryption standard (AES) and authentication scheme (AS). Int. J. Inf. Syst. Eng. **4**(1) (2016). https://doi.org/10.24924/ijise/2016.11/v4.iss1/18.39, ISSN: 2289-7615

Data Security Using Extended ECS (Encryption, Compression, Steganography)

Surbhi Verma(✉), Gagandeep Kaur, and Deepak Garg

National Institute of Technology, Kurukshetra, Haryana, India
surbhil996verma@gmail.com,
gagandeepkaurl895@gmail.com, erdeepakgarg2l@gmail.com

Abstract. In today's scenario where everything is internet based, data security is on high demand. Data is considered as a crucial asset and is required to be protected. Data Security includes data confidentiality, integrity, authenticity and much more. Despite of several approaches to data security such as encryption, compression, steganography, data is still prone to potential security threats. The major reason identified is the shortcomings of these individual techniques when certain factors are taken into account. Cryptography ensures security but it comes at cost in terms of time and space. Compression techniques encrypts data and saves disk space but these compressed files can easily be uncompressed by attackers. Steganography a technique which hides data instead of encrypting it also has its merits and demerits. In this paper, approaches for data security (Encryption, Compression, Steganography) and their potential advantages and disadvantages are studied in detail. A comparison of these approaches has been generated successfully and a hybrid approach is proposed named as Extended ECS (Encryption, Compression, and Steganography) by taking selected sub approaches only with aims to overcome the flaws of existing approaches keeping high data security and low complexity as aims in mind.

Keywords: Data security · Cryptography · Compression · Steganography · Encryption · Decryption

1 Introduction

Data security is the act of protecting data from uncertified access. Any type of information transferred over the internet has a possibility of being misused. Hence various techniques such as cryptography, compression, steganography is used to safeguard data from threat while sharing it over Internet [1–3]. Cryptography is a technique that make use of mathematics for data security. It works by jumbling plaintext into ciphertext, then back again. To encrypt data, two keys either symmetric (encryption and decryption is done using same key) and asymmetric (encryption and decryption is done using public and private key respectively) key algorithms [1, 3]. Steganography is a method that conceals the message in a way it cannot be seen by a unauthorized person. It hides the fact that a secret message is being transmitted [2] Compression is a method that reduces the number of bits occupied. It works by eliminating redundancy in data. It

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 816–826, 2020.
https://doi.org/10.1007/978-3-030-37051-0_91

ensures lesser storage, minimum cost and requires less amount of time to transfer a file over network [1].

1.1 Our Contribution

Several studies showed that Compression, Encryption, Steganography provides Data security from unauthorized access but these techniques can be compromised as none alone is perfect [1, 2]. These data security approaches have been compared on their merits and demerits in subsequent sections. We proposed a hybrid approach named as Extended ECS (Encryption, Compression, and Steganography) which aims to overcome the flaws of existing approaches.

1.2 Organization

Following paper is sectioned as—Sect. 2 describes Cryptography including its goals, security attacks, classification, Symmetric-Asymmetric comparison, Asymmetric sub approaches comparison, hashing techniques. Section 3 describes Compression, its goals, classifications & comparison of few approaches under it. Section 4 describes Steganography its goals, attacks, & comparison of few approaches under it. In Sect. 5 we successfully proposed certain hybrid methods using Extended ECS (Encryption, Compression, Steganography) on the basis of comparisons done in Sects. 2, 3 and 4. Finally Sect. 6 concludes & discusses future scope of the proposed work.

2 Cryptography

While dealing with data security, Cryptography has a significant role to play. 'Crypto' signifies something that is hidden. It is the examination and utilization of methods for secure correspondence within the sight of unapproved parties. It deals with developing and analysing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security [1, 3].

2.1 Goals

Access Control, Authentication, Confidentiality, Integrity, Non-Repudiation.

2.2 Security Attacks

Cipher text-only attack, Known-plaintext attack, Chosen-plaintext attack, Chosen-cipher text attack, Chosen-text attack, Brute-force attack.

2.3 Classification and Comparison

Cryptography is classified as "Symmetric key cryptography", "Asymmetric key cryptography" and "hash functions".

2.4 Symmetric Key Ciphers

It uses one single key often called secret key for both encryption and decryption algorithms [3] (Fig. 1).

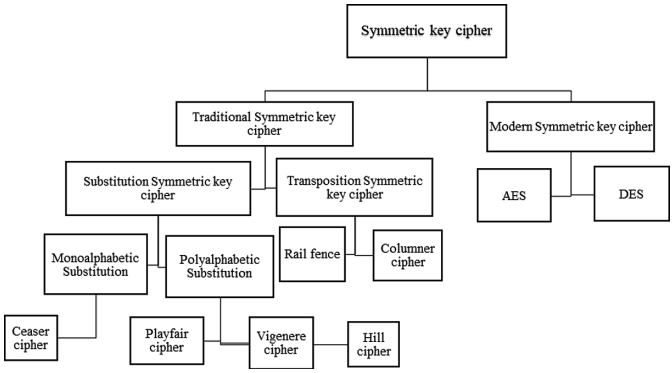


Fig. 1. Classification of symmetric key cipher

2.5 Asymmetric Key Ciphers & Comparisons

It involves usage of public key and private key for encryption and decryption algorithms. From Table 1, it can be inferred that Asymmetric key cipher performs better over Symmetric key ciphers as far as security of data is concerned. Below is a comparison among various Asymmetric ciphers [3] (Table 2).

2.6 Hashing Functions & Comparison

in this technique, plain-text is converted it to a hash value of fixed size using a hash function. This process ensures integrity of the message as the hash value on both, sender's and receiver's side should match if the message is unaltered [3] (Table 3).

Following table generates a comparison among all the three techniques of Cryptography mentioned above (Table 4).

3 Compression

It is a way of reducing the size of original data by using certain encoding techniques which in turns saves storage capacity, transfer of file speed up and reduces the cost for storage hardware and network bandwidth [8].

3.1 Goals

Reduce the file and save disk space [9].

Table 1. Symmetric versus asymmetric key ciphers

Features	Symmetric key	Asymmetric key
Numbers of keys	a single key is required to be shared	a pair of public keys and a private key is used
Security	Same key is shared hence is prone to data threat	Eliminates the need of key sharing due to the concept of public private keys
Time complexity	It takes less time for execution as only single key is used	Use of separate keys for operations makes it a time-consuming process
Lack of delay in Execution	both the operations can be carried out pretty quickly due to its simplistic nature	Since both the operations are done by two separate keys, it makes it a slow procedure
Need of keys	here, we have n (n − 1)/2 keys. This is O (n^2) keys	for n users, we have 2(n) keys, which is O(n) keys
Specific key features	1 randomly generated k-bit strings 2 Simple to generate 3 have no special properties	1 have special structure (e.g., are large primes) 2 are expensive to generate
Length of key	Execution is faster due to small length of key	Key length can be up to 1024 bits hence process of encryption-decryption is slower

Table 2. RSA versus ECC versus ELGAMAL [4]

Features	RSA	ECC	ELGAMAL
Security	Based on difficulty of factoring large integers	Based on theory of elliptic functions	based on difficulty of computing discrete logarithms
Base	Large prime number	Elliptic functions	Logarithmic functions
Encryption (ms) keysize-256	37	7098	8242
Decryption (ms) keysize-256	37	37	3932
Key generation time for key-size 256	1957	895	6451

3.2 Classification & Comparisons

From the above points we conclude that Lossless data compression technique is better so we further use it in our study (Tables 5 and 6).

Table 3. MD5 versus SHA1

Features	MD5	SHA 1
Output length	128 bits	160 bits
Required attempts to try and find two messages providing the same output value	264 operations (4 rounds * 16 steps)	2^{80} operations (4 rounds * 20 steps)
Required attempts to try and find original message corresponding to output	2^{128} operations	2^{160} operations
Speed	Faster	Slower
Chain variables	4 (a-d)	5 (a-e)
Mathematical expression in each round	a = b + ((a + Process p (b, c, d) +M[i] +T[k]) <<< s), b = b, c = c d = d	a = (e + Process P +S5 (a) + W [t] + K[t]), b = a, c = s 30 (b), d = c, e = d
Attacks	Collision attack	SHAttered attack

Table 4. Comparison & conclusion on cryptography

Features	Hashing function	Symmetric	Asymmetric
Required No. of keys	0	1	2
Approved key length by NIST	256 bits	128 bits	2048 bits
Often used	SHA	AES	RSA
Key sharing	N/A	Pose problems	Secured and easy
Effect of key compromise	N/A	Sender and receiver both bears lose	Loss is only for owner of asymmetric key
Speed	Fast	Fast	Slow
Complexity	Medium	Medium	High
Examples	Sha 224, Sha 256,	AES, DES	RSA, Elgamal, ECC

Table 5. Lossy versus lossless

Lossy	Lossless
Reconstruction of an approximation of the original data	Whole of the data is retrieved.
Quality id degraded	Quality remains the same
Used for audio, video	Used for text, audio, video, image

Table 6. Comparison of compression techniques

	Run length	Huffman	LZW
Input	Variable	Fixed	Variable
Output	Fixed	Variable	Fixed
Speed	Fast to execute	Fast to execute	Fast compression
Drawbacks	Can't achieve high compression ratio	Interpreting is troublesome because of various code lengths [10]	The executives of string table is troublesome
Time Complexity	O(n)	O(n(log n)	O(n)
Space complexity	0(2n)	O(k) for the tree and O(n) for the decoded text	O(n)
Decoding (Input)	No information required	Required	No prior information
Cost	Complicates decoding process so increases time cost	Extra cost of transmitting the encoding tree	Low time cost Cost of transmission is less as table is not passed
Applications	TIFF, PDF, BMP	GIF, ARJ, JPEG, MPEG	TIFF, GIF, PDF

4 Steganography

Stenography is a technique which is used in communication which allows hiding the secret data within any cover media. In this a sender some information by encoding it into some other media. The media used to hide data can be audio, video, text or any image. Message is embedded in cover media using any algorithm and a "stego" file and send it along the communication channel [11] (Fig. 2).

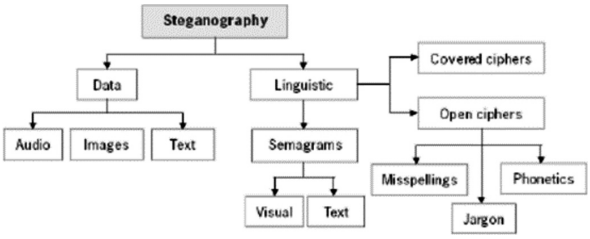


Fig. 2. Steganography

4.1 Goals

The objective is to adjust the transporter in a subtle way just, with the goal that it uncovers nothing—neither the installing of a message nor the implanted message itself [12] (Table 7).

Table 7. Comparison of steganographic methods

	Audio	Images	Text
Cover media	Audio	Image	Text
More prone to attacks	Least	Less	Most
Difficult	Most difficult in hiding data in audio	Less	Least
Main feature	The message is embedded into cover audio file as "noise" at frequency which is out of hearing range	Computerized picture are the most famous spread media because of their high level of repetition	The content steganography is a strategy for utilizing composed common language to cover a mystery message
Applications	Skype, Phone Calls	TCP/IP packets	SMS texting, CSS, emails
Undetectability	Poor [13]	Very large [14]	very small [15]
Bit rate	Medium [13]	Good [14]	Poor [15]
Resistance to modification	Weak [13]	Very good [14]	Average [15]

5 Proposed Work

After studying cryptography, compression and steganography techniques in detail, we came to a conclusion that none alone is perfect. After comparing cryptography techniques in Sect. 2, we concluded that RSA performs exceptionally well in asymmetric encryption cipher and also it can be blended with symmetric key ciphers (Playfair and Columnar) to generate a system which ensures data security in minimal time and space complexity. From Sects. 3 and 4 we concluded that compression techniques help in compressing redundant bits of data and steganography helps in hiding data in any media form, hence steganography and compression techniques can also form a secure hybrid system. So, we applied encryption approaches (identified in Sect. 2), then steganography approaches (identified in Sect. 4) and compression approaches (identified in Sect. 3) in series to encrypt a plain text for providing high level data security depicted in Fig. 3. On the basis of this we demonstrated few examples that can be used for securing data using the above-mentioned techniques in combination of one another along with their algorithms.

Fig. 3. Proposed extended ECS (Extended Compression Steganography)

5.1 Example 1

This method is a blend of Symmetric (Playfair and columnar ciphers) and Asymmetric (RSA) ciphers. Since Symmetric cipher suffers from key sharing issue, this is eliminated by blending it with a Asymmetric cipher technique.

Step 1: Encryption

1.1. Generate a 5*5 matrix utilizing given keyword. Fill rest of entries in the matrix using remaining alphabets avoiding duplicates.
1.2. Encrypt the plaintext using generated matrix according to the rules of the Playfair cipher.

Example: Keyword: tutorial

Table 1

3	1	2
V	E	Z
R	F	K
B	N	

Table 2

T	U	O	R	I/J
A	L	B	C	D
E	F	G	H	K
M	N	P	Q	S
V	W	X	Y	Z

Plaintext: MA YI HE LP Ciphertext: VE ZR FK BN

1.3. The ciphertext so obtained will be fed to the columnar cipher as plaintext.

Order: 3 1 2 Ciphertext: EFNVRBZK (Table 2)

1.4. The text now obtained will be the plaintext which will be finally encrypted with the public key of RSA.

Let's assume two prime number are: p = 5 and q = 7, n = p*q = 35, e = 3 (as $1 < e < n$)
Hence public key:(n, e) = (35,3) Ciphertext = $(\text{plaintext})^e \bmod n$
Plaintext: EFNVRBZK Ciphertext: TFNHVHFA

Step 2: Hide the so obtained cipher text using Image Steganography.
Step 3: Apply any of the Compression techniques (RLE/LZW) to reduce the redundant bits and hence obtaining a compressed file.

5.2 Example 2

In this method, Cryptographic technique (2 round columnar cipher) is merged with image steganography and compression (Run length encoding) in series to build a hybrid system which aims to overcome the spatial flaw of cryptography and at the same time ensures data security.

Step 1 The plaintext is fed to columnar cipher and the ciphertext is read column wise in round 1

Plaintext: How are you now Ciphertext: weuw____oroohayn (Table 1) Order: 4 3 1 2

Table 1

4	3	1	2
H	O	W	_
A	R	E	_
Y	O	U	_
N	O	W	_

Table 2

2	1	3	4
W	E	U	W
_	_	_	_
O	R	O	O
H	A	Y	N

1.2. The ciphertext obtained acts as plaintext for columnar cipher for round 2.

Plaintext: weuw____oroohayn Order: 2 1 3 4 Ciphertext: E_RAW_-OHU_OYW_ON (Table 2).

Step2: Steganography (Encrypt above ciphertext into below image) (Fig. 4).

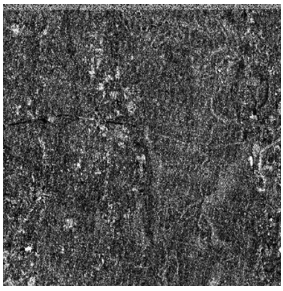


Fig. 4. Image with hidden text

Step 3. Now apply run length encoding on this image on the basis of similarity of pixels.

6 Conclusion & Future Scope

Seeing the growing threats to data, the techniques such as cryptography, steganography, compression and many more existing can't handle attacks single headedly [8]. Encryption though in a secret form can't be just seen and predicted but can be breached by cryptanalyst. Steganography hides information behind a cover file but if its bypassed then it serves whole of the information at one go in its original form. Compression encodes the message but it arises suspicion and hence can be decompressed to get the

information. So, the combined form of above techniques with selective good sub approaches can be used to safeguard the data keeping high data security and low complexity as aims in minds. This paper provides a review of some common algorithms and schemes that combine two or all three of these techniques including good sub approaches under it which will be used. For example hybridization of RSA (as asymmetric approach), Columnar or Playfair (as symmetric approach), Image steganography & Run Length Encoding or LZW (as compression) is good combination for providing high data security and low complexity. Future work may envelop diverse blends and study of Cryptography (Modern and classical) or Cryptography and steganography or Cryptography joined with steganography and from that point being packed to help security and drop down the existence complexity.

References

1. Izhar, S.: Enhancement in data security using cryptography and compression. In: International Conference on Communication Systems and Network Technologies, pp. 212–215 (2017)
2. Menon, N.: A Survey on Image Steganography IEEE International Conference on Technological Advancements in Power and Energy (TAP Energy) (2017)
3. Rajani, T.: Importance of cryptography in network security. In: International Conference on Communication Systems and Network Technologies (2013), pp. 462–467 (2013)
4. Agoyi, M.: Sms security: an asymmetric encryption approach. In: Sixth International Conference on Wireless and Mobile Communications, pp. 448–452(2010)
5. Gaba, J., Sharma, M.K.: A Review based study of hybrid security schemes based on compression, encryption and steganography. Int. J. Eng. Trends Technol. **4**(7), 3243–3246 (2013)
6. Ibrahim, A.M.A., Mustafa, M.E.: Comparison between (RLE And Huffman) algorithms for lossless data compression. Int. J. Innov. Technol. Res. **3**(1), 1808–1812 (2015)
7. Maan, A.J.: Analysis and comparison of algorithms for lossless data compression. Int. J. Inf. Comput. Technol. **3**(3), 139–146 (2013)
8. SearchStorage.: What is data compression?—Definition from WhatIs.com. https://searchstorage.techtarget.com/definition/compression (2019). Accessed 25 Mar 2019
9. Anon: https://www.researchgate.net/publication/273011398_A_Secure_Data_Communication_System_Using_Cryptogaphy_And_Steganography (2019). Accessed 24 Mar 2019
10. En.wikipedia.org.: Decoding_methods. https://en.wikipedia.org/wiki/Decoding_methods (2019). Accessed 25 Mar 2019
11. En.wikipedia.org.: Steganography. https://en.wikipedia.org/wiki/Steganography (2019). Accessed 25 Mar 2019
12. Workshops, C., Hiding, I., Pfitzmann, A., Information Hiding, P., Science, L., Mittelholzer, T., Watermarking., A., Shin, N., Steganography., O., Franz, E., Pfitzmann, A., Cover-Stego-Attacks., S., Fridrich, J., Du, R., Images., S., Westfeld, A., Pfitzmann, A., Systems., A., Smith, J., Dodge, C., Steganography., D., Furon, T., Duhamel, P., Technique., A., Craver, S., Detection., Z., Adelsbach, A., Pfitzmann, B., Sadeghi, A., Content., P., Guth, H., Pfitzmann, B., Data, E.: dblp: 3. Information Hiding 1999: Dresden, Germany. Dblp.uni-trier.de. https://dblp.uni-trier.de/db/conf/ih/ih99 (2019). Accessed 25 Mar 2019

13. En.wikibooks.org.: Steganography/Covers—Wikibooks, open books for an open world. https://en.wikibooks.org/wiki/Steganography/Covers#Audio (2019). Accessed 25 Mar 2019
14. En.wikibooks.org.: Steganography/Covers—Wikibooks, open books for an open world. https://en.wikibooks.org/wiki/Steganography/Covers#Photos (2019). Accessed 25 Mar 2019
15. En.wikibooks.org.: Steganography/Covers—Wikibooks, open books for an open world. https://en.wikibooks.org/wiki/Steganography/Covers#Text (2019). Accessed 25 Mar 2019

Dual-Band Graphene Based Planar Antenna for WLAN Communication Applications

Ronak Vashi[1(✉)], Trushit Upadhyaya[2(✉)], Arpan Desai[2], and Riki Patel[2]

[1] Birla Vishwakarma Mahavidyalaya, V.V.Nagar, Gujarat, India
ronak.vashi@bvmengineering.ac.in
[2] Charotar University of Science and Technology, Changa, Gujarat, India

Abstract. Graphene-based antennas are artistic concept for wireless communications. In this paper, a Dual Band antenna using Graphene and FR4 is proposed. Graphene is used a patch and ground plane whereas FR4 is used as a substrate material. The graphene antenna is evaluated in terms of return loss, radiation pattern and current distribution. The radiation pattern of Graphene antenna shows omnidirectional pattern with no null. The simulated impedance bandwidth of the graphene-based antenna is 5.06% (2.43–2.30 GHz) and 3.80% (5.52–5.12 GHz), which makes the antenna suitable for Dual-Band Wireless Local Area Network (WLAN)/WiMAX communication.

Keywords: Dual band · Flexible · Graphene antenna · WLAN

1 Introduction

In the new era of wireless communication; the demand for small size, robust, efficient and flexible antenna working in the range of wireless local area network (WLAN) is increasing. Due to impressive properties like electrical and thermal conductivity, strength, stiffness, and toughness enable a whole new diversity in the applications. This is one of the prime reasons Graphene-based antennas are the qualifying technology for a wireless communications system. As Graphene is a two-dimensional (2D) honeycomb lattice with monolayer crystal carbon atomic structure. Graphene material provides 15 to 20 times more mechanical strength and 5 times lighter than copper. Graphene is also zero band gap semiconductor material as the electric field is applied to this material electron and holes carriers emerged, which allows the control of conductivity and surface resistance, and controlled by doping and electric field biasing method [1]. Graphene, Young's Modules (E) (Tensile Elastic Capacity) in the range of 1000GPa, and copper have only 110–130 GPa. With this Graphene have moderately low resistance approx. 35 to 50 Ω/sq, 80–90% optical transparency, carrier density of 2to 6 × 1011 holes per sheet and a mobility of 200 to 1900 cm2/V-s [2]. Aeronautics & Automotive industries are already shifted metal to Carbon based materials due to its lighter structure, high durability, and energy-harvesting properties. These will push the Graphene to "Metal Replacement" goal in the wireless field. However, high electrical conductivity is required; metals are still preferred to Carbon base material.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 827–833, 2020.
https://doi.org/10.1007/978-3-030-37051-0_92

This deficiency can be overcome by upgrading plastics with conductive fillers such as carbon black and graphite fibres.

Scida et al. presented wearable and highly flexible antenna using Graphene Paper structure for NFC communication and RFID tags for the frequency of ISM band 13.56 MHz [3]. Metallic heavy material structure deformation with repetitive bending occurred, production costs and disposal issues also tried to overcome. Graphene based antenna for 2.67–2.92 THz with a different substrate of Si3N4, Al2O3, BN, Silica, and Quartz was performed and achieved higher bandwidth and radiation efficiency to other conventional substrate material, Rajni Bala et al. [4] Optically transparent antenna with multi walled carbon Nano tube (MWCNT) in terahertz frequency range with (> 2 dB) high gain and (7.56 dB) directivity was achieved by A. Thampy et al. [5] in wearable wireless communication systems, the transmission line is also prime structure to carry signal in electronic devices, and it should be highly flexible needed was performed by printed graphene material in the frequency range of 1.97 GHz by Huang et al. [6]. A reconfigurable antenna made from hybrid Metal- Graphene structure performance analysis was presented by Alvarez et al. [7] Recent development of Graphene conductive ink has brought the possibility along with its superiority in a high conductivity, mechanical flexibility, and lightweight with low cost can extract from the carbon granules [8, 9]. A smart way to construct conductive patterns on rigid or flexible substrates is by the printing of conductive ink solutions; conductive adhesive ink can be manufactured with low cost and can be suitable for Graphene grow on a dielectric substrate. With this method, average conductivity can be obtained with reducing electrical resistivity surface [10]. Graphene based antennas falls into the category of transparent antenna where many researchers have proposed dual band [11], wideband antennas using metametrials, array structures for WLAN, 5G and MIMO applications [12–18]. Other graphene based antennas working in dual band for terahertz frequencies and satellite frequencies are also proposed by researchers [19]. Size of this kind of antennas can be reduced if we use the concept of electrically small antennas [20] and metamaterials antennas [21, 22].

In this paper, a Dual Band antenna is proposed using Graphene as a conductive material with etching out copper from FR4 substrate for designing and performance analysis. Sections 2 has characterized the proposed antenna designs and the system setup parameter. In Sect. 3 simulation results are presented and discussed. In the end, Sect. 4 is the conclusion.

2 Proposed Antenna Design

A Graphene based dual-band antenna using FR4 is proposed. Antenna is composed of a Graphene paper as patch and Ground plane, with total dimensions L × W × H is 38.5 mm × 33 mm × 1.45 mm and its suspended on a FR4 dielectric substrate having parameters, h = 1.4 mm, ε_r = 4.4 and tan δ = 0.02.

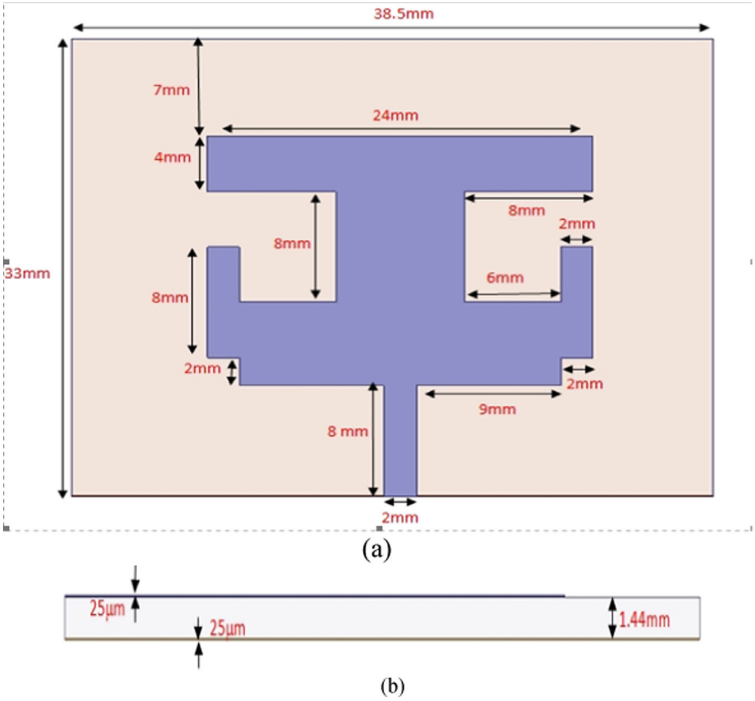


Fig. 1. Proposed antenna **a** top view, **b** side view

Table 1. Design parameters of proposed antenna

Antenna	Dimension	Value
Patch length	Lp × Wp × hp	24 mm × 18 mm × 25 µm
Dielectric substrate length, width and thickness	$L_s \times W_s \times hs$	38.5 mm × 33 mm × 1.4 mm
Dielectric constant (FR4)	ε_r	4.4
Microstrip line length and width	$L_l \times W_l$	8 mm × 2 mm

Graphene antenna inquire into simulation to evaluate the performance using Table 2. Due to skin depth effect, thickness of the Graphene sheet is major concern in the terms of performance. For that in this simulation 25 µm of Patch and Ground plane has taken as a reference to simulate and optimise the design on Ansys HFSS 17.0 full electromagnetic solver on FEM method software is used for numerical modeling of the designed antenna at operating frequency range of 1 to 6 GHz.

Table 2. Graphene sheet electrical and mechanical properties [2]

Parameters	**Value**	**Unit**
Carbon content	97%	–
Thickness	25	μm
Density	1.98	g/cm^3
Electrical conductivity	3.70×10^5	S/m
Thermal conductivity	1300–1500 (x–y plane) 13–15 (z plane)	W/(m) × (k)
Tensile strength	30	MPa
Sheet resistance	2.88×10^{-2}	ohm/sq

3 Results and Discussion

In this paper, a challenge has been made to examine the effect of patch and ground base material on the performance with the microstrip feed line antenna. From the Fig. 2, calculate the B.W. of resonance antenna of $|S_{11}|$ plot; consider return loss more than −10 db. Result shows the B.W. of an antenna is 5.06% (2.43–2.30 GHz) and 3.80% (5.52–5.12 GHz).

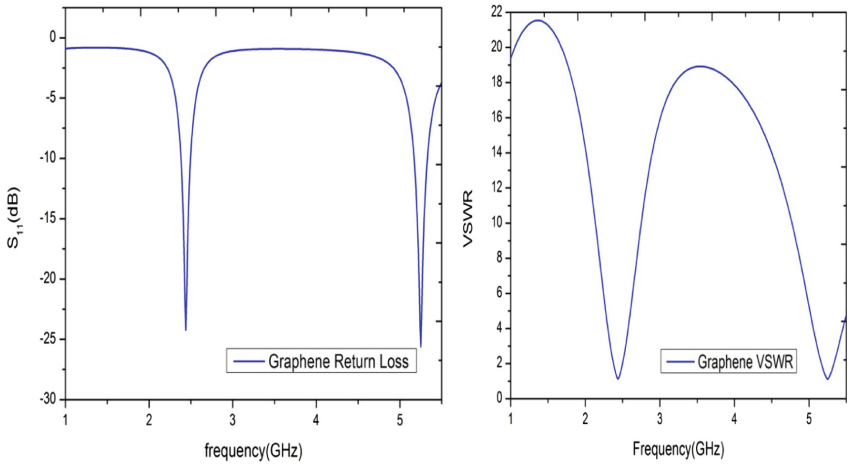


Fig. 2. Simulated S_{11}(dB) and VSWR for Graphene antenna

A VSWR with the ideal value of 1.0 means that there is no power being reflected to the source. At a VSWR of 2.0, approximately 10% of the power is reflected to the source. High VSWR value create problem of power wasted, and the reflected power can cause problems such as heating antenna or connector to the cable. Figure 3 shows that Graphene antenna VSWR with the value of 1.03 at 2.41 GHz and 1.12 at

5.45 GHz, which enhanced the performance of an antenna in terms of Gain and radiation efficiency (Table 3).

Table 3. Performance parameters of Graphene based antenna

Frequency	Return loss (dB)	Impedance bandwidth (%)	VSWR	Gain (dBi) E-field	H-field
2.41 GHz	−24.25	3.04	1.03	1.39	2.41
5.45 GHz	−25.62	4.92	1.12	2.59	1.57

As shown in Fig. 3(a), surface current is uniformly distributed at middle of I section antenna at lower frequency 2.41 GHz, so patch is well matched and radiates at this frequency. As shown in Fig. 3(b), at higher frequency 5.45 GHz current is concentrated on the lower edge of radiator which means that the antenna affects impedance characteristics at higher frequencies.

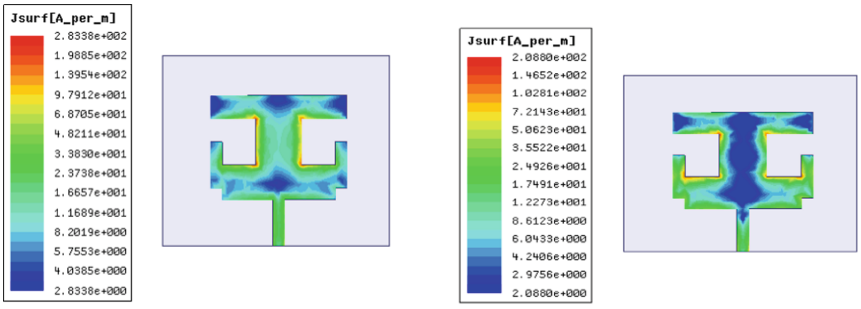
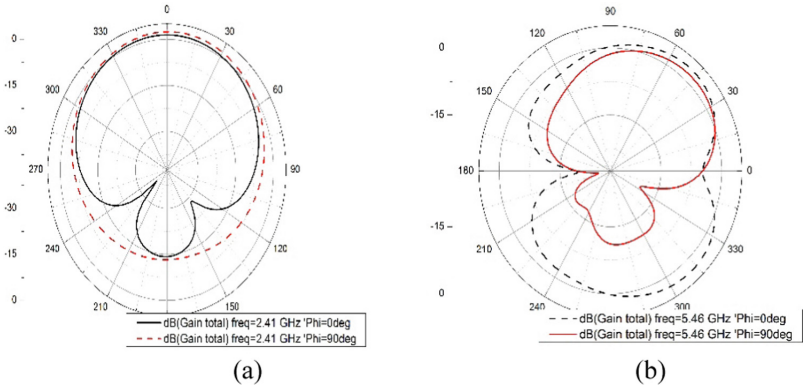


Fig. 3. Current Distribution of Graphene antenna for **a** 2.44 GHz **b** 5.45 GHz

The radiation pattern of the proposed antenna is shown in Fig. 4. We can see that the simulated radiation patterns are approximately in a good agreement. The radiation pattern exhibit two peaks along the ±z axis at resonance frequencies of both 2.41 GHz at 0° E-field and H-field gain is 1.39 dBi and 2.41dBi respectively. While 5.45 GHz at 45°° E-field and H-field gain is 2.59 dBi and 1.57 dBi respectively.



(a) (b)

Fig. 4. Radiation patterns of graphene antenna with E-plane & H-plane for **a** 2.41 GHz **b** 5.45 GHz

To validate the advantages of Graphene antenna over the conventional patch antenna, the antenna designed using FR4 substrate. Due to lower conductivity of Graphene material to copper and high relatively permittivity, which is depend on the height of substrate are the prime reasons to get low value of Gain and radiation efficiency, but it can be overcome with the help of material science research and modern fabrication technology.

4 Conclusion

The accomplished results confirm that a Graphene-based patch antenna resonates in the Network (WLAN)/WiMAX band, consistently with the conventional model. The bandwidth of a proposed antenna is achieved 3.04% for 2.41 GHz and 4.92% for 5.45 GHz band with high return-loss to the conventional antenna; with consistent of VSWR value near to one with good gain at 2.41 and 5.45 GHz.

Graphene is made up a mono carbon lattice structure, available in very thin layer and it can be utilized on a flexible substrate. Wearable and Transparent miniaturized gadgets are the future of electronic wireless system; and proposed antenna described in this work is a pioneer step towards this goal.

References

1. Geim, A.K., Novoselov, K.S.: The rise of graphene-nature materials. Nat. Mater. **6**, 183–191 (2007)
2. Bunch, J.S.: Mechanical and electrical properties of graphene sheets, Ph.D. dissertation, Cornell University, (2008)
3. Scida, A., Haque, S., Treossi, E., Smerzi, S., Ravesi, S., Borini, S., Palermo, V.: Application of graphene based flexible antennas in consumer electronic devices. Mater. Today **21**(3) (2018)

4. Bala, Rajni, Marwaha, Anupma: Investigation of graphene based miniaturized terahertz antenna for novel substrate materials. Eng. Sci. Technol. Int. J. **19**, 531–537 (2016)
5. Thampy, A.S., Darak, M.S., Dhamodharan, S.K.: Analysis of Graphene based optically transparent patch antenna for terahertz communications. Physica E **66**, 67–73 (2015)
6. Huang, X., Leng, T., Zhu, M., Zhang, X., Chen, J.C., Chang, K.H.: Highly flexible and conductive printed graphene for wireless wearable communications applications. Sci. Rep. **5**, 1–8(2015)
7. Álvarez, C.N., Cheung, R., Thompson, J.S.: Fellow, Performance analysis of hybrid metal–graphene frequency reconfigurable antennas in the Microwave Regime. IEEE Antennas Wirel. Propag. Lett. **65**(4), 1558–1569 (2017)
8. Sajal, S., Marinov, V.R.: A microstrip patch antenna manufactured with flexible graphene-based conducting material. Antennas Propagation & USNC/URSI National Radio Science Meeting (2015)
9. Perruisseau-Carrier, J.: Graphene for antenna applications: opportunities and challenges from microwaves to THz. In: Loughborough Antennas and Propagation Conference, UK, Nov. 2012
10. Lee, Y., Ahn, J.: Graphene-based transparent conductive films. World Sci. **8**(3), 1330001, 1–16 (2013)
11. Dong, Yanfei, Liu, Peiguo, Dingwang, Yu., Li, Gaosheng, Tao, Feng: Dual-band reconfigurable terahertz patch antenna with graphene-stack-based backing cavity. IEEE Antennas Wirel. Propag. Lett. **15**, 1541–1545 (2016)
12. Desai, A., Upadhyaya, T., Palandoken, M., Gocen, C.: Dual band transparent antenna for wireless MIMO system applications. Microwave Opt. Technol. Lett. (2019)
13. Li, H., Zheng1, Q., Ding, J., Guo, C.: Dual-band planar antenna loaded with CRLH unit cell for WLAN/WiMAX application. IET Microw. Antennas Propag. **12**(0. 1), 132–136 (2018)
14. Desai, A., Upadhyaya, T.: Transparent dual band antenna with μ- negative material loading for smart devices. Microwave Opt. Technol. Lett. **60**(11), 2805–2811 (2018)
15. Desai, A., Upadhyaya, T., Palandoken, M.: Dual band slotted transparent resonator for wireless local area network applications. Microwave Opt. Technol. Lett. **60**(12), 3034–3039 (2018)
16. Chamanara, N., Sounas, D., Szkopek, T., Caloz, C.: Optically transparent and flexible graphene reciprocal and nonreciprocal microwave planar components. Microwave and Wireless Components Letters, vol. 7, pp. 360–362. IEEE, Piscataway, July, 2012
17. Desai, A., Upadhyaya, T., Patel, R.: Compact wideband transparent antenna for 5G communication systems. Microwave Opt. Technol. Lett. **61**(3), 781–786 (2018)
18. Upadhyaya, T., Desai, A., Patel, R., Patel, U., Kaur, K.P., Pandya, K.: Compact transparent conductive oxide based dual band antenna for wireless applications. In: 2017 Progress in Electromagnetics Research Symposium-Fall (PIERS-FALL), pp. 41–45. IEEE, 2017
19. Kumar, Jayendra, Basu, Banani, Talukdar, Fazal A., Nandi, Arnab: Graphene-based multimode inspired frequency reconfigurable user terminal antenna for satellite communication. IET Microw. Antennas Propag. **12**, 67–74 (2017)
20. Patel, R.H., Desai, A., Upadhyaya, T.: A discussion on electrically small antenna property. Microwave Opt. Technol. Lett. **57**(10), 2386–2388 (2015)
21. Upadhyaya, T.K., Dwivedi, V.V, Kosta, S.P., Kosta, Y.P.: Miniaturization of tri band patch antenna using metamaterials. In: 2012 Fourth International Conference on Computational Intelligence and Communication Networks, pp. 45–48. IEEE, 2012
22. Upadhyaya, T.K., Kosta, S.P., Jyoti, R., Palandöken, M.: Novel stacked μ-negative material-loaded antenna for satellite applications. Int. J. Microwave Wirel. Technol. **8**(2), 229–235 (2016)

Identity Based Reliable Data Sharing with Revoked System in Cloud

Sneha D. Raut and Nagaraju Bogiri(✉)

K. J. College of Engineering and Management Research, Savitribai Phule, Pune Univercity Pune, Pune, Maharashtra, India
Sneha.raut320@gmail.com, mail2nagaraju@gmail.com

Abstract. In cloud storage services, users can store their data remotely on the cloud and exchange data with others. The cloud files consist of sensitive information. At the time of file sharing, may realizing the sensitive information of files hide, but this shared file cannot be used by others. The problem is to how to perform data sharing with sensitive information. To solve this problem, propose a Revocation algorithm to avoid the use of sensitive files from unauthorized users. In the system first, The system sanitizes the data blocks and data blocks corresponding to the organization's sensitive information, sanitizes the sanitized data blocks signatures, and finally, sanitizers the sanitized files and their corresponding signatures in the cloud. These signatures are used to verify the integrity of files sanitized during the integrity audit phase. TPA then checks the integrity of the disinfected file. In this way, we are provide security for sharing data.

Keywords: Cloud storage · Data integrity auditing · Revocation algorithm · Sensitive information hiding

1 Introduction

The growth of data puts a heavy burden on users to store all of their data in the cloud. However, if the accumulated data of the cloud is damaged or lost, such as software, hardware failure, human error of the cloud. We can store the data, to verify whether the data is safe and secure, will be the first to the owner needs of the owner of the data on the file private cloud before uploading, many remote data integrity audit into the cloud properly. These signatures audit the Phase health of the data blocks have a sense of Identity Cloud. After that, the owner of the data is a signature work within the data block.

Data stored in the cloud can accumulate a lot of users, but this is limited to cloud storage apps such as Google Drive, Dropbox and iCloud. Cloud storage is a very important feature of data exchange. Data stored in the Cloud consists of confidential information [1].

For example, electronic medical records (EHRs) that are stored and shared in the cloud usually contain sensitive information about the patient (patient name, phone number, id number, etc.) and confidential information of the hospital (hospital name that is directly uploaded to the Cloud Sharing study for the purpose of confidential

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 834–844, 2020.
https://doi.org/10.1007/978-3-030-37051-0_93

information of the patient and the hospital Ehr, but not necessarily cloud, and will be In addition, there is a cloud of human mistakes and software/hardware failures, so you need to ensure the integrity of the EHR. Therefore, the achievement of a remote data integrity audit is important, provided that the total data confidential information is protected. The question is how to perform data sharing of sensitive information [1, 2].

To reduce the computational load on the client, third-party auditor (TPA) [1–4], has been introduced, which helps the client to periodically check the integrity of the data in the cloud. While all existing protocols focus on cloud failure or fraud, the procedure for dealing with client private key disclosure for security weakness and secure cloud storage audit is a very important issue for clients. This process includes downloading the entire data from the cloud, creating a new authentication system, and re-uploading all the data to the cloud. When the client regenerates new authenticators, no guarantees to cloud provide an original data [3]. Another important issue in cloud storage auditing is the recent review of key issues.

The problem itself is not self-evident in nature. When a client's private key for storage auditing is exposed to the cloud, the cloud can easily hide data loss incidents to maintain its reputation [4]. In order to solve this problem, propose a Revocation algorithm to avoid the use of a sensitive file from unauthorized users. In the first system, the sanitizer [1] sanitizes the data block and the data block blind block corresponding to the organization's sensitive information, and in the end, the sanitizer sends this sanitized file and its corresponding signature to the cloud. These signatures are used to verify the integrity of files sanitized during the integrity audit phase. TPA sanitizes the process of verifying the integrity of sanitized files stored in the cloud, and then sends the audit challenge to the cloud, and finally, TPA verifies the integrity of sanitized files by verifying that this audit proof is correct. In this way, we are in charge of system security that we propose.

Our contribution: The system proposes a Revocation Algorithm to avoid the use of sensitive files from unauthorized users. This allows the owner at any time to directly revoke any user from cloud servers and to distinguish unauthorized users because the security model of the cloud service allows you to share data and protect the data of trusted users. User cancellation is the most difficult, clouds in which a single user revocation affects other users who share a common attribute space.

As a result, reducing the cost of data sharing services provided by cloud computing. Mobile cloud computing is a mobile smart terminal used from anywhere when the cloud of convenience, data access to the user. The user stores personal data on the cloud server and it is easy to share only with authorized customers who have access to the data. A lot of traditional systems provide access control for users of the service, a service based on user attributes. Today, the business is usually outsourcing to the cloud with shared encrypted data for users and, moreover, cloud services are new cloud service partners to respond to in its traditional access control system distributed in different geographical areas. In addition, the cloud server was completely reliable, large-scale users from different domains did not leak the contents of the data collusion correspondence with these data leaks is difficult, and the user can cancel the scheme for multiple users to access the cloud service. To solve this problem design a Revocation algorithm for multiple user accessing in cloud service.

2 Literature Review

The author proposes a scheme to audit the integrity of remote data that enables you to share data with confidential information hidden. In this scheme, a sanitizer is used to block data corresponding to the confidential information of the file, and these blocks of data on the valid signature for the sanitized File are used to encrypt the file. Using this signature to, verify sanitized file integrity in the integrity auditing phase. These techniques are capable of ensuring the storage and exchange of files in the cloud and also to hide confidential information. This technique is based on Cryptography-based identity [1].

For group, user-author proposes the cloud storage audit scheme. It is used to reduce the computational load on the user side. This method introduces a third-party media (TPM) which performs lengthy operations on behalf of the use and also used to verify the integrity of the data. In this way, data is protected from TPA. Simple operation to blind data Phase data uploads, data audit [2].

In this article, the author focuses on the auditing of cloud storage. The author study, the damage of the client's key exposure on how to reduce in cloud storage auditing and set the solution to this problem. The definition of auditing protocol and the security model are formulated using the key Exposure resilience and this protocol is proposed. In this design, a binary tree structure and a leading traversal technique are adapted to update the client's secret key. The development of such a new certification construction will help to ensure the security and reliability of blocking less certification [3].

The author will explain how to update the key as a key update, and how to ensure the transparency of the new paradigm proposed by the client, called cloud storage auditing and verification of outsourcing keys. In this paradigm, key renewal can be safely entrusted to some authorized parties, and thus the burden of key renewal on the client is particularly acute [4].

Cloud storage services have been widely adopted by more and more institutions, through the user's convenience per share data. In this paper, the author proposes efficient public auditing of the preservation of privacy and identity. The system also allows you to achieve data during your privacy authentication generation by using blind signature technology. Using the proposed method, the auditing system for the actual scenario is designed further [5].

The author proposes a new public audit mechanism for the integrity of the shared data with the user's efficient cancellation in mind. By utilizing the idea of quitting the proxy, you can re-sign the block on behalf of an existing user upon user revocation, and then re-sign the existing user. In addition, the organization provides a comprehensive audit of the audit work at the same time [6].

Data per user group and share in cloud storage services. The author proposes a new Public Audit scheme for the integrity of shared data using the concept of Shamir secret sharing. In addition, this scheme supports safe and efficient auditing by improving authentication tags based on polynomials [7].

The paper proposes an identity-based proxy oriented data upload and remote data integrity check model. The formal definition of a system model is the security model. Next, they design a specific ID-PUIC protocol using a bilinear combination [8].

Patent application securing system i.e. SecCloud, cloud. Not only does SecCloud generate data tags before the client uploads them, it also always encrypts the data before the customer uploads it and encrypts the data's storage [9].

The author proposes a new server-side de-duplication scheme for encrypted data. Not only to prevent this data leakage but also to cancel the user's own data is also a sincere or strange cloud storage server. Furthermore, the proposed scheme guarantees the integrity of the data against arbitrary tag contradiction attacks. As a result of the efficiency analysis, it is shown that the proposed scheme is as efficient as the previous scheme, but the additional computational overhead is negligible [10].

3 Proposed Approach

3.1 Problem Statement

The file in the cloud may contain sensitive information. The problem is how to perform data sharing with sensitive information. In order to solve this problem, propose a Revocation algorithm to avoid the use of a sensitive file from unauthorized users.

3.2 Proposed System Overview

A detailed description of the system architecture is as follows:

The system architecture includes five types of different entities: the cloud, the user, the sanitizer, the Private Key Generator (PKG) and the Third Party Auditor (TPA) (Fig. 1).

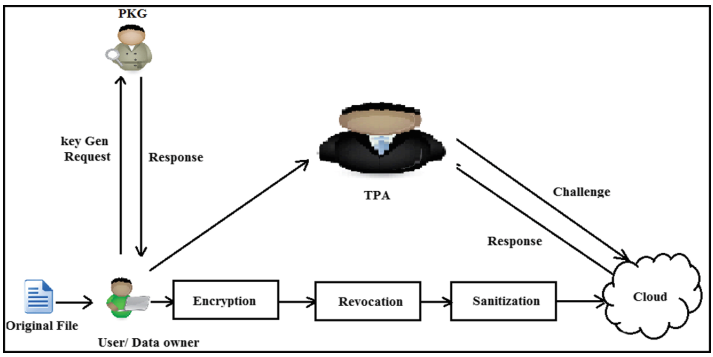


Fig. 1. Proposed system architecture

The cloud: On the cloud, users save a lot of data. Users to upload and share data with other users.

Sanitizer: The sanitizer, which is responsible for sanitizing data blocks that correspond to sensitive information in files (such as personal and organizational information), is responsible for sanitizing data blocks.

The Public Key Generation (PKG): Other entities rely on the generation of Public Key. The functionality of this PKG is the generation of public parameters and private key for the user according to their identity ID.

Revocation: Whenever data owner wants to share reliable data with some selected authorized user from the set of all authorized user of organization, we use revocation algorithm to revoke the particular set of user as input then select the encrypted reliable data and time stamp used for at what time period revoked user is removed from organization, then we update the list of authorized and sent it to the server with encrypted reliable data.

The Third Party Auditor (TPA): Third party Auditor is a public verifier. It checks the integrity of data stored in the cloud on behalf of users.

On the cloud, users save a lot of data. The sanitizer [1], which is responsible for sanitizing data blocks that correspond to sensitive information in files (such as personal and organizational information), is responsible for sanitizing data blocks. Other entities rely on the generation of Public Key. The functionality of this PKG is the generation of public parameters and private key for the user according to their identity ID. Whenever data owner wants to share reliable data with some selected authorized user from the set of all authorized user of organization, we use revocation algorithm to revoke the particular set of user as input then select the encrypted reliable data and time stamp used for at what time period revoked user is removed from organization, then we update the list of authorized and sent it to the server with encrypted reliable data. Third party Auditor is a public verifier. It checks the integrity of data stored in the cloud on behalf of users.

In this system first blinds sensitive information data from files and then generate the corresponding signature for those blinding files. These signatures are used to verify the integrity of sanitized files during the integrity audit phase (Fig. 2).

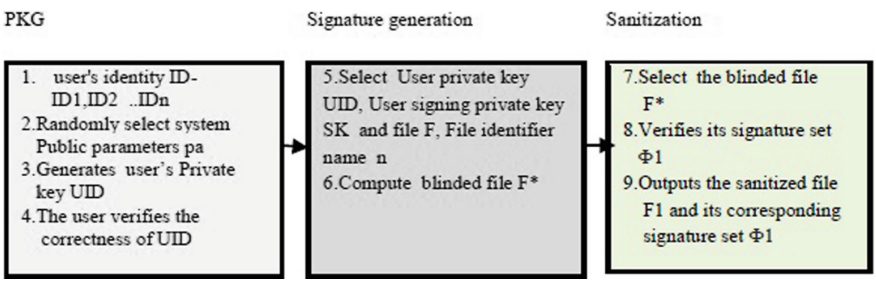


Fig. 2. The processes of signature generation, sensitive information sanitization

After sanitizes the process the TPA wants to check the integrity of the cleaned file stored in the cloud, it sends an audit challenge to the cloud. And then, the cloud responds to TPA with proof of verification of data possession. Finally, TPA verifies the integrity of the clean file by checking whether this proof of verification is correct or not. In this way, our proposed system provides security for data sharing (Fig. 3).

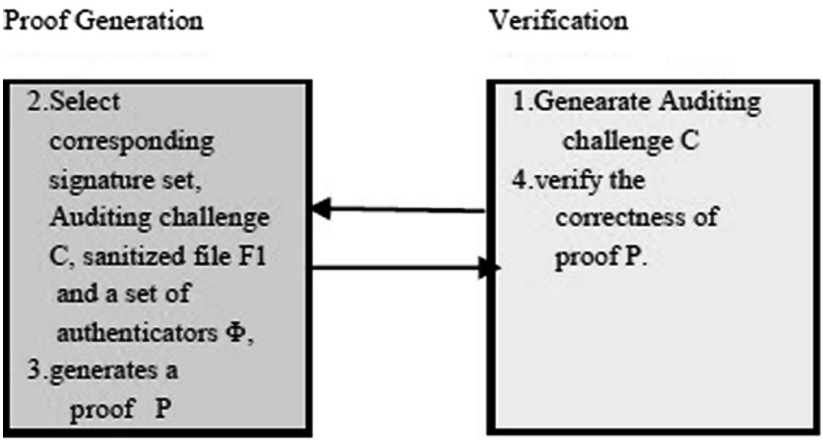


Fig. 3. The processes of proof generation and verification

In the revocation system, We can add some user those who cannot able to download that sensitive file called revoked user. When user makes a request to download the file from the cloud: cloud firstly checks requested user if the revoked user if it is revoked user then the cloud will not allow downloading that file. If it is not revoked user then he/she can download the file using the private key. In addition, we add the validation period to the file.

3.3 Algorithm

Revocation

Revocation algorithm to revoke the particular set of user as input then select the encrypted reliable data and time stamp used for at what time period revoked user is removed from organization, then we update the list of authorized and sent it to the server with encrypted reliable data.

In this algorithm, The owner generates a new list of revoked user and upload that list to cloud. PKG run this algorithm for validate the user is revoked or not.

Input: List of the user for revocation
Output: Revoke user from an organization
Process:

(1) Start
(2) Take encrypted File and TimeStamp
(3) Remove selected user from the organization for
(4) Update list of user
(5) Upload updated revoked list of user to a server with encrypted file
(6) user request for private key to PKG
(7) PKG validate the user is revoked or non-revoked.
(8) if the user is revoked it does not share the private key to that user and does not

(9) provide access to download the data
(10) End

3.4 Mathematical Model

System S can be defined as:

1. Private Key Generation

   Choose g, a number whose multiplicative order modulo p is q
   q is the smallest positive integer such that
   Prime p such that p − 1 is a multiple of q
   Choose an element μ', μ1, μ2…… μn;
   Let H be hashing function
   U = {UI, UF, Uu} is a user
   UI = {UI1, UI2} set on I/P
   UI1 = User authentication detail contain UID = (UID1, UID2, UIDn)
   UI2 = File data
   Compute private key of user [1]

$$sk_{ID} = (g_2^x\left(\mu' \prod_{j=1}^{l} \mu_j^{UID}, g^{rID}\right)$$

rID = Randomly picks values from user ID.

2. Generate Signature

   Compute Signature Sig [1]

$$sig = \left(g_2^x\left(\mu' \prod_{j=1}^{l} \mu_j^{UID}\right)^{rID}, (H(name), \mu^{mi})^r\right)$$

   Where,
   m_i^* is a blinded file

3. Data Auditor

   DAI = {DAI1, DAI2}\\ A set of input
   DAI1-User Registration Details
   DAI2-Block Details
   τ = tag or file [1]

$$\tau = \tau_0 \| DAI$$

$$\tau_0 = name \| g^{rID} \| g^r$$

4. Sanitization

   The Sanitizer checks the signature is valid or not. The sanitizer respectively verifies the correctness of signature sig as follows: [1]

$$e(sig, g) = e(g1, g2).e\left(\mu' \prod_{j-1}^{l} \mu_j^{ID_j}, g^{rID}\right).e(H(name||i).u^{m_i^*}, g^r)$$

5. Cloud

   CI = {CI1, CI2}, A set of input
   CI1-Block Data
   CI2-Challenge Message
   CF = {CF1 CF2} \\ A set of functions
   CF1 = Save Blocks and its hash
   CF2 = Generate Response
   CO = Output of cloud
   CO = {CO1, CO2}
   CO1 = Set of Blocks = {b1, b2.., bn}
   CO2 = Generated Response of File block

6. Revocation

   P = {L,R,O}
   L = {L1, L2}\\ A set of Input
   L1 = List of user
   L2 = Revoke list of user
   R = {R1, R2} \\ A set Of Function
   R1 = Revoke User
   R2 = Secret key updating
   O = {OP} \\ A set Of Output
   OP = List of revoked user

4 Result and Discussion

4.1 Experimental Setup

The system uses Java framework on Windows platform. The Net bean IDE is used as a development tool. As on tested on the real cloud it takes less time when sharing with authorised users. For a dataset, the system uses a number of files in different size.

4.2 Result and Analysis

This section discussed the experimental result of the proposed system.

The Fig. 4 shows that the auditing computation overhead of proof verification, proof generation and challenge generation, these three procedures linearly increases with the number of challenged blocks. The verification procedure takes longer than the other two phases, and the challenge generation procedure takes the shortest time among the three procedures. In the case of this graph, all the blocks will be threatened, and these three stages will require a large amount of computational overhead.

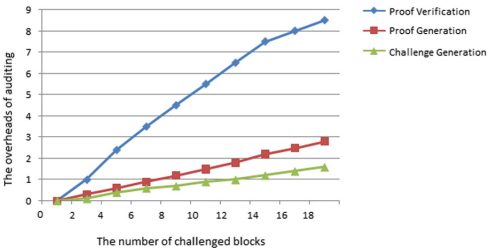


Fig. 4. Computation overhead in auditing phase

Table 1 shows, the time comparison between the existing and proposed system algorithm. Figure 5 shows the time require to access data of the proposed system with the existing system. It shows that the data accessing time of the proposed Revocation algorithm is less because of data sharing with selected authorized users and there is no traffic in the data accessing process. Suppose, the hundred of users send a request to the admin to access the file, the admin gives the permission only authorized 60 users. So the less time requires accessing the file and there is no traffic in the data accessing process.

Table 1. Time comparison

Algorithm	Time in ms
Data access time without revocation	90
Data access time with revocation	40

Table 2 shows, the performance Comparison. Figure 6 shows that if a number of users increased the performance of the system with revocation and without revocation. The graph shows that the performance of the system with revocation is better than the performance of the system without revocation.

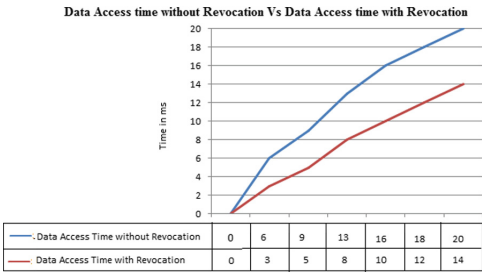


Fig. 5. Data access time without revocation versus data access time with revocation

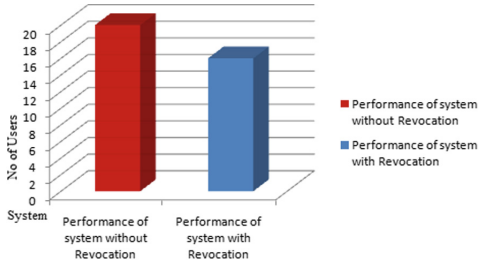


Fig. 6. Performance graph

5 Conclusion and Future Scope

Proposes a Revocation algorithm for reliable data sharing that supports data sharing with sensitive information hiding. This supports data sharing with selected authorized users within an organization. Data accessing time of the proposed Revocation algorithm is less because of data sharing with selected authorized users and there is no traffic in the data accessing process. The results show that the proposed system provides security to data sharing.

In future we can implement traceability method to trace or detect the fake user and make system more secure.

References

1. Yu, J., Shen, W., Qin, J., Hao, R., Hu, J.: Enabling identity-based integrity auditing and datasharing with sensitive information hiding for secure cloud storage (2018)
2. Zhang, H., Lu, X., Shen, W., Xia, H., Yu, J., Hao, R.: Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium (2017)
3. Ren, K., Wang, C., Yu, J., Varadharajan, V.: Enabling cloud storage auditing with key-exposure resistance. IEEE (2015)
4. Ren, K., Yu, J., Wang, C.: Enabling cloud storage auditing with verifiable outsourcing of key updates (2016)

5. Shen, W., Yang, G., Su, Q., Fu, Z., Yu, J., Hao, R.: enabling public auditing for shared data in cloud storage supporting identity privacy and traceability (2016)
6. Li, B., Wang, B., Li, H.: Panda: public auditing for shared data with efficient user revocation in the cloud (2015)
7. Wang, D., Xu, M., Fu, S., Luo, Y., Deng, J.: Efficient integrity auditing for shared data in the cloud with secure user revocation (2015)
8. He, D., Wang, H., Tang, S.: identity-based proxy oriented data uploading and remote data integrity checking in public cloud (2016)
9. Xie, D., Li, J., Li, J., Cai, Z.: Secure auditing and deduplicating data in cloud (2016)
10. Koo, D., Hur, J., Shin, Y., Kang, K.: Secure data deduplication with dynamic ownership management in cloud storage (2016)
11. Dhivya, J., Aanjan Kumar, S.: Efficient cloud data sharing with strong key analysis using intelligent crypto system. Int. J. Innov. Res. Comput. Commun. Eng. (2018)
12. Prasanna, A.H.N.V.L., Surya Ram Prasad, K., Suri Babu, D.D.D.: Simple protocol to restrict client key exposure over cloud storage systems for auditing. Int. Res. J. Eng. Technol. (IRJET) (2016)

A Study: Machine Learning and Deep Learning Approaches for Intrusion Detection System

C. H. Sekhar(✉) and K. Venkata Rao

Department of Computer Science and Engineering,
Vignan's Institute of Information Technology, Visakhapatnam, India
sekhar1203@gmail.com, vrkoduganti@gmail.com

Abstract. System security is one of the real worries of the difficult time. With the fast advancement and monstrous utilization of web over the previous decade, the vulnerabilities of system security have turned into an important issue. Interruption identification framework is utilized to distinguish unapproved get to and uncommon assaults over the verified systems. High volume, assortment and fast of information produced in the system have made the information examination procedure to identify assaults by conventional strategies extremely troublesome. To comprehend the present status of usage of Machine and Deep learning methods for tackling the interruption recognition issues, this study paper listing out the related examinations in the continuous period focusing. This overview paper gives the various models of the detection system and briefly on Machine and Deep learning algorithms.

Keywords: Intrude · Intrusion Detection · Machine Learning · Deep Learning

1 Introduction

With the increasingly deep integration of the Internet and society, the Internet is changing how individuals live, study and work. However, the different security dangers that we face are winding up increasingly genuine. Step by step instructions to distinguish different system assaults, particularly unexpected assaults, is a certain key specialized issue. An Intrusion Detection System (IDS), a vast research accomplishment in the data security field, can distinguish an attack, which could be a progressing intrusion or an interruption that has just happened. Actually, interruption identification is typically proportional to a grouping issue, such as a binary or a multiclass classification problem, i.e., identifying whether network traffic behaviour is normal or anomalous, or a five-category classification problem, i.e., identifying whether it is reasonable or any one of the other four attack types: Denial of Service (DOS), User to Root (U2R), Probe (Probing) and Root to Local (R2L). In short, the primary motivation of intrusion detection is to improve the accuracy of classifiers in effectively identifying the intrusive behavior [1].

This paper is described as follows: Sect. 2 provides the research topic overview where several techniques for intrusion detection have been described in Machine

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 845–849, 2020.
https://doi.org/10.1007/978-3-030-37051-0_94

learning. Section 3 describes the deep learning techniques. Sections 4 and 5 gives in the detailed view of the intrusion detection system life cycle and various approaches to detecting intrusions and types of attacks. Section 6 describing the comparison analysis among machine and deep learning

2 Machine Learning Techniques

AI Approach Machine learning is a unique part of man-made reasoning that gains information from preparing information dependent on well-established actualities. AI is characterized as an examination that enables PCs to learn information without being customized referenced by Arthur Samuel in 1959 [2]. Machine learning mainly focuses on prediction. Machine learning techniques are classified into broad categories such as.

(a) **Supervised Learning.** Task Driven methodology. As a matter of first importance, you should name information like encouraging a model with instances of executable records and saying that this document is malware or not. In view of this marked information, the model can settle on choices about the new information. The detriment is the farthest point of the named information.
(b) **Unsupervised Learning.** Information Driven methodology. The methodology can be utilized when there is no named information, and the model ought to be one way or another imprint it without anyone else's input dependent on the properties. It usually is expected to discover inconsistencies in information and viewed as progressively incredible as a rule as it is practically difficult to check all information. As of now, it works less decisively than managed approaches.
(c) **Semi-supervised learning.** As the name infers, semi-regulated taking in attempts to consolidate profits by both managed and unsupervised methodologies, when there are some marked information
(d) **Reinforcement learning.** Condition Driven methodology can be utilized when the conduct ought to be one way or another respond on the evolving condition. It resembles a child who is learning condition by experimentation.
(e) **Active learning.** It is progressively similar to a subclass of Reinforcement, discovering that most likely will develop into a different class. Active learning takes after an instructor who can help correct mistakes and conduct notwithstanding condition changes.

3 Deep Learning Techniques

Deep learning was inspired by the structure and depth of the human brain. The reason for the multiple levels of abstraction, the network learns to map the input features to the output. Given a set of conditions, the machine can use a series of mathematical methods to determine if classification is accurate based on the likelihood of error. Within the realm of deep learning [4].

4 Intrusion Types

Attacks can come in many forms. Several behavioural samples that would trigger a flag for an anomaly can be port scans coming from one host on a network across an entire subnet, download file count/size in a shared network folder, multiple USB file transfers, etc… NIDS can be configured to account for many behavioural examples. Highly targeted configurations can account for known signatures for malware transferred across the network compared to a database containing hashes for the malware. Attacks are of active and passive type attacks, Endeavour to get the unapproved access and change data in the framework with intent to destroy the entire network is of active type attacks. Whereas attackers listen stealthily however do not alter any data in the framework treated as passive attacks [5] (Table 1).

Table 1. Different attack types

Attack type	Name of attack	Description	Researchers
Active	Spoof	While an attacker imitates someone else's tool or person so that it will provoke assaults against network hosts, pass get entry to control, thieve facts, or unfold malware	[6]
	Gray hole	Behaves like a malicious node to drop malicious packets, however later switches again to everyday	
	Malicious packet dropping	It is a type of DDoS attack similar to black hole attacks	
Passive attacks	Eavesdropping	Network layer attacks that intercept a private communication	[8]
	Traffic analysis	An assault that examines the communication styles among entities in a system	
	Location disclosure	Can reveal something about the network structure or the nodes points	
DDOS or DOS		A DoS assault is a kind of assault wherein the programmer makes a processing or memory assets excessively occupied or too full to even think about serving genuine systems administration demands and subsequently denying clients access to a machine	
Probe		Probing is an assault wherein the programmer filters a machine or a systems administration gadget so as to decide shortcomings or vulnerabilities that may later be misused in order to bargain the framework	

Intrusion Detection System working with various types such as Host Based, Network-based Hybrid and Distributed.

- Host Based: In this type, the IDS mechanism was installed on the server system to monitor and audit the information received from the operating system to identify the intrusion. It can deal with the encrypted environment at the transport layer—no need for additional hardware.
- Network-Based: In this type of IDS mechanism, observing the network traffic and application protocol activities between two systems. It is able to handle the attacks which are missed at Host Based model, Faster response and easy to deploy. Need full-time monitoring and unable to detect encrypted packets.
- Hybrid Model: It is the combination of above to type's, i.e. Host and Network-based models. It uses mobile agents and combined anomaly and misuse based approaches. Log file checked by the mobile agent
- Distributed Type: Different IDS are combined by working as faraway sensors and generate a report about intrusion at the end send to a centralized system treated as distributed IDS. In this centralized model system able to monitor intrusion detection and responses. Able to analyze the incident and instant attack data.

Intrusion Detection System (IDS) is a vital component of security measures shielding computer systems and networks from potential abuse and misuse. In 1980, John Anderson published one of the earliest papers on IDS in the Computer Security Threat Monitoring and Surveillance. Since then, many different efficient approaches for IDS have been proposed and implemented in practice. However, the research on intrusion detection is still an active field and attracts the attention of many researchers because of its challenges and necessity of IDS for our computing resources when using the Internet. Some of the challenges in current IDS are:

Adaptability: IDS should perpetually learn changes in the environment over time and adjust to them accordingly. Adaptability is a major challenge and arguably the most desired characteristic for IDS. Generally, achieving adaptability automatically is a harder problem for misuse detection systems which rely on manual creation of signatures. Anomaly detection systems by definition, look for novel attacks, but they also need to adapt their learnt models of normal behaviour relative to changes in the environment.

Speed: dealing with the high-performance network—Diversity of environments: needs to operate in changing and adversarial network environments with diverse protocols, services, and applications.

Fault tolerance: the IDS not becoming security vulnerability itself.—Inter-Operability and transparency ease of use.

Timeliness: handle large amounts of data. Concerned with how quickly the IDS can propagate the information through the network to react to potential intrusions. It is also referred to as scalability [3].

5 Comparative Analysis

Specialists in Machine and Deep learning have not yet achieved agreement on these ideas. The significant difference between Deep and Machine learning as follows,

In Deep learning, a lot of information is expected to convey the calculation structure to the ideal. The algorithms are able to extract the features from the data. These algorithms able to work on high-performance machines; the problem is solved end to end.

Machine learning can be worked on normal CPUs doesn't require any high-performance systems. The problems are generally partitioned into pieces, these parts are understood one by one, and afterward, the arrangements are shaped because of the arrangements.

6 Conclusion

Based on the various approaches of deep learning and machine learning, here we are provides a study with comprehensive explanation of intrusions in terms of their detection and corresponding methods used. This paper has mentioned various methodologies used by Machine learning and deep learning for intrusion detection. Listing out the various types of attacks pointed out by various researchers.

References

1. Yin, C.L., Fei, Y., Zhu, Y., Fei, J., He, X.: A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, Digital Object Identifier. https://doi.org/10.1109/access.2017.2762418
2. Haq, N.F., et al.: Application of machine learning approaches in intrusion detection system: a survey. Int. J. Adv. Res. Artif. Intell. **4**(3) (2015)
3. Machine Learning based Research for Network Intrusion Detection: A state-of-the-art. Int. J. Inf. Netw. Secur. (IJINS) **3**(3), 01–20 (2014)
4. Lee, et al.: Comparative study of deep learning models for network intrusion detection. SMU Data Sci. Rev. **1**(1), Art. 8 (2018)
5. Anwar, S., Zain, J.M., Zolkipli, M.F., et.al.: From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms **10**, 39 (2017). https://doi.org/10.3390/a10020039 www.mdpi.com/journal/algorithms
6. Inayat, Z., Gani, A., Anuar, N.B., Khan, M.K., Anwar, S.: Intrusion response systems: foundations, design, and challenges. J. Netw. Comput. Appl. **62**, 53–74 (2016)
7. Hajian, S., Domingo-Ferrer, J., Martinez-Balleste, A.: Discrimination prevention in data mining for intrusion and crime detection. In: Proceedings of the 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), Paris, France, pp. 47–54, 11–15 Apr 2011
8. Inayat, Z., Gani, A., Anuar, N.B., Anwar, S., Khan, M.K.: Cloud-Based intrusion detection and response system: open research issues, and solutions. Arab. J. Sci. Eng. **7**, 1–25 (2017)
9. Karatas, G., et al.: Deep learning in intrusion detection systems. International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, Ankara, Turkey, 3–4 Dec 2018

Systematic Literature Survey on IDS Based on Data Mining

C. Amali Pushpam[1(✉)] and J. Gnana Jayanthi[2]

[1] Rajah Serfoji College, Thanjavur, Tamil Nadu, India
joemarycap@gmail.com
[2] Department of Computer Science, Rajah Serfoji College, Thanjavur, Tamil Nadu, India
jgnanajayanthi@gmail.com

Abstract. In this digital era, the usage of internet and information grows rapidly. Every fraction of second, huge volume of data is transferred from one network to another. This information and information system are subjected to attack. It is necessary to protect this valuable information and network from intruders generally named as crackers or hackers who are threat to system security. System security is a common, current and critical problem which is a challengeable task to researchers. Intrusion Detection System (IDS) offers good solution to this problem. With aim of boost up the performance of IDS, it is integrated with data mining. Various data mining techniques in IDS, based on certain metrics like accuracy, false alarm rate, detection rate and issues of IDS have been analyzed in this paper. A total of 43 papers were reviewed in the period 2008 to 2018. It is observed that more number of articles support SVM or ANN Techniques. Also it is observed that hybrid methods produce better performance than single. This survey shows that in hybrid methods, frequently K-means or SVM technique are combined with others and gives good result.

Keywords: Intrusion · Attack · Data mining · Intruders · Security

1 Introduction

An intrusion in network is an unauthorized access to resources and a threat to network security. A number of popular attack vectors like Asymmetric Routing, Buffer Overflow Attacks, Common Gateway, Interface Scripts, Protocol-Specific Attacks, Traffic Flooding, Trojans, and Worms pose a serious security risk in network environment existing in network. A number of new technologies and methods are available to diminish the potential effectiveness of each one. One of the important solutions is "Intrusion Detection system" (IDS). It performs a very important task in identifying intrusion in network. When data mining concept is incorporated with IDS to mine the useful, relevant, hidden and valuable information for the user, it increases the efficiency with less execution time. IDS are data analysis process. It handles a large amount of 5 V characteristics data i.e. Volume (size of data), Velocity (speed of incoming data), Value (trustworthiness of data), Variety (heterogeneous nature) and Veracity (value of data changing dynamically). As Data mining analyzes an enormous amount of data

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 850–860, 2020.
https://doi.org/10.1007/978-3-030-37051-0_95

with high speed in less amount of time, it is integrated with IDS. A number of tools and technologies are available and working on current and new platforms. Both normal and abnormal activities leave evidence on data. Hence it is quite easy to develop models through supervised and unsupervised learning. All these models are combined with IDS in detecting attacks.

2 Research Access

This paper works a thorough study on Intrusion detection in network published in various journals/conferences.

2.1 Research Issues

RQ1: What are the various data mining techniques used in Intrusion detection systems from 2008?
RQ2: What are the limitations of various data mining techniques used in IDS?
RQ3: What are the issues/challenges that are addressed in the research papers?
RQ4: What are the techniques proposed to solve the issues?

To answer RQ1, a systematic analysis and review on research spanning from 2008 up to 2018 are carried out. For RQ2, various data mining techniques have been analyzed to find out their limitations. Regarding RQ3, challenges addressed in research papers have been identified. RQ4 is framed to understand the existing proposed.

2.2 Requirement System

For essential case papers for the study, search has been done and papers are obtained from various data repository.

Various search terms have been compiled using Boolean operators AND/OR. Based on these terms, advance search is done on selected articles related to IDS.

2.3 Paper Enclosure Standard

Papers with the following criteria are included: (i) Papers that describe various data mining techniques used in IDS, (ii) Papers that use testing methodologies for vulnerability detection in network services, (iii) Papers that address web service attacks such as Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R) and Proof, etc. (iv) Papers that are published after 2007.

2.4 Data Compilation

Information that extracted from selected articles are (i) Title and Publication year of papers, (ii) Synopsis of Paper, (iii) Type of Web service attack (DoS, R2L, U2L and Proof), (iv) Area of Research (Intrusion detection and prevention).

3 Outcome and Discussion

In this part, Research queries and answers for these queries obtained from this review are discussed. Section 3.1 gives an overall idea about selected articles. The total numbers of 43 articles have been selected for the literature study. These articles are retrieved from various journals and proceedings which have published between 2008 and 2018.

3.1 Data Mining Techniques with Their Merits and Demerits (RQ1, RQ2)

A list of top 10 data mining techniques which have been applied by researchers in the field of IDS is listed out and they are.

(i) Artificial Neural Network (ANN), (ii) Support Vector Machine (SVM), (iii) Decision Trees (DT), (iv) K-Means, (v) Genetic Algorithm (GA), (vi) Fuzzy c-means, (vii) Y-Mean, (viii) Naive Bayesion (NB), (ix) K-Nearest Neighbors (k-NN), (x) Random Forest.

Table 1, consist of detailed information about the data mining techniques used by the selected articles in this review.

Table 1. Summary of review findings

S. no	DM Alg	Merits	Demerits	Ref. no
1.	K-means	Less execution time on small data set, ease of use, better accuracy and efficiency, easy for parallel implementation	More execution time on large data set, Speed is less, sensitive to outlier and noise and selection of the cluster centroids	[1], [2], [8], [18], [19], [20], [28], [31], [35], [36], [39]
2.	Y-mean	Eliminate the empty clusters, overcomes the limitations namely dependency on the number of clusters, degeneracy and dependency on the initial centroids	As data set updation is not done dynamically during process, it is not applicable to real time anomaly detection	[1], [18], [19]
3.	Fuzzy c-means	Performance and efficiency are best for small and large data sets. It measures quality of partitioning though it allows an item to belong to many clusters	Time consuming	[1], [2]

(*continued*)

Table 1. (*continued*)

S. no	DM Alg	Merits	Demerits	Ref. no
4.	Naïve Bayesion	Accuracy and speed is high in larger data set, easy to construct Naïve Bayes without any complex iterative parameter	Time complexity increases when size of data points grows	[1], [8], [23], [26], [31], [39], [41]
5.	SVM	High accuracy than other classifiers, SVM is preferred by researchers than KNN, decision tree, genetic algorithm, able to model complex and nonlinear decision boundaries, performs better for U2R attack, it works well in small data set and produces high accuracy by reducing execution time. Independent of feature space. Here classification accuracy is quite impressive or high fast accurate while training as well as during testing	Extensive memory requirement, training and testing speed slow high algorithmic complexity the choice of the kernel is difficult	[1], [4], [8], [10], [11], [13], [14], [16], [18], [19], [20], [23], [25], [26], [30], [32], [34], [37], [38], [40], [41], [42]
6.	ANN	More stable and reliable than other algorithms, highly tolerate the noisy data, multiple training algorithms available	Long training time, over fitting, requires more sample-training phase	[1], [3], [9], [13], [18], [19], [20], [22], [24], [26], [29], [43]
7.	KNN	Simple to understand and implement, noise and larger K-value affect accuracy and prediction time	High storage requirement, slow in classifying and testing tuplets	[1], [6], [8], [28]
8.	DT	Simple to understand and easy to generate rules, when dataset is large, tree based classifier has highest	Unstable, limited to one output attribute mostly non-backtracking methods are used in	[1], [3], [4], [8], [13], [18], [23], [26], [30],

(*continued*)

Table 1. (*continued*)

S. no	DM Alg	Merits	Demerits	Ref. no
		performance and has high detection rate	constructing decision tree	
9.	GA	Efficiency is increased through feature selection	It is difficult to understand as method is complex	[1], [3], [7], [17], [19], [21], [25], [30]
10.	Random forest	Build the patterns automatically instead of coding rules manually, powerful algorithm in detecting probe and DOS attack	It suffers due to bag error that is generated during training phase	[1], [11], [27], [29], [32], [33], [34], [35], [41]

Figure 1 shows most popular data mining techniques used in intrusion detection systems.

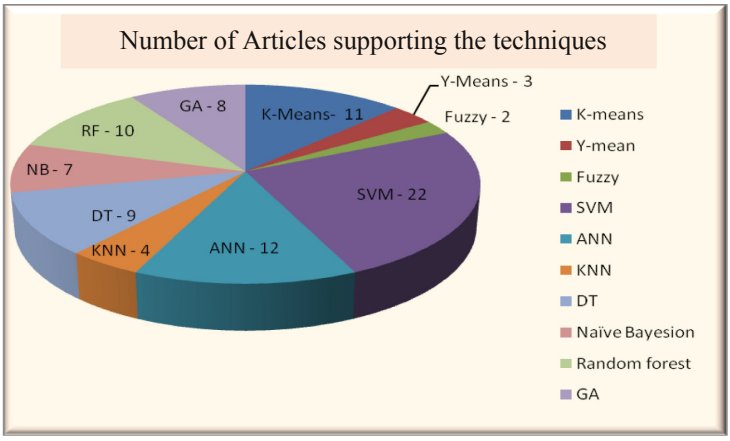


Fig. 1. Number of Articles supporting the techniques

3.2 Techniques Proposed to Solve Issues (RQ4)

In Sect. 4, various issues and challenges that existing in IDS have been discussed. A number of techniques are available in the field to solve these issues. As data mining is a data analytic tool, it is integrated with IDS to analyze huge volume of data to differentiate the normal and intrusion events. Frequently used data mining techniques are depicted in the Fig. 1. From the survey in this paper, it is identified that hybrid methods perform better than single methods. Those details are given in Table 2. From the findings, summarized in Table 2, it is observed that SVM or K-Means techniques are frequently combined with other techniques and produces better results.

Table 2. Summary of hybrid methods—review findings

S. no	Ref. no	Year	Hybrid methods	Results/outcome
1	[1]	2017	**K-means**, Fuzzy NN, **SVM**	Accuracy achieved is 98.80% for DoS attack, 97.31% for PROBE attack 97.5% for R2L (Remote to Local) and U2R (User to Root) attacks
2			Combination of classifiers random forest & random tree, J48 & Random forest, J48 & Random tree,	Achieve better result for U2R and R2L type of attack when compare to other classifier, Achieves better attack detection rate
3			**SVM**, Decision tree Naïve Bayes	High accuracy is maintained by reducing false positives
4	[7]	2017	Particle swarm optimization(PSO) neural network	Effectively detect intrusive attacks achieves a low false positive rate
5	[8]	2017	k-Medoids clustering **SVM** classification	Gives better performance in both accuracy and detection rate than K-Medoids with Naïve Bayes while reducing false alarm rate
6				
7	[18]	2013	**k-means** clustering k-nearest neighbor classification Naïve Bayes classification	Attains good detection rate and low false alarm rate than existing methods
8				
9	[2]	2017	C4.5, **SVM classification**	Improvement in detection rate and accuracy
10			**K-means** Naïve Bayes (KMNB)	Increases the detection rate and accuracy
11			**SVM**, CSOACN (Clustering based on Self Organized Ant Colony Network)	Takes merits of these methods and avoids the weaknesses
12	[25]	2013	Fuzzy genetic algorithm	Gives good results in all categories with a detection rate of 99.53 but FAR is high (1.94)
13	[27]	2017	Average one-dependence estimator (AODE), random forest (RF)	Overcome the problem of attribute dependency in Naïve Bayes classifier and accuracy, false alarm rate and detection rate are good
14	[28]	2017	KNN **K-Means**	Performs well over CIDDS-001 dataset and gives high Detection rate & Accuracy and low false positive rate
15	[31]	2015	Naïve Bayes decision tree	Works well in KDD (Knowledge Data Discovery) cup data set and attains 99% accuracy, high detection rate and reduce false positive. But while handling R2U attack, some enhancement is required

(*continued*)

Table 2. (*continued*)

S. no	Ref. no	Year	Hybrid methods	Results/outcome
16			**SVM,** DT	Gives 100% accuracy in tested datasets
17			**SVM classification** k-medoids clustering	Accuracy is Higher and Time complexity increases when data set grows
18			k-Medoids clustering Naïve Bayes classification	High detection Rate and low false alarm rate. Performance of Naïve Bayes is not same on different environments
19			**k-Means**, ID3 decision tree	Performs well than individual k-Means and ID3 and works well on specific data sets
20	[35]	2015	**K Means**, **Support vector machine**	Produces better result on KDDCUP'99 data set
21	[37]	2011	Principal component analysis (PCA), **SVM**	Increases detection rate and reduces false alarm in anomaly intrusion detection
22	[39]	2012	**KMeans**, Naive Bayes	Detection rate is higher than single method. At the same time, it suffers due to more false positive rate
23			K-Medoids, Naïve Bayes	Works well and increase accuracy & detection rate by reducing false alarm rate on KDD dataset than combined K-means and Naïve Bayes
24	[12]	2016	**K-Means** C4.5	True positive rate is high
25	[40]	2018	Random forest, **SVM** (RFSVM)	Provide good stability and accuracy by taking merits of both random forest and SVM

4 Introduction Detection Systems Based on Data Mining—Issues and Challenges (RQ3)

In this hi-tech world, usage and growth of network is rapid and interminable one. Through Net, Society gets a lot of benefits and at the same it faces a lot of challenges also. Especially security is the one of the important issue which needs more research and focuses. Intrusion detection systems support security by identifying anomaly activities and alert the system. Though much advancement in IDS, sometimes IDS itself is subjected to attack and faces a lot of problems. It is listed below [5, 7, 15, 17, 19].

(i) Data overload, (ii) False positives/False Alarm rate, (ii) False negatives, (iv) Almost all techniques are designed to protect one or two web attacks only (v) Integrating many IDS will produce more rate of misreporting, (vi) Most anomaly based NIDSs depend on training data which is difficult to obtain it in network environment, (vii) Data feature selection, (viii) Increase network services is also a challenge, (ix) Quick updation of database of patterns of known attack.

5 Research Result

On the whole this survey gives an outlook about Intrusion Detection System based on Data Mining. As it is given, the introduction part covers the fundamentals of IDS. Then the core concept of integrating data mining with IDS is explained. Data mining techniques are categorized into three concept i.e. Classification, Clustering and Association Rule. Under this, various data mining algorithms used in IDS are analyzed. Each algorithm has its own pros and cons. Based on various metrics like accuracy, false positive rate and detection rate performance of algorithms in IDS is assessed and degrees of these factors are varying based on applications. Sometimes hybrid methods yield good results. Hence, as per our literature studies, our research is focused on designing a framework for IDS with high performance where data mining is integrated with it.

6 Conclusion

Every second huge volume of information is transferred from one network to another and they are subjected to attacks. Hence it is very necessary to protect these valuable information and information system. To provide and maintain the security in terms of confidentiality, availability and Integrity is a very tedious job. Intrusion Detection System (IDS) performs well in detecting anomalies by analyzing the data. Growth of data and attacks are higher than analysis speed. As data mining techniques are quickly analyzing huge volume data, it is integrated with IDS to increase the efficiency of IDS with less execution time.

After surveying many research papers, it is observed that most researches in intrusion detection use SVM and ANN. Because SVM produces high accuracy with smaller dataset in IDS and its execution time is less and ANN is much more stable and reliable than other models and algorithms. Though data mining increases efficiency of IDS, still there are some loopholes. To rectify this, researchers try hybrid methods that perform better than single methods. In hybrid methods, high detection rate and low false rate can be accomplished. Still, more researches are to be carried out in this area to get better result and to meet the fast growing challenges in this field.

Acknowledgements. I sincerely thank my Guide Professor Dr. J. Gnana Jayanthi for her guidance and support given.

References

1. Kavitha, N., Boaz, B.: A survey on intrusion detection system using data mining techniques. Int. J. Innov. Res. Sci. Eng. Technol. (IJIRSET) **6**(Special Issue 11), 460–465 (2017). e-ISSN: 2319-8753
2. Josemila Baby, J., Jeba, J.R.: Survey paper on various hybrid and anomaly based network intrusion detection system. Res. J. Appl. Sci. **12**(3–4), 304–310 (2017). ISSN: 1815-932X
3. Yeo, L.H., Che, X., Lakkaraju, S.: Understanding Modern Intrusion Detection Systems: A Survey, Nov 2017. arXiv:1708.07174 [cs.CR]
4. Baravati, H.B., et al.: A new data mining-based approach to improving the quality of alerts in intrusion detection systems. Int. J. Comput. Sci. Netw. Secur. (IJCSNS) **17**(8), 194–198 (2017)
5. Liu, W.: Research of Data mining in Intrusion Detection System and the Uncertainty of the Attack. In: ISBN: 978-1-4244-5273-6/09/$26.00 ©2009 IEEE
6. Chaudhari, R.R., Patil, S.P.: A study on data mining & machine learning for intrusion detection system. Int. J. Adv. Res. Comput. Commun. Eng. (IJARCCE) **6**(2), 114–118 (2017)
7. Agrawal, S., Jain, G.: A review on intrusion detection system based data mining techniques. Int. Res. J. Eng. Technol (IRJET) **04**(09), 402–407 (2017). e-ISSN: 2395-0056
8. Chaudhari, R.R., Patil, S.P.: Intrusion detection system: classification, techniques and datasets to implement. Int. Res. J. Eng. Technol. (IRJET) **04**(02), 1860–1866 (2017). e-ISSN: 2395-0056
9. Kumarl, S., Yadav, A.: Increasing performance of intrusion detection system using neural network. In: The Proceedings of the IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), India, pp. 546–550 (2014). ISBN No. 978-1-4799-3914-5/2014
10. Mewada, A., Gedam, P., Khan, S., Reddy, M.U.: Network intrusion detection using multiclass support vector machine. Spec. Issue IJCCT **1**(2–4), 172–175 (2010)
11. Tang, Y., Krasser, S., He, Y., Yang, W., Alperovitch, D.: Support vector machines and random forests modeling for spam senders behavior analysis. In: Proceedings of IEEE Global Communications Conference (IEEE GLOBECOM 2008), Computer and Communications Network Security Symposium, New Orleans, pp. 1–5 (2008)
12. Singh, V., et al.: Intrusion detection system using data mining a review. In: Proceeding of 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication, pp. 587–592. IEEE, Piscataway (2016). ISBN: 978-1-5090-0467-6/16
13. Sawant, T.S. Itkar, S.A.: A survey and comparative study of different data mining techniques for implementation of intrusion detection system. Int. J. Curr. Eng. Technol (IJCET) **4**(3), 1288–129 (2014). e-ISSN 2277 – 4106
14. Eid, H.F., Darwish, A., Hassanien, A.E., Abraham, A.: Principle components analysis and support vector machine based intrusion detection system. In: The 10th International Conference on Intelligent Systems Design and Applications, Cairo, pp. 363–367 (2010)
15. Latha, S., Prakash, S.J.: A survey on network attacks and intrusion detection systems. In: International Conference on Advanced Computing and Communication Systems (ICACCS-2017), Coimbatore, India, 06–07 Jan 2017. ISBN: 978-1-5090-4559-4
16. Chauhan, A., et al.: Survey on data mining techniques in intrusion detection. Int. J. Sci. Eng. Res. **2**(7), 1–4 (2011)

17. Yusufovna, S.F.: Integrating intrusion detection system and data mining. In: International Symposium on Ubiquitous Multimedia Computing, Uzbekistan, pp. 256–259 (2008). ISBN: 978-0-7695-3427-5
18. Wankhade, K., et al.: An overview of intrusion detection based on data mining techniques. In: International Conference on Communication Systems and Network Technologies, pp: 626–629 (2013). ISBN : 978-0-7695-4958-3
19. El Moussaid, N.: Overview of Intrusion Detection Using Data-Mining and the Features Selection, Morocco (2014). ISBN : 978-1-4799-3824-7
20. Abdullah, A., et al.: Data mining approaches on network data: intrusion detection system. Int. J. Adv. Res. Comput. Sci. (IJARCS) **8**(1), 316–319 (2017)
21. Jain, N., Srivastava, V.: Data mining techniques: a survey paper. Int. J. Res. Eng. Technol. (IJRET) **02**(11), 116–119 (2013). e-ISSN: 2319-1163
22. Ramageri, B.M.: Data mining techniques and applications. Indian J. Comput. Sci. Eng. (IJCSE) **1**(4), 301–305 (2010). ISSN: 0976-5166
23. Desale, K.S., et al.: Efficient intrusion detection system using stream data mining classification technique. In: Proceeding of 2015 International Conference on Computing Communication Control and Automation, 469–473. IEEE, Piscataway (2015). ISBN: 978-1-4799-6892-3/15
24. Chaturvedi, P., Saxena, A.: A systematic literature survey on IDS. Int. J. Recent Innov. Trends Comput. Commun. (IJRITCC) **5**(6), 671–676 (2017). ISSN: 2321-8169
25. Subramanian, U., Ong, H.S.: Systematic review and comparison of anomaly based network intrusion detection systems based on efficiency. J. Emerg. Trends Comput. Inf. Sci. **4**(11), 844–851 (2013). ISSN 2079-8407
26. Goeschel, K.: Reducing False Positives In Intrusion Detection Systems Using Data-Mining Techniques Utilizing Support Vector Machines, Decision Trees, and Naïve Bayes for Off-Line Analysis. ISBN : 978-1-5090-2246-5/16/$31.00 ©2016 IEEE
27. Pan, S.: Developing a hybrid intrusion detection system using data mining for power systems. In: IEEE Transactions on Smart Grid, 1–10. IEEE, Piscataway (2015). ISSN : 1949-3053_c
28. Zhu, M., et al.: Intrusion Detection System Based on data mining for Host Log, pp. 1742–1746. IEEE, Piscataway (2017). ISBN : 978-1-4673-8979-2/17/
29. Zhao, Y., et al.: Realization of intrusion detection system based on the improved data mining technology. In: Proceeding of the 8th International Conference on Computer Science & Education (ICCSE 2013), Colombo, Sri Lanka, pp. 982–987, 26–28 Apr 2013
30. Kezih, M. et al.: Evaluation effectiveness of intrusion detection system with reduced dimension using data mining classification tools. In: Proceeding of 2nd International Conference on Systems and Computer Science (ICSCS), Villeneuve d'Ascq, France, 26–27 Aug 2013
31. Mahapatra, B., et al.: Self adaptive intrusion detection technique using data mining concept in an Ad-Hoc network. In: Proceeding of 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016). Procedia Computer Science, vol. 92, pp. 292–297 (2016)
32. Mohammed, M.N., Sulaiman, N.: Intrusion Detection System Based on SVM for WLAN, pp. 313–317. Published by Elsevier Ltd, Malaysia (2012). ISSN: 2212-0173 © 2012
33. Farnaaz, N., Jabbar, M.A.: Random forest modeling for network intrusion detection system. In: The Proceedings of the Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016), vol. 89, pp. 213–217. Published by Elsevier, India (2016). ISSN : 1877-0509
34. Hasan, M.A.M., Nasser, M., Pal, B., Ahmad, S.: Support vector machine and random forest modeling for intrusion detection system (IDS). J. Intell. Learn. Syst. Appl. **6**, 45–52 (2014)

35. Ravale, U., Marathe, N., Padiya, P.: Feature selection based hybrid anomaly intrusion detection system using K means and RBF Kernel function. In: International Conference on Advanced Computing Technologies and Applications (ICACTA-2015), vol. 45, pp. 428–435. The Journal Published by Elsevier (2015). ISSN: 1877-0509
36. Jianliang, M., Haikun, S., Ling, B.: The application on intrusion detection based on k-means cluster algorithm. In: International Forum on Information Technology and Application, pp. 150–152. IEEE, Piscataway (2009)
37. Somwang, P., Lilakiatsakun, W.: Computer network security based on support vector machine approach. In: 11th International Conference on "Control, Automation and Systems (2011)
38. Xie, Y., Zhang, Y.: An intelligent anomaly analysis for intrusion detection based on SVM. In: International Conference on Computer Science and Information Processing (CSIP), pp. 739–742. IEEE, Piscataway (2012)
39. Tiwari, S.K., Sharma, S.K., Pande, P., Sisodia, M.S.: An improved network intrusion detection technique based on k-means clustering via naïve bayes classification. In: International Conference on Advances in Engineering, Science and Management (ICAESM) (2012)
40. Al Amrani, Y., Lazaar, M., El Kadiri, K.E.: Random forest and support vector machine based hybrid approach to sentiment analysis. In: The First International Conference on Intelligent Computing in Data Sciences, vol. 127, pp. 511–520. Published by Elsevier B.V., Morocco (2018). ISSN : 1877-0509
41. Belavagi, M.C., Muniyal, B.: Performance evaluation of supervised machine learning algorithms for intrusion detection", In the Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016), Procedia Computer Science, vol. 89, pp. 117–123. Published by Elsevier B.V. (2016). ISSN : 1877-0509
42. Zaman, S., Karray, F.: Feature selection for intrusion detection system based on support vector machine. In: 6th Annual IEEE Consumer Communications & Networking Conference IEEE CCNC (2009)
43. Kukielka, P., Kotulski, Z., Analysis of the different architectures of neural networks usage for Intrusion Detection Systems. In: Proceedings of the International Multiconference on Computer Science and Information Technology, IMCSIT 2008, pp. 807–811. IEEEXplore (2008)

Implementation of Reputation Based Framework for Detecting Misbehaving Nodes and Illustration of Vampire Attack in Manets

Hasansab Sheikh[1], V. Geetha[1(✉)], and S. A. Hariprasad[2]

[1] Information Science and Engineering, RVCE, 59 Bengaluru, India
[2] Jain University, Bengaluru, India

Abstract. A Mobile ad-hoc Network is set of nodes which are self organized in a wireless system. The attack on the network will be either attack or passive attack. The malicious node in the network can act as a base node for vampire attack which drains the life of other nodes in the network. In this study, we have proposed a reputation based framework for detecting malicious and selfish nodes in manets using AODV and PLGP protocol and illustrating several cases on how vampire attack can be prevented in the network using backtracking technique.

Keywords: PLGP (Parno, Luk, Gaustad and Perrig) · AODV · Backtracking technique (BT) · Reputation based framework

1 Introduction

The development of electronic devices since 1990s like PCs PDAs, Wi-Fi systems made MANETs a well known research subject [8]. MANETs are infrastructure-less remote framework, i.e. they don't require a base station to convey what's more, can be sent quickly to any remote spots. They don't have central controller, consequently the hubs move unreservedly toward any path [12]. This prompts interesting and correspondence challenges in MANETS. MANETs are organized in such a way that the hub which is a companion can speak with other friend just in the event that they achieve each other's range [11]. MANETs are additionally self-healing and self-configurable networks. Each node performs three duties: as a router or host or as an intermediate node. Each node is independent of other node, hence it can move freely in the network. The presence of each node in the network is determined with the energy constraint assigned. Every node energy drains down quickly because each node acts as a router or an intermediate node [9]. The energy usage of every node acts as a key attribute to keep the node and network active or alive. The routing protocol plays major role in transmission of packet from source to destination [1, 5]. There are several protocols such as DSR protocol. There are several approaches used for detecting the attacks on the MANETs like: Watchdog, intrusion detection system and random feedback. Components of detecting intrusion in the network involves: Data Collector, Detection Engine and Alarming System [2].

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 861–869, 2020.
https://doi.org/10.1007/978-3-030-37051-0_96

PLGP [3] a clean-slate sensor network routing protocol by Parno Luk Gaustad perrig. PLGP consists of two phases: Topology discovery and packet forwarding phase. Initially during discovery phase each node knows only itself. Nodes discover their neighbors using local broadcast and starts expanding. Throughout this phase, tree like structure is built that is later used for routing and addressing.

The proposed system includes two routing protocols such as PLGP and AODV. The main objective of the paper is to detect malicious nodes and selfish nodes using reputation based framework and prevention from vampire attack.

2 Related Work

Many research and related approaches are proposed for detection of misbehaving nodes. Some of them illustrates the concept only for malicious node and some for only selfish nodes, but none of paper proposed describes reputation based framework for detection of abnormal nodes in the network and prevention from vampire attack.

Sathya Bama [4] proposes an algorithm called chord algorithm, which is a structured protocol. To give P2P Nodes Service in Mobile Adhoc Network Chord is connected in MANET. The real preferred stand point of Chord calculation is sending, forceful update, bootstrapping and overlay broadcasting. Chord in MANET may be effective, in light of the fact that it isn't just giving direct routing yet in addition gives indirect routing.

Momin Kashif [7] proposes the detection of selfish behaviour in the node on essential attributes such as routing and packet dropping. The proposed system increase in detection ratio and packet delivery ratio. Here each node independently monitors the packet forwarding behaviour to neighboring node. The proposed system was simulated in NS-2 and results show that the scheme is highly robust and has performance improvement.

Verma [3] proposes a system to investigate vampire attack and implemented a framework to improve the performance. Vampire attack uses RREQ flooding and packet to establish malicious node connection. At the point when attack is exploited the quantity of broadcast counter is increased and threshold values are determined. Based on this misbehaving nodes are removed from network.

Kargl [6] proposed different sensors to detect misbehaving nodes in network. Multiple sensors are running in parallel and a selfish behaviour of node is detected by these sensors, then that node is marked as misbehaving node and further could not participate in the routing process again. All the threshold values are set manually.

Nimje [10] proposes the concept of clustering, where entire network is divided in to clusters, and every cluster has cluster head that is used to send and receive packets. Every node is assigned with selfish node and normal node such as friend and enemies. Every friend node send packet to enemy node, and enemy node act selfish and does not forward the packet to other nodes. Watchdog process in used and hence the proposed system may fail in complex networks.

3 Proposed Work

The aim of this paper is to detect malicious node and selfish node using reputation based framework, and prevention from vampire attack which uses malicious node in the network to drain life of nodes present in network. Reputation based framework proposed as illustrated below: (Fig. 1)

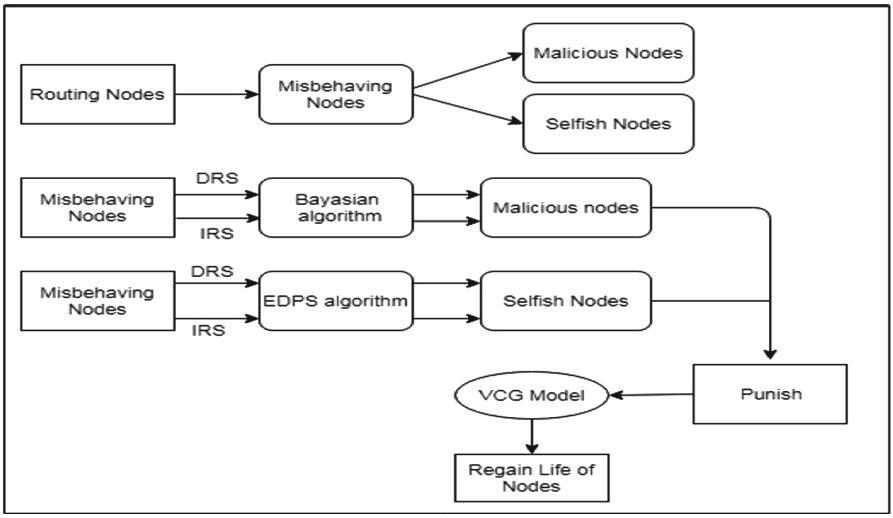


Fig. 1. Reputation based framework

The proposed system consist of two algorithms and two routing protocols namely EDPS (extensive deep packet scrutiny) algorithm with AODV as a routing protocol and Bayasian algorithm with PLGP as a routing protocol. Here reputation based framework and EDPS algorithms are integrated to enhance the security of the network.

3.1 Final Reputation Score Calculation

Both Algorithm_FRS_Selfish and Algorithm_FRS_Malicious algorithms are used to calculate the final reputation score of each node individually present in the network using direct and indirect reputation score of the node.

Direct reputation score calculation

Direct Reputation Score of a node 'n' is calculated based on the ratio of packets received to that of packets transmitted for a given time.

Indirect reputation score calculation

Indirect reputation score of a node 'n' is calculated based on the node history behavior to that of neighboring nodes i and j. (Table 1)

Table 1. Simulation parameters

Parameter	Value
Channel	Wireless channel
Network simulation tool	NS2
Topology dimension	1000 * 1000 (m)
Number of nodes	30, 40
Simulation time	50 s
Antenna model	OmniAntenna
Speed	0.5 (m/s)
MAC type	802_11

Algorithm_FRS_Selfish(node n)// Selfish node Detection

```
Start
Set of nodes N={N1,N2.....Nn}
Initialize set of nodes with reputation value DRS=1.0
Initialize local watchdog system node behavior
for i=1 to N do
        Discover neighoring nodes
        Check for node behavior with DRS and IDRS
İf  (Node i and j do not communicate) then
 Node ‘n’ is selfish node
   DRS[n]=1.0
Else
         İf FRS[n]>DRS[n] then
                Calculate DRS[n] using equation 1
                Calculate IDRS by applying DRS values in equation 2
                FRS[n]= DRS[n]+IDRS[n]
         End if
    End if
 End for
End
```

3.2 Formulae Used

Direct Reputation Score: Formula used to calculate Direct Reputation score is as given below:

$$DRS_{ij}[n] = |\beta^f \times w1 \times S_{P_{ij}}[n] + w2 \times 1 - R_{P_{ij}}[n] + w3 \times CD_{ij}[n] + w4 \times 1 - TF_{ij}[n] + w5 \times HP_{ij}[n] + 1 - TF_{ij}[n] \times DRS_{ij}[n-1]| \quad (1)$$

Where $S_{P_{ij}}[n]$ = no. of packets successfully transmitted from source to destination, $R_{P_{ij}}[n]$ = packet rate, $CD_{ij}[n]$ = data consistency, $TF_{ij}[n]$ = time frequency, $HP_{ij}[n]$ = Hello packets sent and ACK, β^f = network field, $w1, w2, \ldots\ldots, w5$ are the weights assigned.

Indirect Reputation Score: Formula used to calculate Indirect Reputation score is as given below:

$$IDRS_{ij}[n] = \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} DRS_{ij}(n)}{N} + \beta^f \quad (2)$$

Algorithm_FRS_Malicious(node n)// Malicious node Detection

```
Start
Set of nodes N={N1,N2.....Nn}
Initialize set of nodes with reputation values DRS=1.0
Set Destination node=s[i]
for i=1 to N do
      Discover neighoring nodes
      Check for node behavior with DRS and IDRS
if (node i do not communicate with node j) then
    if(Route discovery does not equal to s[i]) then
        node 'i'is malicious node
        DRS[n]=1.0
    Else
       İf FRS[n]>DRS[n] then
            Calculate DRS[n] using equation 1
            Calculate IDRS by applying DRS values in equation 2
            FRS[n]= DRS[n]+IDRS[n]
       End if
     End if
  End if
End for
End
```

3.3 Vampire Attack Cases

Vampire attack on network is executed with the help of malicious nodes in the network. Vampire attack uses Route Request Packet (RREQ) to establish connection with malicious node. There are certain cases where vampire node drains the life of normal nodes in the network as discussed below:

Case(i) Both Source and destination are free from vampire attack.
Case(ii) Both Source and destination are under vampire attack.
Case(iii) Source is under vampire attack and destination is free from attack.
Case(iv) Source is free from attack and destination is under vampire attack.

Case(i) Here both source and destination are free from vampire attack, here after the detection of misbehaving nodes, data will be safely routed from source to the destination.

Case(ii) Here both source and destination are under vampire attack, hence there is use of backtracking technique, where the source and destination node will be re-routed. During the transmission each node verifies the identity of source using backtracking process.

Case(iii) Here source is under vampire attack and destination is free from attack. In this case when source is down, energy value is assigned dynamically to source node, hence the transmission continues to destination.

Case(iv) Here destination is under vampire attack and source is free from attack. In this case when destination is down, energy value is assigned dynamically to destination node, hence the transmission continues from source to destination.

4 Results and Discussion

The simulation is done using Network Simulator 2, dynamic environment where nodes are spreaded around the network. The results describe the identification of misbehaving nodes using reputation based framework in the network and illustration of vampire attacks on the nodes with different cases.

4.1 Throughput Comparison and Simulation Results

Figure 2 shows the simulation graph throughput for detecting intruders nodes in network without using reputation based framework. The system uses AODV as a routing protocol and accuracy for detecting misbehaving nodes is about 65%.

Figure 3 shows the throughput graph using reputation based framework. The proposed system uses AODV and PLGP as a routing protocol and accuracy for detecting misbehaving nodes is about 75–85%.

Figure 4 shows the simulation of which is captured at the particular time of simulations. Here set of nodes spreaded across the network. Malicious nodes and Selfish nodes in the network are identified and prevented from the routing process. It demonstrates the **case(i)** in vampire attack where both source and destination are free

from being attacked by vampire node, hence packet is securely transmitted from source node(0)-6-18-33-(22) being destination.

Figure 5 İt illustrates the **case(ii),** where both source and destination are under attack by vampire node, hence using backtracking technique, the data is re-routed from different source to destination. As shown in figure data is transmitted from source node (7)-3-1-9-(2)being destination (Figs. 6, 7, 8, 9).

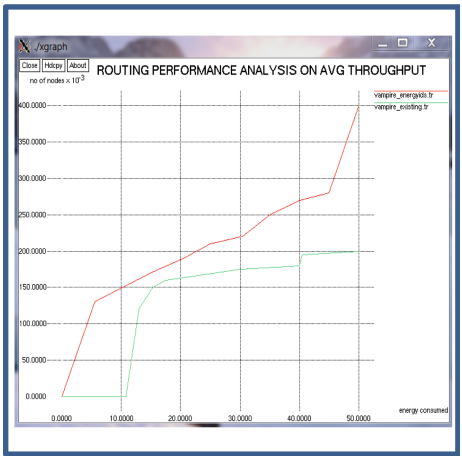


Fig. 2. Throughput without reputation based framework

Fig. 3. Throughput using reputation based framework

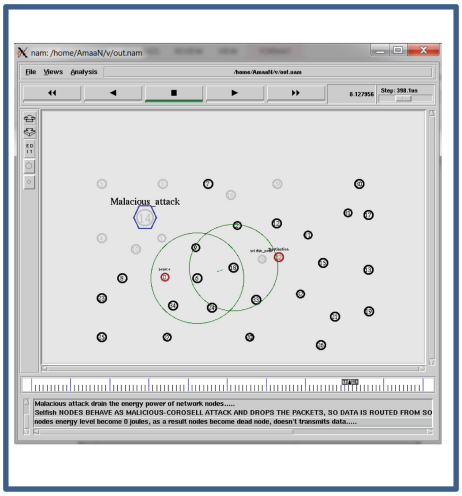


Fig. 4. Illustrates **Case(i)** transmission of data from source to destination

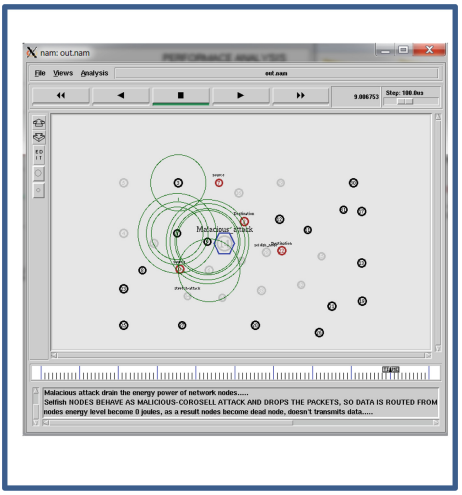


Fig. 5. Illustrates **Case(ii)** transmission of data from source to destination using BT

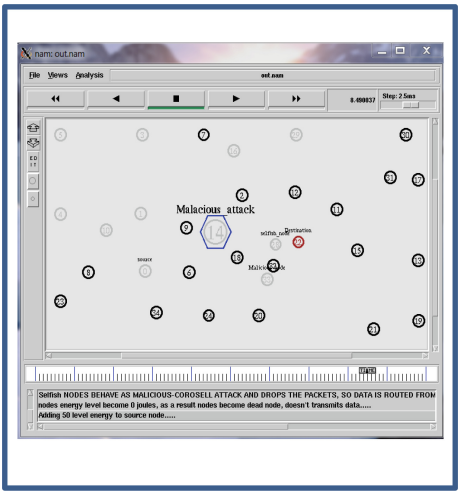


Fig. 6. Illustrates **Case(iii)** where source node is under attack

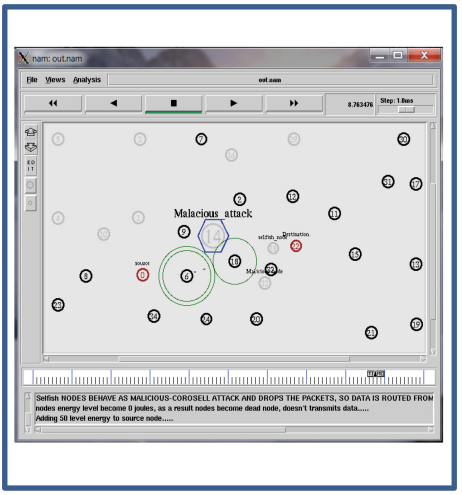


Fig. 7. Adds energy value dynamically to source node

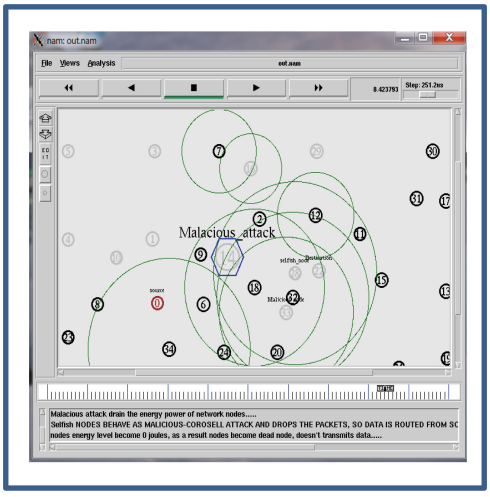


Fig. 8. Illustrates **Case(iv)** where destination node is under attack

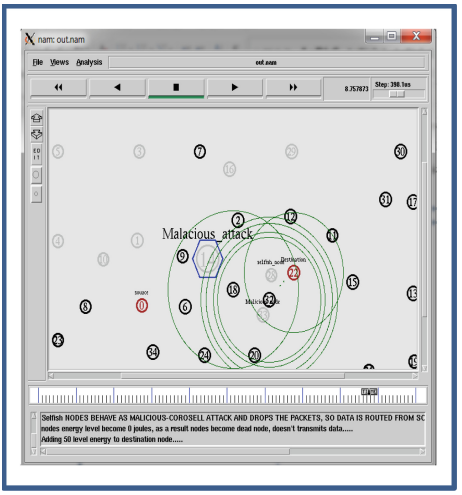


Fig. 9. Adds energy value dynamically to destination node

5 Conclusion and Future Work

The security of nodes present in the network is a major issue to improve the Quality of data transmission from source to destination.

In this paper we have proposed a reputation based framework which detects both malicious nodes and selfish nodes in the network, and illustration of all the cases which are caused by vampire nodes to the honest nodes. Hence future work will be adapting concept of regaining the life of lost nodes or drained out nodes using VCG model to again participate in routing process.

References

1. Mohammed, N., Otrok, H., Wang, L., Debbabi, M., Bhattacharya, P.: Mechanism design-based secure leader election model for intrusion detection in MANET. IEEE Trans. Dependable Secure Comput. **8**(1), 89–103 (2011)
2. Liu, J., Yu, F.R., Lung, C.-H., Tang, H.: A framework of combining intrusion detection and continuous authentication in mobile Ad Hoc networks. In: 2008 IEEE International Conference Communications, pp. 1515–1519 (2008)
3. Verma, D., Singh, G., Patidar, K.: Detection of vampire attack in wireless sensor networks. Int. J. Comput. Sci. Inf. Technol. **6**(4), 3313–3317 (2015)
4. Sathya Bama, B., Indira, K.: Detection of selfish and malicious node in mobile Ad-Hoc network with NS-2 using chord algorithm. Int. J. Eng. Technol. **9**(2) (2017)
5. Mayur, M., Lathi Garab, L.A.M.: Wormhole attack detection and prevention technique in mobile Ad-hoc network: a review. Int. J. Innov. Emerg. Res. Eng. **2**(2), 2015
6. Kargl, F., Klenk, A., Schlott, S., Weber, M.: Advanced detection of selfish or malicious nodes in Ad Hoc networks. Springer, Berlin (2005). ISBN: 3-540-24396-8 978-3-540-24396-0
7. Momin Kashif, M., Kadam, V.S.: Improved collaborative watchdog system for detection of selfish node in MANET. Int. J. Sci. Eng. Technol. Res. (IJSETR) **5**(2) (2016)
8. Geetha, V., Hariprasad, S.A., Vanke, P.: Reputation based extensive deep packet sc-rutiny algorithm for detecting selfish nodes in MANETs. Springer Nature (2019)
9. Sampada, H.K., Shobha, K.R.: Performance analysis of energy-efficient MANETs-using modified AODV (M-AODV). Int. Conf. Comput. Netw. Commun. Technol. 978-981-10-8681-6_9
10. Nimje, C., Junghare, P.: Detection of node activity, selfish & malicious behavioral patterns using exwatchdog algorithm. Int. J. Eng. Sci. Comput. **7**(3), (2017)
11. Savitha, M., Manavalan, R.: Efficient data transmission using energy efficient clustering scheme for wireless Ad-Hoc sensor network. Int. J. Comput. Trends Technol. (IJCTT) 17(2) (2014)
12. Girdhar, V., Banga, G.: A incentive based scheme to detect selfish nodes in MANET. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **5**(8) (2015)

Design and Implementation of Smart Mirror for Pilot Assistance

G. Dhanalakshmi[1(✉)], T. BalaGuru[2], T. Selvakumar[2], and A. Mohammed Imran[2]

[1] Ashoka Institute of Engineering and Technology, Hyderabad, Telangana, India
dhanarjun@gmail.com

[2] Aeronautical Engineering, Sri Ramakrishna Engineering College, Coimbatore, India
{balaguru.1508006, selvakumar.1508040, mohammedimran.1508025}@srec.ac.in

Abstract. In modern world, high performance is achieved with the advancement of science and technology. In the fast way of life, the developments of automation projects are required. Automation systems are mainly developed by using Internet of Things. Likewise, the project represents the implementation of the Smart Mirror for an individual use instead of a normal mirror. The project is based on the Intel Atom Processor- Z-series which runs with the help of an open source operating system. Using speech processing techniques, the pilot can interact with the Smart Mirror through verbal commands. It actively listens to the pilot's command and once the subsequent voice command is recognized, it performs the function associated with it. Smart Mirror provides common functionalities such as daily weather, time corresponding to the location, using social applications and more. The Smart Mirror can make the people to use other devices with low contribution and get them the entire world into hands through their voice commands itself.

Keywords: Smart mirror · Intel atom processor · IOT · Mobile internet devices · LCD HD · Sensor

1 Introduction

Recently there has been a growing interest in Internet which changed our lives by bringing the entire world into hands. Mobile phones had become smart phones and then this concept has turned into Internet of Thing. The concept of a smart mirror that the user can interact with is attractive and is more in fantasy movies [1].

Home Mirror is developed by electronic people with changing degrees of interactivity. This project describes the method of building a smart mirror using an Intel atom processor and the android operating system. The aim of the project is to design a Mirror that user could interact with it and also to develop further so that new applications would be developed and installed. Finally the results are good because the level of interactivity is being achieved with the help of voice commands through the microphone of a smart phones [2]. A few hurdles are being faced in the construction of

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 870–875, 2020.
https://doi.org/10.1007/978-3-030-37051-0_97

hardware and software of the project and those drawbacks are rectified by making many trails for the future development of the smart mirror.

2 Literature View

The smart mirror with artificial assistance is designed and developed for commercial uses as well as security purposes in various industries. The project collects real world data and the data is processed by the Intel atom processor. The Smart Mirror which is used as digital personal assistance device is made with equipments such as Intel atom processor, microphone, HD Screen covered with a sheet of reflective one-waymirror provides the basic information like in other electronic gadgets such as daily weather of the city, time corresponding to the location. The speech processing techniques in the speech application makes the Mirror to interact using verbal commands, functions and responds them instantly. ISSN: 2320-2084 (Volume-5, Issue-1, Jan. 2017).

The paper prevails that the development of a smart mirror which is more like an unobtrusive interface for the smart homes. Paper: Ambient Intelligence Vole 5, No 4 (2004).

3 Methodology

The smart mirror is a home mirror with an HD display behind it. The display can be an Android tablet or an HD display. Figure 1 shows the component available in the smart mirror.

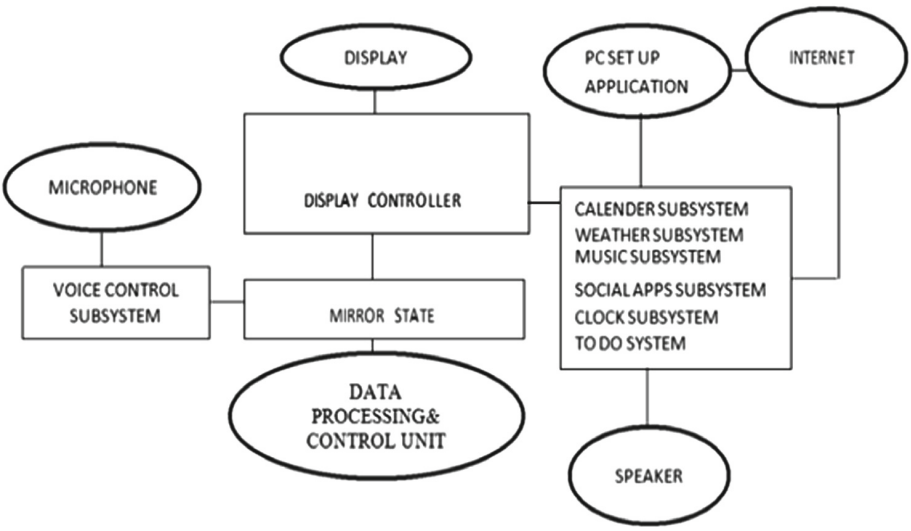


Fig. 1. Smart mirror component

The project collects real world data such as weather reports, time corresponding to the location etc., The data is sent from the machine and managed in a central database by the processing unit. The Smart Mirror which is used as digital personal assistance device is made with equipments such as Intel atom processor, microphone, HD Screen covered with a sheet of reflective one way mirror provides the basic information like in other electronic gadgets such as daily weather of the city, time corresponding to the location. The mirror display is provided by an HD display which displays all the necessary information which are useful to the user. A one way mirror is used to display the things located in front of the Smart Mirror using atom processor. As a result, the smart mirror gives the function of a regular mirror.

4 Workıng and Requirements

The objective is to provide an unobtrusive interface with artificial assistance for the individual convenience. It includes downloading the Android operating system and performing the following steps [3].

- The working is done by Intel atom processor.
- The screen can be an HD display.
- The project collects real world data.
- Use of speech application.
- Displays all the information which is asked by the user.
- One way reflective mirror is used.

4.1 Workıng

- Preparation of the display: HD display is unmounted and is adjusted for the project.
- Preparation of the aircraft Cabin: The cabin made up of wood holds the complete mechanism inside it [4].
- Mounting: The mirror and the HDdisplay are mounted on the cabin.
- Configuration of the processor: The Intel atom processor z-series is configured.
- Configuring Sound and then voice.
- Configuration of the smart mirror.
- Booting the android os on the processor.
- Voice Commands are used to run the Smart Mirror.

4.2 Requirements

4.2.1 Dısplay Unit

For the display a 14.1-inch HD screen display is used for its high graphics resolution. The resolution of the graphics display in the smart mirror is based on the width and height dimension of an electronic visual display device. A display of resolution 1366 × 768 displays photo or video content sharper with pixel art smaller [5].

4.2.2 Intel Atom Processor

Intel atom processors are mainly used in embedded applications ranging from health care to robotics. The Intel Atom x5-Z8350 is the power efficient quad-core SoC for Windows and Android [6–8]. It is clocked at 1.44–1.92 GHz. The SoC offers a Directx 11.2-capable GPU. The memory types this processor is LPDDR3 Memory Controller ($2 \times$ 4 bits and 25.6 GB/s) to the CPU cores. The processor in smart mirror uses the processor count to be 1. In this project, we used a graphics coprocessor called Intel HD Graphics 400 [6]. HD Graphics operates on the Intel Gen8 architecture supporting Directx 11.2. The GPU supports 4 K/H.265 video acceleration [9, 10].

- Microphone.
- Sensors.
- Wooden Frame.

5 Experimental Results

The proposed design of smart mirror used as a normal mirror and also bringing data when ever required based on the voice command of authorized pilot. The Fig. 2 shown the front panel of the product. Figure 3 states that the output given by the product based on request.

Fig. 2. Front panal

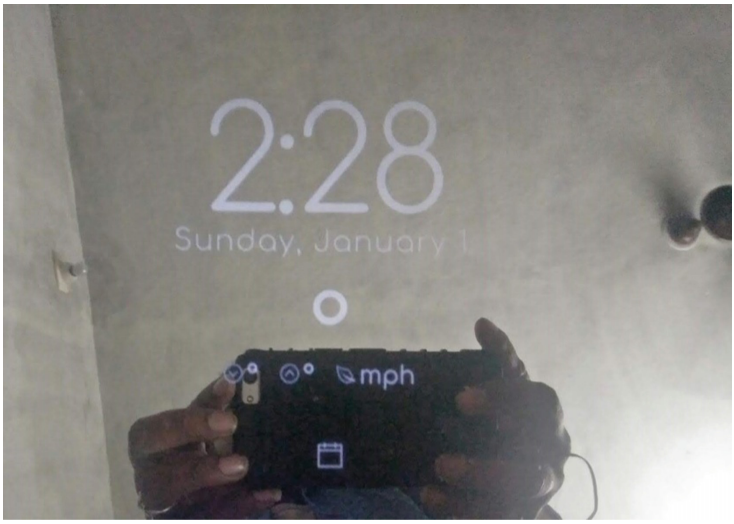


Fig. 3. Output from smart mirror

6 Conclusion

The Smart Mirror provides the pilot with a mirror experience. By making use of smart mirror, the pilot can update the time, weather while preparing for the day with the functioning of the Smart Mirror. Hence the smart mirror that provides interaction between pilot in the aircraft moving in the air and the base station in the earth. The Smart Mirror makes the people to use other devices with low contribution and get them the entire world into hands through their voice commands itself. In the future we would design a separate store to download and install smart mirror applications such as play store and google store, apple store etc., For security purpose, pairing the smart devices with mirror using a QR code is also under construction.

References

1. Emiliani, P.L., Stephanidis, C.: Universal access to ambient intelligence environments: opportunities and challenges for people with disabilities. IBM Syst. J. (2005)
2. Raisinghani, M.S., Benoit, A., Ding, J., Gomez, M., Gupta, K., Gusila, V., Power, D., Schmedding, O.: Ambient intelligence: changing forms of human computer interaction and their social implications. J. Digital Inf. **5**(4) (2004)
3. Poh, M.Z., McDuff, D., Picard, R.: A medical mirror for non-contact health monitring. In: ACM siggraph 2011 Emerging Technologies SIGGRAPH'11, NewYork, USA. ACM (2011)
4. Emiliani, P.L., Stephanidis, C.: Universal access to ambient intelligence environments: opportunities and challenges for people with disabilities. IBM Syst. J. (2005). "What is a Raspberry Pi?" Raspberry Pi What Is a Raspberry Pi Comments. Accessed 06 May 2016. https://www.raspberrypi.org/help/what-is-a-raspberry-pi/

5. Internet of Things Global Standards Initiative. ITU. Accessed 26 Apr. 2016. http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
6. Maker Culture (chapter in Innovating Pedagogy 2013). The Open University (April 2016). http://www.open.ac.uk/people/my-profile
7. Cohen, E.: Smart Mirror. http://smart-mirror.io/
8. Mittlestaedt, H.: Homemirror. https://github.com/HannahMitt/HomeMirror
9. Sukeda, H., Horry, Y., Maruyama, Y., Hoshino, T.: Information accessing furniture to make our everyday lives more comfortable. IEEE Trans. Consum. Electron. Consum. Electron. **52** (1), 173–178 (2006)
10. Ding, J.R., Huang, C.L., Lin, J.K., Yang, J.F., Wu, G.H.: Interactive multimedia mirror system design. IEEE Trans. Consum. Electron. **54**(3), 972–980 (2008)
11. Yusri, M.M., Kasim, S., Hassan, R.: Smart mirror for smart life. In: 2017 6th ICT International Student Project Conference, 23 Oct. 2017 (2017). ISBN: 978-1-5386-2996-3
12. Nathan, S.S., Sulaiman, A., Kamarulzaman, A.A., Tiera, F., Berahim, M.: Brilliantreflect: smart mirror for smart life. Int. J. Electr. Comput. Eng. (IJECE) **9**(3), 1663–1668 (2019)

A Novel Hybrid RNN-ELM Architecture for Crime Classification

K. B. Sundhara Kumar(✉) and N. Bhalaji

SSN College of Engineering, Chennai, India
{sundharakumarkb, bhalajin}@ssn.edu.in

Abstract. Extreme Learning Machine (ELM) is a single layer feedforward neural network (SLFN) that has shown remarkable results in regression and classification (multi-class) problems. The theories on ELM indicates that the hidden neurons can be randomly generated. In this paper, we introduce a hybrid Recurrent Neural Network(RNN) – ELM hybrid structure for crime hotspot classification. The RNN extracts the features from the data and learns using Long Short-Term Memory (LSTM) and finally ELM is applied at the end of the layers for our classification problem. The dataset used for this study is Philadelphia's crime data. The dataset is also tested with RNN using back-propagation without ELM. With ease of implementation, fast learning speed and better accuracy, RNN-ELM clearly outperformed RNN with backpropagation.

Keywords: Classification · Recurrent neural networks · Back propagation · LSTM · Extreme learning machine · Crime hotspots

1 Introduction

Crime hotspot analysis is increasingly becoming popular among researchers. One of the core areas in crime hotspot detection is pattern analysis. It is a very tedious process to understand crime patterns and how they vary under different conditions. The methodology of understanding and analysing such patterns are not fully matured in real-world scenarios.

Crime usually is a well planned activity and it is not something which occur randomly. The theory of repeat-crimes state that a crime is prone to occur in a place where it has already occurred in near-past [1]. The crime data are analogous to time series data as the description of the crime and the period of occurrences are very much essential to capture the patterns. In recent days, deep learning algorithms are proving to be very effective in classification/regression problems. In this aspect, Recurrent Neural Networks (RNN) [2] and its variants are used predominantly for data that follows a sequence e.g.: Time Series data [3].

RNN are the networks that are capable of storing previous inputs and pass on this stored information to the next layer. So, whenever the data is sequential, RNN can be deployed. RNN is a special type of neural network that have loops in them. Typically, RNN comes with Backpropagation through time (BPTT), which helps in adjusting the weights of nodes in the hidden layer. The vanishing gradient problem of RNN was solved by using Long Short Term Memory (LSTM). The LSTM network unit act as a

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 876–882, 2020.
https://doi.org/10.1007/978-3-030-37051-0_98

memory unit which stores the prior information for a short span of time. This is very effective in identifying crime patterns especially the repeat-crimes as there is a need to capture the information about a similar crime occurring in the near-past. In order to improve the accuracy of predictions through RNN-LSTMs, plethora of works are carried out by various researchers.

Extreme Learning Machine (ELM) [4] is a single layer feedforward neural network (SLFN) that has shown remarkable results in regression and classification (multi-class) problems. The hidden layer biases and the input weights are randomly generated. ELM has been proved to be an efficient algorithm because of its capability to learn from the data quickly, better training speed and very minimal human intervention [5].

In this paper, we propose a novel hybrid RNN-ELM algorithm structure to leverage full advantage of both RNN and ELM. This hybrid architecture not just exploits the two algorithms but it is also used for crime classification. The hybrid architecture also prevents overfitting to a larger extent than the classical RNN. The dataset used for this analysis is Philadelphia's crime data [6]. However, the dataset is first segregated into three classes namely hotspot, coldspot and warmspot based on cluster analysis. With ease of implementation, faster training speed and better accuracy, RNN-ELM cleary outperformed RNN with backpropagation dropout. The reminder of this paper is organized as follows: Sect. 2 provides the reviews of existing works. Section 3 explains our proposed hybrid architecture model and Sect. 4 discusses the results. The conclusion has been provided in Sect. 5.

2 Related Works

Thangavelu et al. [7] used GIS implementations for analyzing spatial distributions of rural crime. The work focused on allocation of police stations, assigning boundaries to the police station, identifying the crime rate and density in specific locations, top five prominent crime types, etc. for Coimbatore rural police stations. The crime rate in that jurisdiction was calculated by dividing the number of crimes in the area by the total population of the area. The authors concluded that these GIS implementations would provide effective insight on the jurisdiction that might need more police intervention to avoid a crime from occurring. Sundharakumar and Bhalaji [8] suggested some methods for crime classification.

Tayal et al. [9] proposed a method for the design and implementation of crime detection and criminal identification for Indian cities using data mining techniques. The work comprises of data extraction, data pre-processing and clustering techniques for extracting the unstructured crime dataset from various web sources. The authors used 7 Indian cities under study based on the maximum amount of crime (in percentage). K-Means clustering algorithm was implemented for looking into underlying patterns and relations in the crime data. The results were validated using WEKA tool. They concluded that their tool Crime detection and criminal identification (CDCI) could speed up the crime solving process by processing and filtering the voluminous data within a short span of time.

Wang et al. [10] studied on forecasting crime data using deep learning algorithms. The authors compared predictable events with crime and came to a conclusion that crime predictions were sparse. They also suggested that at different spatio-temporal scales, the crime distributions exhibited different patterns. The authors adapted an existing state-of-art deep learning method called ST-Resnet that was proposed by Zhang et al. [11]. The methods used by them had Convolutional Neural Network (CNN). The authors collected crime records of LA for the last six months of year 2015. They performed a spatio-temporal analysis due to low regularity in the crime data and concluded that using a CNN, they acquired more accuracy.

ELM [4, 5, 12] is emerging to be one of the most prominent methods in machine learning. It was first formulated as a single layer feed forward neural networks [13]. Huang et al. [4] proposed the ELM which was used primarily because of the lesser training error and better generalization performance than the Backpropagation algorithm. The hidden node parameters in ELM are randomly generated prior to obtain the train data [14]. Minimum training error, minumum norm of weights and faster training process makes the ELM models more credible.

Though ELM has lot of advantages, using it along with other machine learning or deep learning algorithms provide better results than deploying ELM separately. The novelty of this work encompasses the usage of deploying a hybrid deep learning algorithm – RNN and ELM by leveraging the advantages of both the techniques.

3 Hybrid Architecture of Our RNN-ELM Model

İn this section, we describe our hybrid architecture of RNN-ELM model. As discussed in the earlier section, ELM is a single layer feed forward neural network which can be observed in Fig. 1. The ELM contains an input layer, a hidden layer with 'n' neurons and an output layer.

For N distinct observations of (x_i, y_i), where x_i are the neurons in the input layer and y_i are the neurons in the output layers, the standard ELM can be defined as:

$$\sum_{i=1}^{n} \beta_i g_i(x_j) = \sum_{i=1}^{n} \beta_i g(w_i * x_j + b_i) = y_j \tag{1}$$

where j = 1,2…N, w_i represents the weights associated with input neurons and the i^{th} hidden neurons, βi are the weights connecting the i^{th} hidden neurons and the output layer, b_i's are the bias vector.

The weights and bias are randomly generated for the ELM. A generic form of Eq. 1 can be written as shown in Eq. 2

$$H\beta = Y \tag{2}$$

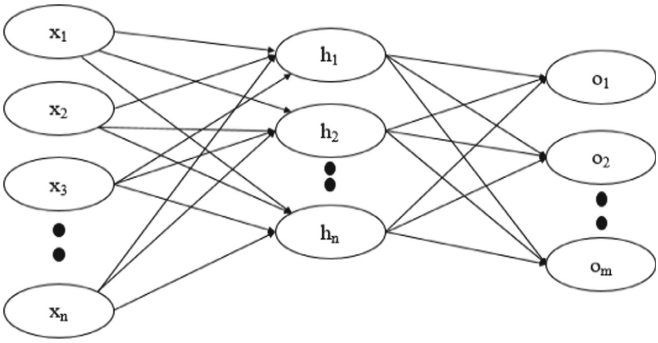


Fig. 1. Single layer feedforward neural network (ELM architecture)

With the randomly assigned values to the weight vector wi and bias b, the output vector H is determined. Then the output weight β can be found using Eq. 3.

$$B = H'Y \tag{3}$$

where H′ is the Moore-Penrose generalised inverse of the matrix H.

ELM is widely used in regression and classification problems. In our usecase, ELM is used for multi-class classification. Our hybrid architecture involves Recurrent Neural Network with LSTM which can extract relevant features, store and remember the intermediate results and ELM can be used for classifying the crime.

3.1 Design of RNN-ELM Hybrid Architecture

The aim of this paper is to leverage the advantages of using Recurrent Neural Network and Extreme Learning Machine. The data that is used for this study is Philadelphia's crime data [6]. The data from the source is preprocessed and clusted into three groups/classes. We assigned the three groups of clusters as hotspots, cold spots and warm spots. Hotspots are the regions in which there are very high crime rate, cold spots are those regions in which the crime rate has decreased due to increased policing activities and warm spots are those regions in which the crime rate is increasing, failing to monitor these regions could lead them to become hotspots. Repeat crimes can be modelled as a time series data since they are sequential, i.e., there is high possibility of a crime occurring in the region where it had earlier occurred (in recent past). This type of data requires an architecture which can store prior information. For this requirement, Recurrent Neural Networks are the apt architecture as they have LSTM which can store prior information and pass on that to the successive layers. Usually, a backpropagation mechanism would be used, which feeds back the output to the input layer again in order to increase the accuracy.

Our hybrid architecture is shown in the Fig. 2 below.

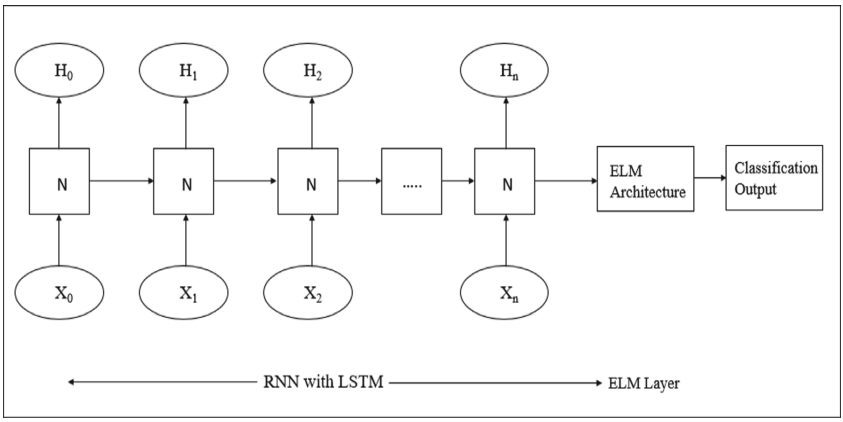


Fig. 2. RNN ELM Hybrid architecture

We propose to use ELM architecture after RNN for classification and provide a comparative analysis on how our RNN-ELM hybrid and traditional RNN with BP perform for the data under study.

4 Results and Discussions

In this paper, we provide a comparative analysis of RNN with Backpropagation and RNN-ELM hybrid architecture. The dataset contains 16000 records which is split into training dataset and testing dataset in the ratio of 70% & 30% respectively. Firstly, a RNN model is built for the training dataset. RNN with LSTM extracts relevant features from the dataset. Then the model is used to predict the classes for the test dataset upon which backpropagation (BP) technique is applied as a feedback to the trained model to improve the accuracy of the resultant model. Performance measures such as accuracy, precision and recall are calculated for the test dataset.

For the second part of our analysis, we retain the trained RNN model and the feature selection. Instead of applying the backpropagation, we apply the ELM at this juncture to predict the classes for the test dataset. We calculate the same performance measures such as accuracy, precision and recall. The Table 1 shows the performance measures for our dataset.

Table 1. Performance measure values

	Accuracy	Precision	Recall
RNN with BP	86.67	93.4	85
RNN with ELM	92.3	94.4	89.47

The Table 1 shows the performance measure values for the two different approach. The first row shows the accuracy, precision and recall values for RNN with Back-propagation technique and the second row shows the same values for RNN with ELM. Figure 3 below shows the visual form of the above table, i.e., performance measure values such as accuracy, precision and recall.

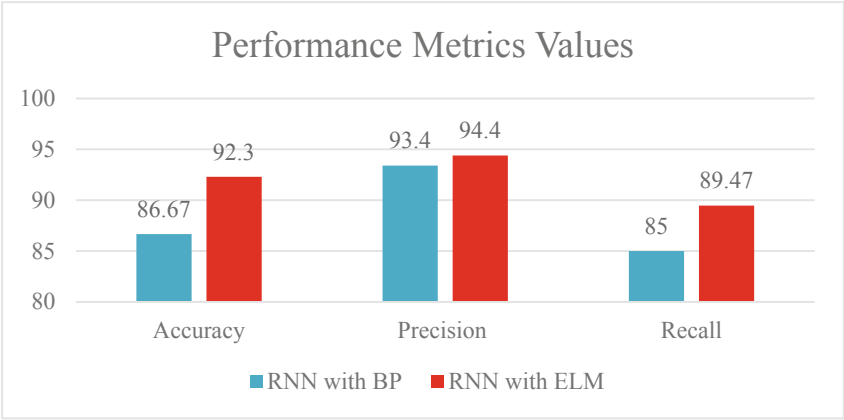


Fig. 3. Comparison of performance metrics

The accuracy of the model with traditional RNN is found to be 87% for the data under study, whereas the accuracy using our hybrid RNN-ELM is found to be 92.3%. It is very evident that RNN with ELM outperforms the traditional RNN with Back-propagation algorithm.

5 Conclusion

The RNN-ELM hybrid architecture is created to analyse the performance metrics of the dataset under our study. The crime classification is a very challenging task and hotspot analysis has already become one of the interesting research topics among researchers across the globe. RNN with LSTM network provides the feature extraction and also aids in classification. However, we introduce the ELM architecture in the end to add another layer of classification. A comparative analysis of RNN with BP and RNN with ELM is provided. The results indicates that RNN with ELM hybrid architecture show an increase in accuracy of the model.

References

1. Wang, T., et al.: Learning to detect patterns of crime. In: Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer, Berlin (2013)
2. Understanding Long Short-Term Memory. http://colah.github.io/posts/2015-08-Understanding-LSTMs/
3. Overview of Recurrent Neural Networks. https://www.analyticsindiamag.com/overview-of-recurrent-neural-networks-and-their-applications/
4. Huang, G.-B., Zhu, Qin-Yu., Siew, C.-K.: Extreme learning machine: theory and applications. Neurocomputing **70**(1–3), 489–501 (2006)
5. Huang, G.-B., Chen, L., Siew, C.K.: Universal approximation using incremental constructive feedforward networks with random hidden nodes. IEEE Trans. Neural Netw. **17**(4) 879–892 (2006)
6. Philadelphia's crime data. https://www.kaggle.com/mchirico/philadelphiacrimedata
7. Thangavelu, A., Sathyaraj, S.R., Balasubramaian, S.: Assessment of spatial distribution of rural crime mapping in India: A GIS perspective. Int. J. Adv. Remote Sens. GIS **2**(1), 70–85 (2013)
8. Sundhara Kumar, K.B., Bhalaji, N.: A study on classification algorithms for crime records. In: International Conference on Smart Trends for Information Technology and Computer Communications, pp. 873–880. Springer, Singapore (2016)
9. Tayal, D.K., Jain, A., Arora, S., Agarwal, S., Gupta, T., Tyagi, N.: Crime detection and criminal identification in India using data mining techniques. AI & Soc. **30**(1), 117–127 (2015)
10. Wang, B., Zhang, D., Zhang, D., Brantingham, P.J. and Bertozzi, A.L.: Deep learning for real time crime forecasting (2017). arXiv:1707.03340
11. Zhang, J., Zheng, Y., Qi, D.: Deep spatio-temporal residual networks for citywide crowd flows prediction. AAAI (2017)
12. Duan, M., Li, K., Liao, X., Li, K.: A parallel multiclassification algorithm for big data using an extreme learning machine. IEEE Trans. Neural Netw. Learn. Syst. **29**(6), 2337–2351 (2018)
13. Huang, G.-B., Ding, X., Zhou, H.: Optimization method based extreme learning machine for classification. Neurocomputing **74**(1–3), 155–163 (2010)
14. Duan, M., Li, K., Yang, C., Li, K.: A hybrid deep learning CNN–ELM for age and gender classification. Neurocomputing **275**, 448–461 (2018)

Cohort of Crowdsourcıng – Survey

N. Bhaskar[1(✉)] and P. Mohan Kumar[2]

[1] Department of IT, KCG College of Technology, Chennai, India
bhaskarannedumaran@gmail.com
[2] Centre for Resarch, Jeppiaar Engineering College, Chennai, India
mohankumarmohan@gmail.com

Abstract. Crowdsourcing is developing as a conveyed critical thinking and business creation in recent years. The expression "crowdsourcing" was authored by Jeff Howe in 2006. From that point forward, a great deal of work in Crowdsourcing has concentrated on various parts of publicly supporting, for example, computational procedures and performance analysis. Declarative crowdsourcing frameworks help diminish the complexities and conceal them from users and manages the weight of the crowd. Crowdsourcing has been a critical perspective with regards to locate a specific information in a database. Crowdsourcing gives an amazing platform to execute inquiries that require progressively human talents, insight and investigation rather than simply counterfeit canny computers, which use picture acknowledgment, information filtration and tagging. Crowd optimization realizes how to adjust among cost and latency and accordingly query optimization targets are increasingly effective. CROWDOPT for upgrading three sorts of questions: selectionquires, join quiries and complex quires. In this paper, we give the outline of the survey of Crowdsourcing worldview which are arranged by the Crowdsourcing operators and datasets. In view of this study we sketch the vital components that essential to be estimated to improve Crowdsourced data management.

Keywords: Crowdsourcing · Crowdsourcing operators · Query optimization · Datasets

1 Introduction

1.1 Crowdsourcing

Crowdsourcing has turned out to be exceptionally mainstream for the two governments and organizations to assemble information and sentiments. Crowdsourcing is essentially used to finish little assignments or get little bits of data, as bigger and increasingly complex undertakings are not appropriate to the stage. Crowdsourcing is utilized to depict the system of re-appropriating to a substantial group of free specialists instead of through a solitary element or organization. Crowdsourcing enables an organization to associate with a far reaching system of ability however foregoes huge numbers of the quality controls that normally exist when redistributing to a solitary organization. The principle disadvantage of crowdsourcing is an absence of value control. Particularly with microwork, crowdsourcing will in general be of low quality– it's for the most part

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 883–892, 2020.
https://doi.org/10.1007/978-3-030-37051-0_99

fit towards work that does not need to be done precisely but rather basically needs to complete. Crowdsourcers themselves have their very own arrangement of concerns, most moral and money related: crowdsourcers in general be from low-pay economies and some trust that their ability to work for such low rates is in effect unjustifiably promoted upon. Crowdsourcing is the way toward getting work or financing, normally on the web, from a horde of individuals. The word is a blend of the words 'crowd' and outsourcing. The thought is to take work and redistribute it to a horde of workers. Model: Social Media like Facebook, Twitter. People are presented the messages on their companions, relatives and so forth., this can't be accomplished by the car frameworks like labeling the picture.

1.2 Crowdsourcıng Data Through Mobıle Devıces

The huge infiltration of cell phones is a marker demonstrating their effect on our everyday life, saw by means of the assorted administrations offered through them. In the vitality area, they can be utilized as a device for bidirectional correspondence between the vitality presumes and the other for imagined on-screen characters in the Smart Grid. Most preliminaries today require extra equipment establishments at the client's side so as to gather metering information and use it for vitality improvement; anyway comparative data can be gained from the clients and by and large the nature of data might be similar or superior to anything the uninvolved techniques connected today (particularly while considering assessed future client conduct). We trust that cell phones can assume a key job in client helped information obtaining and forecast, just as enable methodologies managing investigation, imagine a scenario in which reenactments and so forth. In this limit Crowdsourcing, vitality data through the utilization of cell phones can fill in as an empowering innovation until the SmartGrid and its administrations are completely conveyed.

2 Taxonomy of Crowdsourcıng System

The Crowdsourcing classification discussed in this paper is:

2.1 Crowdsourcing Users
2.2 Database used in Crowdsourcing system
2.3 Query Optimization
2.4 Crowdsourcing Operators
2.5 Human Intelligent Tasks (HIT's).

2.1 Crowdsourcing Users

The Crowdsourcing system classifies into two different types of users namely: Requestors and Workers.

2.1.1 Requestors

Users (or requesters) submit micro jobs, frequently several at a time, and fixed a monetary price or incentive for Workers. At any point, there are various micro jobs on proposal in the fair. [R1]

2.1.2 Workers

Human workers attain at the fair at any time, and can leave at any time. When on the fair, workers can select to work on any of the available micro jobs. They are allowed to work on a single micro job at a time. Once they complete micro jobs, they will obtain the incentive or value assigned for the task by the Requester. [R1]

2.2 Database Used in Crowdsourcing System

- CrowdDB [5]
- Qurk data model [2]
- Deco's data model [3].

2.3 Query Optimization

Query Optimization is to work the query in various ways that it gives a similar outcome however the speed to recover the information increments. The inquiries ought to be proficient with the goal that information can be recovered in less time or getting to database turned out to be quick. There are elective approaches to play out the query that give a similar outcome. The best approach to play out the query should give the outcome in least time and should build the execution of the query.

Cost Components for Query Execution: [T1]

1. Access cost to secondary storage
2. Storage cost
3. Computation cost
4. Memory usage cost
5. Communication cost.

2.4 Crowdsourcing Operators

The Crowdsourcing operators are shown in the Table 1:

Table 1. Crowdsourcing operators

S. no	Operators	Description	References
1	Fill	Crowd Fill in missing values in databases	R1, R2
2	Selection	Filter items satisfying certain constraints	R6, R7
3	Join	Join between the tables and retrieved the results	R15, R16
4	TopK/Sort	Top answers-ranking/Sorting in either Ascending order or Descending order	R2
5	Aggregate functions	Max, Min (R4), Count (R9), Avg, Stddev, Group By (R12)	R4, R9, R12

2.5 Human Intelligent Tasks (HIT's) [R5]

A Human Intelligent Task, or HIT, specifies thetiniestunit of effort a worker mayagree to do. HIT's comprise single task or more tasks. The unit is splitted intoMicroTask and complete as HIT's in the Crowsourcing Platform.

CreateHuman_Int_Task(H_domain, H_spec,H_query,H_hint,H_pay, H_time, H_Bound_Assignment, validity)!

HitNo: Calling this method creates a new Human_Int_Task on the Crowdsourcing Platform. The CREATE Human_Int_Taskprocessyields HitNo to the requester is to find the HIT for all further communication. TheH_domain, H_spec, and H_payfields are used by Crowdsourcing Platform to associate HITs into HIT Groups.

The queryfactorsummarizes the user interface that workers use to find the answer for the HIT, containing HTML pages. The H_timeparameter specifiesto what extent the worker needs to finish a task in the wake of tolerating it. The validity attribute shows a measure of time after which the HIT will never again be accessible for workers to acknowledge. Requesters can likewise oblige the arrangement of workers that are permitted to process the HIT. CrowdDB, in any case, does not presently utilize this capacity so the subtleties of this and a few different parameters are excluded for curtness.

getAssignHIT(HitNo)!list(docID, workerId, response):

This strategy restores the answers of all assignments of a HIT that have been given by workers (maxAssignments solutions as indicated when the requester made the HIT). Every solution of a task is given adocID which is utilized by the requester to accept or cancel that task.

acceptAssignment(docID)/cancelAssignment(docID): Endorsement triggers the fee of the reward to the worker and the intermediate fee to Crowdsourcing Platform.

ForceTerminateHIT(docID): Terminates a HIT straightaway. Assignments that have just been acknowledged might be finished.

3 Survey on Declaratıve Crowdsourcıng

Several researchers worked to make crowdsourcing techniques to reduce cost and latency with different aspects which are briefed in this survey.

3.1 Crowdop: Query Optimization for Declarative Crowdsourcing Systems

Fan et al. [1] researched the query optimization issues in the declarative crowdsourcing systems. The methods like cost and latency are the performance metrics for the Query Optimization. The algorithms were developed for optimizing three types of queries: Selection queries join queries, and complex selection-join queries and it validated with the Crowdsourcing platform.

3.2 Crowdsourced Databases: Query Processing with People (Qurk)

Marcus et al. [2] researched for Crowdsourced Databases is a has studied the problem of the HIT's(Human Intelligent Tasks) workflow from the crowdsourcing platform between the requestor and worker. Requestor are the person who is issuing the HIT's to the crowdsourcing Platform and the workers are those who are answers posted by the requestors in the Crowdsourcing Platform. The team has briefed about the Crowd Database functions, Optimizations functions like Runtime Pricing, Input Sampling, Batch Predicates, Operator Implementations, Join Heuristics, Task Result Cache and Model Training and the Execution of the Queries.

3.3 Deco: Declarative Crowdsourcing

Parameswaran et al. [3] researched Deco is a system for getting the results from the Crowdsourced data answers along with the existing database. The team used the conceptual schema as a Data Model for the Crowdsourced Database. The concepts used are Fetch, Resolve, Join in Deco. Fetch is the retrieval of additional data for raw table using Fetch rules. Resolve is the conversion of incompatible raw data and make it compatible data. Join is used to outer join the compatible data from more than one table to produce the conceptual relation. In Deco model uses the "AtLeast n" clause is used to retrieve the data without empty value. By using "AtLeast n" Deco collects more values to produce n result tuples with better quality data. And the differences compared with CrowdDB in Interfaces, Cleansing and Design.

3.4 So Who Won? Dynamic Max Discovery with the Crowd

Guo et al. [4] researched the Crowdsourcing System is a platform for answering queries through HIT's by the Crowdsourcing Requestor and the worker. Next, the answers were received from the worker and it is stored in the CrowdDB (Crowd Database). If the received answers were more than one right answer means how it will be decide which one is the right answer. Hence, the research team used Max Function to get the maximum number of responses posted by workers. i.e. PageRank is used to sort the received answers from the CrowdDB. Then the Top-1 answer will be assumed as the right answer. The team solved the Judgement Problem with PageRank Heuristic and Next Votes Problem with Complete Tournament Heuristic are the best strategies to find the right answer by the MaxFunction.

3.5 CrowdDB: Answering Queries with Crowdsourcing

Franklin [5] and team researched the CrowdDB and define how to create the Crowd Table, Crowd Column in the Relational Database Systems with the constraints like Primary Key, Foreign Key etc., with the knowledge of SQL. CrowdSQL discussed the issues of Incomplete Data and the Subjective Comparisons in the CrowdDB. Next, the team explained about the Query Processing techniques used in the CrowdDB. The differences are the CrowdDB parser for CrowdSQL. Crowd Operators are CrowdProbe,

CrowdJoin, CrowdCompare. The team proposes the future work for Answer Quality should be improved.

3.6 CrowdScreen: Algorithms for Filtering Data with Human

Parameswaran et al. [6] proposed the CrowdScreen calculation for the settling issue of sifting the appropriate responses dependent on a lot of properties with the motivation behind canister be checked by people. The group created deterministic and probabilistic algorithms to upgrade the evaluated cost and assessed error. The deterministic algorithm that plans a roughly ideal deterministic procedure. Furthermore, the Probabilistic methodologies the group made a straight programming outcome to build the best probabilistic methodology. This probabilistic procedure encircled for the inquiries finding more than one solutions, for example, hues: white, dark, orange and so on. The group inferred that the emergency of streamlining sifting of information utilizing people. The best and heuristic algorithms competently find separating procedures to encourage result in significant cost investment funds met all requirements to ordinarily utilized techniques in crowdsourcing applications.

3.7 Finding with the Crowd

Das Sarma et al. [7] proposed the CrowdFind algorithm and it was configuration best algorithm that degree the horizon of cost and time. This paper centers around separating the information things dependent on cost and time. There are some basic angles talked about in this paper are:

(1) The Crowdsourcing framework as a rule accept an inflexible number of processors working in similar to however while in sensible usage that can contrast the quantity of processors. Here the substitute methodology is, it can powerfully change the quantity of people working on the undertakings anytime. The complete cost is the absolute number of inquiries or tasks total cost.
(2) The Central facilitator which does the calculation among stages and utilizing human processors on interest to do basic errands. This paper proposes the arrangements on the horizon of expense and inactivity for two reasons. i.e., when people react accurately and when they conceivably will make mistakes.

3.8 Counting with the Crowd

Marcus et al. [8] proposed the selectivity estimation problem in a Crowdsourced database. The group tests the workers creativity by assessing the appropriate responses from the Crowdsourcing workers. They are detecting the spammers using Spammer Detection Algorithm (SDA) and implemented in both label-based approach and count based approach in the crowdsourcing platform. Once the spammer is detected using SDA then the spammer answer gets rejected from the database and the same question will be assigned with some other Crowdsourced worker. As a result by applying SDA it improves the result in monetary cost and latency.

3.9 CrowdMiner: Mining Association Rules from the Crowd

Amsterdamer et al. [9] proposed CrowdMiner: an engine for Well Being portal application, the objective of engine is to find the data patterns associated from the CrowdSourced data. The CrowdMiner is implemented in the Well-Being portal to find the new patterns from the existing questions and answers supplied by the crowd. The team followed two approaches namely: Closed Questions (X->?Y) and Open Questions (?->??). Then the engine finds the support and confidence of the corresponding X->Y. The collected in sequence of information on every rule is separated from the crowd.

3.10 Crowdsourcing Based Description of Urban Emergency Events Using Social Media Big Data

Xu et al. [10] researched how to detect the urban emergency events like fire, storm, flood, etc. to ensure the security of people from uncertainty using Social Media Big Data. Crowdsourcing is the concept of obtaining information from the big and heterogeneous data generated by variety of sources in urban liberty, such as sensor, transportation mediums, mobile devices and from humans. The research team proposes the five W's to recognize the constant urban crisis occasion. The main sources of data received from Social Media users, the spatial and temporal information and GIS based annotation. The team proposed the hierarchical structure of three layers namely, Social sensors layer, Crowdsourcing layer, 5 W based description layer. The proposed structure is implemented in the emergency management field to get the desired result.

3.11 Using the Crowd for Top-k and Group-by Queries

Davidson et al. [11] learn the crisis of examining top-k and group-by queries by means of the crowdsourcing. Top-k queries are used to know the higher order/Max result and Group-by queries is used to get the result in a cluster form. These Top-K and Group-by Functions are played the major role in the crowdsourced database. The team proposed two evaluating strategies of Top-K and Group-By queries either by Type Questions and Value Questions. Type Questions are Yes/No questions and Value Questions are answered based on the data information. Example: image annotation. And the team also proposed Variable error model for the flawed results from the crowd, and Bayesian Model designed for the workers can approach for the grouping. Finally, the goal of the work is to minimize the number of comparisons perform by the crowd to get the correct top-k elements or the correct groups.

4 Research Challenges

See Table 2.

Table 2. Contrast between the algorithms

S.no	Algorithm	Features	Enhancing features
1	Query optimization algorithm	Streamlining three kinds of queries: Selection queries Join queries Complex selection-join queries	CrowdOp don't bolster further developed SQL operators, as Sorting and aggregation
2	Query processing	Workflow of the HIT's in the crowdsourcing platform	Dynamic allocation of cost for HIT's
3	Deco	Concepts: Fetch Resolve Join	1. Execution time varies between the Number of questions 2. Query optimization techniques can be improved
4	Maximum function	Judgement problem Next votes problem	Not getting the optimal solution
5	CrowdProbe, CrowdJoin, CrowdCompare	1. CrowdProbe- Crowdsourcers missing information of CROWD columns 2. CrowdJoin used an index nested-loop join in excess of two tables 3. Crowd Compare –this operator executes the CROWDEQUALand CROWDORDER functions	Answer quality may be improved
6	CrowdScreen	Deterministic approach Probabilistic approach	An answer from the crowdsourcing applications includes human accuracy, handling correlations between multiple filters Clustering problems
7	CrowdFind	Skyline between cost and latency	1. Single predicate 2. Distinguishing spam workers and learning correctness of workers after some time
8	Spammer detection algorithm	Count based approach Label based approach	Query optimization technique
9	CrowdMiner: association rule mining	Closed question approach Open question approach	Not utilizing the gathered information on several rules at once (it will gather information on each rule separately from the crowd.)

(*continued*)

Table 2. (*continued*)

S.no	Algorithm	Features	Enhancing features
10	Social Media, Big Data	Five W (What, Where, When, Who, Why)	Can be Implemented in Traffic analysis or any real time applications
11	Top-K Queries, Group-by Queries	Type and valued questions, Bayesian model, Variable error model	Cost function-latency or quantity of rounds of inquires asked from the groups of peoples
12	1. Addition approximation to minimize the upper bound of mis-classification probabilities. 2. Multiplication approximation to maximize the lower bound of correct classification probabilities	Construction of optimal decision tress	Level-by-level decision tree construction only achieves local optimality

5 Inferences

Crowdsourcing systems features, Classifications are discussed from the above sections. Research challenges focused on the algorithms and the enhancement features that may need to be improved. From the above study we can improve the dataset performance that used in the Crowdsourcing system. The optimal dataset can be implemented in any of the crowdsourcing platform and we have measure the execution of the crowd-sourcing frameworks as far as idleness and query optimization.

References

T1. "Fundamentals of Database Systems" by Ramez Elmasri, 5th Edition

1. Fan, J., Zhang, M., Kok, S., Lu, M., Ooi, B.C.: Crowdop: query optimization for declarative crowdsourcing systems. IEEE Trans. Knowl. Data Eng. **27**(8) (2015)
2. Marcus, A., Wu, E., Karger, D.R., Madden, S., Miller, R.C.: Crowdsourced databases: query processing with people. In: CIDR, pp. 211–214 (2011)
3. Parameswaran, A., Park, H., Garcia-Molina, H., Poluzotis, N., Widom,J.: Deco:declarative crowdsourcing. In: CIKM, pp. 1203–1212. ACM (2012)

4. Guo, S., Parameswaran, A., Garcia-Molina, H.: So who won? dynamic max discovery with the crowd. In: SIGMOD, pp. 385–396 (2012)
5. Franklin, M.J., Kossmann, D., Kraska, T., Ramesh, S.: Crowd DB: answering queries with crowdsourcing. In: SIGMOD, pp. 61–72 (2011)
6. Parameswaran, A., Park, H., Garcia-Molina, H., Poluzotis, N., Ramesh, A., Widom, J.: CrowdScreen: algorithms for filtering data with humans. In: SIGMOD, pp. 361–372 (2012)
7. Parameswaran, A.G., Boyd, S., Garcia-Molina, H., Gupta, A., Polyzotis, N., Widom, J.: Optimal Crowd-powered rating and filtering algorithms. PVLDB **7**(9), 685–696 (2014)
8. Das Sarma, A., Parameswaran, A., Garcia-Molina, H., Halevy, A.: Finding with the Crowd
9. Marcus, A., Karger, D., Madden, S., Miller, R., Oh, S.: Counting with the Crowd. MIT CSAIL
10. Amsterdamer, Yael, Grossman, Yael, Milo, Tova, Senellart, Pierre: CrowdMiner: mining association rules from the crowd. PVLDB **6**(12), 1250–1253 (2013)
11. Xu, Z., Liu, Y., Yen, N.Y., Luo, X., Wei, X., Hu, C.: Crowdsourcing based description of Urban emergency events using social media big data
12. Davidson, S.B., Khanna, S., Milo, T., Roy, S.: Using the crowd for top-k and group-by queries. In: ICDT, pp. 225–236 (2013)
13. Wang, J., Kraska, T., Frankli, M.J., Feng, J.: CrowdER: crowdsourcing entity resolution. PVLDB **5**(11), 1483–1494 (2012)
14. Vesdapunt, N., Bellare, K., Dalvi, N.N.: Crowdsourcing algorithms for entity resolution. PVLDB **7**(12), 1071–1082 (2014)
15. Wang, G., Li, T., Kraska, M., Franklin, J., Feng. J.: Leveraging transitive relations for crowdsourced joins. In: SIGMOD (2013)
16. Wang, S., Xiao, X., Lee, C.: Crowd-based deduplication: an adaptive approach. In: SIGMOD, pp. 1263–1277 (2015)
17. Geng, B., Li, Q., Varshney, P.K.: Decision tree design for classification in crowdsourcing systems. Cornell University Library (May 2018)

Analysis for Optimal Interleaver in Multi-user IDMA Communication System

Shelesh Krishna Saraswat(✉), Vinay Kumar Deolia, and Aasheesh Shukla

G.L.A. University Mathura, Mathura, India
{Shelesh.saraswat, vinaykumar.deolia, aasheesh.shukla}@gla.ac.in

Abstract. In IDMA conspire interleavers are utilized to recognize the distinctive clients that subsequently influence the framework throughput. In this paper the execution of Random interleaver (RI), Tree based Interleaver (TBI) and clamorous interleavers are dissected dependent on memory necessity, multifaceted nature and mistake rate. The reproduction results demonstrate that disorder based interleaver configuration can accomplish the better execution.

Keywords: IDMA · Chaos theory · Chaos based interleaver · Logistic interleaver

1 Introduction

The Code Division Multiple Access (CDMA) frameworks has been broadly utilized in the third era of versatile cell frameworks because of better transfer speed proficiency, preparing gain [1]. However it has been seen that, numerous entrance obstruction (MAI), Inter symbol interference(ISI) and Multi-User discovery (MUD) multifaceted nature are the significant requirements, which obstacle the utilization of CDMA in future radio communication(FRC) [2].

To overcome above expressed issues, Interleaver-division numerous entrance (IDMA) conspire has been proposed, in which the restrictions of CDMA have been diminished by utilizing chip level interleavers as a discretionary method to recognize diverse clients in multi client condition. The utilization of interleaver is for the most part to revamp the requesting of twofold groupings or codeword which lighten the huge burst commotion into little blasts more than a few bits rather than a solitary coded image, and along these lines give more clamor resistance and better mistake rate execution. The fundamental execution standards of interleavers can be recorded as [3, 4]:

Interleaver groupings ought not crash to one another.
Less calculation multifaceted nature.
Less memory and data transfer capacity assets necessity.

Chip level interleavers are fundamentally utilized for recognizing the clients in IDMA framework so a similar interleavers is additionally required at the recipient side

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 893–901, 2020.
https://doi.org/10.1007/978-3-030-37051-0_100

for appropriate disentangling the information and consequently beneficiary multi-faceted nature can likewise be the execution paradigm for Interleaver age. Figure 1 demonstrates the randomization of burst clamor at the receiver [5].

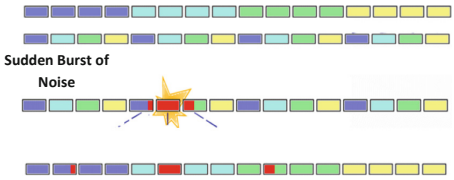


Fig. 1. Randomization of burst error due to the use of efficient interleaver

Numerous interleavers are proposed by specialists, for example, arbitrary Interleaver, symmetrical interleaver, pseudo irregular interleavers and tree based Interleaver and so on. Albeit these interleavers guarantee great interleaving execution, less memory prerequisite. Be that as it may, some restricting components spur for further research [5]. In this way, this paper gives a similar investigation of as of late proposed interleaving calculations, for example, arbitrary, tree based and turbulent interleavers in IDMA correspondence framework. Segment 2 exhibits the IDMA framework portrayal. Segment 3 characterizes arbitrary, tree based and turbulent interleavers. Next the execution investigation and correlations are made among above said interleavers in segment 4 and segment 5 talks about the ends drawn based on BER execution examination and computational multifaceted nature.

2 IDMA System Description

In Fig. 2, the Interleave Division Multiple Access (IDMA) system with K users is considered. At the transmitter, "a n-length input data sequence $y_k = [y_{k1}, y_{k2}\ldots\ldots\ldots y_{ki}\ldots y_{kn}]$ of k-th user is spreaded and encoded into chips $c_k = [c_{k1}, c_{k2}, \ldots\ldots c_{kj}]$" somewhere j is the chip length. Now chips are interleaved by a specific interleaving pattern (based on chaotic maps) to produce transmitted chip succession "$x_k = \lfloor x_{k1}, x_{k2}\ldots\ldots x_{kj} \rfloor$". For performance evaluation multipath Rayleigh fading channel is opted [1, 6–8]. In receiver section, the received signal from the k-th users with channel coefficient h k for k^{th} user and for the samples of fading $\{\zeta_j\}$ can be written as

$$R_j = \sum_{k=1}^{k} h_k x_{kj} + \zeta_j \tag{1}$$

"The iterative MUD detector also consists Elementary signal Estimator (ESE) and a posteriori decoder. The output of ESE is known log likelihood ratios and defined as"

$$e_{ESE}(x_k(j))_w = 2h_k \frac{R_{j+w} - E(\zeta_{k,w})}{\mathrm{var}(\zeta_{k,w}(j))}$$

"The output of APP-DEC is called as extrinsic log likelihood ratio. Based on the iterative process, the final outcome is decided. Now by using total probability theorem the output of estimator extrinsic LLR can be written as"

$$\ln \frac{\sum_{c'_{m,n,k=+1}} P\{y_n | x_{n,k} = x\} \prod_{m' \neq m} P\left\{c'_{m',n,k} = d_{m'}\right\}}{\sum_{c'_{m,n,k=-1}} P\{y_n | x_{n,k} = x\} \prod_{m' \neq m} P\left\{c'_{m',n,k} = d_{m'}\right\}}$$

As it has discussed that along with iterative process the effective interleaver can enhance throughput of the IDMA system.

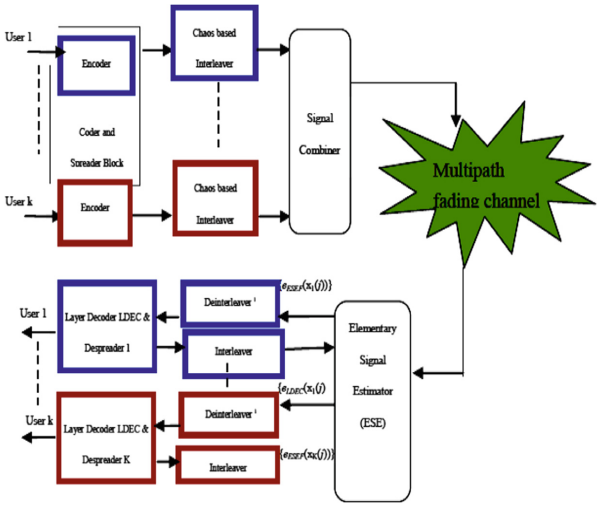


Fig. 2. IDMA transmitter and receiver model for k simultaneous users

3 Interleavers in IDMA

As talked about that interleaver calculation has the crucial job in enhancing the effectiveness and forward blunder remedy execution of IDMA framework. Essentially, the way toward interleaving is a procedure to modify the requested paired data bits in the deterministic method to drop the impact of burst commotion mistake. In this segment, three mainstream interleavers are contemplated and broke down to discover ideal interleaver grid.

3.1 Random Interleaver

The irregular interleaver scrambles the situation of bits arbitrarily. For a given introductory esteem the interleaver calculation is appeared in Fig. 3. In any case, in uproarious condition with profound blurring parameters, typically clamor meddle with the back to back bits and produce burst blunder which diminishes the likelihood of location at the recipient. Consequently the utilization of irregular interleaver coverts burst mistakes into arbitrary blunders and make flag effectively perceptible [8–10]. Memory necessity of arbitrary interleaver is the fundamental constraining element since extensive space is involved at to store the calculation at beneficiary side.

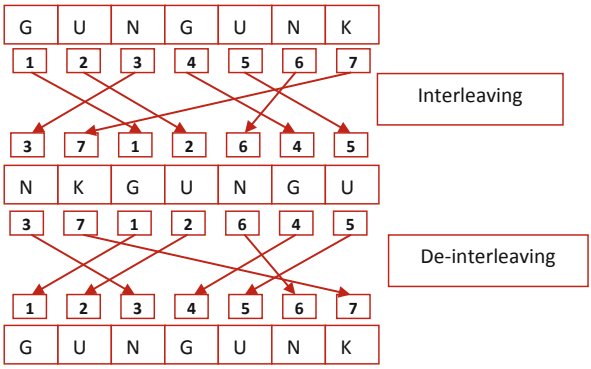


Fig. 3. Random interleaver and de-interleaver process

3.2 Tree Based Interleaver

The algorithm for TBI is base on the selection of mixture of two master interleavers. The odd number of users is taken plus while even number of users is taken downside. In this manner, a large number of users may be allocated with user specific interleavers with extremely less complexity. The memory needed of TBI is tremendously low as in comparison to that of the random interleaver, while is a little high if compared with master random interleaver [3], as shown in Fig. 4.

To overcome the restrictions of irregular interleaver new tree based interleaver is proposed, which diminishes the capacity necessity just as computational intricacy. The data required to share between the base stations and portable stations is additionally decreased [11]. To create TBI succession, initialstarted two irregular interleaver arrangement and are chosen π. Presently for much number of client the lower part of tree is considered and upper branch is considered for odd number of clients The calculation for interleaver age is plain as day in the Fig. 4. For instance for client no5theinterleaing example will be $\pi_1(\pi_2)$.

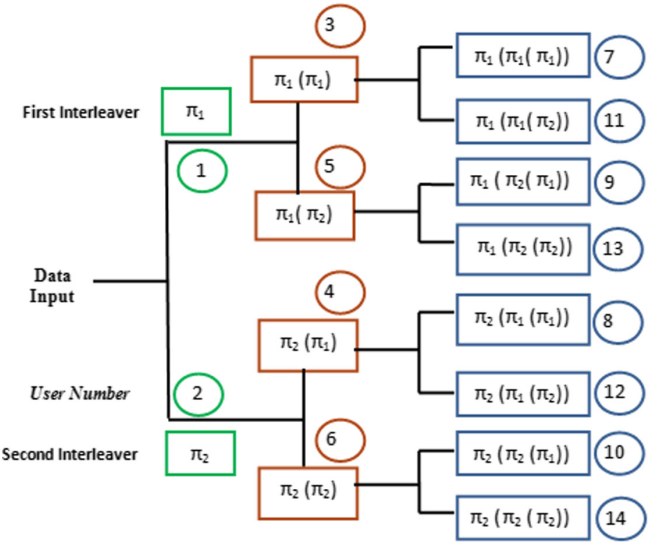


Fig. 4. Tree based interleaver

3.3 Chaos Based Interleaver

Disorder based interleavers are as of late proposed strategy which depends on mayhem hypothesis. It is noticed that any disorganized framework pursues certain properties, for example, the framework is deterministic, clamor like arbitrary in nature and high reliance on beginning conditions with the goal that distinctive signs could be created. Here the prevalent Logistic guide is utilized for interleaver age [12–14]. Steps required for the interleaver design age is depicted beneath.

Algorithm of Interleaver design based on logistic Map

Initialization:

$\lambda > 3.58$, N= Interleaver length, I= no. of users

$X_j^I = I^{th} user$: $0 < X_j^I < N$ τ = Foot step, $F_0^I = |X_0^I|$: the first element ($\Pi^I \equiv F_0^I$), j=0 and n=0

Main operation:

a) If n< N

- Calculate X_{j+1}^I

$F_{j+1}^I \equiv |X_{j+1}^I|$

$\Pi^I \equiv \Pi^I \cup F_{j+1}^I$

b) If n >N:

$X_{j+1}^I = \{\}$

$\Pi^I \equiv \Pi^I \cup |X_{j+1}^I|$

Increment j by 1 and
Repeat the main operation Otherwise
Check - If F_{j+1}^I is in the set Π^I

4 Execution Analysis of IDMA with Various Interleavers

4.1 Computational Complexity

Computational multifaceted nature is the imperative parameter to choose the nature of correspondence. Here, unpredictability implies that number of cycles required for the age of spreading codes and interleaver framework as far as clients. In this area, multifaceted nature is determined for disorder based calculated guide interleaver and for other famous calculations utilized for interleaver age. Table 1 demonstrates that the computational multifaceted nature increments with the quantity of client k for symmetrical, Nested and Tree based interleaver (TBI). It implies intricacy is subject to clients for all referenced plans aside from disarray based interleaver. Actually, the intricacy is O (1) which implies that computational unpredictability of calculated guide interleaver is autonomous from the quantity of clients [6].

Table 1. Computational complexity of interleaver generation of different algorithms

No. of Users	RI	*TBI*	CBI
1	1	1	1
2	2	1	1
4	4	2	1
16	16	4	1

4.2 Error - Rate Examination

In this segment, the nature of transmission of regular IDMA is assessed for tumult based interleaver. Irregular Interleaver is additionally considered for bit mistake rate (BER) examination of traditional IDMA framework. For straightforwardness, BPSK adjustment is considered in multipath Rayleigh blurring channel. The spreading code for all clients is just a reiteration code with the length sl = 16. Figure 5 demonstrates the reenactment results for information length = 1024 bits. Reproduction results confirm the execution of tumult based IDMA framework. This is clear in assume that the bedlam based interleaver accomplishes comparative BER execution contrasted with RI and fairly better for higher estimations of Eb/N0.

"In Fig. 5, reenactment results demonstrate alike BER execution of RI tumult based interleaver and TBI". The information length is accepted 8192 bits. No. of emphases are 10 and spread length sl is viewed as 16. Simulation figure infers that the execution of disorder based IDMA have almost same or better contrasted with RI-and TBI based IDMA (Fig. 6).

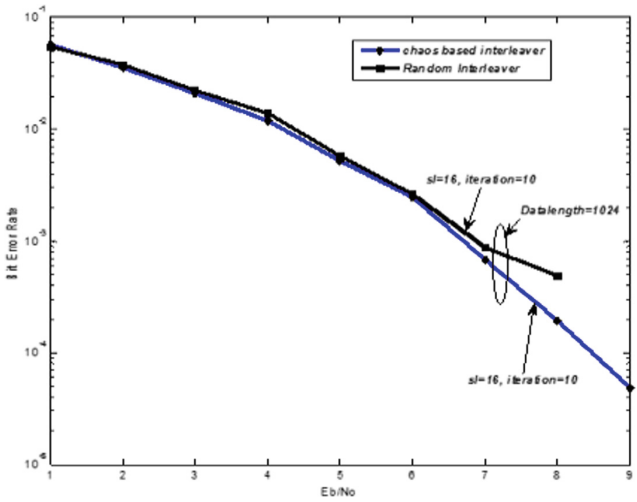


Fig. 5. BER comparison of RI and chaos based interleaver for data length = 1024, sl = 16, no of iterations = 10

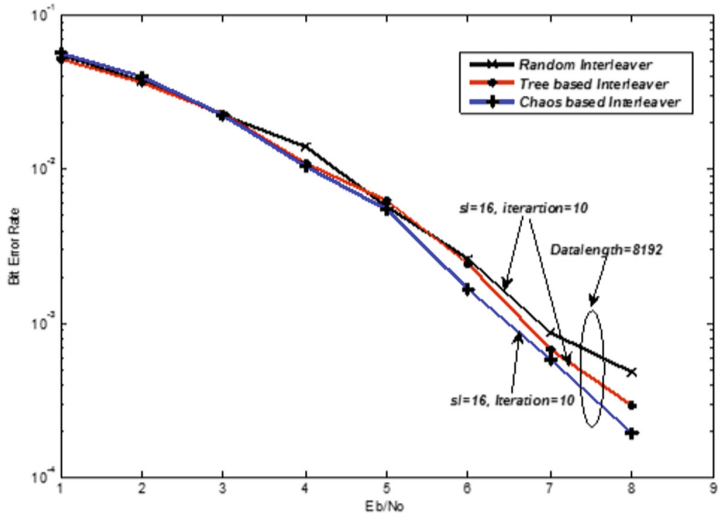


Fig. 6. BER comparison of RI, TBI and chaos based interleaver for data length = 8192, sl = 16, no. of iteration = 10

4.3 Memory Requirement

For the best possible preparing of flag at beneficiary, it is necessitated that the interleaving network ought to be known to the collector. The source needs to broadcast the interleaving framework with the information. For the bigger number of clients, the substantial measure of memory is required to store interleaver lattice along the edge of

transmitter and beneficiary. It builds the memory necessity of the framework. This issue turns into another test in the structuring of interleaver for IDMA framework. Memory prerequisite per client for various interleavers are appeared Table 2. The proposed turmoil based interleaver calculation recommends the need of just instatement parameter to produce a particular interleaver. Henceforth just single piece for example instatement parameter is required to share between transmitter (MS) and collector (BS). Along these lines, the mayhem based interleaver is proficient in memory prerequisite. In Table 2, memory prerequisite for various interleaver is displayed. The spreaded information is spoken to as chip-length and k is no. of clients.

Table 2. Memory requirement (Per user) for different interleavers

Interleavers	Memory requirement (chips/user)
Random interleaver	$k \times cl \times \log_2(cl)$
Tree based interleaver	$2 \times cl \times \log_2(cl)$
Chaos based interleaver	$cl \times \log_2(cl)$

5 Conclusion

This paper exhibits the examination of three well known interleaver calculations, for example, irregular, tree based and disorder based interleaver to locate an effective and ideal interleaver plan. All the three calculations are dissected to register stockpiling necessity, computational multifaceted nature and BER execution. Further, the reenactment results demonstrate that confusion based interleaver outflanks the RI and TBI as far as BER. Furthermore, the capacity is additionally ideally required by tumult based interleaver. Computational intricacy is additionally free from client limit in confused interleaver. Henceforth tumult based interleaver can be treated as a proficient interleaver plan and increasingly appropriate for IDMA framework.

References

1. Escribano, F.J., Wagemakers, A., Sanjuan, M.A.F.: Chaos-based Turbo systems in Fading channels. IEEE Trans. Circuits Syst. **61**(2), 530–541 (2014)
2. Kitada, A., Ogasawara, Y.: On a property specific to the tent map. In: Proceedings of Chaos, Solutions & Fractals, vol. 29, pp. 1256–1258 (2006)
3. Ping, L., Liu, L., Wu, K., Leung, W.K.: Interleave-division multiple-access. IEEE Trans. Wirel. Commun. **5**(4), 938–947 (2006)
4. Eisencraft, M., Fanganiello, R.D., et al.: Chaos based communication systems in non-ideal channels. Commun. Nonlinear Sci. Numer. Simul. 4707–4718 (2012). Elsevier
5. Eisencraft, M., Kato, D.M., Monteiro, L.H.A.: Spectral properties of chaotic signals generated by the skew tent map. Signal Process. 385–390 (2010). Elsevier
6. Shukla, M., Srivastava, V.K., Tiwari, S.: Analysis and design of optimum interleaver for iterative receivers in IDMA scheme. Int. J. Wirel. Mob. Comput. (2009)

7. Pupeza, I., Kavcic, A., Ping, L.: Efficient generation of interleavers for IDMA. In: International Conference on Communications, vol. 4, pp. 1508–1513 (2006)
8. Manoharan, S., Bhaskar, V.: PN codes versus chaotic codes: performance comparison in a Gaussian approximated wideband CDMA system over Weibull fading channels. Sci. Direct 3378–3404 (2014). Elsevier
9. Tseng, S.M.: IDMA based on deterministic interleavers. Int. J. Commun. Netw. Syst. Sci. **3** (1), 94–97 (2010)
10. Zhang, C., Hu, J.: The shifting interleaver design based on PN sequence for IDMA systems. In: Proceedings of International Conference on Future Generation Communication and Networking, Korea (2007)
11. Akbil, B., Ferre, G., Aboustajdine, D.: The NLM interleaver design for IDMA system. In: Proceedings of IEEE International Conference on Complex System, pp. 1–5 (2012)
12. Shan, L., Qiang, H., Li, J., Wang, Z.: Chaotic optimization algorithm based on Tent map. Control Decis. **20**(2), 179–182 (2005)
13. Kwon, O.M., Park, J.H., Lee, S.M.: Secure communication based on chaotic synchronization via interval time-varying delay feedback control. Nonlinear Dyn. **63**(2), 239–252 (2011)
14. Manoharan, Sangeetha, Bhaskar, Vidhyacharan: PN codes versus chaotic odes: Performance comparison in a Gaussian approximated wideband CDMA system over Weibull fading channels. J. Frankl. Inst. **351**(6), 3378–3404 (2014)
15. Osseiran, A., et al.: Scenarios for 5G mobile and wireless communications: the vision of the METIS project. IEEE Commun. Mag. **52**(5), 26–35 (2014)
16. Boccardi, F., Heath, R.W., Jr., Lozano, A., Marzetta, T.L., Popovski, P.: Five disruptive technology directions for 5G. IEEE Commun. Mag. **52**(2), 74–80 (2014)
17. Scott, A.W., Frobenius, R.: Multiple access techniques: FDMA, TDMA, and CDMA. In: RF Measurements for Cellular Phones and Wireless Data Systems, pp. 413–429. Wiley, Hoboken (2008)
18. Li, H., Ru, G., Kim, Y., Liu, H.: OFDMA capacity analysis in MIMO channels. IEEE Trans. Inf. Theory **56**(9), 4438–4446 (2010)
19. Higuchi, K., Benjebbour, A.: Non-orthogonal multiple access (NOMA) with successive interference cancellation for future radio access. IEICE Trans. Commun. **E98-B**(3), 403–414 (2015)

RETRACTED CHAPTER: A Study on Home Automation System for Dysarthric Persons Dependent on Speech Recognition

V. Shenbagalakshmi(✉) and T. Jaya

Department of ECE, Vels Institute of Science, Technology and Advanced Studies(VISTAS), Chennai, India
Shenbha1992@gmail.com, jaya.se@velsuniv.ac.in

Abstract. Automation could be a trending topic in twenty first century since it's a significant job in our day by day lives. Automation decreases the human work, time, exertion and a couple of human mistakes moreover. This paper aims to debate home automation systems for Dysarthric persons by speech recognition and to work home appliances by their own voice. Defect of speech could be a neurologic incapacity that damages the management of motor speech articulators. It can even be outlined as a speech that's characteristically unintelligible and slow. Someone with defect of speech might also suffer from issues like dominant the pitch, loudness, rhythm, and voice qualities of his or her speech. Several home automation systems are developed for old and disabled persons. Similar manner, this subject discussion will certainly pave the manner for several researchers in future to develop a sensible connected home for dysarthric persons.

Keywords: Home automation system · Dysarthria · Speech recognition

1 Introduction

Speech is that the primary communication medium between folks. This speech contains a complicated structure consisting not solely of the transmission of voice however conjointly embrace gestures, the language, subject that also contributes to the present method [1]. Speech recognition is one in all the foremost complicated areas of engineering science and partially due to it's knowledge base. Speech also known as Discourse, which is obviously unique in nature. There are a few methodologies utilized in discourse acknowledgment like fake neural systems (ANN), design acknowledgment, language displaying and connected math investigation. The basic model of discourse acknowledgment incorporates preprocessing, highlight extraction and demonstrating is performed (Fig. 1).

The original version of this chapter was retracted. The retraction note to this chapter is found at https://doi.org/10.1007/978-3-030-37051-0_109

© Springer Nature Switzerland AG 2024, corrected publication 2024
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 902–909, 2020.
https://doi.org/10.1007/978-3-030-37051-0_101

RETRACTED CHAPTER

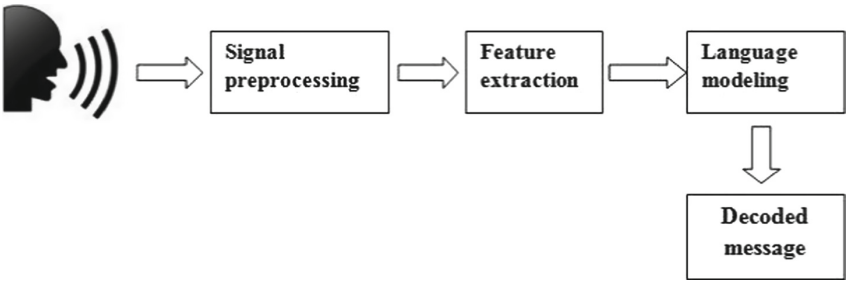


Fig. 1. Basic working of speech recognition

The home computerization frameworks have gotten distinction everyday gratitude to their direct use and wide operational abilities and a great deal of utilizations. These automation systems have seen a forceful modification within the recent times. These natural procedure patterns of homes mechanization are predominantly focused on numerous fundamental components like security, culture, recreation, comfort, vitality reserve funds, the board and financial exercises. Throughout the years loads of work has been cleared out the area of programmed discourse acknowledgment for mechanization frameworks. Therefore integration of speech recognition technology and residential automation systems for dysarthric persons will build the persons lighter and comfort. These home robotization frameworks will give a greater help for the elderly people. There are various queries and enhancements for the home robotization systems. We have a tendency to discuss thoroughly relating speech recognition, home automation and therefore the attainable ways in which of integration each within the following section.

2 Previous Self Assessment Studies

Variety of techniques and strategies are on the market for Home automation system. Some common strategies are given as:

(i) Home Automation System Victimization GSM Technology

Home Automation Systems are by and large made by using microcontroller as a central controlling unit. The Central Control Unit is the inside point and cerebrum of a home mobilization system. We consider three options for correspondence with GSM, to be explicit SMS based, GPRS based and DTMF based Home Automation systems. Home machine control system gives security on disclosure of interference through SMS using GSM advancement. In this framework, client sends SMS from remote to the GSM module related with Microcontroller and subject to SMS different gadgets in the house are turned on/off. This structure offers adaptability to customer with the objective that customer can murder on/off devices from wherever on the planet. Regardless it is past the area of imaginative vitality to would like to execute this structure where the client is old created or debilitated with ailment because of the rule two reasons. The essential basic reason is that to use this structure a customer must know the usage of flexible for sending SMS, generally old developed individual don't ponder making and sending SMS, and second

RETRACTED CHAPTER

is giving mobile phone to each old developed or injured individual isn't monetarily keen. GPRS based progression utilizes a webcam to stream video and photos of the home to its proprietor's adaptable. In GPRS based Home Automation structure client needs to screen his/her telephone always to reasonably guarantee against impedance revelation. In DTMF based Home Automation structure customer calls a SIM number allotted to the home and presses the digits on their phone's keypad to control the home's devices by making a DTMF tone. The tone is gotten and decoded by the GSM module at home using a DTMF decoder. The decoded principles are passed to the microcontroller with the target that client headings can be executed at home. DTMF-based home security frameworks also remain defective. They are fragile against—fuzzing attacks, as depicted by R. Sasi. This may make entire home structure to crash.

(ii) Home Automation System Via Gesture Recognition System

In our earlier days, for interaction with the machines we use keyboard and mouse. Those encountering physical disables, for example, Carpel Tunnel Syndrome, Rheumatoid Arthritis may be unfit to use such kinds of devices. In this situation, Gesture acknowledgment is utilized for Home Automation. This Gesture recognition did not depend on voice directions, at the same time, rather, enables a gadget to perceive certain signals. This philosophy does not require any specific learning (like in SMS based computerization system). Old developed or disabled people will use his/her hand to control mechanical assemblies. By using an essential webcam the photos will be taken and will be dealt with at Laptop in MATLAB programming and once a particular movement (gesture) is seen then the corresponding action will be performed. Even though it is a knowledgeable solution, incase suppose these dysarthric people can only shake hand instead of moving his or her hand then hand detection may not be done accurately. In such cases, the probability of false alarm is high. So the hand gesture recognition is done by the skin color of the human instead of hand detection. In order to get this gesture recognition(skin color of human) lighting is more important. Motion acknowledgment framework can be utilized in different applications like Virtual reality, recreations and gesture based communication. Sign language is an important case and it has received a special attention in gesture recognition.

(iii) Home Automation System Utilizing Bluetooth, WIFI, WSN and Zigbee Technologies

Many Wireless Technologies like RF, Wi-Fi, Bluetooth and Zigbee are becoming popular due to their versatility, low working charges, etc. Bluetooth Technology is already been familiar among the people due to its easy and quick set up. In addition to that it is also very cheap comparing with other technology. Bluetooth technology should be utilized for events with little worry for security and short network communication. On the other side, Bluetooth has a high power consumption and they have maximum communication range of 100 m in ideal conditions. Whereas other technologies like WiFi, WSN and Zigbee are not cost effective since they need motors, sensors, transmitters, receivers, etc., for their operation. Moreover these technologies are highly useful for mobile users who remotely access their homes but for aged or disabled people only conventional systems will be helpful.

RETRACTED CHAPTER

2.1 Dysarthria

Dysarthria, it is referred to us as an engine discourse issue which results from neurological damage of the engine part of the engine discourse framework and is portrayed by poor verbalization of phonemes (aphasia: a turmoil of the substance of language). At the end of the day, it can likewise be characterized as a condition in which issues adequately happen with the muscles that assistance produce discourse, regularly making it hard to articulate words. It is detached to any issue with understanding subjective language. In some cases any of the discourse subsystems (breath, phonation, reverberation, prosody, and enunciation) may unfavorably get influenced, which may likewise prompt impedances in understandability, discernability, instinctive nature, and proficiency of vocal correspondence. An individual with dysarthria may likewise have issues, for example, controlling the pitch, din, musicality, and voice characteristics of his or her discourse. As indicated by Duffy [3], Dysarthria is brought about by loss of motion, shortcoming, or failure to arrange the muscles of the mouth. Dysarthria can happen as a formative incapacity. It might be an indication of a neuromuscular issue, for example, cerebral paralysis or Parkinson's ailment. It might likewise be caused because of stroke, mind damage, or cerebrum tumor. Treatment of dysarthria incorporates concentrated language instruction with an expectation on oral-engine expertise improvement. Dysarthrias are grouped in number of ways dependent on the nearness of side effects. Some particular sorts of dysarthrias incorporate spastic (coming about because of respective harm to the upper engine neuron), limp (coming about because of reciprocal or one-sided harm to the lower engine neuron), ataxic (coming about because of harm to cerebellum), one-sided upper engine neuron (exhibiting milder side effects than two-sided UMN (Upper Motor Neuron) harm), hyperkinetic and hypokinetic (coming about because of harm to parts of the basal ganglia, for example, in Huntington's illness), and the blended dysarthrias (here manifestations of more than one kind of dysarthria are available).

Dysarthric people may encounter difficulties in the accompanying:

- Timing: Individuals while talking won't ready to exhibit a word on time since the words are incomprehensible and furthermore because of verbalization challenges.
- Vocal quality: Sometimes the vocal quality might be cruel or now and then it might be deadened relying on the attributes of dysarthria in patients.
- Pitch: Pitch is low, with somecases where pitch breaks occurs. Monopitch and Monoloudness may result from vocal overlap deadens.
- Volume: Patients with dysarthria may not ready to modify their volumes as a result of their poor pitch and vocal quality.
- Breath control, Speed and Strength: Occasionally, just a single vocal overlap is incapacitated. On the off chance that the overlap is incapacitated in an adducted position, the voice will sound brutal and have low volume. In the event that the crease is incapacitated in the stole position, this will cause hoarseness alongside a decrease in clamor. Two-sided vocal overlap loss of motion is the one which is more typical than one-sided loss of motion. the voice is hoarse and inspiratory stridor might be noted, since the folds are in a snatched position, and obviously, loss of motion of both vocal overlap in a totally kidnapped position would comprise a therapeutic crisis; and the aviation route would be shut off.

RETRACTED CHAPTER

- Steadiness, Range and Tone: All the three will change as a result of their low pitch and vocal quality.

2.2 Speech Recognition

Speech Recognition Systems have turned out to be so exceptional and standard that business and medicinal services experts are swinging to discourse acknowledgment answers for everything from giving phone backing to composing therapeutic reports. In our home, there may be old aged or disabled people who regularly needs a caretaker with special attention. But it is practically impossible for any individual to be with them for 24 h. But the problem is that those disabled persons need the caretaker when they are absolutely not present with them. Generally, disabled persons living in Smart homes can feel good, comfortable and secure compared to normal homes. Amid 1960s, the development of mechanization frameworks utilizing speaker distinguishing proof was occurred by content coordinating. The qualities of a person's discourse were believed to have the capacity to recognize the uniqueness of an individual much like a finger impression.

Discourse acknowledgment is the method by which a PC (or other kind of machine) see and recognizes the verbally communicated words. It infers chatting with your PC, and having it adequately see what you are articulating. It is significant to any speech related application. There are essentially more ways to deal with this but the most important is to extract the features from the pronounced word(speech) and after that those obtained features can be used to see the word when it is explained afresh.

The initial step of Speech Recognition is preprocessing (i.e., the input discourse flag must be preprocessed with the goal that quiet and clamor can be evacuated.) The second step is Feature extraction (like GNE, SNR, Skewness and Kurtosis) and next one is Modeling. Utilizing different demonstrating strategies, for example, HMM, GMM, ANN (any one can be picked) discourse can be perceived. We can utilize both Speaker Dependent and Speaker Independent technique. The Speaker subordinate technique implies the client needs to record his/her voice before utilizing the framework and the other way around for Speaker free strategy (Fig. 2).

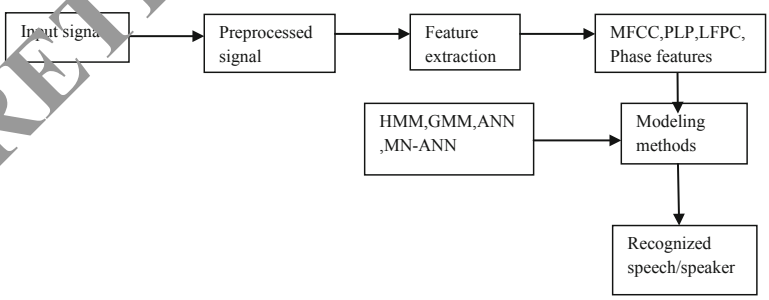


Fig. 2. Block diagram for speech recognition

RETRACTED CHAPTER

3 Discussion

Our past analysts depend on typical speakers for home computerization frameworks. Yet, in this paper we proposed a similar thought for dysarthric speakers. While we go for dysarthric speakers, we have to concentrate on the right demonstrating techniques to remove the discourse. Since the discourse acknowledgment precision may differ among the ordinary speakers and the dysarthric speakers. Since that specific word expressed just goes about as a key to initiate the electrical apparatuses inside the home. Here, we can favor Artificial Neural Network (ANN). In ANN, we can utilize different preparing capacities. So contrasting and other demonstrating procedures, ANN can give better acknowledgment accuracy.' In the execution part we can utilize Voice recognition module. The voice acknowledgment module can be talked about as pursues:

Voice controlled gadgets fundamentally utilizes the main of discourse acknowledgment which incorporates the way toward changing over or changing a discourse waveform into words. Changing over a discourse waveform into an arrangement of words includes the accompanying advances:

1. A speaker gets the standard of the discussion to be seen and changes over it into an electrical pennant. A forefront talk certification framework moreover necessitates that the electrical pennant be tended to digitalized by systems for a simple to-front line (A/D) change process, so it may be dealt with a computerized PC or a microchip.
2. This discussion pennant is then dejected down (in the examination dishearten) to pass on a delineation including striking highlights of the discussion. The most overpowering fragment of talk is gotten from its concise timespan run, assessed powerfully over brief time windows of length 20–30 ms covering at between times of 10–20 ms. Each brief time run is converted into a segment(feature) vector, and these feature vector only forms the speech pattern.
3. This speech pattern is then compared to a store of phonemic patterns in order to generate hypothesis by means of a dynamic programming process. The speech signal has variations among many dimensions.
4. Speaker dependent or Speech dependent system rely only on the individual or the particular words who are trained with the system. So that they result in better accuracy of about 95% in word recognition. The downside to this framework is that the structure just reacts unquestionably just to the person who organized the framework. This is the most exceptional methodology utilized in programming for PCs.
5. Speaker Independent System is the one which deals with the word which is not even trained by the system. So the system should undergo a multiple number of training with the target word. The command word count is usually lower than the speaker (Fig. 3).

4 Software Details

MATLAB Millions of authorities and analyst generally speaking use MATLAB® to separate and structure the systems and things changing our existence. MATLAB is in vehicle dynamic security structures, interplanetary rocket, prosperity watching devices, sharp power cross sections, and LTE cell frameworks. It is used for AI, banner dealing

RETRACTED CHAPTER

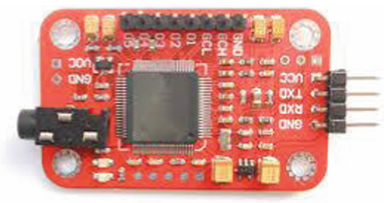


Fig. 3. Speech Identification Kit

with, picture planning, PC vision, correspondences, computational cash, control plan, mechanical self-governance, and essentially more. MATLAB is the least requesting and most advantageous programming for architects and analysts. MATLAB will lov, paying little mind to whether you're dismembering data, making figurings, or making models, MATLAB gives a circumstance that invites examination and revelation. It unites an irregular state language with a work zone condition tuned for iterative planning and intelligent work forms. The work zone condition invites experimentation, examination, and disclosure. These MATLAB mechanical assemblies and limits are generally completely attempted and expected to coordinate (Figs. 4 and 5).

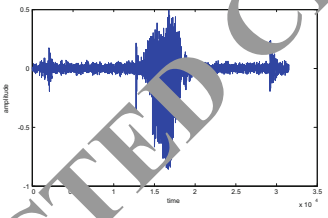


Fig. 4. Normal speech signal for the word "command"

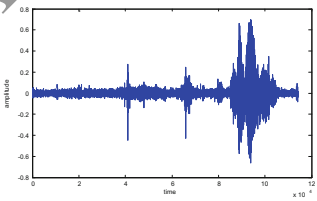


Fig. 5. Dysarthric speech signal for the word "command"

RETRACTED CHAPTER

5 Conclusion

All things considered the fundamental thought is to enable the discourse to scatter people in our general public. Earlier, home computerization frameworks utilizing discourse acknowledgment frameworks have been created by numerous analysts. Be that as it may,

our fundamental point is to help dysarthric people by utilizing brilliant home innovation. The utilization of speech recognition gets out the need to remote controllers and other electronic gadget and makes it simple to interface with the framework to perform automation and control electrical gadgets. For these individuals robotizing a home by discourse acknowledgment with inserting equipment of home with the framework can be gainful. With this thought we can execute a voice worked framework for dysarthric people. In future both speaker dependent and speaker independent home automation system can be organized with lots and lots of comfortness, high efficiency and high preference to security.

References

1. Klabi, I., Masmoudi, M.S., Masmoudi, M.: Advanced user interfaces for intelligent wheelchair system. In: 1st International Conference on Advanced Technologies for Signal and Image Processing (ATSIP) 2014, pp. 130–136 (2014)
2. Gnanasekar, A.K., Jayavelu, P., Nagarajan, V.: Speech recognition based wireless automation of home loads with fault identification for physically challenged. In: 2012 International Conference on Communications and Signal Processing (ICCSP), pp. 128–132 (2012)
3. Kannan, P., Udayakumar, S.K., Ahmed, K.R.: Automation using voice recognition with python SL4A script for android devices. In: 2014 International Conference on Industrial Automation Information and Communications Technology (IAICT), pp. 1–4 (2014)
4. Asadullah, M., Raza, A.: An overview of home automation systems. In: 2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI), pp. 27–31 (2016)
5. bt Aripin, N., Othman, M.B.: Voice control of home appliances using Android. In: Electrical Power Electronics Communications Controls and Informatics Seminar (EECCIS) 2014, pp. 142–146, (2014)
6. Habiba, U., Barua, S., Ahmed, S., Dey, G.K., Ahmmed, K.T.: 3rd hand: a device to support elderly and disabled person. In: 2015 2nd International Conference on Electrical Information and Communication Technology (EICT), pp. 1–6 (2015)
7. Nasrin, S., Radcliffe, P.J.: Novel protocol enables DIY home automation. In: Telecommunication Networks and Applications Conference (ATNAC) 2014 Australasian, pp. 212–216 (2014)
8. Valencia-Redrovan, D., González-Delgado, L., Robles-Bykbaev, V., González-Delgado, N., Panzieri, T.: SA3M: An interactive robot to provide support for the elderly. In: 2014 IEEE International Autumn Meeting on Power Electronics and Computing (ROPEC), pp. 1–6 (2014)
9. Asht, S., Dass, R.: Pattern recognition techniques: a review. Int. J. Comput. Sci. Telecommun. **3**(8) (2012)
10. Arora, S.J., Singh, R.: Automatic speech recognition a review. Int. J. Comput. Appl. **60**(9) (2012)
11. Tychtl, Z., Psutka, J.: Speech production based on the mel-frequency cepstral coefficients. Mulgrew

RETRACTED CHAPTER

Performance Evaluation of Methods for Mining Frequent Itemsets on Temporal Data

Tripti Tripathi(✉) and Divakar Yadav

Department of Computer Science and Engineering, MMMUT, Gorakhpur, India
tripti.gkp7@gmail.com, dsy99@rediffmail.com

Abstract. Data mining is a method, used to extract usable and valuable information from the bulk of the data. Frequent data mining is an interesting task that is used to find frequent patterns from the database. In this paper, we used to perform frequent item set mining on temporal data. Temporal data contains data that primarily ranges over time. The idea of the time hierarchy is introduced to generate rules from temporal data. In this paper, we try to solve the problems using three popular data mining algorithms such as FP growth, Eclat and Apriori algorithm. The main focus of this study is to generate efficient algorithms that consume very less runtime and present the more frequent item set from the dataset. We evaluate our algorithms through experiments.

Keywords: Data mining · Frequent itemset mining · Temporal data · Time hierarchies

1 Introduction

Data mining is a technique that is applied to extract usable and helpful information from the bulk of the data. Data mining is the method for obtaining outright patterns and information from huge data sets. This is the method of obtaining interesting patterns and information from huge amounts of data [1]. These data are extracted from the databases. Some database is in static form while in some database transaction is done frequently, known as a frequent database. The frequent database holds the data that are repeated frequently such as the transactional database. Frequent data mining is an interesting task that is used to find frequent patterns from the database. To perform frequent data mining several methods are used such as correlations, association rule, clustering, classification and some more. Among these methods association rule mining is very popular. The concept of frequent data mining is introduced by [2]. To perform association rule mining couple of steps used. In the very first step, all frequent itemsets are generated. In the second stage, positive association rules are generated with these itemsets [3].

Basically, the motivation behind using association rules came from the requirement to check so-called supermarket transaction data, the order is used to check the consumers purchasing behavior as what product they would like to purchase more. We check the customers purchasing behavior by seeing the transactional database of a

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 910–917, 2020.
https://doi.org/10.1007/978-3-030-37051-0_102

store. For example, a set of items such as cd player and cd disc appears in the transactional database together or frequently. Suppose if a person is going to purchase cd player then there is a more probability that he is going to purchase cd disc too. Frequent Item set Mining (FIM) holds some major analysis issue under data mining [4]. In this paper we perform mining on temporal data by using the three data mining algorithms that is Apriori, FP growth and Eclat algorithm.

The rest of the paper is organized as follow. Section 2 presents the literature review of the paper in Sect. 3 we present the system architecture of the paper. In Sect. 4 we discuss about result and implementation procedure. Finally, we will finish by conclusion.

2 Literature Review

In [4] his paper, the author performs mining on temporal data. He introduces the concept of BTC (basic time cube) and solves the problem using the apriori algorithm. He introduced some basic concepts like density function to solve the overtime estimating problems.

In [2], the author introduced the concepts of the apriori algorithm that usually applies to frequent itemsets to generate meaningful information from that.

In [5], the author discusses the improved apriori version name active apriori. Active apriori rather than scanning whole database it works on the compressed dataset and also optimizes the system performs.

In [6], the author discuss the improved FPGrowth algorithm. In his paper, he presents a comparison between Painting-growth and N Painting-growth algorithm.

In [7], the author discusses the eclat algorithm. In eclat the scanning of the database is performed on the bottom-up approach so, a large number of iterations is required. In this paper eclat, the algorithm is work in a top-down approach that reduces the amount of iterations and escapes time too.

To handle large transactional data a very efficient algorithm is required. In [8], the author discusses the parallel apriori algorithm depend on Map-Reduce, that is a framework that processes large dataset using a huge amount of computers.

3 Methodology

In this paper, we basically perform mining on frequent itemset with respect to time hierarchies. Time hierarchy divides the time segments into primarily three segments: the day, month and year and performs the operation on that particular itemsets. In this paper, the problem of temporal data mining is solved by using the three data mining approaches such as Apriori algorithm, FP growth and Eclat algorithm. In [9], the author proves that frequent data mining algorithms are classified into three groups according to their properties. Namely, Tree-based, joint based and Pattern growth algorithms. Tree-based approach mines the frequent itemset using either depth-first search or breadth-first. Mining is performed using these both algorithms either sequentially or parallelly. After mining itemset a tree is plot. This is very popular technique approach.

In joint based approach mining of itemset is performed by using only the bottom up approach whereas in the pattern growth approach mining is performed by using the concepts of divide and conquer [10] (Fig. 1). In Fig. 2, the flow of the frequent itemset mining algorithm is shown.

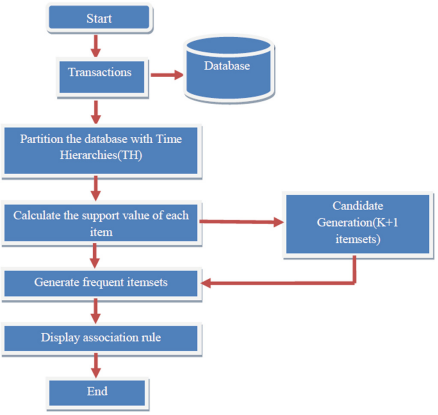


Fig. 1. Flow chart

The above flow diagram shows the basic structure of the flow of the processes.In this particular problem for the extraction of the data we basically use the concepts of the time hierarchy.

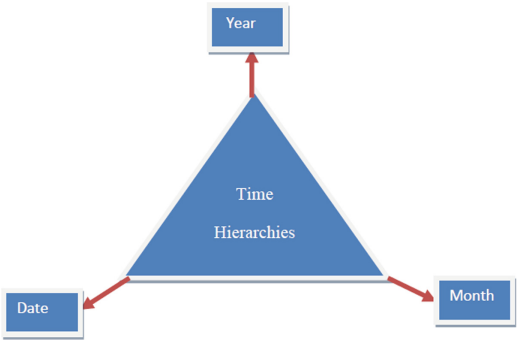


Fig. 2. Time hierarchies

I. **Apriori**
The concepts of the apriori algorithm are introduced by [2]. Basically, the apriori algorithm is designed to work on the transactional database. Apriori uses the concepts of association rule mining to generate the meaningful information from that transactional dataset [8]. Apriori work in two steps: in the first step we

extract all items that have the minimum support and in the second step we generate the rules with these item sets.

II. **FPGrowth**
FP-Based algorithm is the enhanced version of the apriori algorithm. The concepts of FP growth are introduced in [5]. This is an algorithm that generates frequent patterns from the itemset without candidate generation.

III. **EClat**
EClat refers to equivalence class partitioning. This is the algorithm that is basically designed to improve the effectiveness of apriori algorithm [10].

4 Result and Disscussion

In this section, the experimental result is discussed by applying the proposed set of rules. The performance of the algorithm is examined in the experiment on synthetic information. To perform this operation synthetic dataset of around 100 transactions is created. The data-set is a synthetic database containing transactions made up by way of a hundred transactions from 1 January 2013 to 23 February 2013. To perform mining basically, extract the data from the database with respect to time hierarchies (TH). Figure 3 show the synthetic dataset. From this dataset, we extract the temporal data with respect to the time hierarchies.

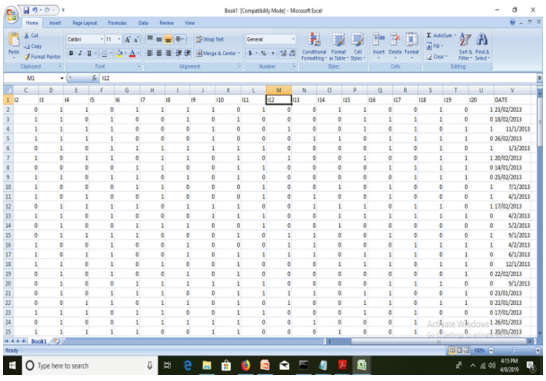


Fig. 3. Synthetic dataset

After extracting data from the dataset with respect to time hierarchy. We get the following item sets. Then a sample is selected as a goal answer. The purpose at the back of the usage of this sort of large dataset for analysis is to ensure that our proposed set of rules is able to manage any common item set mining problem. A synthetic dataset is selected instead of a real dataset in order that a managed test may be conducted to validate the efficiency of our technique. We run the program on the Java platform. We convert the xlx dataset into csv format. Figure 4 shows the temporal data. Temporal data are basically the data that ranges over time. Figure 3 shows the synthetic dataset of

the transaction we perform mining over the dataset while taking date column as the primary factor. We extract the data while applying to filter with respect to time hierarchy and prepare a new dataset shown in table of Fig. 4.

On this particular problem, we execute all three algorithms. Basically, we focus on time hierarchy (TH) to check how long it will take to execute the problem. Value of support varies continuously from 0.1 to 1.0. The main focus of this study is to generate

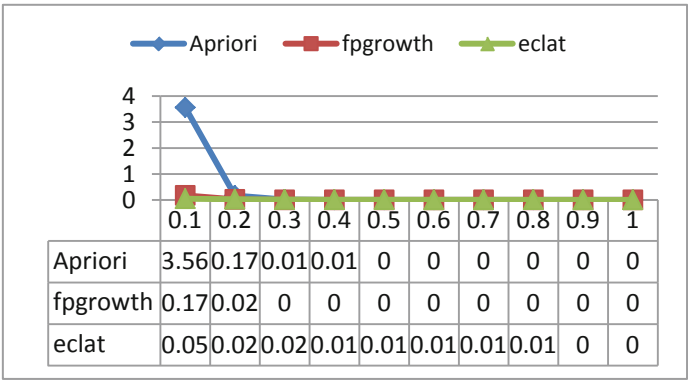
I2,I4, I7,I11,I13,I16,I20
I1,I2,I3,I5,I9,I10,I11,I14,I15,I16,I17,18,I19,I20
I1,I2,I5,I8,I9,I13,I16,I17,I18
I2,I3,I5,I7,I8,I9,I13,I16,I17,I18
I2,I4,I5,I8,I9,I12,I14,I16,I17,I19,I20
I1,I2,I4,I6,I7,I8,I9,I11,I15,I16,I17,I18,I19
I1,I2,I3,I7,I10,I11,I12,I15,I17,I20
I2,I4,I5,I9,I10,12,I14,I16,I18,I20
I2,I3,I4,I6,I7,I10,I11,I14,I15,I16,I17,I18
I1,I3,I6,I9,I14,I16,I16,I18
I3,I4,I5,I6,I7,I13,I14,17,I19
I1,I2,I6,I7,I8,I10,I13,I14,I19
I1,I2,I6,I7,I8,I9,I11,I13,I15,I16,I17,19,I20

Fig. 4. Temporal data

efficient algorithms that consume very less memory space, less runtime and present the more frequent item set from the dataset. Table 1 shows the running time for each algorithm. From Fig. 5 through graph we conclude that the FP-Growth takes less time as compare to the Apriori and Eclat algorithm.

Table 1. Runinng time

Support	Apriori	FP-Growth	Eclat
0.1	3.56	0.172	0.045
0.2	0.166	0.02	0.024
0.3	0.014	0.003	0.017
0.4	0.005	0.003	0.009
0.5	0.002	0.002	0.008
0.6	0.001	0.003	0.005
0.7	0.002	0.001	0.005
0.8	0.002	0.001	0.009
0.9	0.001	0.002	0.003
1	0.002	0.002	0.003



	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
Apriori	3.56	0.17	0.01	0.01	0	0	0	0	0	0
fpgrowth	0.17	0.02	0	0	0	0	0	0	0	0
eclat	0.05	0.02	0.02	0.01	0.01	0.01	0.01	0.01	0	0

Fig. 5. Running time

In this, we implement all three algorithms: Apriori algorithm, FPGrowth and EClat algorithm. On the above temporal dataset, we check the frequency of the items like which item is purchased more. We perform mining over the support value from 0.1 to 1.0. We calculate the time period of execution of each item. From the above implementation, we got the best rule as:

$$[\text{I2}, \text{I9}] \rightarrow [\text{I16}]$$

It means that the purchasing of the item I2 or I9 directly affect the purchasing of I16 like if we bought I2 or I9 then there will be more probability that the I16 is also purchased. The above problem is coded into java programming language and running on windows 10. The dataset is to be available on the website at http://fimi.ua.ac.be/data/. There are a lot of datasets are available at that link. We perform our problem on some datasets that are given below. Table 2 shows dataset along with their number of transactions.

Table 2. Datasets

Datasets	No. of transactions
Retail	88,162
Mushroom	8,124
Chess	3,196
Connect	67,557

We use the same procedure as used on the synthetic dataset to perform mining. Again we use to run the same commands on the standard datasets. Figure 3 Show the comparison of all three algorithms. We run the program on retail datasets. Their running time is shown in Fig. 3.

Table 3. Running time

Support	Apriori	FP-Growth	Eclat
0.1	224.378	1.333	1.387
0.2	223.207	0.905	1.471
0.3	229.878	0.934	1.578
0.4	228.964	0.662	1.353
0.5	243.423	0.412	1.384
0.6	256.015	0.361	1.494
0.7	308.712	0.399	1.35
0.8	309.292	0.426	1.332
0.9	324.243	0.349	1.343
1	302.84	0.446	1.347

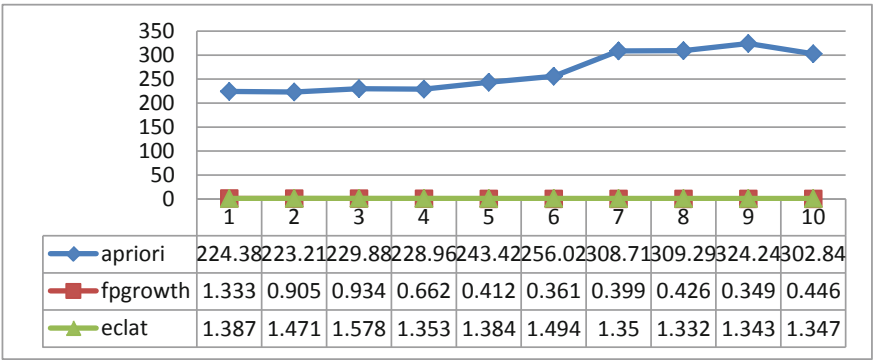


Fig. 6. Running time

In order to compare the result we run all three algorithms where there support value varies between 0.1 and 1.0. The runtime of algorithm is shown in Table 3. In Fig. 6 time performance is shown while comparing all three algorithms FPGrowth gives better performance as compare to Apriori and Eclat.

5 Conclusion and Future Scope

This paper presents a study about the frequent itemset mining on temporal data. Temporal data contains data that primarily ranges over time. Some patterns are occurring at a particular time while others are occurring at other time. In this paper, we perform mining on synthetic datasets using three popular data mining algorithms such as FP growth, Eclat and Apriori algorithm. We applied our algorithm on the retail dataset but it can be used at every place where transactions are performed at a very high rate. In the future, for better result following aspects are proceeded such as the generation of association rule according to user interest and set the different support value for each item present in the database.

References

1. Han, M.K., Pei, J.: Data mining: concepts and techniques. Elsevier, Amsterdam, The Netherlands (2011)
2. Agrawal, R., Imielinski, T., Swami, A.: Mining association rules between sets of items in large databases. ACM SIGMOD Rec. **22**(2), 207–216 (1993)
3. Tsay, Y.-J., Hsu, T.-J., Yub, J.-R.: FIUT: a new method for mining frequent itemsets. Inf. Sci. **179**, 1724–1737 (2009)
4. Ghorbani, M., Abessi, M.: A new methodology for mining frequent itemsets on temporal data. IEEE Trans. Eng. Manag. **PP**(99) (2017)
5. Veena, S., Rangarajan, P.: Optimization of active apriori algorithm using an effective genetic algorithm for the identification of top-l elements in a peer to peer network. Asian J. Appl. Sci. **2**(5) (2014). ISSN 2321–0893
6. Zeng, Y., Yin, S., Liu, J., Zhang, M.: Research of improved FP-growth algorithm in association rules mining. Sci. Program. **2015**, 6 (2015)
7. Kaur, M., Garg, U., Kaaur, S.: Advanced eclat algorithm for frequent itemsets generation. Int. J. Appl. Eng. Res. **10**(9), 23263–23279 (2015)
8. Li, N., Zeng, L., He, Q., Shi, Z.: Parallel implementation of apriori algorithm based on mapreduce. In: 2012 13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, pp. 236–241. IEEE (2012)
9. Aggarwal, C.C.: An introduction to frequent pattern mining. In: Aggarwal, C.C., Han, J. (eds.) Frequent pattern mining, pp. 1–14. Springer, Basel (2014)
10. Essalmi, H., Far, M.E., Mohajir, M.E., Chahhou, M.: A novel approach for mining frequent itemsets: AprioriMin. In: 4th IEEE International Colloquium on Information Science and Technology (CiSt), pp. 286– 289 (2016)
11. http://fimi.uantwerpen.be/data/
12. Goyal, N., Jain, S.K.: A comparative study of different frequent pattern mining algorithm for uncertain data: a survey. In: 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 183–187. IEEE (2016)

A Novel Framework for Spam Hunting by Tracking Concept Drift

V. Bindu[1(✉)] and Ciza Thomas[2]

[1] Sree Chitra Thirunal College of Engineering, Thiruvananthapuram, Kerala, India
bindunn@gmail.com
[2] College of Engineering, Thiruvananthapuram, Kerala, India

Abstract. In mid seventies a new method of exchanging messages between electronic devices originated which revolutionized the global community into a new world of computer networks called internet. The users identified the potential usage of this method presently known as email and started using it as the means of communication and marketing. But the competence of this method was lessened by the wide spread proliferation of spam. Researchers have come up with many proposals and tools to fight against spam. But the dynamic nature of spam makes the tools ineffective and raises the requirement for developing a filter that is to be successful over time in identifying spam. Hence spam filtering is a particularly exigent machine learning task as the data distribution and concept being learned changes over time. This paper explores this phenomenon called concept drift seen in email datasets and proposes a new framework in identifying the strategies for developing spam detection systems.

Keywords: Concept drift · Spam detection · Classification

1 Introduction

The pervasiveness of Internet and the progress of e-commerce have turned email into an essential method for communication, advertising and marketing. But recent surveys have revealed that majority of all email interchanges are spam mails, a sort of undesirable emails that is sent from one who is obscure to a monstrous number of people in light of different purposes. Researchers have developed many sifting methods to recognize and stop the stream of spam messages. These sifting methods are generally artificial intelligence and data mining procedures which fundamentally includes classification. Most of these research concerns static environments, where a fixed set of labeled examples is presented to the learning algorithm which aims at producing the most efficient classification with respect to the accuracy. However, in many real situations learning is not a static task anymore as spam data sources generate rather continuous and time changing data. Specifically it concerns evolving data streams where the distributions and target class definition changes over time. The reason for change is shrouded which can instigate changes in the target concept.

Within the scope of spam filtering the study of concept drift is very important as users interests also changes over time. Moreover even if our comprehension of an

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 918–926, 2020.
https://doi.org/10.1007/978-3-030-37051-0_103

undesirable message may continue as before over a generally significant lot of time, the overall recurrence of various kinds of spam may change radically with time. This phenomenon called concept drift makes it difficult the majority of spam sifting methods to recognize spam messages precisely. Based on this context it is essential to explore clearly the inherent characteristics and behavior of this issue to develop rapid and precise adaptive learning algorithms.

Here we put forward a fathomable investigation of concept drift, its peculiarities and genres, obnoxious impacts with regards to email system and finally propose a new framework in identifying the strategies for developing spam detection system. With the motivation of investigation regarding concept drift briefed in this section, the rest of the paper is organized as: Sect. 2 explains the state of art regarding concept drift; Sect. 3 provides a hypothetical study of concept drift describing its peculiarities, behavior characteristics, types and how can it be addressed; Sect. 4 describes concept drift in the e-mail domain; Sect. 5 portrays a framework for distinguishing spam by tracking concept drift in email domain. Section 6 concludes presenting the future outlook.

2 State of the Art

Concept drift happens on a very basic level in online supervised learning circumstances where the relations between the information data and the target variable changes after some time. The impact of concept drift is seen in many multidisciplinary domains like medicine, artificial intelligence (AI) systems, decision making, ubiquitous environment applications, personal assistance and information, management and strategic planning, monitoring and control systems etc. Hence dealing with concept drift has turned into an alluring subject of research and have a rich state-of-the-art approaches available. This includes study of the phenomena of concept drift, handling/tracking methods and techniques in different application areas, enhancing the accuracy of classifiers by adapting drift mechanisms etc.

Concept drift term was named by Schlimmer and Granger in 1986 when they formulated an adaptive learning algorithm named STAGGER [1] while formulating the problem of incremental learning from noisy data. Since this work talks about the negative effect of concept drift on the viability of an incremental learning framework, numerous researchers began chipping away at this idea to handle the issue in supervised classification. The work has its peak interests during these time periods 1998, 2004 & after 2007.

The authors [2] came up with a new algorithm named FLORA which was the first supervised incremental learning systems for evolving data. This algorithm uses a fixed length sliding window which stores only the recent examples in the first-in, first-out sequence with model updation at each time step. The updation is done based on two processes a learning process (updating based on new data) and forgetting process (discarding based on old data). An instance based algorithm named as IB3 was introduced [3] to improve the performances of nearest neighbor algorithms that keep record of correct and incorrect classification decisions that are made by the saved data points. For real time-varying approaches in dynamic control system, the authors in [4] assessed the ability and appropriateness of various Neural Networks arrangements (for example single-layered, multi-layered and intermittent). Later Harries and Horn acquainted a few methodologies to improve the pursuance of C4.5 decision trees to manage both concept drift and non-

determinism in time series area [5]. The authors in [6] proposed a new method by implementing Support Vector Machine (SVM) to track concept drift. In unsupervised situations introduction of COBBIT by Kilander and Jansson [7], OLINDDA, one-class clustering-based approach by [8] were the solutions. High performance algorithm named CWA [9] was proposed which talks about the effect of having three various windows of various sizes to foresee concept drift. In detail, the creators proposed the CWA method that executes three windows of various sizes. Moreover the authors clearly explains the details of concept drift with its characteristics, different types, how to identify the drift as well as methods for handling drift.

In the area of email there isn't much significant work completed. Among the significant works are [10–14]. In [10] a case-based reasoning strategy was created utilizing a lot of methods where singular outcomes are joined to get a last characterization (ensemble). A lazy learning hybrid model called Spam Hunting [12] dependent on an Instance Based-Reasoning framework was acquainted to perform spam naming and sifting within the sight of concept drift. Nosrati and Pour acquainted a novel algorithm [13] to identify two sorts of concept drifts by remaking the classifier when needed. An empirical study was carried out regarding the detection of concept drift in email data sets by [14].

3 Concept Drift

Concept drift refers to a pivotal perspective that exists in some genuine real world information streams where the characteristics of the information changes illogically overtime. It is an unanticipated substitution of one information source S1 (with an underlying probability distribution pS1), with another source S2 (with distribution pS2) as depicted in Fig. 1.

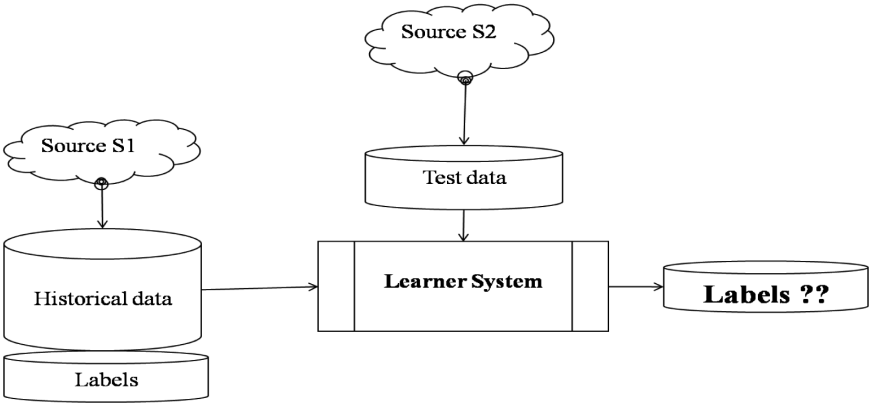


Fig. 1. Architecture for learning with concept drift

The center presumption, while dealing with the concept drift problem, is vulnerability about what's to come. It tends to be expected, evaluated, or anticipated, however

there is no sureness. According to Bayes classification rule any posterior prediction of class depends on prior probabilities, likelihood and the evidence. Hence concept drift may occur in three ways:

1. Class priors P(c) might change over time.
2. The distributions of one or several classes' p (X|c) might change.
3. The posterior distributions of the class membership's p (c|X) might change.

The change of p (X|c) is called virtual drift and change of p (c|X) is called real drift where c represents set of class labels and X is an instance in any dimensional feature space. Depending on the domains these drifts can often happen together or individually. In the domain of spam detection the virtual concept drift alone happens as our insight about an obscure message may continue as before over a moderately extensive stretch of time while the overall recurrence of various kinds of spam may change definitely with time [16].

3.1 Change Types

In actuality, circumstances changes in data distribution over time may show in various structures. Subsequently we can say that concept drift is a perplexing blend of numerous sorts of drifts. In the event that an information stream of length 't' has only two information creating sources S1 and S2, the quantity of conceivable change patterns is '2^t'. Since information streams are conceivably unbounded, the quantity of source dispersion changes can be endless. Nevertheless, it is vital to distinguish basic structural sorts of drift, since the presumption about the change types is totally required for structuring adaptivity strategies. Basically six kinds of changes can happen in a solitary variable along time which is shown in Fig. 2.

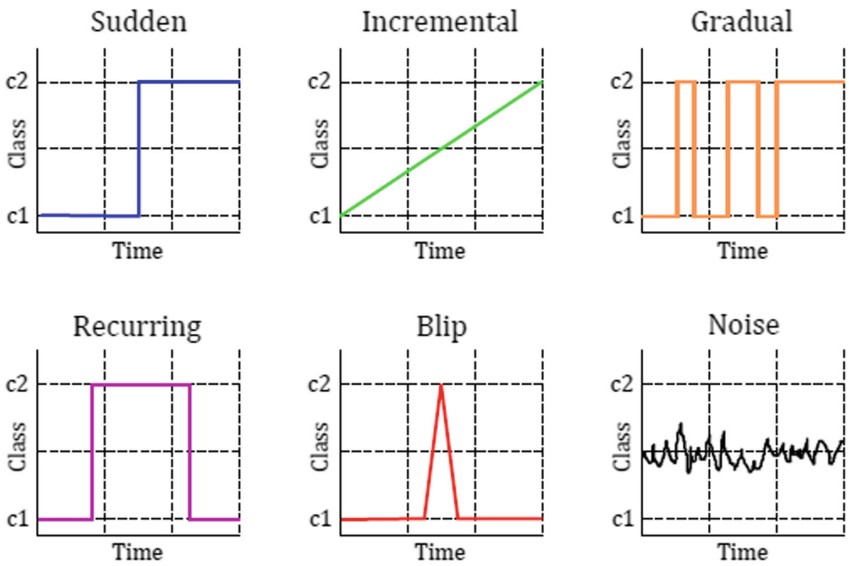


Fig. 2. Types of changes [15]

A change that happens unexpectedly at a moment and that irreversibly change the class label are called sudden drift while the incremental and gradual drifts are changes that happen gradually after some time. Incremental drift happens when variables gradually change their characteristics after some time, and gradual drift happens when the change includes the class distribution of variables. Transitory changes in which factors get returned after some time is called recurring drift which are frequently viewed by certain researchers as local drift. It happens when a few information generating sources are required to switch over time and reappear at unpredictable time interims. Due to the vagueness about when the source may return this drift is not certainly periodic. The blip viewed as an anomaly in a static distribution speaks to an uncommon occasion. In streaming data, distinguished blips ought to be disregarded as the change they speak too is irregular. The last plot represents random changes, which ought to be sifted through. Noise should not be considered as concept drift as it is an immaterial variance that is not associated with any adjustment in the source distribution.

3.2 Drift Detection Methods

The most significant element of research on concept drift is to create precise models that have methods to recognize and adjust to evolving information over time. The models ought to have the option to (1) recognize concept drift (and adjust if necessary); (2) recognize drifts from noise and be versatile to changes, yet strong to commotion; (3) operate in less than example arrival time and utilize not in excess of a fixed measure of memory storage. In case of streaming data basically two types of approaches are usually used: passive drift detection and active drift detection. The passive methodology adjusts a learner at standard breaks without pondering whether changes have really occurred, and it tracks changes heedlessly and revives the model constantly without requiring unequivocal change identification, while the active or dynamic methodology perhaps makes modification when a drift occurs. Dynamic methodologies commonly require change location modules. They function admirably in sudden drifting situations while passive methodologies work better for gradual drift which is in any case increasingly hard to recognize. To react to different sorts of concept drift rapidly, methodologies can be developed to utilize both passive and active frameworks to help learning in non stationary circumstances, which attempt to merge the best segments of both.

4 Concept Drift in the E-mail Domain

In email domain basic problem faced by the users is the filtering of spam messages. Rather than considering the accuracy as the main issue false positives and false negatives which happens due to the responses of spam is to be considered. Not only the spam behavior a concept drifting issue but also a problem that exhibits an overlap of perpetual, periodic and picaresque phenomena. The challenging problems faced in the filter design are issues like skewed and dynamic class distributions; unbalanced and

unpredictable error costs; complicated patterns; mind boggling, disjunctive and floating target idea; and difficulties of intelligent, versatile foes.

The skewed class distribution resulting from the uneven proportion of spam to ham is a serious issue as the prior distribution probability is not generally known. As a result the ratio of ham to spam varies considerably between the individuals. The quantity of spam got relies upon the email address, the level of exposure, the publicly assessed time and the upstream sifting. As the spam domain is dynamic, the class-conditioned feature probabilities also changes. The spam topics can be perpetual like advertisements for pornography sites, mortgage re-financing offers, job offers, money making schemes bids etc. It can also be bursty in nature with respect to some prevalent situation or happen as pandemics. Henceforth no clear claim case about the volume of spam as it can shifts impressively and non-monotonically on a day by day or week after week scale.

Another entanglement in filtering is the uneven error costs associated with the classification of spam and ham. In view with spam classifier, a spam mails are treated as a positive occurrences while ham mails as negative occurrences. Settling on a choice about a legitimate email to be spam (a false positive error) is regularly undeniably more lamentable than condemning a spam email to be veritable mail (a false negative error). A false negative basically purposes slight exacerbation as the customer sees an unwelcome message, however the false positive can result in exceptive issues. Such vulnerability is really regular in real scenarios, where specialists may experience issues expressing the careful expense of a mistaken activity, or the expense of the activity may change contingent upon outside conditions. On account of spam sifting, the vulnerability of error expenses may not change transiently but rather they do differ between clients.

The point for researchers is that the spam concept should drift accordingly with the changes that happens in spam content. But a few segments of the concept representations ought to stay steady or change just gradually. Others will rise amid scourges, as explicit tricks or promoting plans come into vogue. Indeed, even persistent topics don't reveal consistent term frequencies. As there are no standard metrics accepted by the society to evaluate the amount it is difficult to anticipate "spam" as a concept to linger over time. The spam streams get evolved over time as the spammers come up with new tricks and trades for promotion.

There is an alternate reason for concept drift: spammers are busy with an endless "arms race" with email filters. In due spammers have ended up being dynamically refined in their strategies for avoiding filtering could be checked for too. To sidestep basic filtering, spammers began to use content obscuring frameworks, for instance, embeddings counterfeit accentuation, using false HTML marks and including HTML comments in the midst of words. Whatever new sifting techniques emerge, it is simply a question of time before spammers discover approaches to sidestep them. In artificial intelligence concepts, spammers have a strong enthusiasm for developing the "spam" and "authentic" classes indistinct. Since the segregation capability of spam filters improves consistently, the subsequent concept drifts. Co-developing abilities show up frequently when access to a desired resource is all the while looked for and obstructed by keen, adaptive intelligent parties.

5 A System Framework for Hunting Concept Drift in Email Domain

The primary reason for concept drift in email classification and spam filtering is because of evolving e-mail content and presentation alluded as virtual drift. It also occurs due to the versatile conduct of spammers endeavoring to beat spam filters (virtual or real) and clients changing their frame of mind towards specific classes of messages beginning or ceasing to think of them as spam as real drift. In view of the behavioral changes the kinds of drift that are reflected by email are sudden, incremental, gradual and recurring. The greater part of the filtering systems can't identify spam messages precisely when the concepts drift occurs. In this way, it is required to have a separating framework to deal with concept drift precisely and rapidly. Our framework provides a six phase workflow as in Fig. 3: (1) Dataset selection (2) Parsing the email (3) Processing the content of the mail (4) Obtain the metadata and topics of the mail (5) Develop a drift detection algorithm (DDA) (6) Updating the classifier.

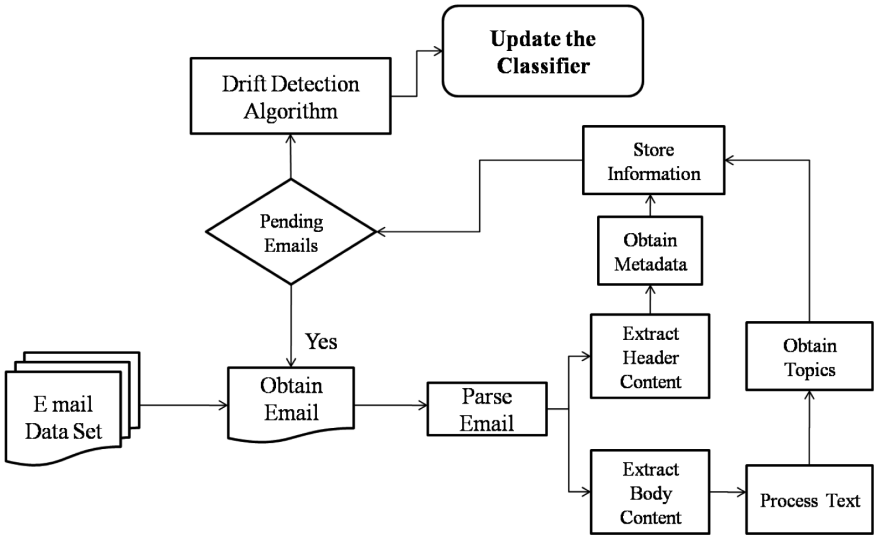


Fig. 3. Framework for spam detection

The benchmark data sets are necessary to evaluate the performance of any learning algorithms developed. To track the concept drift problem real-world spam and legitimate email datasets should be chronologically ordered according to their date and time of arrival. In our work we suggest Enron [17] as the benchmark dataset as the presence of concept drift is higher in this corpus. This data set was made public by the US Federal Energy Regulatory Commission (FERC). The topics of the messages in this corpus are identified with the business exercises of the venture so as to support seasonal changes maintenance in power supplies. These mails give the brilliant instances of recurring and gradual concept drift. Moreover, sudden drift in Enron corpus is

straightforwardly associated with the acquiring of new pursuits or the course of action of novel organizations.

Initially each email from the dataset is stacked into memory for further handling. At the second stage they are parsed to extricate the significant highlights from the header and body areas of mail. The header module gives the data with respect to email date, sender address considered the metadata that can be utilized as the underlying element for classification. If the email is from the known contact list of the user chances of being it a spam will be lesser. Hence they can be directly classified as ham and if the user is a strict user, he can adopt other information from the header like subject, timestamps or even use the body module information for updating the classification. Considering these points a single level strategy is better to be developed based on the metadata and content information. While parsing the body several preprocessing operations are carried out like stemming the word, removal of HTML tags, stop word removals etc. The information obtained from the header and the body is stored in a specific manner so as to retrieve it easily for the experimentation. For every topic associated with the mail a document frequency time series with time stamps are estimated to detect concept drift occurrences. This is then given as the input to the drift detection algorithm that predicts the type of drift that is involved. As already stated we look upon three types of drift sudden, recurring and gradual. The drift detection algorithm is designed to distinguish between three drifts. The classifier choice is a difficult task as the inherent characteristics related with each kind of concept drift require the utilization of explicit learning methodologies and classification systems. We prefer to use a single classifier like decision trees to classify the emails.

6 Conclusion and Future Outlook

We have presented a study of the phenomena called concept drift especially in the field of email domain. As spam is a co evolutionary problem researchers should be able to find solutions to track the drift or handle the evolving features. To handle such problem we have proposed a framework to discover such evolving features and handle the effects of the drift problem so that classifier will be able to adapt rapidly and precisely to improve the accuracy. The research is only in its initial stage where more experimentation is required to evaluate our method in the real scenario, develop new evaluation criteria to measure the effects of concept drift so that handling strategies can be easily developed and finally a novel classifier for classifying the emails.

References

1. Schlimmer, J.C., Granger, R.H.: Incremental learning from noisy data. Mach. Learn. **1**(3), 317–354 (1986)
2. Widmer, G., Kubat, M.: Learning in the presence of concept drift and hidden contexts. Mach. Learn. **23**(1), 69–101 (1996)
3. Aha, D.W., Kibler, D., Albert, M.K.: Instance-based learning algorithms. Mach. Learn. **6**(1), 37–66 (1991)

4. Narendra, K.S., Parthasarathy, K.: Identification and control of dynamical systems using neural networks. IEEE Trans. Neural Netw. **1**(1), 4–27 (1990)
5. Harries, M., Horn, K.: Detecting concept drift in financial time series prediction using symbolic machine learning. In: Proceedings of the 8th Australian Joint Conference on Artificial Intelligence (ACAI) (1995)
6. Klinkenberg, R.: Concept drift and the importance of examples. In: Text Mining—Theoretical Aspects and Applications, pp. 55–77. Physica-Verlag (2003)
7. Kilander, F., Jansson, C.G.: COBBIT—a control procedure for COBWEB in the presence of concept drift. In: Brazdil, P.B. (ed.) Proceedings of European Conference on Machine Learning (ECML), pp. 244–261. Springer, Berlin (1993). https://doi.org/10.1007/3-540-56602-3_140
8. Spinosa, E.J., de Leon F., de Carvalho, A.P., Gama, J.: Olindda: A cluster-based approach for detecting novelty and concept drift in data streams. In: Proceedings of the 2007 ACM Symposium on Applied Computing, pp. 448–452, March 2007. ACM (2007)
9. Lazarescu, M.M., Venkatesh, S., Bui, H.H.: Using multiple windows to track concept drift. Intell. Data Analy. **8**(1), 29–59 (2004)
10. Delany, S.J., Cunningham, P., Tsymbal, A.: A comparison of ensemble and case-base maintenance techniques for handling concept drift in spam filtering. In: FLAIRS Conference, pp. 340–345, January 2006
11. Delany, S.J., Cunningham, P., Tsymbal, A., Coyle, L.: A case-based technique for tracking concept drift in spam filtering. In: International Conference on Innovative Techniques and Applications of Artificial Intelligence, December 2004, pp. 3–16. Springer, London (2004)
12. Fdez-Riverola, F., Iglesias, E.L., Díaz, F., Méndez, J.R., Corchado, J.M.: Applying lazy learning algorithms to tackle concept drift in spam filtering. Expert Syst. Appl. **33**(1), 36–48 (2007)
13. Nosrati, L., Pour, A.N.: DWM-CDD: dynamic weighted majority concept drift detection for spam mail filtering. World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng. **5**(8), 829–832 (2011)
14. Ruano-Ordas, D., Fdez-Riverola, F., Méndez, J.R.: Concept drift in e-mail datasets: an empirical study with practical implications. Inf. Sci. **428**, 120–135 (2018)
15. Brzezinski, D., Stefanowsk, J.: Mining data streams with concept drift. Poznan University of Technology Faculty of Computing Science and Management Institute of Computing Science (2011)
16. Tsymbal, A.: The problem of concept drift: definitions and related work. Computer Science Department, Trinity College Dublin, vol. 106, no. 2, p. 58 (2004)
17. https://www.cs.cmu.edu/∼/enron/

Product Design Using Virtual Reality

V. Ansal(✉), M. Shruthi, Grynal D'Mello, Subhin Antony, and I. C. Sharath

NMAMIT, Nitte, Udupi, Karnataka 574110, India
{ansal.v, shruthim.gatty, grynal}@nitte.edu.in,
{subhin7, icsharathlll}@gmail.com

Abstract. Product design is an important step in creation of a new product or service. It involves the modelling of the product and also various other steps to make it unique. Conventional CAD modelling involves the usage of standard peripheral like keyboard or mouse. In this paper, Virtual Reality (VR) is used for developing a 3D product design tool. This supports more control over the dynamic models and gives a more improved user experience. Using this tool user can access 3D modelling area along with the toolbox through the VR headset. User can then create the model and interact with it using his/her hand. These interactions are monitored which in turn gives response to the processing unit to generate the model. Once the modelling is done, the model can be saved to the system in a format supported by a 3D printer or any other format supported by different modelling tool.

Keywords: Product design · Virtual reality · CAD modelling · 3D printing

1 Introduction

Activities involved in the creation of a new product are called product design. Product design consists of several stages. The first stage is the identification of a problem to be solved. The objectives to be met by creating new product will be defined next by the designers. This will in turn establish the parameters within which they are supposed to work. After the initial phases, original ideas will be created from brainstorming sessions. This will produce a pool of ideas. From this a few promising concepts will be selected. Designers then start creating drawings for these selected ideas. Traditionally pencil and paper were used for drawing the sketches. Later CAD tools became popular choice of most of the designers. Numerous revisions will be done on the selected concepts during the prototyping phase. This will bring light to any issue with the physical product. The final prototyping stage will undergo after sorting out these issues. This will be the representation of final finished product. The model is finally ready for production.

Virtual reality is a modern technology where users will be able to view a complete secondary world using headset. It is described as Computer Generated Simulation of a Three-Dimensional Image or Environment. It allows users to interact with it in a way that is not possible with other medium.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 927–935, 2020.
https://doi.org/10.1007/978-3-030-37051-0_104

One important aspect that is affected by virtual reality in design and manufacturing is design for assembly [1]. A detailed review of the understanding of the field and support tools for an effective computer support tool is done in [2]. The use of virtual reality in 3D CAD modelling, the construction of complex 3D model and the method of reading based on VR is introduced in [3]. The emergence of motion sensing devices is highlighted in [4], which will better help designers in creating 3D models. The authors have introduced Leap Studio which is a solution for interactive communication between users and 3D modelling applications. This gives high accuracy in sensing the movements of hands and fingers. This brings comfort and convenience to the user. A study on a marker less human robot interface is conducted in [5]. This is derived from the idea that the manipulator copies the movements of human hands. This method has advantage of operating dual robots through user's hands in a marker less and contact less environment. LeapMotion (LM) sensor, which gives the position and orientation of human hands in real-time is introduced in this paper. An integrated urban 3D modelling and rendering system using standard mobile 3D graphic API (Application programming Interface), and OPENGL-ES (Open GL for Embedded System), with MS EVC 4.0 MFC is implemented in [6]. Paper [7] discusses about product design system through intranet or internet, which can facilitate the partners to contribute and/or share their design ideas to get optimal design. In [8] a study is conducted for using virtual construction methodology, and suggests some methodologies for using it in the design phase of construction project. The methodologies are also verified using a virtual construction system linked with 4D CAD tool. 4D CAD system is a simulation tool used for visualizing the completed picture of construction facility by construction schedule. Prototype of an integrated progress control system is developed to visualize construction progress in [9]. This system uses 4D CAD linked with telepresence tool. Two site images are compared to get the progress status. By integrating computer graphics, VR and network into Web based learning environment, an attempt is made in [10] to apply the principle of virtual reality (VR) distributed virtual environments (DVE) technologies to a complex graphics design system (CGDS). An improved link methodology in 4D CAD system for plant project management is done in [11]. The real time visual feedback is realized in the VR screen by creating an interactive design system based on a graphics tablet and VR device in [13]. This gives theoretical reference for professional design software.

In this work LeapMotion [12] sensor in combination with VR is used to support 3D CAD modelling, which enables users to have immersive experience while modelling. Leap Motion sensor is a sensor which directly gives the position and orientation of human hand. This makes the user possible to draw models in 3D. Software is developed using WebGL which supports a wide variety of platforms including Android, Windows, Linux, Mac etc., without the need of writing for different graphics card. To enable VR support in multiple browsers, an open specification called WebVR, "Bringing Virtual Reality to Web" is being used to create the application. To enable easy integration WebGL library called Three.js is also used. This application is explicitly developed for modelling of 3D objects.

2 Hardware Description

The hardware setup consists of three main components, VR headset, LeapMotion Sensor and a 3D printer. It is described in detail below.

2.1 VR Headset

It is mounted on head of the user and it will give the virtual images to the user. VR headsets are very common in computer games. It is also used widely for training purpose. It consists of a stereoscopic HMD (Head Mounted Display) which provides separate images for each eye. Figure 1 shows the components of a mobile VR headset.

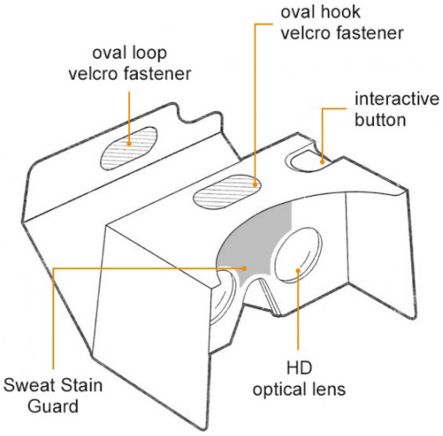


Fig. 1. Components of a mobile VR headset

2.2 LeapMotion Sensor

LeapMotion sensor senses finger and hand movements. The major components of LeapMotion sensor are two cameras and three infrared LEDs as shown in Fig. 2. Infrared light of 850 nm wavelengths is tracked using this. Since it is outside the visible spectrum human eye cannot see these lights. The wide-angle lens of LeapMotion sensor gives an interaction space of less than eight cubic feet. The shape of the space is a pyramid similar to the field of view of intersection of binocular cameras. The sensor data then stored in device's local memory and resolution adjustments are done if there any. LeapMotion Tracking software is used to stream the data through USB.

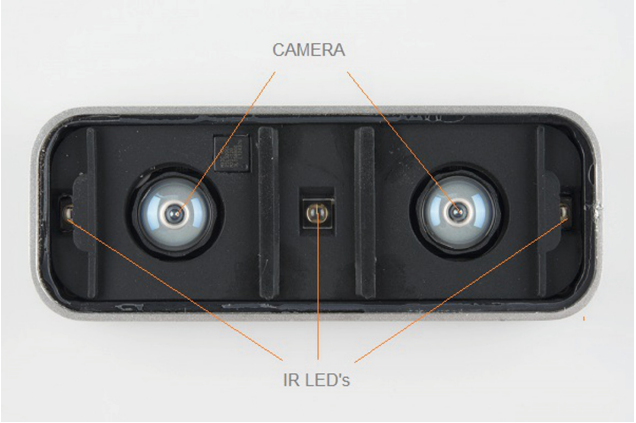


Fig. 2. LeapMotion Sensor

2.3 3D Printer

3D printer is used to print three dimensional objects from a digital file. Additive process is used to create 3D objects. In the additive process, successive layers of materials are laid down until the object is created. Compared to traditional manufacturing method 3D printing consumes less material to create complex shapes.

An open source firmware called *Marlin* is used popularly for 3D printers. This software runs on 8-bit microcontrollers like AVR. Arduino Mega2560 with RAMPS 1.4 is the reference platform for *Marlin*.

3 Working

Cross-browser JavaScript library and Application Programming Interface(API) *three.js* is used to create and display animated 3D graphics in the web browser which also uses WebGL. *THREE.WebGLRenderer()* is used as the default renderer. A perspective camera is provided by calling *THREE.PerspectiveCamera()* function. *WebVR UI* library provided by Google which provides javascript object *webvrui* is used for calling *EnterVRButton()*, which also returns the object for calling *requestAnimationFrame()*. *Three.js* library *VREffect* is used to provide the stereo-scopic view to the renderer. So *VREffect* is called on *requestAnimationFrame()* only when supported VR is obtained. Object returned by *EnterVRButton()* is again called with *VRDisplay()* to provide the display component on which *requestAnimationFrame()* is called. Leap Motion Controller JavaScript API provides data at the rate of 60 frames/s (depends upon browser rendering rate) using *WebSocket*. This data contains information about each finger on hand. If all part of a finger is not visible, the finger characteristics are estimated based on recent observations and anatomical model of the hand. LeapJS(Leap Motion Java Script) API includes a function called *Leap.loop()*. The Leap Motion service runs a *WebSocket* server on the local host domain at port 6437. *A WebSocket* service provides

tracking data in the form of JSON messages and presents the data as regular Javascript objects. *Leap.loop()* is used for automatically setting update loop for the application which creates a controller object and connects to the *LeapMotion* WebSocket server.

In this work, browser animation loop called *requestAnimationFrame()* is used for looping through frames. To support WebVR, request *AnimationFrame()* should be called on the VR animation loop. *webvr-ui* library provides the object on which *requestAnimationFrame()* is called. *Leap.loop()* provide *frame.gesture* object to provide feedback when a gesture is recognized. These gestures are recorded and used for clicking elements, creation of new points etc. This also provides the points at which the gesture has been recognized. LeapJS API provides way to add additional plugins to support modification, usage improvements to the data provided by the Leap Motion Controller. A *riggedHand* feature is used to render a rigged hand and *boneHand* is provided to get a bone hand in view. "transform" plugin is used to invert the hand to support VR and to fix the hand to the camera, so that user has the hand in view all the time. *riggedHand* provides a default scene, camera and light setups in its default setup. Due to the inability of providing anti aliasing support, default scenes and camera are not used, which also provides more control over the animation loop. Working block diagram is shown in the Fig. 3.

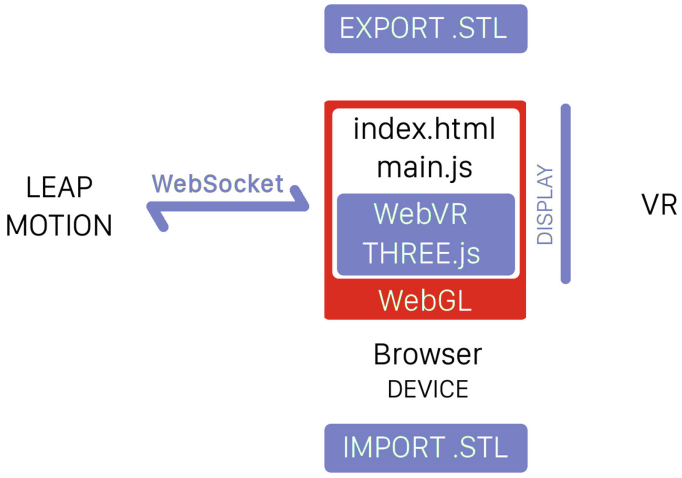


Fig. 3. Working model

4 Results

A working prototype of 3D modelling software is implemented. There are various features that are missing from traditional modelling software due to its long history of development process. This software enables users to create sketches, which includes drawing lines, circles, splines, Bezier curves with LeapMotion and VR support. User will be able to extrude sketches and cutout one extruded model or any part of the design. Browser requires more enhancement to handle multiple data requests at the same time, 200 frame/sec of LeapMotion gets interrupted on various other data requests.

A user interface is developed based on the analysis of existing CAD modelling software and understanding how it should be changed to meet the need of VR

requirement. Hand is fixed near to the camera, so around 50 cm is kept for easy handling of gestures and easier hand movement. An Interactive Plane defined in *LeapJS-Widget* is used as buttons, others being designed using *Three.Js*. Workings of various modelling tools are described below.

4.1 Sketching Tool

A Screen Tap gesture defined in the *LeapJS* library is used as the gesture for creating new points for custom sketching. Sketching for custom shapes, arc, triangle, polygons are enabled. Every point that is being clicked upon is converted into shapes as shown in the Figs. 4 and 5.

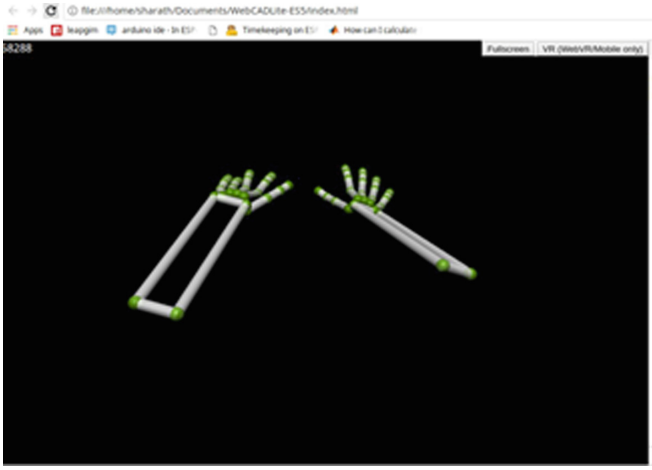


Fig. 4. Hand gesture recognition

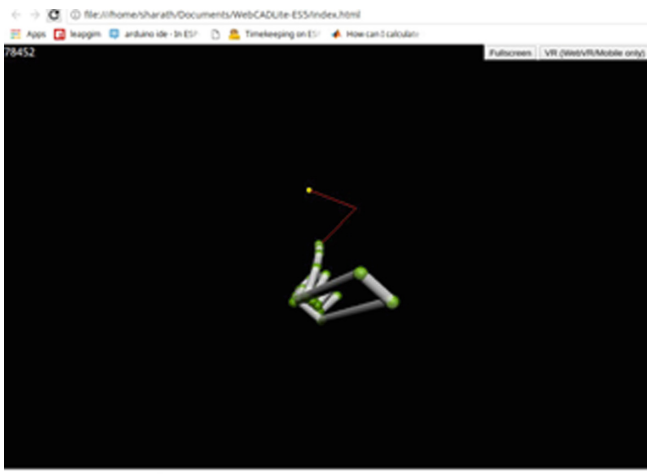


Fig. 5. Drawing shapes using hand gesture

4.2 Extrude Tool

It is used to create 3D solids from an enclosed area as shown in Fig. 6. Objects can be extruded orthogonally from the plane of source object. Extrusion is done from the shape created from sketch. *Three.js*. *makeGeometry()* is called for converting from shape to geometry. Extrude feature of Three.js is used for extruding the shape. This includes the size of the extrusion to be passed as shown in the Fig. 7.

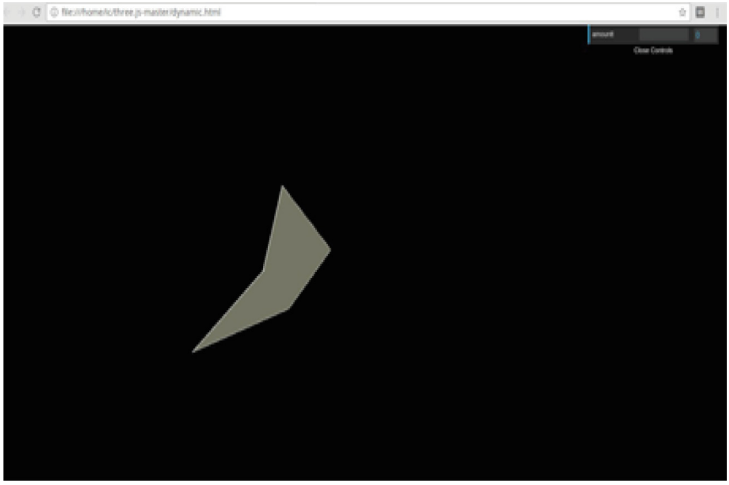


Fig. 6. Creating a closed area

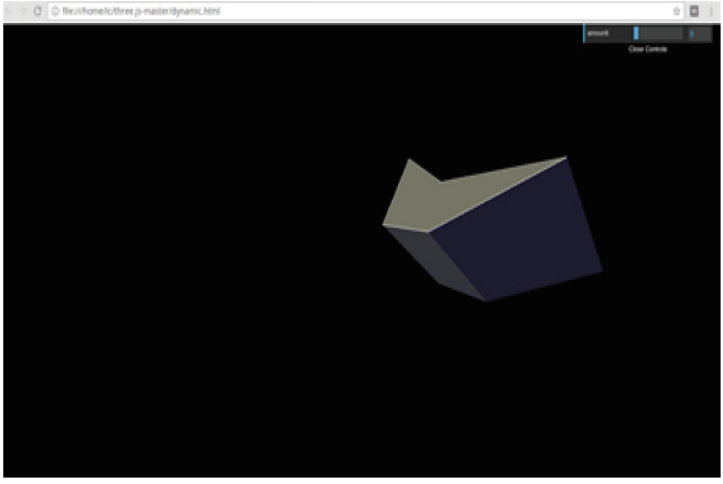


Fig. 7. Extruding a closed area

4.3 Cutout Tool

Cutout tool creates a cutout in a walled object (e.g., a pipe) to another walled object. User is able to sketch the cutout as shown in Fig. 8 and give the depth to which the cutout has to be made. Cutout is done by creating two 3D models and subtracting one from the other using *csg.js* as shown in the Fig. 9.

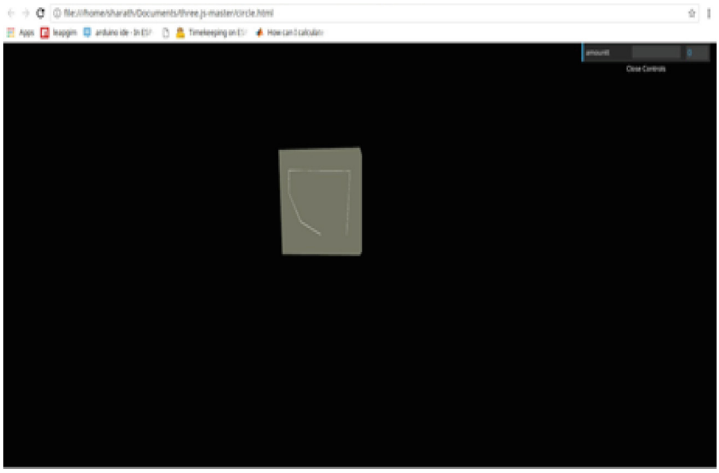


Fig. 8. Selecting an area to cut

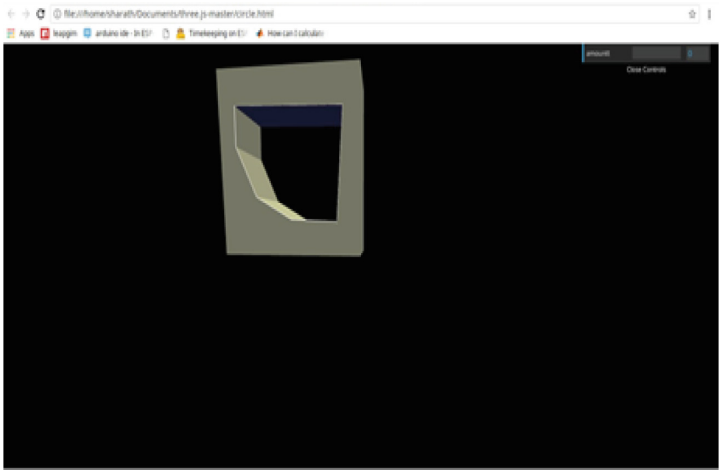


Fig. 9. Selected area is cut using cut-out tool

5 Conclusion

In this work, WebGL is used instead of OpenGL for graphics processing for this project. Elimination of a software platform leverages further advancement that existing technology cannot provide. One of the highlights of 3D modelling in WebGL is it

benefits a lot on platform independent development. VR and LeapMotion introduces a new way of interactive sensing, making software based inputs more customizable. By optimizing the software and by adding further additional features it can be commercialised. Further improvements can be done by creating user interface supporting hand gesture feature as well as support for AR and VR. Other than LeapMotion sensor input also can be inspected.

References

1. Jayaram, S., Connacher, H.I., Lyons, K.W.: Virtual assembly using virtual reality techniques. Int. J. Comput.-Aided Des. **29**(8), 575–584 (1997)
2. Chandrasegaran, S.K., Ramani, K., Sriram, R.D., Horva, I., Bernard, A., Harik, R.F., Gao, W.: The evolution, challenges, and future of knowledge representation in product design systems. Int. J. Comput.-Aided Des. **45**(2), 204–228 (2013)
3. Fu, J.: Study on realization of dynamic interaction with CAD complex model in virtual reality system. In: Proceedings of Second International Conference on Digital Manufacturing and Automation (ICDMA), pp. 1168–1171. IEEE (2011)
4. Do, N.Q., Cai, H., Jiang, L.: Leap studio: a virtual interactive 3D modeling application based on web GL. In: Proceedings of 5th International Conference on Digital Home (ICDH), pp. 374–379. IEEE (2014)
5. Du, G., Zhang, P., Liu, X.: Markerless human manipulator interface using leap motion with interval Kalman Filter and improved particle filter. In: IEEE Transactions on Industrial Informatics, vol. 12, no. 2, pp. 694–704 (2016)
6. Lee, K.: 3D urban modeling and rendering with high resolution remote sensing imagery on mobile 3D and web 3D environments; System architecture and prototype implementation. In: Proceedings of Urban Remote Sensing Joint Event, pp. 1–5. IEEE (2007)
7. Ma, S.-Q., Gao, Z.-L.: A solution to integrate CAD/CAE system and VR for complex product design processes. In: Second International Conference on Information and Computing Science, Manchester, UK (2009)
8. Kang, L.-S., Park, S.-Y., Kim, H.-S., Kim, C.-H.: Application of VR technology linked with 4D CAD system for construction project. In: International Conference on New Trends in Information and Service Science, Beijing, China (2009)
9. Kang, L.-S., Moon, H.-S., Kim, H.-S., Choi, G.-R., Park, N.-J., Kim, C.-H.: Visualizing work progress information of construction project by web and VR application. In: Fifth Asia Modelling Symposium, Kuala Lumpur, Malaysia (2011)
10. Sung, W.-T., Ou, S.-C.: Development of a distribution VR-based complex graphics design system. In: IEEE/ASME International Conference on Advanced Intelligent Mechatronics Proceedings, Como, Italy (2001)
11. Seok, K.L., Seong, K.H., Seok, M.H., Hak, K.C.: Improvement of link process in 4D CAD viewer by using interface board for construction project management. In: 2009 Third International Conference on Advanced Engineering Computing and Applications in Sciences, Sliema, Malta (2009)
12. Nho, Y.-H., Seo, J.-W., Seol, W.-J., Kwon, D.-S.: Emotional interaction with a mobile robot using hand gestures. In: 11th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI), Kuala Lumpur, Malaysia (2014)
13. Shen, D., Zhou, Y.: Effect of VR interactive design system on visual feedback and operational experience. In: 10th International Symposium on Computational Intelligence and Design (ISCID), Hangzhou, China (2017)

Smart Museum Using Li-Fi Technology

T. Kavitha(✉) and C. R. Angel Reena

Veltech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai, India
drkavitha@veltech.edu.in

Abstract. Light-Fidelity is a wireless technology which uses visible light as a medium instead of radio waves. To improve the performance in this technology, various studies have been carried out. Development of new technologies in the today's world everything is extended to smart and smarter. Our environment needs to become smarter to match these smart things. In the smart museum environment, Li Fi is an efficient technology with superior bit error rate. Free space optical communication is also called as visible light communication referred ad Li-Fi. In this paper we transmit the data using LEDs in visible light region of electromagnetic spectrum. Using simple light sources we attain the transmission of data. In this paper, the Li-Fi technology is used to transmit the data in museums in order to provide the visitors a better understanding and knowledge of the ancient artefacts and technologies present around them.

Keywords: Light fidelity · Free space optical communication · Smart museum · Light emitting diode · Microcontroller

1 Introduction

Wireless communication technologies and wireless-fidelity are operating in the radio frequency spectrum. Alternate methods are developed due to the interference, over-crowded RF band, limited bandwidth in the existing system. Small portion of the electromagnetic spectrum is called the RF band used to transfer the data. German physicist proved that the visible light band is useful for data transmission and also introduced Li-Fi technology. Light generated by the LED bulbs acts as a transmission medium for short range of wireless communication. It contributes more than the existing technology (Bluetooth, WI-Fi, RFID) and possible to transmit data with high transmission rate. The integration of illumination and communication services from same source reduces the power consumption and infrastructure complexity [1–3].

Wireless fidelity (WI-Fi) and blue tooth recent wireless communication technologies use the radio waves for transmitting the data. New alternative techniques are expected to transmit data efficiently and wirelessly, even though the current techniques are widely spread. The reason is that there is a band limitation in radio frequency and also affected by the interference. More research has been conducted to confirm the possibility of transferring a data over wireless medium through visible light, called light-fidelity [4–6].

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 936–942, 2020.
https://doi.org/10.1007/978-3-030-37051-0_105

Light fidelity is basically a wireless optical communication technology. Li-Fi uses LED's for the data communication purposes. The Li-Fi technology originated in the nineteenth century where a photo-phone was used to transmit data over a several hundred meters and that was done with the help of sunlight [7, 8]. The development of Li-Fi was in phase with the advancement of LED's. In the smart museums, the light emitting diodes are used instead of lasers. Although lasers are more accurate, the LED's are safer to use than the lasers. One of the greatest benefits of using a Li-Fi technol0gy is that it promotes faster transmissions than WI-Fi [9].

Li-Fi provides high speed data transmission, much higher than wifi. It's frequency spectrum is 10000 times more than radio. It enables data transfer using common LED's used in the homes and speeds up to 224 Gb/s. It has the greatest potential of changing the internet usage over the years. Both WI-Fi and Li-Fi broadcast data electromagnetically. Radio waves are used in WiFi and Visible light is used in LiFi such as LED's for the transmission of data. For receiving the light signal and signal processing element for converting the data into a stream able content Li-Fi uses photo detector. Although Li-Fi is more accessible and also ought to be used on a major scale, it requires the LED's to stay switched on all the time even when not in use. This is one of the major drawbacks of the Li-Fi technologies [10].

In human being lives art and cultural plays an important role. Mainly a museum is a collection of artifacts, cultural, historical and scientific data's. Public museum displays permanent or temporary for public viewing. In us alone 35,000 museums are available (Washington Post). Nowadays it is a tool for entertainment. Art galleries and museums provide a human guides or paper booklet. Frequent visit of museum is reduced; it is difficult for the center keepers to concentrate on all customers. Therefore, smart museums need to be created for customized historical center visits [11, 12]. Physical labor, hazardous and automated agents are replaced in Smart environment. This paper proposed to design a system for smart museum using LiFi technology. The paper is organized as follows. Section 2 discuss about the related works in the area of smart museum and visible light communication. System design and working is explained in Sect. 3. Hardware results are discussed in Sect. 4 and conclusion in Sect. 5.

2 Related Work

G. J. Sullivan, et al. stated WI-Fi to be the most trending domain as the internet users almost double every year. And this leads to an enormous load on radio spectrum that leads to congestion. To get better bandwidth, efficiency and speed, the Li-Fi has was made to replace. As it is a 4 bidirectional and wireless mode of communication using light. It uses the unused visible spectrum and reduces the load on radio spectrum. Instead of radio waves he used light as a medium. Instead of using modems, Li-Fi uses LED bulbs with transceiver. Data transmission in Li-Fi is about 100 times faster than WI-Fi. Priyanka et al. proposed a smart system that enables a mobile device, it interacts with an IoT based environment and acts as a museum guide. RFID tag is provided to the user. Through GSM module OTP is send to the mobile device. This OTP is used to access the smart museum environment. The visitors can scan the QR code of the artwork, it gives the profile of that artwork. The database is maintained by the museum

guardian. At last the visitors share the feedback about the artwork through the smart museum application. Mainetti et al. proposed a location aware architecture for heterogeneous building automation system. Their architecture removes the heterogeneity of smart devices for smart environment and automatically manages the environment based on the user defined rules. Thinagaran et al. proposed a light weight IoT device management framework for smart home services. The framework can be deployed at home gateways and consumer smart devices. A prototype implementation and performance evaluation results are also presented. Majed et al. designed a smart electronic guide for museums. It provides the pictorial, scripted and vocal information about each object in the museum to the museum visitors. AVR microcontroller is used to transfer the information to the visitors.

3 System Design and Working

The process comprises of very simple procedures. Initially the data of the object is fed into to microcontrollers. The controller used, acts as a flash memory and stores the data. The data storage is the work done by the memory unit. For every data stored the memory location is addressed. The control line also known as the read write line carries out the data to and from the memory. Here the Special Function Registers will be utilized by the CPU and fringe modules are used for controlling the coveted task of the gadget. The Special Function Registers can be grouped into center (CPU) and fringe. The number-crunching status of the ALU, RESET status and the bank select bits for information memory are list in STATUS, the goal for a guideline that influences the Z, DC or C bits, at that point the keep in touch with these three bits is crippled. These bits are set or cleared by the gadget rationale. The TO and PD bits are not writable, in this way, the consequence of a direction with the STATUS enroll as goal might be not quite the same as expected. For r/w = 1, read r/w = 0, write (Figs. 1 and 2).

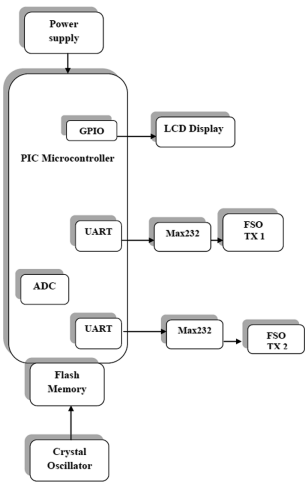


Fig. 1. Transmitter

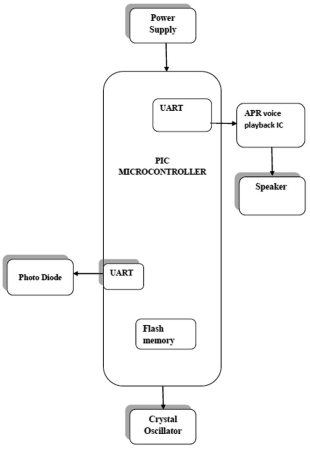


Fig. 2. Receiver

4 Results and Discussions

The output is in two forms. They are both displayed through the LCD and a audio description is also given. The LCD displays are pretty common. Whereas the Li-Fi audio is quite different as the audio input is given to the transmitter section by means of a voice play back. The transmitted voice play is transmitted and gets received in a Li-Fi receiver. The received data gets amplified by an audio amplifier and the output is given to the speaker. The speaker carried by the user is actually embodied in the photodiode which acts both as the sensing end and also a speaker. Thus the data is displayed via light.

The kit 1 consists of a LED light that is used to transmit date in the form of light as shown in Fig. 3. A step down transformer is used to convert the 230 V into 12 V. This

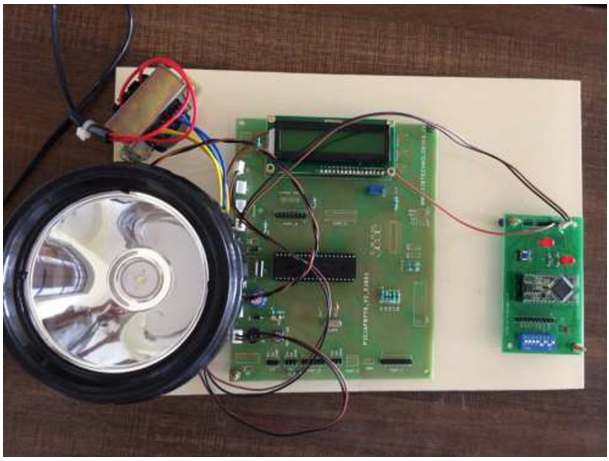


Fig. 3. Hardware kit 1

12 V is given to the PIC16F877A Micro-controller board and also to the LED light. 5 V supply is given to the speaker with the amplifier. Another 12 V is given to the Photo-diode. This photo-diode is used to detect the light signal and converts it into the audio format that is already stored in the chip APR9600. This chip is again given a 12 V supply and the data in the form of audio is recorded manually in the APR9600 board (Fig. 4).

The kit 2 consists of a LED light that is used to transmit date in the form of light. A step down transformer is used to convert the 230 V into 12 V. This 12 V is given to the PIC16F877A Microcontroller board and also to the LED light. 5 V supply is given to the speaker with the amplifier. Another 12 V is given to the Photodiode. This photodiode is used to detect the light signal and converts it into the audio format that is

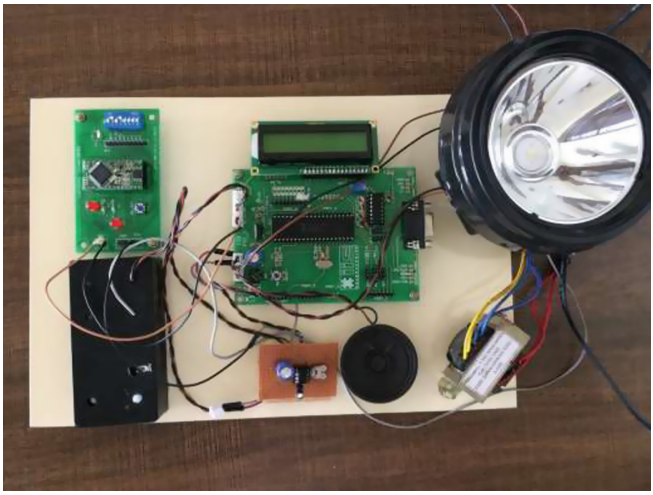


Fig. 4. Hardware kit 2

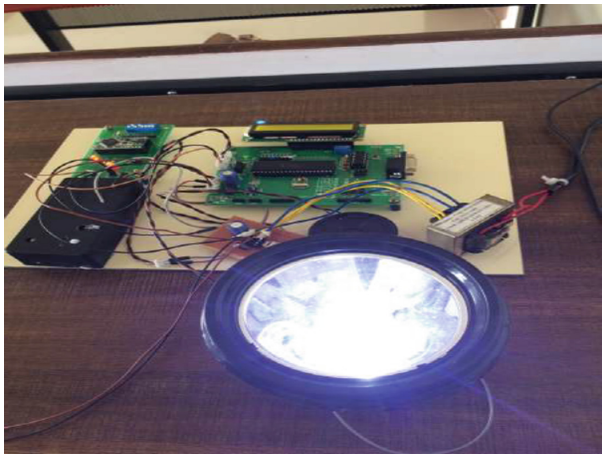


Fig. 5. LCD Light Transmits data

already stored in the chip APR9600. This chip is again given a 12 V supply and the data in the form of audio is recorded manually in the APR9600 board.

In these images, the data transmission through light is shown. In Fig. 5 the LED light is switched ON and the photodiode is in contact with the LED. The data is read and the output is displayed in the form of audio through the speakers (Fig. 6).

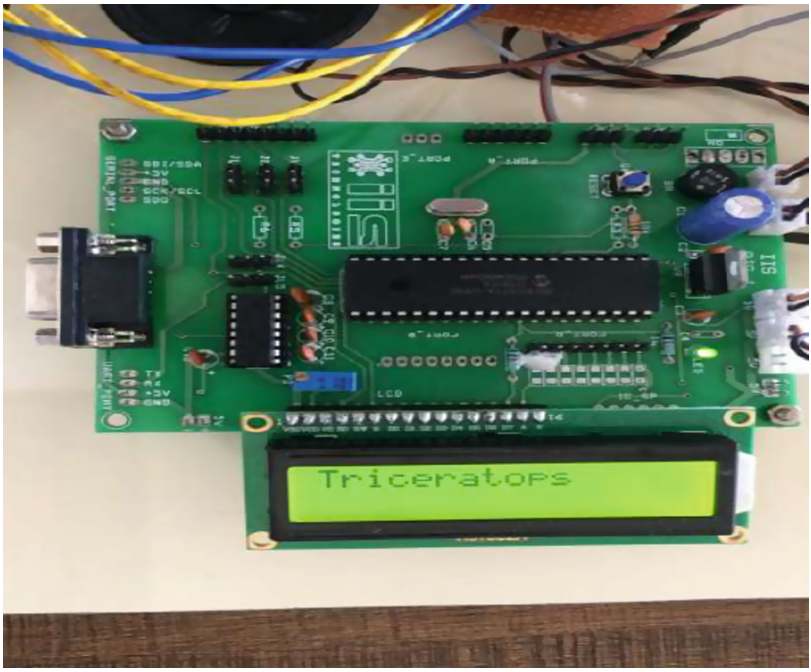


Fig. 6. The title of the data is displayed using a LCD screen.

5 Conclusion

This new technology promises a great potential in the field of wireless communication. This growing and upcoming technology overcomes the demerits in radio communication. Therefore, there is certainty of development of future applications of the Li-Fi which can be extended to different platforms and various walks of human life. Also Li-Fi is pretty easy to use and as far as security reasons are concerned, Li-Fi technology promises high security as this uses LED's instead of lasers. Hence lasers are harmful to human eyes, LED's are used which are more feasible and cheap. They are also pretty accessible when it comes to reliability. Thus the technology proves to be a success and can be relied on in every field in the future.

References

1. Kulkarni, S., Darekar, A., Joshi, P.: A survey on Li-Fi technology. In: IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1624–1625 (2016)
2. Leba, M., Riurean, S., Ionica, A.: LiFi–the path to a new way of communication. In: 12th Iberian Conference on Information Systems and Technologies (CISTI) (2017)
3. Parwej, Y.: The next generation of wireless communication using Li-Fi (Light Fidelity) technology. J. Comput. Netw. **4**(1), 20–29 (2017)
4. Sutrave, P., Smt. Rekha, S.: Authenticated and automated museum using RFID and IOT. Int. J. Comput. Eng. Technol. (IJCET) **9**(3), 69–75 (2018)
5. Dutta, S., Sharma, K., Gupta, N., Lovedon Bodh, T.: Li-Fi (Light Fidelity)—a new paradigm in wireless communication. Int. J. Innov. Res. Comput. Commun. Eng. **1**(8), 1654–1658 (2013)
6. Khasbag, S., Ranade, S., Wani, A., Hiralikar, P.: Smart museum design based on indoor localization. IJCSN Int. J. Comput. Sci. Netw. **5**(2), 299–301 (2016)
7. Medina, C., Zambrano, M., Navarro, K.: LED based visible light communication: technology, applications and challenges—a survey. Int. J. Adv. Eng. Technol. **8**(4), 482–495 (2015)
8. Salim Sayed, S., Ghanshyam Agrawal, N.: Li-Fi: an alternative to Wi-Fi. IJCSN—Int. J. Comput. Sci. Netw. **6**(6), 787–791 (2017)
9. Sullivan, G.J., Ohm, J.-R., Han, W.-J., Wiegand, T.: Overview of the high efficiency video coding (HEVC) standard. IEEE Trans. Circuits Syst. Video Technol. **22**(12), 1649–1668 (2012)
10. Mainetti, V.M., Patrono, L.: A location-aware architecture for heterogeneous building automation systems. In: IFIP/IEEE International Symposium on Integrated Network Management (IM), 11–15 May 2015
11. Perumal, T., Datta, S.K., Bonnet, C.: IoT device management framework for smart home scenarios. In: IEEE 4th Global Conference on Consumer Electronics (GCCE), October 2015
12. Rostamian, M., Parsa, M., Groza, V.: Design and fabrication of a smart electronic guide for museums. In: IEEE Transaction on Applied Computational Intelligence and Informatics (SACI), 30 July 2012

Analyzing the Power of Social Media in Solving Urban Issues: A New Aged Community Helper

Pranali Yenkar(✉) and S. D. Sawarkar

Datta Meghe College of Engineering, Airoli, Navi Mumbai, India
pranaliyenkar@yahoo.com, sudhir_sawarkar@yahoo.com

Abstract. Citizens living in the city are the real asset for the city. The main aim of the smart city concept is to have a satisfied citizen with better quality of life. Constant innovation in the field of ICT allows smart citizens uses this opportunity to sense the city surrounding and express their opinions and concerns on online platforms like Social Media. Hence in the era of a smart city, instead of using the traditional ways of collecting the needs and complaints of citizens like surveys and polls, government can also uses social media posts to understand the civic problems and provide the upgraded service in a timely manner. So this study presents the survey of the existing work where social media has been used to identify needs and issues faced by the people.

Keywords: Natural language processing · Sentiment analysis · Smart governance · Social media analytics

1 Introduction

1.1 Smart Government

Tremendous amount of growth in the field of information and communication technologies i.e. ICT fuels the economic and technical advancement which eventually helps a city progresses to the 'smart city'. Smart city domain is having multiple facets to it ranging from infrastructure, mobility, energy, social science, education, economics, safety and many more. This attracts the continuous flow of people to the smart city in anticipation of better opportunities and fulfills the basic requirement of good quality of life. Unfortunately the vast amount population caused several other issues like excessive land utilization, waste management, traffic congestion, water and noise pollution which actually deteroits the overall environment. It became a massive challenge to the existing traditional government to manage the ever- increasing issues of the city. Hence one of the key pillar in the journey of becoming a 'Smart City' is 'Smart Government'. The aim of the smart government is to take the smart decisions for better utilization of available critical recourses and provide a livable city to its residents [1]. One of the major steps taken by Smart government to achieve the goal is to sense and analyze the valuable information about the city by integrating modern techniques like IOT devices, sensors planted across the areas and smart vehicles, open data etc. [2]. Figure 1 depicts different ways to gather the information related to city events.

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 943–954, 2020.
https://doi.org/10.1007/978-3-030-37051-0_106

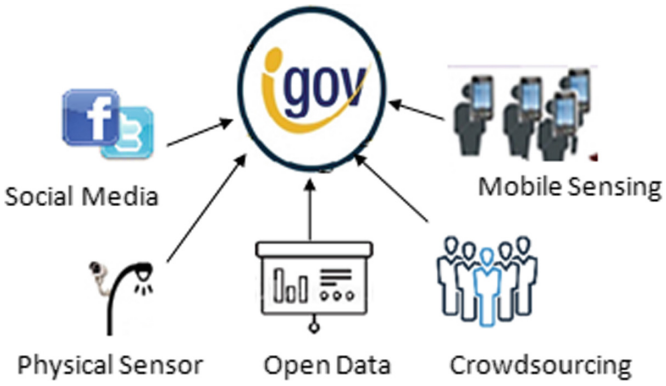


Fig. 1. Information gathering techniques

Innovative digital technologies provides the static information about the surroundings like what is happening and where but most of the times the invisible factors cannot be captured [3]. Citizens plays a very crucial role in capturing all the unrecorded details as they are the ones using the city resources in their daily lives. Hence crowd sourcing techniques has become a powerful tool of improvement in the service delivery. Government can take help of surveys and polls to discuss the urban issues but these are very time consuming and cumbersome ways to collect the data. Considering the revolution in information and communication technologies, efforts has been taken to understand citizen's needs and concerns by developing different websites, online portals and mobile applications like FixMyStreet, PublicStuff, seeClickFix, Novoville, imcity. Along with these existing platforms, citizens also prefers to share their observations and feelings on widely spreaded online platform like social media [4].

1.2 Social Media

Social media has been proved a goldmine of data where citizens acting as a sensor continuously uploading their issues, opinions and thoughts on the city environment. Government can use this medium to listen to citizen's voice very quickly and precisely. Even though social media platforms like Twitter and Facebook can be considered as a promising tools for collaborating, sharing and monitoring the urban issues, interpreting the vast amount of data written in the natural language by the netizens and extracting the useful insights of data to reach to some smart decision is a very challenging task.

1.3 Social Media Analytics

Social media analytics starts with extracting the relevant information using keywords or hash tags using crawlers or the supported API like REST API, Streaming API or Facebook Graph API. The huge amount of data needs to be processed further to remove the noise which could affect the overall result. The important preprocessing and cleaning methods are like spell correction, stop word removal, stemming, lemmatization, slang detection, removal of useless symbols etc. Several Natural Language

processing tasks like tokenization, POS tagging, NER and sentiment analysis along with the machine learning algorithms are applied on the curated data to discover the hidden pattern and bring out the meaningful change in the city environment (Fig. 2).

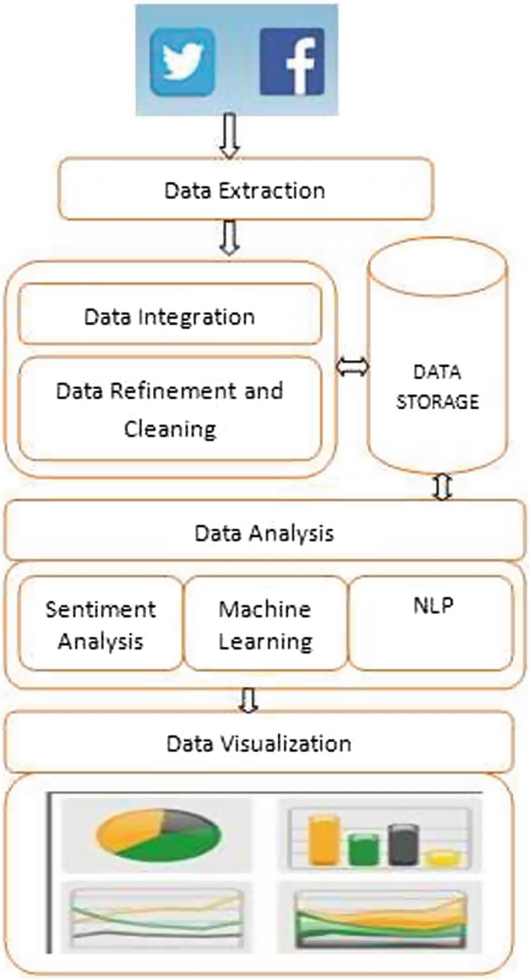


Fig. 2. Social media analytics lifecycle

Even though social media has become an important platform for sharing and spreading the information, analyzing the same poses serious challenges [27] which includes:

1. Noisy Data
2. Short Messages
3. Ambiguous Statements

4. Multilingual
5. Lack of Location Information
6. Sarcasm.

2 Existing Work

Being the service provider, the aim of the smart government is to have a transparent, quick and interactive service delivery to the citizens and increase their quality of life index. To achieve this government has taken initiative and developed various apps and platforms with which citizens can submit their issues and opinions instantly. Social media proved to be another prominent way to collect views and concerns of the people. But the identification the urban issues from the specifically developed apps [5] are easy as compared to mining and extracting the exact problems of the citizens from the social media sites. In case of the official websites and portals dedicated for complaint registration most of the information is provided by the users themselves like exact location or location coordinates of the issue, date, event, complaint category, severity etc. [6, 7]. Whereas using social media, the vast amount of information needs to be extracted, segregated into the complaint and non complaint data and mined for the expected knowledge [8] which may be present explicitly or implicitly. In some of prominent studies [9, 10], the author has performed the text analytics on the tweets extracted from the tweeter handles belonging to the primary departments of Indian government to identify the grievances lodged by the citizens. Along with the complaint tweets, the system has also identified the tweets in different categories like Appreciation posts, Information Sharing and Promotional tweets. In [11] twitter has been used to detect the incidents and events shared by the citizens of Dublin city. The tweets related to traffic and flood were fetched by giving the information like user, location and particular keywords. Geotagger component handled the missing location information using Open Street Map API and Lucene. In this study only the tweets dealing with the problems in the area of flood and traffic were analyzed.

Clustering algorithm seems to be a preferred way to aggregate the civic complaints based upon different parameters like density, frequency and time interval. Authors [12] have tried to overcome the limitation of existing approach of fixed gird based clustering by dynamically changing the size of grids based on the complaints recorded in concerned region. Further the study also identified the regions of the city showing the similar types of issues and critical issues in each region. The important limitation of this approach is the criticality measure is dependant solely on the complaint density and temporal analysis and not considered the sentiments or emotions present in it.

Social media analytics is not only useful in finding day to day issues of the citizens but also plays a crucial role while handling the emergencies. In [13], author has detected the emergencies like fire, accidents by processing and classifying the related tweets. The identified emergencies have also been displayed on the Google map which eventually can help the concerned departments to take immediate action. In the above approach author has only divided the tweets into “emergency” and “non emergency” events by using the supervised learning algorithm. Here the sentiments and emotions

mentioned in the tweets were not considered which can be an impactful factor for handling these kinds of situations by local authority. So in [14], the authors have proposed an approach combining sentiment analysis and emotion mining in which the tweets were analyzed to track the variations in emotions over the spacio-temporal measure which eventually led to the events causing that changes. Emotions expressed by the citizens proved to be an important feature to analyze and prioritize among the several existing issues. In [15], emotions mentioned in the complaints considered as a primitive indicators for deciding the urgency of the civic issues. Researcher in [16], has considered social media like Twitter as a tool to gain insight to the happiness index of the cities which in terms also depends upon the way local government understands the citizen's needs and preferences. Analyzing this data integrated with the responses given in the official issue handling services like 311 leads to effective service allocation.

Though 'English' is the preferred language for issue reporting, researchers have also investigated the social media analytics on the tweets other than English language. Abalı et al. [17] has applied the supervised machine learning algorithm to separate the information containing tweets about any particular location from the tweets which are without location information. The main loophole of this study is here author has only considered the tweets which were having the location names mentioned in it so vast amount of tweets which didn't have the location names mentioned but contained the meaningful information were not analyzed. Also the criteria based on which the author has decided whether the tweets were "Information- containing" or not has not been discussed. One more lacking point of this study seemed to be manual analysis of segregated important tweets to figure out the exact city problem as automated topic extraction is not supported. Mahfud and Tjahyanto [18] has classified the complaints mentioned by the public of Surabaya City in Indonesian language by using TF-IGM and SVM weighing method. Author has proved that the proposed TF-IGM method has outperformed the existing TF-IDF and TF-Binary methods for term weighing which eventually helped the local government to resolve the issues quickly.

For the transformation of traditional local government into "smart government", it is not sufficient to only identify the urban issues from the user generated content but it is important to prioritize them as per the urgency level. In [19] the author has proposed a framework in which the complaint of the citizen is compared with the existing knowledge base using the WordNet based sentence similarity algorithm. If the similarity score is in predefined limit then the quick response is generated for the user's concern. The system has also prioritized the inserted complaints based on the sentiment analysis output calculated using SVM classifier. Due to the free form nature of social media, most of the time comments contain grammatical errors and transliterated words. Hence using traditional features like POS tags are not sufficient to get the relevant result so the author [20] proposed a hybrid approach combining POS tagging and N gram based features to perform the Aspect Based Sentiment Analysis of the comments shared by the residents of the Bhopal city. The identified aspects represent the issues faced by them. Government can prioritized the extracted urban issues depending upon the sentiment score at both aspect level and category level. External sources of information like news of the area, weather condition and historical data also seems to be a great value addition to the social media analytics to not only understand the current issues faced by the people but also to predict the future problems. In [21], researches

Table 1. Analysis and comparison of existing work in the field of SMA for smart governance

References	Goal	Dataset	Language	Algorithm	Features	Success rate	Limitations
[25]	Prioritizing urban governance issues in health, education, transportation, electricity, surveillance, water categories from user-generated contents	myGov.in portal for Bhopal	English	*Aspect based Sentiment Analysis (ABSA) *Random Forest, Bagging, Naïve Bayes, ZeroR	N-gram, POS bag of words	Precision score = 86.32	*Removed punctuation and smiley which could treat as features *Not Multilingual *No semantic analysis of extracted aspects
[17]	Detects problems of citizens along with its locations	Tweets from the Aegean Region, Turkey	Turkish	Naive Bayes location recognizer using Python pyparsing and regular expression Lib	Location information	Accuracy = 0.86 Precision = 0.90 Recall = 0.92 F-measure = 0.91	Analyzed only tweets having location names mentioned
[18]	Improving classification performance of public complaints	Media center e-Wadul app for Surabaya city	Indonesian	TF-IDF, TF-Binary, TF-IGM, R studio, Naive Bayes, KNN and SVM	–	Accuracy = 80.11% Precision = 80.70% Recall = 80.10% F-measure = 80.20%	Limited training data class imbalance
[19]	Priority based sentiment analysis for quick response to citizen complaints	PMC	English	Word based sentiment similarity algorithm SVM	POS NER	–	Mined the structured database having limited variations as compared to tweets
[23]	City events prediction with map- based visualization utilizing crowd sourced geodata, topic modeling and topic correlation	Twitter	English	Prediction: linear regression Topic Identify:GSDMM Topic Similarity:Eucliden Dist, Leaflet library and OpenStreetMap	Resolved reports	–	Cant process the data having multiple topics in one complaint
[9]	Identify citizens complaints and grievances	Twitter	English	Ensemble learning based (SVM) classifier topic modeling: Alchemy concept API Landmark identification: OpenStreetMap API Issue identification: CoreNLP, POS Tagging, ConceptNet location identification:Indico API	N-Grams locations landmarks	Precision = 76% Accuracy = 67% Recall = 65%	Used Topic modeling which may not be suitable for short and unstructured tweets

(*continued*)

Table 1. (*continued*)

References	Goal	Dataset	Language	Algorithm	Features	Success rate	Limitations
[12]	Identify critical urban issues in a region	NYC311 data I change my city portal	English	Dynamic grid based clustering	Valid set of latitude and longitude	Correlation of Noise to construction and fire alarm = 0.93 and 0.87 resp Accuracy: 1. Euclidean = 66.68% 2. Cosine similarity = 85.71%	Only applicable for the location based complaints Criticality based on density and timeline
[13]	Emergency detection in urban areas	Twitter	English	SVM, multi-class Naive Bayes classifier Jazzy spell checker Google maps geocoding API	Unigrams trigram	Emergency detection and categorization F-scores exceeding 70% and 90%	Doesn't handled ambiguous statements other features like POS, NER, Bigram, Trigram should be required
[14]	Analyze feelings and perceptions in the community during emergency	Twitter	English	R packages: 'TwitterR' and 'Sentiment' for SA, 'Syuzhet' for EA, 'Bayesian Change point detection packages in R LDA	Hash tags, punctuation, emoji	–	Sparse emotion tweets and emotion overlapping affected performance
[21]	Identify and predict traffic events and problems, their root cause proposed suggestions and predict next day's events	News, Facebook, Tweets Weather data	English	Random Forest- frequent pattern mining	Location	Accuracy = 80%	Considered issues mentioned in large no of post. Severe issues mentioned in one or two post ignored
[10]	Killer road complaints identification	Twitter	English	NER OSMAPI concept net rule based classifier	Part of speech named entity recognition	Accuracy = 67% Recall = 65%	Replaced the symbols like '?????' With '?' in tweets which could indicate the sentiment strength

(*continued*)

Table 1. (*continued*)

References	Goal	Dataset	Language	Algorithm	Features	Success rate	Limitations
[22]	Predict traffic congestion severity level	Data about Thailand roads, Twitter, congestion data	English	C4.5 decision tree	Day of week, hour and minute info of day, no of tweets	Precision = 0.89 Recall = 0.898 F-measure = 0.89	Limited to single domain
[15]	Prioritizing urban issues based on emotions and votes	SeeClickFix hackathon data	English	NB SVM Associative classifier Ordinary least square Support vector regression	Unigram Bigram Author Type of issue	Precision = 0.805 Recall = 0.820 MAP for SVR = 0.833	Limited to Static structured database
[8]	Automated identification of complaint tweets and their topics	Twitter	English	One-class parallel ensemble SVM Alchemy concepts and taxonomy API	NER N-gram POS	Precision = 76%	Replaced the symbols like '?????' with '?' in tweets which could indicate the sentiment strength
[7]	Identify unresolved problems of Sejong City	Sejong City.com	English	KindKorean Morpheme Analyzer Naïve Bayes SQL, R Hadoop	–	Accuracy = 75%	Static structured database of complaints
[25]	Extracting the hazardous condition of road using tweets	Twitter	English	KNN NB DLM	N-gram	Precision = 0.775	Only applicable for the location based complaints
[16]	Understand and ranking happiness index of cities Analyze correlation between complaint tweets and 311 data	Twitter 311 data	English	NB MNB LR RF bagging	Emoticon	Accuracy = 95%	The reason of the unhappiness is not identified

(*continued*)

Table 1. (*continued*)

References	Goal	Dataset	Language	Algorithm	Features	Success rate	Limitations
[26]	Studying citizen's opinion analysis regarding city services and their behavior tends	Twitter	English	Elastic search Textalytics core API topics extraction API sentiment analysis API user demographics API	POS NER	–	Due to non structured nature of the tweets, POS may not be the ideal features for topic modeling
[5]	Predict no of 311 calls wrt time, location and complaints	311 data	English	Random forest	Day of the week, holiday, temp parameters, snow, no of request in Last week	MSE reduced by 9%	Studied Static structured database which is far simpler to handle compared to social media

have used the similar information source along with the traffic related Facebook posts to extract the severe problems faced by the people and predict the upcoming problems. Also in [22] author has used some more training attributes like days of week, minutes and hours of day and tweets density to predict the traffic congestion severity. In the work [23], the concept of topic modeling and topic similarity have used to predict the next day's event from social media data. The novel Map based and mind map based techniques were used for visualization of the predicted events.

3 Analysis

Overall, civic data analytics by government [24] seems to be an interesting area of research and the analysis of the existing work would definitely help in carrying out the future research. An overview of various papers representing the same area of interest is listed in Table 1 along with their algorithm, success rate and limitations identified.

4 Conclusion

Smart Government has always been focused on providing the livable environment in the city. Tremendous amount of information is needed to find out the factors which are affecting the quality of life of the citizens. Along with the physical sensors planted across the city, social media is a new aged tool to identify the needs and pain areas for the citizens. So in this survey we have briefly discussed various data extraction, data processing and classification methods used by the researchers to get the situational awareness. Natural language processing techniques are hugely discussed due to the non structured nature of the social media data. It is observed that in most of the studies, machine learning algorithms are preferred to extract the complaints and opinions of the residents and helping government official to better utilize the limited resource smartly. Though most of the past studies only aimed to summarize the spacio-temporal analysis of existing urban issues, very less efforts are pointing towards the 'predictive analytics' which could anticipate the issue before it exists. Increasing the accuracy of the result by applying context based sentiment analysis also good direction to explore.

References

1. Ahmed, K.B., Bouhorma, M., Ahmed, M.B.: Smart citizen sensing: a proposed computational system with visual sentiment analysis and big data architecture. Int. J. Comput. Appl. **152**(6), 20–27 (2016)
2. Zhang, J., Guo, B., Chen, H., Yu, Z., Tian, J., Chin, A.: Public sense: refined urban sensing and public facility management with crowdsourced data. In: 2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing and 2015 IEEE 12th International Conference on Autonomic and Trusted Computing and 2015 IEEE 15th International Conference on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), pp. 1407–1412. IEEE (2015)

3. Doran, D., Gokhale, S., Dagnino, A.: Human sensing for smart cities. In: Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 1323–1330. ACM (2013)
4. Mejova, Y.A.: Sentiment analysis within and across social media streams. PhD (Doctor of Philosophy) thesis, University of Iowa, (2012). https://doi.org/10.17077/etd.zze4b252
5. Zha, Y.F., Veloso, M.: Profiling and prediction of non-emergency calls in NYC. In: Workshops at the Twenty-Eighth AAAI Conference on Artificial Intelligence (2014)
6. Bousios, A., Gavalas, D., Lambrinos, L.: CityCare: crowdsourcing daily life issue reports in smart cities. In: 2017 IEEE Symposium on Computers and Communications (ISCC), pp. 266–271 (2017)
7. Jang, J.-S., Lee, B.-I., Choi, C.-H., Kim, J.-H., Seo, D.M., Cho, W.-S.: Understanding pending issue of society and sentiment analysis using social media. In 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 981–986. IEEE (2016)
8. Mittal, N., Agarwal, S., Sureka, A.: Got a complaint? Keep calm and tweet it! In: International Conference on Advanced Data Mining and Applications, LNCS, vol. 10086, pp. 619–635. Springer, Cham (2016)
9. Agarwal, S., Sureka, A.: Investigating the role of twitter in e-governance by extracting information on citizen complaints and grievances reports. In: International Conference on Big Data Analytics, LNCS, vol. 10721, pp. 300–310. Springer, Cham (2017)
10. Agarwal, S., Mittal, N., Sureka, A.: Potholes and bad road conditions: mining Twitter to extract information on killer roads. In: Proceedings of the ACM India Joint International Conference on Data Science and Management of Data, pp. 67–77. ACM (2018)
11. Panagiotou, N., Zygouras, N., Katakis, I., Gunopulos, D., Zacheilas, N., Boutsis, I., Kalogeraki, V., Lynch, S., O'Brien, B.: Intelligent urban data monitoring for smart cities. In: Joint European Conference on Machine Learning and Knowledge Discovery in Databases, LNCS, vol. 9853, pp. 177–192. Springer, Cham (2016)
12. Bansal, P., Toshniwal, D.: Analyzing civic complaints for proactive maintenance in smart city. In: 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), pp. 1–6. IEEE (2016)
13. Kanojia, D., Kumar, V., Ramamritham, K.: Civique: using social media to detect urban emergencies. arXiv preprint arXiv:1610.04377 (2016)
14. Singh, N., Roy, N., Gangopadhyay, A.: Analyzing the sentiment of crowd for improving the emergency response services. In: 2018 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 1–8. IEEE (2018)
15. Masdeval, C., Veloso, A.: Mining citizen emotions to estimate the urgency of urban issues. Inf. Syst. **54**, 147–155 (2015)
16. Eshleman, R., Yang, H.: "Hey# 311, Come Clean My Street!": a spatio-temporal sentiment analysis of Twitter data and 311 civil complaints. In: 2014 IEEE Fourth International Conference on Big Data and Cloud Computing, pp. 477–484. IEEE (2014)
17. Abalı, G., Karaarslan, E., Hürriyetoğlu, A., Dalkılıç, F.:. Detecting citizen problems and their locations using Twitter data. In: 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), pp. 30–33. IEEE (2018)
18. Mahfud, F.K.R., Tjahyanto, A.: Improving classification performance of public complaints with TF-IGM weighting: case study: Media center E-wadul surabaya. In: 2017 International Conference on Sustainable Information Engineering and Technology (SIET), pp. 220–225. IEEE (2017)
19. Deshmukh, K.V., Shiravale, S.S.: Priority based sentiment analysis for quick response to citizen complaints. In: 2018 3rd International Conference for Convergence in Technology (I2CT), pp. 1–5. IEEE (2018)

20. Kumar, A., Jiang, M., Fang, Y.: Where not to go?: detecting road hazards using Twitter. In: Proceedings of the 37th International ACM SIGIR Conference on Research & Development in Information Retrieval, pp. 1223–1226. ACM (2014)
21. Semwal, D., Patil, S., Galhotra, S., Arora, A., Unny, N.: STAR: real-time spatio-temporal analysis and prediction of traffic insights using social media. In: Proceedings of the 2nd IKDD Conference on Data Sciences, p. 7. ACM (2015)
22. Wongcharoen, S., Senivongse, T.: Twitter analysis of road traffic congestion severity estimation. In: 2016 13th International Joint Conference on Computer Science and Software Engineering (JCSSE), pp. 1–6. IEEE (2016)
23. Witanto, J.N., Lim, H., Atiquzzaman, M.: Smart government framework with geo-crowdsourcing and social media analysis. Fut. Gener. Comput. Syst. **89**, 1–9 (2018)
24. Anggoro, T.P., Nainggolan, B., Purwandesi, E.: Social media analysis supporting smart city implementation (Practical study in Bandung district). In: 2016 International Conference on ICT for Smart Society (ICISS), pp. 80–86. IEEE (2016)
25. Kumar, V., Jenamani, M.: Identification and prioritization of urban issues from Smart City data. In: 2018 International Conference on Smart City and Emerging Technology (ICSCET), pp. 1–7. IEEE (2018)
26. Villena-Román, J., Cobos, A.L., Cristóbal, J.C.G.: TweetAlert: semantic analytics in social networks for citizen opinion mining in the city of the future. In: UMAP Workshops (2014)
27. Bontcheva, K., Rout, D.: Making sense of social media streams through semantics: a survey. Semant. Web **5**(5), 373–403 (2014)

Review of Handover in Li-Fi and Wi-Fi Networks

Jaafaru Sanusi[1(✉)], Abiodun Musa Aibinu[2], Steve Adeshina[1], Gokhan Koyunlu[1], and Sadiq Idris[1]

[1] Electrical and Electronics Engineering Department, Nile University of Nigeria, Abuja, Nigeria
jafarsanusiliman@yahoo.com, {steve.adeshina, g.koyunlu, sadiq.idris}@nileuniversity.edu.ng
[2] Mechatronics Engineering Department Federal University of Technology, Minna, Niger State, Nigeria
maibinu@gmail.com

Abstract. Light Fidelity (Li-Fi) is a visible light communication technology that uses light as a medium to provide high-speed data communication. Since the spectrum utilized by Li-Fi does not overlap with the spectrum utilized by Radio Frequency (RF) spectrum, they can be hybridized so as to improve quality of service and quality experience (Qoe) of the users. However in a hybrid Li-Fi/Wireless-Fidelity (Wi-Fi) network, movement of users may prompt frequent handover which may degrade the system throughput. Therefore there is the need to mitigate frequent handover in a hybrid Li-Fi/Wi-Fi network. This paper surveys various types of handovers that could be used to mitigate unnecessary handovers in a hybrid Li-Fi/Wi-Fi network. This paper also focuses on the working principles of Li-Fi, its applications, modulation techniques and areas of applications.

Keywords: Light fidelity · Radio frequency · Visible light communication · Wireless fidelity

1 Introduction

In today's world, multimedia data services demand has grown up rapidly [1]. The Radio Frequency (RF) band used for wireless communication is overcrowded therefore there is the need to utilize other frequency bands that are not explored [2]. There have been a lot of innovations to enhance the spectral efficiency of the RF wireless networks like Multiple Input Multiple Output (MIMO) etc. but as a result of continuous demand and increase in traffic, the existing RF spectrum cannot be able to meet up with the future demand of data traffic.

Visible Light Communication (VLC) technology can be a complement to the existing Radio Frequency (RF) wireless communication because it uses visible light (380–780 nm) as a carrier for data and has a bandwidth that is 1000 times higher than RF communications [3]. The visible light spectrum is unregulated unlike RF spectrum

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 955–964, 2020.
https://doi.org/10.1007/978-3-030-37051-0_107

and so it is cheaper than RF communication. VLC is capable of providing data rates of up to 1 Gb/s or even higher [3, 4].

The data rates can be increased in VLC by using Multiple Input Multiple Output (MIMO) techniques. These makes it possible for VLC to be part of future 5G technologies [5, 6].

VLC and RF communication can be used together without interferences to complement each other forming a hybrid or heterogeneous networks in order to improve the performance of the network [7].

VLC is also safe for human health unlike RF where radio waves can cause cancer [8–10]. VLC can also be used where the usage of RF is restricted (airplanes, hospital, nuclear plants). Moreover, VLC is energy efficient because it needs no additional energy to transmit data because the same source of light is used for both illumination and as a carrier for the data [3].

While RF waves can penetrate through nonmetallic materials, the visible light can only penetrate transparent materials which limit mobility or the coverage area but on the other hand it prevents eavesdropping.

VLC can be used to provide high data rate for internet connection or broadcast for indoor applications while for outdoor applications, VLC can be used in communication between vehicles and/or between traffic infrastructure and vehicles [11–13]. The challenge in indoor application is to provide fast internet services while achieving long distance communication is the challenge in automotive applications.

The Li-Fi requires a transmitter which in most cases is an LED to transmit data and at the receiver a photodiode detector is needed to convert the signals at the receiver a photodiode detector is needed to convert the signals to electrical for further processing [14, 15].

The remaining part of this paper is organized as follows: In Sect. 2 the modulation techniques used in Li-Fi is provided. In Sect. 3, hybrid Li-Fi/Wi-Fi network was discussed and the possibility of the two networks working together to complement each other was shown. In Sect. 4, dynamic handover, in Sect. 5 Li-Fi and Wi-Fi was discussed. Advantages, Applications and Limitations of Li-Fi were addressed in Sect. 6. And lastly, conclusions of the paper are given in Sect. 7.

2 Modulation Techniques for Li-Fi

In this section, two of the digital modulation schemes used in Li-Fi are discussed namely.

2.1 Single-Carrier Modulation (SCM)

On-Off Keying (OOK), Pulse Amplitude Modulation (PAM) and Pulse Position Modulation (PPM) are the most widely used Single-Carrier Modulation (SCM) schemes in VLC [16]. On-Off keying (OOK) is widely used because it is simple to implement and offers a good tradeoff between the performance and complexity of the system. PPM is better than OOK in terms of power-efficiency but it has lower spectral efficiency than OOK. Optical spatial modulation is another modulation scheme used in

Li-Fi has been proven to be power and bandwidth efficient for indoor wireless communication [17]. Quadrature Amplitude Modulation (QAM) is another modulation technique used in single carrier Li-Fi systems to transmit signals [18].

2.2 Multi-carrier Modulation (MCM)

In Li-Fi networks as the data rate increases, single carrier schemes like OOK, PAM and PPM begin to suffer from signal distortion therefore to support high data rates, multi-carrier modulation techniques should be used. Multi-carrier modulation offers better bandwidth efficiency but lower energy efficiency when compared to single carrier modulation [14]. Multicarrier modulation (MCM) in Li-Fi networks is realized using OFDM [19, 20] in which parallel data streams are simultaneously transmitted using closely separated orthogonal subcarriers. A typical OFDM modulator is realized by taking Inverse Fast Fourier Transform (IFFT) then followed by digital-to-analogue converter (DAC). The OFDM signal generated is complex and bipolar but in order to fit the IM/DD requirement the OFDM signal generated is supposed to be real-value signal. In order to get a real-valued signal at the output after IFFT, hermitian symmetry on the subcarriers must be taken. Again the intensity of light cannot be negative and so the Li-Fi signal should be unipolar. In order to get a unipolar signal, DCO-OFDM should be used because it uses positive direct current (Dc) bias to generate unipolar signals which leads to higher power consumption but without any effects to spectral efficiency.

3 Hybrid Li-Fi/Wi-Fi Networks

Li-Fi and Wi-Fi networks can be used together in order to guarantee system performance and equal Quality of Service (Qos) to users. Since Li-Fi and Wi-Fi use different spectra, there is no interference between the two technologies [7]. Hence, a hybrid Li-Fi/Wi-Fi network can achieve the sum throughput of both stand-alone networks.

By IEEE802.11 ad standard, wireless Gigabit alliance(WiGig) the latest Wi-Fi protocol can provide a data rate up to 7 Gb/s [21] and recently research has shown that up to 3 Gb/s can be achieved with a LED. High spectral efficiency can be achieved in Li-Fi network because of the large number of Access Points (AP) in an indoor environment especially when lightning infrastructures are in use [22].

By deploring a hybrid Li-Fi/Wi-Fi system, users irrespective of their location within a coverage area can get an enhanced data services and Quality of Service (Qos). While the Wi-Fi system benefits from reduced RF spectrum usage, the Li-Fi benefits from coverage at dead spots.

3.1 Hybrid Li-Fi/Wi-Fi System Model

It consists of transceivers both for Li-Fi and Wi-Fi links with a Central Unit (CU) that integrates the two networks. Users are equipped with RF antenna and PD for both Wi-Fi and Li-Fi signals. The CU is saddled with the responsibility of monitoring the entire network and regularly receives CSI of the users for both Li-Fi and Wi-Fi links and

based on that the CU assigns an AP to a user and the RA of users connected to Access point is determined. Because Li-Fi Access point share the same modulation bandwidth, interference may be experienced by users located where Li-Fi atto cells overlap. The Wi-Fi AP covers the entire indoor area and the channel model of the Wi-Fi is based on IEEE 802.11 g [23]. The hybrid Li-Fi/Wi-Fi networks have a lot of advantages like robustness, security, reliability and capacity.

3.2 System Load Balancing

As a result of multiple Access point and multiuser communication, a load balancing technique should be put in place to address Access point assignment and resource allocation [24] in hybrid network. These two main issues that should be addressed by an effective load balancing technique can be formulated as a joint optimization technique. A utility function can be used to combine the two optimization objects. A logarithmic utility function is mostly used because it is simple and practical as it ensures proportional fairness for users [24, 25].

4 Dynamic Handover

Handover is the process of transferring an ongoing wireless communication from a currently serving AP to another AP [26]. When a user equipment moves out of the coverage area of an adjacent Ap, handover will be prompted. Again handover will be necessary if the channel of transmission is degraded as a result of interference or if the current cell is fully loaded. Handover is classified into vertical and horizontal handover [27]. Horizontal handover is a situation when mobile equipment is transferred from one Ap to another in the same network. However vertical handover occurs when a mobile equipment is transferred from one Ap to another that have different access technologies (e.g. from Wi-Fi to Li-Fi or Wi-Fi to LTE) [27].

In real life, the channel state information of Li-Fi and Wi-Fi is time-varying as a result of constant or random movements of users. If a user is served by a Wi-Fi network detects a stronger Li-Fi signal, the user will transfer to the Li-Fi network. As a result of this, users in a hybrid Li-Fi/Wi-Fi network will experience constant handovers depending on the movement of users and strong signal been detected by the user [28].

When a user is switched maybe from Li-Fi to Wi-Fi, the load at the Wi-Fi cell will increase thereby leading to transfer of users served by a particular APs to neighboring Wi-Fi APs or decrease in data rates. Again, as a result of decrease in load of the LiFi cell, existing users will experience increase in data rates. A ping-pong handover effects between the two different network (Li-Fi and Wi-Fi APs) will arise if there is a blockage or if the receive angle is varied.

In [24], a dynamic load-balancing scheme with handover in a hybrid system was presented. The two basic types of handover are hard and soft handover. In the case of hard handover, the user equipment (UE) is basically disconnected from its serving AP before it's connected to the next AP. Even though it is easy to implement and has lower complexity, interruption of service is experienced by the user [26]. In soft handover, the UE continues to remain connected to its serving AP until its connected to the next

Ap. This process provides better user experiences but it needs more wireless transmission resources.

Handover decision making is key in any handover procedure. It helps in meeting the users' needs and also in the better utilization of the network. There are a lot of criteria used in handover decision reported in [27]. Handover metrics helps in deciding how and when handover should be done and to which networks etc. Various Qos parameters that affect vertical handover are considered in order to keep the users connected. The following parameters should be considered in other to enable vertical handover [28–31].

- *Received signal strength indicator (RSSI)*: It is one of the key decision making factors in handover. RSSI indicates the power received and its level increases or decreases depending on how close the UE is close to an AP.
- *Network load:* some services such as real-time video, streaming etc. require higher bandwidth to perform well depending on the needs of their users.
- *Monetary service cost*: If two network providers can provide the same quality of service, users are more likely to go for the cheaper network.
- *Handover delay/Latency:* delay affects the performance of the system negatively. Therefore delays should be avoided.
- *User preferences*: Users may prefer a certain network over the other. Users prefer a high bandwidth, low cost and reliable network etc.
- *Number of unnecessary handovers:* constant handover may degrade the performance of the system. Handover from AP1 to AP2 and back to Ap1 may be considered unnecessary because it causes extra consumption of network resources. This scenario is known as ping- pong effect.
- *Handover failure probability*: if a handover is initiated by "X" network to "Y" target network, is not successful due to lack of resources or availability of free channels, handover failure occurs.
- *Security control*: Security control is one of the main issues that is of great concern when networks are converged. A mobile user must comply to the security and privacy options of each network during the handover process. The process of handover would require improved security and privacy from eavesdropping.
- Throughput: Mobile users usually prefer networks that can provide high data rates.
- *Bit error rate (BER)*: This can be enhanced by selecting a network with strong signal.
- *Signal to Noise Ratio (SNR)*: It is also a parameter used in handover decision making and it shows the Qos of a network.

In horizontal handover, RSS is usually used as the handover decision parameter but in vertical handover, RSS and others factors listed above are used in the handover decision making, all aimed at improving Qos and Quality of experiences (Qoe) of users.

Depending on the algorithm used, the process of handover takes 30–300 ms [28, 32] and this additional task affects the system overall throughput. A Fuzzy Logic (FL) dynamic handover method to mitigate the frequent handover experienced in hybrid Li-Fi/Wi-Fi network was proposed in [33]. There are four steps generally involved in FL system: fuzzification, rule evaluation, de-fuzzification and decision

making [33, 34]. In the fuzzy logic system, an input which includes information on average signal to noise ratio of the Li-Fi, the speed of the user and the required data rate of the users are used to determine the best load balancing so as to be able to reduce frequent handover and then improve the overall system throughput. In Table 1, basic types of vertical handover schemes are presented [35–39] and the classification is done based on the parameters used.

Table 1. Classification of vertical handover decision schemes

RSS based schemes	Qos based schemes	Decision function based schemes	Intelligence based schemes	Context based schemes
i. Dwell Timer based schemes	i. Available bandwidth based schemes	i. Utility function based schemes	i. Artificial neural based schemes	i. Mobile agent based schemes
ii. RSS threshold based schemes	ii. SINR based schemes	ii. Cost function based schemes	ii. Fuzzy logic based schemes	ii. AHP based schemes
iii. Channel scanning based schemes	iii. User profile based schemes	iii. Network score function based schemes	iii. Intelligent Protocol based schemes	iii. Mobility prediction based schemes
iv. Prediction based schemes				iv. Cooperation based schemes
				v. MIH based schemes

5 Comaprison Between Li-Fi and Wi-Fi

Comparison between Li-Fi and Wi-Fi are given herewith

(a) **Energy efficiency**: The energy efficiency of radio base station is generally low because a significant amount of energy is actually used in cooling down the base station instead of transmission [40].
(b) **Capacity**: The radio spectrum currently utilized for data transmission is limited and expensive. And with recent innovation like 3G, 4G and so on the radio frequency spectrum is becoming so saturated [41].
(c) **Security**: The radio wave can penetrate through walls and hence are susceptible to interceptions. Knowing this, hackers can easily intercept the radio waves and this is a big security problem for Wi-Fi [6].
(d) **Availability**: The availability of radio waves is another issue and Radio waves may not be used in airplanes etc. because of interference as that could interfere with the operations of the plane.

6 Advantages, Applications And Limitations of Li-Fi

This section addresses some advantages of Li-Fi, area of applications and limitations of Li-Fi. Some of the advantages of Li-Fi include:

(a) **Efficiency**: Energy consumption can be greatly minimized since LED illuminations in homes, offices are used to transmit data, which will make it energy efficient as well as cost effective [40].
(b) **High speed**: Li-Fi network is able to provide up to 1 Gbps of data services as it has low interference, high bandwidths [3] etc.
(c) **Availability**: Getting light sources is very easy because we have that in our homes, offices, shops, streets etc. which can serve as a medium to transmit data.
(d) **Cheaper**: Li-Fi is obviously cheaper because light sources are readily available and it does not need much power to transmit data.
(e) **Security**: One of the advantages of Li-Fi is security. Light cannot penetrate walls or opaque objects, therefore Li-Fi network is best used for indoor communication and so it cannot be intercepted outside the region it operates.

Areas of application of Li-Fi include:

(a) **Education systems**: Since Li-Fi is capable to provide high speed internet services, it can be replaced with Wi-Fi especially in our educational institute where high data rates services are needed [15].
(b) **Aircrafts**: Li-Fi can be used to provide services in aircrafts because visible light spectrum does not interfere with avionic equipments. Therefore Li-Fi can easily be an alternative and the bulbs in the aircrafts can serve as light source [40].
(c) **Medical Applications**: Using Wi-Fi in operation theatres are not allowed because it may interfere with signals that are being monitored by medical equipment which may cause hazardous effect to patient's health due to false readings of these apparatus. Li-Fi serves as an alternative as it does not interfere with medical equipments [40].
(d) **Traffic management**: Li-Fi can be used in traffic management to communicate with vehicles that are moving (using the LED light of the cars to help reduce accidents and smoother flow of traffic.
(e) **Mobile connectivity**: Laptops, tablets, mobiles can be connected to each other easily. Li-Fi network can provide high data rates and high security.
(f) **Replacement for other technology**: Li-Fi can be used as alternative where Bluetooth, infrared, Wi-Fi are banned.

Some of the limitations of Li-Fi are as follows:

Li-Fi only works if there is a light source, absence of that might make internet inaccessible [14]. Line-of-sight is needed to be established to enable data transmission [40].

Opaque obstacles may affect line of sight hence it affects data transmission. The range of Li-Fi is shorter than Wi-Fi. Since light waves can't penetrate walls [41] and also it has high cost of initial installation.

7 Conclusion

In this paper, a Li-Fi/RF hybrid network was reviewed and it was shown that the hybrid network can provide higher throughput compared to a standalone network. Various strategizes used in mitigating frequent handover in Li-Fi/RF Network were reviewed. Load balancing, access point assignments, different modulation and multi access schemes used in Li-Fi were addressed.

References

1. Cisco Visual Networking index: Global mobile data traffic forecast update, 2015–2020. Whitepaper, CISCO (2018). https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf. Accessed 7 Nov 2018
2. Hanzo, L., Haas, H., Imre, S., O'Brien, D., Rupp, M., Gyongyosi, L.: Wireless myths, realities, and futures: from 3G/4G to optical and quantum wireless. In: Proceedings of the IEEE, vol. 100, no. pp. 1853–1888 (2012)
3. Chun, H., Rajbhandari, S., Faulkner, G., Tsonev, D., Xie, E., Gu, E., Dawson, M., Haas, H.: LED based wavelength division multiplexed 10 Gb/s visible light communications. J. Light. Technol. **34**(13), 3047–3052 (2016)
4. Wu, S., Wang, H., Youn, C.-H.: Visible light communications for 5G wireless networking systems: from fixed to mobile communications. IEEE Netw. **28**(6), 41–45 (2014)
5. Wang, C.X., Haider, F., Gao, X., You, X.-H., Yuan, D., Aggoune, H., Haas, H., Fletcher, S., Hepsaydir, E.: Cellular architecture and key technologies for 5G wireless communication networks. IEEE Commun. Mag. **52**(2), 122–130 (2014)
6. Ayyash, M., Elgala, H., Khreishah, A., Jungnickel, V., Little, T., Sao, S., Hilt, J., Freund, R.: Coexistence of WiFi and LiFi toward 5G: concepts, opportunities, and challenges. IEEE Commun. Mag. **54**(2), 64–71 (2016)
7. Li, X., Zhang, R., Hanzo, L.: Cooperative load balancing in hybrid visible light communications and WiFi. IEEE Trans. Commun. **63**(4), 1319–1329 (2015)
8. IARC classifies radio frequency electromagnetic fields as possible carcinogenic to humans. International Agency for Research Cancer, World Health Organization, Geneva, Switzerland, Technical Report, May 2011. http://www.iarc.fr/en/media-centre/pr/2011/pdfs/pr208_E.pdf. Accessed 20 Mar 2017
9. Fact Sheet 296—Electromagnetic Fields and Public Health, World Health Organization, Geneva, Switzerland, December 2005
10. Fact Sheet 193—Electromagnetic Fields and Public Health: Mobile Phones, World Health Organization, Geneva, Switzerland, October 2014
11. Akanegawa, M., Tanaka, Y., Nakagawa, M.: Basic study on traffic information system using LED traffic lights. IEEE Trans. Intell. Transp. Syst. **2**(4), 197–203 (2001)
12. Pathak, P., Feng, X., Hu, P., Mohapatra, P.: Visible light communication, networking, and sensing: a survey, potential and challenges. IEEE Commun. Surv. Tutor. **17**(4), 2047–2077 (2015)
13. Kim, B., Song, D., Lee, J., Jung, S.: VLC based positioning scheme in Vehicle-to-Infra (V2I) Environment. J. Kor. Inst. Commun. Inf. Sci. **40**(3), 588–594 (2015)
14. Haas, H., Yin, L., Wang, Y., Chen, C.: What is LiFi? J. Light. Technol. **34**(6), 1533–1544 (2016)

15. Li-Fi: How this LED Technology works and differs from Wi-Fi. TechTreme (2018). https://www.techtreme.com/internet/li-fi-vs-wi-fi-how-it-works/. Accessed 9 Dec 2018
16. Kahn, J., Barry, J.: Wireless infrared communications. Proc. IEEE **85**(2), 265–298 (1997)
17. Mesleh, R., Elgala, H., Haas, H.: Optical spatial modulation. J. Opt. Commun. Netw. **3**(3), 234 (2011)
18. Wu, F., Lin, C., Wei, C., Chen, C., Huang, H., Ho, C.: 1.1-Gb/s white-LED-based visible light communication employing carrier-less amplitude and phase modulation. IEEE Photon. Technol. Lett. **24**(19), 1730–1732 (2012)
19. Komine, T., Haruyama, S., Nakagawa, M.: Performance evaluation of narrowband OFDM on integrated system of power line communication and visible light wireless communication. In: 2006 1st International Symposium on Wireless Pervasive Computing (2006)
20. Afgani, M., Haas, H., Elgala, H., Knipp, D.: Visible light communication using OFDM. In: 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, TRIDENTCOM (2006)
21. Hansen, C.: WiGiG: multi-gigabit wireless communications in the 60 GHz band. IEEE Wirel. Commun. **18**(6), 6–7 (2011)
22. Stefan, I., Burchardt, H., Haas, H.: Area spectral efficiency performance comparison between VLC and RF femtocell networks. In: 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, pp. 1–5, 9–13 June 2013
23. Perahia, E., Stacey, R.: Next generation wireless LAN: 802.11n and 802.11ac. Cambridge University Press, Cambridge, UK (2013)
24. Wang, Y., Haas, H.: Dynamic load balancing with handover in hybrid Li-Fi and Wi-Fi networks. J. Light. Technol. **33**(22), 4671–4682 (2015)
25. Malviya, L., Waoo, A.A., Sharma, S.: New load balanced multi-path dynamic source routing protocol for mobile ad-hoc network. Int. J. Comput. Appl. **61**(19), 25–27 (2013)
26. Miao, G., Zander, J., Sung, K., Slimane, S.: Fundamentals of mobile data networks. Cambridge University Press, Cambridge (2016)
27. Ahmed, A., Boulahia, L., Gaiti, D.: Enabling vertical handover decisions in heterogeneous wireless networks: a state-of-the-art and a classification. IEEE Commun. Surv. Tutor. **16**(2), 776–811 (2014)
28. Vegni, A.M., Little, T.D.C.: Handover in VLC systems with cooperating mobile devices. In: IEEE Proceedings of International Conference on Computer Networks and Communication, Maui, HI, USA, pp. 126–130, January 2012
29. Ahmed, A., Merghem-Boulahia, L., Gaïti, D.: An intelligent agent-based scheme for vertical handover management across heterogeneous networks. Ann. Telecommun.—annales des télécommunications **66**(9–10), 583–602 (2011)
30. Corici, M., Fiedler, J., Magedanz, T., Vingarzan, D.: Access network discovery and selection in the future wireless communication. Mob. Netw. Appl. **16**(3), 337–349 (2011)
31. Dong, P., Zhang, H., Luo, H., Chi, T., Kuo, S.: A network-based mobility management scheme for future Internet. Comput. Electr. Eng. **36**(2), 291–302 (2010)
32. Kassab, M., Bonnin, M., Belghith, A.: Fast and secure handover in WLANs: an evaluation of the signaling overhead. In: Proceedings of IEEE Communications Network Conference, USA, pp. 770–775, January 2008
33. Wu, X., Safari, M., Haas, H.: Three-state fuzzy logic method on resource allocation for small cell networks. In: 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (2015)
34. Burchardt, H., Sinanovic, S., Bharucha, Z., Haas, H.: Distributed and autonomous resource and power allocation for wireless networks. IEEE Trans. Commun. **61**(7), 2758–2771 (2013)
35. Kassar, M., Kervella, B., Pujolle, G.: An overview of vertical handover decision strategies in heterogeneous wireless networks. Comput. Commun. **31**(10), 2607–2620 (2008)

36. Lin, T., Wang, C., Lin, P.: A neural-network-based context-aware handoff algorithm for multimedia computing. ACM Trans. Multimed. Comput. Commun. Appl. **4**(3), 1–23 (2008)
37. Yan, X., Ahmet Şekercioğlu, Y., Narayanan, S.: A survey of vertical handover decision algorithms in Fourth Generation heterogeneous wireless networks. Comput. Netw. **54**(11), 1848–1863 (2010)
38. Fernandes, S., Karmouch, A.: Vertical mobility management architectures in wireless networks: a comprehensive survey and future directions. IEEE Commun. Surv. Tutor. **14**(1), 45–63 (2012)
39. Zekri, M., Jouaber, B., Zeghlache, D.: A review on mobility management and vertical handover solutions over heterogeneous wireless networks. Comput. Commun. **35**(17), 2055–2068 (2012)
40. Cailean, A., Dimian, M.: Current challenges for visible light communications usage in vehicle applications: a survey. IEEE Commun. Surv. Tutor. **19**(4), 2681–2703 (2017). https://doi.org/10.1109/comst.2017.2706940
41. Chowdhury, M., Hossan, M., Islam, A., Jang, Y.: A comparative survey of optical wireless technologies: architectures and applications. IEEE Access **6**, 9819–9840 (2018)

Retraction Note to: A Study on Email Security Through Cryptographic Techniques

Akhilesh Kumar Singh(✉), Vinesh Kumar, and Sharad Pratap Singh

GLAU, Mathura, UP, India
{akhileshkr.singh, vinesh.kumar, sharad.singh}@gla.ac.in

Retraction Note to:
Chapter "A Study on Email Security Through Cryptographic Techniques" in: S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 342–348, 2020.
https://doi.org/10.1007/978-3-030-37051-0_40

The editors have retracted this chapter "Singh A.K., Kumar V., Singh S.P. (2020) A Study on Email Security Through Cryptographic Techniques. In: Smys S., Senjyu T., Lafata P. (eds) Second International Conference on Computer Networks and Communication Technologies. ICCNCT 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 44. Springer, Cham (https://doi.org/10.1007/978-3-030-37051-0_40)" because it reports research undertaken by Shafiya Afzal Sheikh and M. Tariq Banday. A K Singh agrees to this retraction, and V Kumar and S P Singh have not responded to any correspondence from the editor/publisher about this retraction.

The retracted version of this chapter can be found at https://doi.org/10.1007/978-3-030-37051-0_40

© Springer Nature Switzerland AG 2020

S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. C1–C1, 2020.
https://doi.org/10.1007/978-3-030-37051-0_108

Retraction Note to: Second International Conference on Computer Networks and Communication Technologies

S. Smys[1](✉), Tomonobu Senjyu[2], and Pavel Lafata[3]

[1] Department of Computer Science Engineering, RVS Technical Campus, Coimbatore, Tamil Nadu, India

[2] University of the Ryukyus, Okinawa, Japan

[3] Department of Telecommunication Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Prague, Czech Republic

Retraction Note to:
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 342–348, 2020.
https://doi.org/10.1007/978-3-030-37051-0

The Series Editor and the Publisher have retracted these chapters. An investigation by the Publisher found a number of chapters, including this one, with various concerns, including but not limited to compromised editorial handling, incoherent text or tortured phrases, inappropriate or non-relevant references, or a mismatch with the scope of the series and/or book volume. Based on the findings of the investigation, the Series Editor therefore no longer has confidence in the results and conclusions of this chapter. The authors have not responded to correspondence regarding this retraction.

The retracted version of these chapters can be found at
https://doi.org/10.1007/978-3-030-37051-0_44
https://doi.org/10.1007/978-3-030-37051-0_82
https://doi.org/10.1007/978-3-030-37051-0_89
https://doi.org/10.1007/978-3-030-37051-0_101

© Springer Nature Switzerland AG 2024
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. C3–C3, 2020.
https://doi.org/10.1007/978-3-030-37051-0_109

Author Index

© Springer Nature Switzerland AG 2020
S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 965–968, 2020.
https://doi.org/10.1007/978-3-030-37051-0