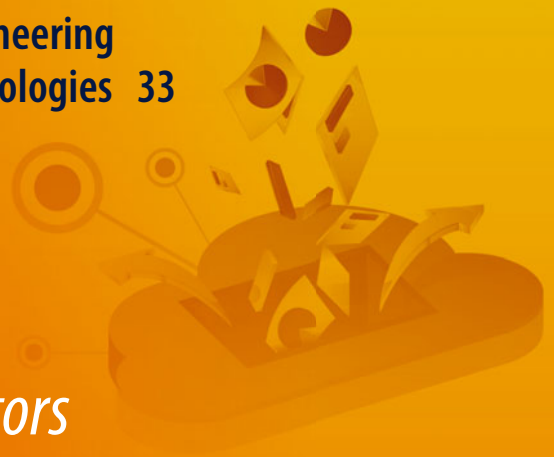


Lecture Notes on Data Engineering  
and Communications Technologies 33

S. Balaji  
Álvaro Rocha  
Yi-Nan Chung *Editors*



# Intelligent Communication Technologies and Virtual Mobile Networks

ICICV 2019

 Springer

# **Lecture Notes on Data Engineering and Communications Technologies**

Volume 33

## **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 ISI Proceedings, MetaPress, Springerlink and DBLP \*\***

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

S. Balaji · Álvaro Rocha · Yi-Nan Chung  
Editors

# Intelligent Communication Technologies and Virtual Mobile Networks

ICICV 2019

 Springer

*Editors*

S. Balaji  
Department of CSE  
Francis Xavier Engineering College  
Tirunelveli, Tamil Nadu, India

Álvaro Rocha  
Departamento de Engenharia Informática,  
Faculdade de Ciências e Tecnologia  
University of Coimbra  
Coimbra, Portugal

Yi-Nan Chung  
Department of Electrical Engineering  
National Changhua University of Education  
Changhua County, Taiwan

ISSN 2367-4512                      ISSN 2367-4520 (electronic)  
Lecture Notes on Data Engineering and Communications Technologies  
ISBN 978-3-030-28363-6              ISBN 978-3-030-28364-3 (eBook)  
<https://doi.org/10.1007/978-3-030-28364-3>

© Springer Nature Switzerland AG 2020

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 grateful to dedicate the ICICV 2019 conference proceedings to all the participants and editors of the Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2019).*

# Foreword

ICICV was honored to host the proceedings of the ICICV 2019 held in, Tirunelveli, Tamil Nadu, February 14–15, 2019.

Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2019) aims to bring together leading academic scientists, researchers, and research scholars to exchange and share their experiences, the state of the art, and practice of cloud computing, identify emerging research topics and communication technologies, and define the future of intelligent communication approaches, cloud computing, and research results about all aspects of Engineering Technology and Innovation.

All topics regarding cloud computing align with the theme of virtual mobile cloud and communication technologies. The integration of virtual mobile cloud computing and communication technologies and engineering permits new applications that provide resources and services on an intelligent basis, process big data collected from mobile sensors, and assist Internet of things with massive cloud-based backend, where the 5G technology is expected to be an important enabler of this integration.

This ICICV 2019 conference program signifies the efforts of many researchers. We want to express our thankfulness to the steering committee members, volunteers, and the external reviewers for their hard work in the success of ICICV 2019.

Regards,  
S. Balaji

# Preface

This conference proceedings brings you the collection of articles selected and presented from Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2019). The prime focus of this conference is to bring the academic scientists, researchers, and research scholars for sharing their knowledge in future of all aspects of Engineering Technology and Innovation.

We have celebrated our 2019 version of gathering, to strive to advance the largest international professional forum on virtual mobile cloud computing and communication technologies. We have received 220 papers from various colleges and universities and selected 66 papers based on strictly peer-reviewed by the reviewers and experts. All the selected papers are in high quality, and it exactly matches the scope of the conference.

ICICV 2019 would like to express our gratitude toward all contributors to this conference proceedings. We would like to extend our sincere thanks to all reviewers and expertise for their valuable review comments on all papers. Also, we would like to thank our organizing committee members for the success of ICICV 2019.

Lastly, we are most indebted for the generous support given by Springer for publishing this volume.

Regards,  
S. Balaji



# Acknowledgment

It is our pleasure to present this conference proceedings consisting of selected papers based on oral presentations from the ICICV 2019, held February 14–15, at the Francis Xavier Engineering College, Tirunelveli. Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2019) aims to bring together leading academic scientists, researchers, and research scholars to exchange and share their experiences, the state of the art, and practice of cloud computing, identify emerging research topics and communication technologies, and define the future of intelligent communication approaches, cloud computing, and research results about all aspects of Engineering Technology and Innovation.

The organizers wish to acknowledge Dr. S. Cletus Babu, Dr. X. Amali Cletus, Mr. C. Arun Babu, Dr. K. Jeyakumar, Dr. D. C. Joy Winnie Wise, Dr. S. Balaji, and Dr. I. Jeena Jacob for the discussion, suggestion, and cooperation to organize the keynote speakers of this conference. We would like to take this opportunity to thank once again all of the participants in the conference keynote speakers, presenters, and audience alike. We would also like to extend our gratitude to the reviewers of the original abstracts and the papers submitted for consideration in this conference proceedings for having so generously shared their time and expertise.

We extend our sincere thanks to all the chairpersons and conference committee members for their support.

# Contents

<b>Cluster Restructuring and Compressive Data Gathering for Transmission Efficient Wireless Sensor Network</b> .....	1
Utkarsha Sumedh Pacharaney and Rajiv Kumar Gupta	
<b>Condition Monitoring of Coal Mine Using Ensemble Boosted Tree Regression Model</b> .....	19
R. Uma Maheswari, S. Rajalingam, and T. K. Senthilkumar	
<b>Performance Analysis of Image Compression Using LPWCF</b> .....	30
V. P. Kulalvaimozhi, M. Germanus Alex, and S. John Peter	
<b>Facial Analysis Using Deep Learning</b> .....	42
Priyanka More, Poonam Desale, Mayuri S. Gothwal, Pradnya S. Sahajrao, and Aarzoo A. Shaikh	
<b>Detection of Primary Glaucoma Using ANN with the Help of Back Propagation Algo in Bio-medical Image Processing</b> .....	48
G. Pavithra, T. C. Manjunath, and Dharmanna Lamani	
<b>RTMDC for Effective Cloud Data Security</b> .....	64
Pankaj Verma, Nilima Dongre, and Vijaylaxmi Bittal	
<b>Human Tracking Using Wigner Distribution and Rule-Based System in RGB Video</b> .....	74
J. R. Mahajan and C. S. Rawat	
<b>Agent Technology Based Resource Allocation for Fog Enhanced Vehicular Services</b> .....	84
Daneshwari I. Hatti and Ashok V. Sutagundar	
<b>Various Face Annotation Techniques: Survey</b> .....	94
Bhavini N. Tandel and Urmi Desai	

<b>Cyber Security: A New Approach of Secure Data Through Attentiveness in Cyber Space</b> . . . . .	103
Kumar Parasuraman and A. Anbarasa Kumar	
<b>Algo_Seer: System for Extracting and Searching Algorithms in Scholarly Big Data</b> . . . . .	116
M. Biradar Sangam, R. Shekhar, and Pranayanath Reddy	
<b>A Review on Infrared and Visible Image Fusion Techniques</b> . . . . .	127
Ami Patel and Jayesh Chaudhary	
<b>Implementation of the Standard Floating Point DWT Using IEEE 754 Floating Point MAC</b> . . . . .	145
R. Prakash Rao, P. Hara Gopal Mani, K. Ashok Kumar, and B. Indira Priyadarshini	
<b>A Novel for Analytical Healthcare Using Message Queue Telemetry Transfer</b> . . . . .	157
C. Anna Palagan and K. Soundara Rajan	
<b>Impact of Mobility and Density on Performance of MANET</b> . . . . .	169
Vaishali V. Sarbhukan and Ragha Lata	
<b>Next Generation Web for Alumni Web Portal</b> . . . . .	179
Marmik Patel, Devangi Rami, and Mukesh Soni	
<b>VLSI Implementation of Image Encryption Using DNA Cryptography</b> . . . . .	190
P. Vinotha and Deepa Jose	
<b>Comparative Analysis of Privacy Preserving Approaches for Collaborative Data Processing</b> . . . . .	199
Urvashi Solanki and Bintu Kadhiwala	
<b>Damage Detection and Evaluation in Wireless Sensor Network for Structural Health Monitoring</b> . . . . .	207
S. Surya and R. Ravi	
<b>Improvement of Web Performance Using Optimized Prediction Algorithm and Dynamic Webpage Content Updation in Proxy Cache</b> . . . . .	212
K. Shyamala and S. Kalaivani	
<b>An Approach for Generating SQL Query Using Natural Language Processing</b> . . . . .	226
Priyanka More, Bharti Kudale, Pranali Deshmukh, Indira N. Biswas, Neha J. More, and Francisco S. Gomes	
<b>Sentiment Analysis and Deep Learning Based Chatbot for User Feedback</b> . . . . .	231
Nivethan and Sriram Sankar	

**Semantic Concept Detection for Multilabel Unbalanced Dataset Using Global Features** . . . . . 238  
 Nita Patil and Sudhir Sawarkar

**A Survey on the Impact of DDoS Attacks in Cloud Computing: Prevention, Detection and Mitigation Techniques** . . . . . 252  
 Karthik Srinivasan, Azath Mubarakali, Abdulrahman Saad Alqahtani, and A. Dinesh Kumar

**A Study of Biology-Based Congestion Control Algorithms for Wireless Sensor Network** . . . . . 271  
 S. Panimalar and T. Prem Jacob

**A Comparison of GFDM and OFDM at Same and Different Spectral Efficiency Condition** . . . . . 282  
 Chhavi Sharma, S. K. Tomar, and Arvind Kumar

**Modified Multinomial Naïve Bayes Algorithm for Heart Disease Prediction** . . . . . 294  
 T. Marikani and K. Shyamala

**Discovering Web Users’ Web Access Pattern Based on Psychology** . . . . . 301  
 E. Manohar and E. Anandha Banu

**Non-invasive Haemoglobin Measurement Using Photoplethysmographic Technique** . . . . . 311  
 S. Selva Nidhyananthan, R. Dharshana Shahini, and S. Hari Priya

**A Novel Method to Safeguard Patients Details in IoT Healthcare Sector Using Encryption Techniques** . . . . . 317  
 R. Venkat Tejas and N. Rakesh

**An Extensive Survey on Recent Machine Learning Algorithms for Diabetes Mellitus Prediction** . . . . . 328  
 R. Thanga Selvi and I. Muthulakshmi

**Rawism and Fruits Condition Examination System Victimization Sensors and Image Method** . . . . . 336  
 J. Yamuna Bee, S. Balaji, and Mukesk Krishnan

**An Approximation to m-Ranking Method in Networks** . . . . . 344  
 K. Reji Kumar and Shibu Manuel

**Cloud Service Prediction Using KCFC Approach** . . . . . 353  
 K. Indira, C. Santhiya, and K. Swetha

**Detection and Classification of Tumors Using Medical Imaging Techniques: A Survey** . . . . . 363  
 Sheetal Garg and S. R. Bhagyashree

<b>Cab Service Communication in Transportation Classification Techniques</b> . . . . .	373
Prachi Singhal and G. Vadivu	
<b>Analysis on Emotion Detection for Infant Cry</b> . . . . .	380
M. Meenalochini, M. Janani, P. Manoj, and A. ShakulHameed	
<b>Computational Model for Hybrid Job Scheduling in Grid Computing</b> . . .	387
Pranit Sinha, Georgy Aeishel, and N. Jayapandian	
<b>A Comparative Analysis of LEACH, TEEN, SEP and DEEC in Hierarchical Clustering Algorithm for WSN Sensors</b> . . . . .	395
Anitha Amaithi Rajan, Aravind Swaminathan, Brundha, and Beslin Pajila	
<b>Investigation of Power Consumption in Microcontroller Based Systems</b> . . . . .	404
Rakhee Kallimani and Krupa Rasane	
<b>An Analogical Study of Hyperledger Fabric and Ethereum</b> . . . . .	412
A. V. Aswin and Bineeth Kuriakose	
<b>Smart City Traffic Control System</b> . . . . .	421
Kakan Adwani and N. Rakesh	
<b>An Investigation of Hyper Heuristic Frameworks</b> . . . . .	431
Rashmi Amardeep and K. ThippeSwamy	
<b>Detection of DDoS Attack Using SDN in IoT: A Survey</b> . . . . .	438
P. J. Beslin Pajila and E. Golden Julie	
<b>Impartial Clustering Algorithm to Increase the Lifetime of Wireless Sensor Networks</b> . . . . .	453
V. Asanambigai and A. Ayyasamy	
<b>Energy Efficiency Analysis of Cluster Based Routing in MANET</b> . . . . .	460
Parveen Kumari, Sugandha Singh, and Gaurav Aggarwal	
<b>Efficient and Secure Data Storage CP-ABE Analysis Algorithm</b> . . . . .	470
V. SenthurSelvi, S. Gomathi, V. Perathu Selvi, and M. Sharon Nisha	
<b>An Adaptive Thresholding Approach Based on Improved Harris Corner Detection for Estimation of Built up Region from Remote Sensing Images</b> . . . . .	477
N. M. Basavaraju, T. Shreekanth, and L. Vedavathi	
<b>Sentiment Classification Using Recurrent Neural Network</b> . . . . .	487
Kavita Moholkar, Krupa Rathod, Krishna Rathod, Mritunjay Tomar, and Shashwat Rai	

**Secure Data Transmission in VANETs Using Efficient Key-Management Techniques** . . . . . 494  
 Mahalakshmi Gopalakrishnan and Uma Elangovan

**Proof of Shared Ownerships and Construct A Collaborative Cloud Application** . . . . . 504  
 S. Ganesh Velu, C. Gopala Krishnan, K. Sivakumar, and J. A. Jevin

**Life at Ease with Technologies-Study on Smart Home Technologies** . . . 511  
 M. S. Meghana, K. Pavithra, S. Sahana, N. Shubha, and K. Panimozhi

**Data Analysis in Social Networks Based on Similarity Measurements on Multi-attribute Trajectories** . . . . . 518  
 K. Monica Rachel, D. C. Joy Winnie Wise, K. Raja Sundari, and N. Raja Priya

**Defender Vs Attacker Security Game Model for an Optimal Solution to Co-resident DoS Attack in Cloud** . . . . . 527  
 S. Rethishkumar and R. Vijayakumar

**Fuzzy Systems: A Human Reasoning Approach Using Linguistic Variables** . . . . . 538  
 Shama Parveen, Suraiya Parveen, and Nafisur Rahman

**Graph-Based Denormalization for Migrating Big Data from SQL Database to NoSQL Database** . . . . . 546  
 V. Rathika

**Quality Aware Data Aggregation Trees in Sensor Networks** . . . . . 557  
 Preeti Kale and Manisha J. Nene

**Light Tracking Bot Endorsing Futuristic Underground Transportation** . . . . . 568  
 Ragul M. Gayathri, Bisati Sai Venkata Vikas, and J. Thomas

**A Survey of ECG Classification for Arrhythmia Diagnoses Using SVM** . . . . . 574  
 Doshi Ayushi, Bhatt Nikita, and Shah Nitin

**An Efficient Trust and Energy Aware Protocol Using TAODV-ACO in MANETs** . . . . . 591  
 Ambidi Naveena and Katta Rama Linga Reddy

**An Octagonal Shaped MIMO UWB Antenna with Dual Band Notched Characteristics** . . . . . 599  
 V. N. Koteswara Rao Devana and A. Maheswara Rao

**On the Construction of Impacts of Mobility in Multicast Routing Protocol in Mobile Ad Hoc Networks** . . . . . 607  
 K. Muthulakshmi, S. Nithya Devi, and N. Archana

**Dynamic Trust Based Secure Multipath Routing for Mobile Ad-Hoc Networks** ..... 618  
V. Sathiyavathi, R. Reshma, S. B. Saleema Parvin, L. SaiRamesh, and A. Ayyasamy

**A Review on Various Approaches in Video Steganography** ..... 626  
S. Raja Ratna, J. B. Shajilin Loret, D. Merlin Gethsy, P. Ponnu Krishnan, and P. Anand Prabu

**Detection of DOM-Based XSS Attack on Web Application** ..... 633  
Shubhangi Ninawe and Rakhi Wajgi

**A Review on Clustering Algorithms in Wireless Sensor Networks for Optimal Energy Utilisation** ..... 642  
Bhagyashri Julme and Pragati Patil

**Error Performance Analysis of RF Subcarrier Adjusted FSO Communication Framework over Robust Environmental Disturbance** . . . 647  
Bobby Barua and Satya Prasad Majumder

**A Method for Identifying Human by Using Gait Cycle** ..... 655  
Snehal N. Kathale and Supriya Solaskar

**Author Index** ..... 667



# Cluster Restructuring and Compressive Data Gathering for Transmission Efficient Wireless Sensor Network

Utkarsha Sumedh Pacharaney<sup>1</sup>(✉) and Rajiv Kumar Gupta<sup>2</sup>

<sup>1</sup> Department of Electronics, Datta Meghe College of Engineering, Airoli, India  
utk21pac76@gmail.com

<sup>2</sup> Department of Electronics and Telecommunication,  
Terna College of Engineering, Nerul, India  
rajivmind@gmail.com

**Abstract.** Densely deployed Wireless Sensor Network (WSN) generates massive amount of data, which is processed and transmitted by resource constrained sensor nodes. The challenge of reducing high transmissions with low cost on-node processing can be achieved using Compressive Sensing (CS) CS data gathering from these nodes is designed under various routing mechanisms. Cluster-based routing integrated with CS, reduce transportation cost, but overall transmissions in the network are not reduced. When the density of nodes is high, advantage can be taken of their spatial closeness to form clusters. Motivated with this, we propose a novel Spatially Correlated Cluster (SCC) and integrate CS at cluster head. Different from other spatially correlated clusters, clusters with radius equal to sensing range of sensors is formed. Comparing our work with the state of the art methods, the proposed system reduces overall number of transmissions, hence reducing energy consumption and prolonging the network lifetime.

**Keywords:** Wireless Sensor Networks · Spatial correlation · Cluster · Topology · Compressive Sensing

## 1 Introduction

Wireless sensor network (WSN) is characterized by dense distribution of sensor nodes to support sensing, processing, transmitting and connectivity of the network. Due to dense deployment, redundant data gathering and transmissions take place in WSN. Data transmission contributes majority of energy consumption in a battery operated network [1], which is traditionally reduced using compression. Various in-network compression schemes exist such as entropy coding, principal component analysis or transform coding [2–4]. But due to significant computations and control overheads, these are often not suitable for sensor networks. The primary challenge of less data transmission with low cost on-node processing can be achieved using Compressive Sensing (CS). CS is an emerging new technology, which provides a new perspective for compression while gathering data at a node in WSN. CS compresses the signal before recording it in contrast to the usual method of sensing and then compressing a signal.



Decompression of CS is usually performed at the sink/Base Station (BS), which is computationally powerful. Hence, by leveraging ideas from CS, we can enable the more economical use of sensing resource in WSN [5].

A brief idea of CS is as follows:

Consider a signal  $f = [f_1, f_2 \dots f_N]$ , denoting a set of sensor readings from  $N$  nodes. If signal  $f$  is  $k$ -sparse then we can obtain  $y = [y_1, y_2, \dots, y_M]$ , by multiplying it with measurement matrix  $\Phi$ , i.e.  $y = \Phi f$ , and  $M \ll N$  but includes most of the information of  $f$ . Recovery of  $f$  from  $Y$  is done by solving  $l_1$  optimization problem, i.e.  $\|x\|_{l_1} \in \mathbb{R}^n \min$  subject to  $y = \Phi \Psi x$ , where  $f = \Psi x$ , represented in proper basis. Figure 1 shows the CS framework.

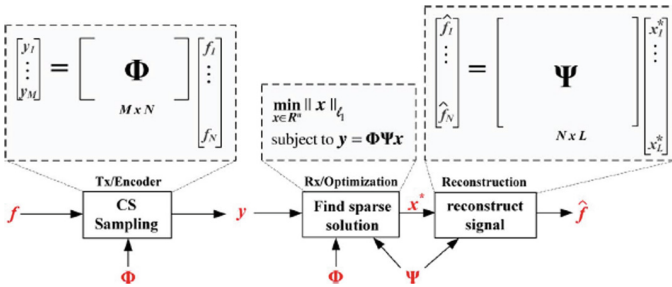


Fig. 1. Compressive sensing framework [6]

While powerful, CS theory is mainly designed to exploit intra-signal structure at the single node by collecting fewer measurements,  $M$ , than the original sensor data,  $N$  [7]. Applying plain CS will force every node to generate  $M$  samples leading to higher data transmissions in the early stage of the network. Therefore, the appropriate way of applying CS is to start CS coding when the outgoing samples become not lesser than  $M$ , otherwise raw data transmission is used. This hybrid CS framework induces two types of traffic into the network, i.e. encoded and raw. Hybrid CS is further integrated with routing mechanisms such as Gossip based [8], Random walk [9], Tree based [10] and Cluster based [11]. Since clustering has many advantages over other methods, hybrid of CS and cluster are extensively used for data gathering [12–14]. In a cluster, every node transmits raw data to the Cluster Head (CH) via intra cluster communication, and then CH applies CS, further transmitting compressed data to the sink. These methods reduce the number of CS transmissions in the clustered region but do not reduce the intra-cluster communication cost by making all nodes to participate in the transmission. The total amount of transmissions in a cluster depends on the number of transmitting nodes available and their location in data gathering process. Existing methods of clustering with CS, randomly group sensor nodes together and divide the entire network into clusters.

In a densely deployed network, spatial correlation exists between spatially proximal sensors that can reduce data transmission. Hence, instead of randomly clustering nodes together, in this work we consider spatial correlation to form clusters. Taking advantage of structural superiority of hexagonal shape, we hierarchically divide the network into hexagons further these hexagons are restructured into correlated clusters by

subdivision of hexagon. In the correlated region, only one node senses, gathers and transmits data to the CH of that region which further compressively send measurements to the sink. No intra-cluster communication cost is involved in data transmission within correlated area, which reduces overall transmissions in the network. The proposed system reduces the total number of transmissions, hence reducing energy consumption and prolonging the network lifetime.

The main contribution of this paper is to-

1. Present a transmission-efficient data gathering scheme with the integration of CS and restructured hexagon.
2. Prove that the correlation is maximum within the sensing range hence nodes in these regions are more correlated.
3. Unlike the conventional clustering approach used with CS, in which CH collects data from its members and then transmits it to the BS, we save on the intra-cluster communication cost with only the CH sensing and gathering data in the correlated region and then transmitting to the sink.

The remainder of this paper is organized as follows: Sect. 2 reviews the related works. We define problem statement in Sect. 3. In Sect. 4 we present the derivation of correlation based on sensing range of a node. The system model is discussed in Sect. 5. Section 6 demonstrates the simulation setup and evaluation. Finally, we conclude this work in Sect. 7.

## 2 Related Work

In general, for minimizing high data transmission and increasing the lifetime of WSN, data compression is one of the best techniques. With this aim, Duarte *et al.* in [15] has overviewed and detailed an array of proposed compression methods. In particular, CS is a new approach to simultaneously sense and compress that promises to reduce sampling and computational cost [16]. It is used very economically in an energy constrained sensor network. The First practical implementation of CS called Compressive Data Gathering (CDG) was done by Luo in [17], which use a tree-based aggregation method. Each node transmits  $M$  data packets for a set of  $N$  data items, and the total number of transmissions for gathering data from  $N$  nodes is  $MN$ , which is significantly high. To alleviate this problem, a hybrid version of CS and raw data collection was proposed by Luo in [11] and applied by Xiang [18] in a tree based aggregation. Since clustering, have many advantages over tree based method, integration of clustering and CS was proposed. Xie *et al.* [13] combined hybrid CS with clustering, that is, inside the cluster data gathering is done without CS and between CHs data gathering is done with CS, and analytically found the optimal size of the cluster that lead to minimum number of transmissions. Nguyen *et al.* [19] also calculated the optimal number of clusters and proved that consumed power is a decreasing function of the number of clusters, i.e. more clusters results in more power saving. An algorithm, called Cluster-Based Compressive Sensing Data Collection (CCS), is

proposed in which the CS measurements are generated at each cluster-head (CH). Liu *et al.* in [20] found that in hybrid CS, each CH does  $M$  transmissions for the intracluster data gathering and the number of transmission increases in a large-scale network. He proposed a new hybrid CS method with hexagonal cluster structure where within a cluster sensor nodes transmits collected data directly to the CHs through single hop without CS then CHs transmit data to neighboring CHs without CS if the number of packets in each CH is smaller than the measurement  $M$  else CS is used for data gathering. To keep the cost of transmission low for each measurement, [21] obtained measurements from clusters, sourced from adjacent sensors, using spatially localized sparse projections. Aiming to take advantage of spatial data correlation in a dense WSN, cluster structure can be reorganized with nodes to exploit the spatial correlation in the network to reduce the number of data transmissions and energy consumption.

Various clustering algorithms have been proposed in the survey [22], but little work has been done to group nodes with similar readings in the same cluster. Vuran *et al.* in [23] pointed out that in a dense WSN, significant energy saving is possible by allowing a less number of nodes to send information instead of redundant ones. A dynamic cluster is formed when nodes need to access the transmission media with the radius of cluster equal to  $r_{corr}$ . The CHs, known as the representative node, are chosen based on the distortion constraint of the reconstructed signal. In literature, the judgment of spatial correlation is based on the geographic distance of sensors [24], tolerance error of different sensor reading [25] or area of overlap between sensors [26], and a combination of error tolerance range and spatial correlation range [27] to form correlated clusters. Also, selection of the CH is very crucial in these clusters since they represent data feature of the entire group [28]. Apart from ignoring the cost of learning correlation, drawbacks of these correlated clusters is that there is no uniform measure on tolerance error range or distance between sensors. Also abundant communication overhead for spatial clustering, number of iterations to select the CH and above all, the construction of cluster takes several rounds of message exchange and computation of correlations in these clusters.

From all these works, it is clear that existing CS based data gathering is integrated with clustering to gain benefits of clustering. The clusters formed in this integration neglects the inherent spatial correlation that exists in a dense WSN. Also, spatially correlated cluster in literature has no specific or strict requirement on the similarity measure between nodes or distance. Hence, by considering these facts, we propose a novel clustering method and estimate the spatial correlation in a cluster based on sensing range  $r_s$  of sensor node. In our proposed work, BS assist division of sensing field into regular hexagons with further subdivision into regions and correlated regions by restructuring the hexagon. The radius of correlated region is equal to the sensing range of the sensor node. This region will have same type of information hence only one node, at appropriate location and sufficient energy is necessary to work for the cluster. Further, CS is applied at the CH of that region to reduce data redundancy. The proposed scheme significantly reduces the overall number of transmissions in the network and hence prolongs network lifetime.

### 3 Problem Statement

In, clusters integrated with CS, all nodes in the cluster send data to the CH and CH applies CS further transmitting compressed data to BS. Thus, we have intra-cluster communication between CH and Member Nodes (MN) and inter-cluster communication between CHs of different clusters.

Let WSN consist of  $N$  sensor node with  $C$  clusters. Let  $i^{th}$  cluster be formed by  $S_i$  number of sensor nodes and

$$\sum_{i=1}^C S_i = N \quad (1)$$

In each cluster, one node is CH and  $(S_i - 1)$  nodes are MN. These MNs transmit their data to CH in the transmission phase and then CH performs CS [11]. Therefore, number of transmissions in the network are

$$\sum_{i=1}^C S_i - 1 + \sum_{i=1}^C M_i \quad (2)$$

The first term in Eq. 2 corresponds to number of transmissions of  $(S_i - 1)$  nodes to CH in all  $C$  clusters and the second term corresponds to CS performed by CH. If each cluster contains the same number of nodes  $S$  and each cluster head perform CS to  $M$  number of measurements, then the communication load of the whole network is

$$C \times (S - 1) + C \times M = N + C(M - 1) \quad (3)$$

To reduce communication load of the network, we propose a model in which we divide the network area into regions (which we call cluster) and further into correlated sub regions (called as sub clusters) having CHs and Sub Cluster Heads (SCHs) respectively. In a sub region, only the SCHs gathers and transmit data to the CH of that region while other nodes sleep, saving on intra-cluster communication cost. Only CH performs CS on the data received from the correlated areas and sends it to BS. So the number of transmissions are

$$\sum_{i=1}^{C_R} S_{CH} + \sum_{i=1}^{C_R} M_i \quad (4)$$

Where  $C_R$  is correlated clusters, and  $S_{CH}$  is sub cluster head. Since in each sub cluster, only one  $S_{CH}$  transmits data, and if each cluster head perform CS to  $M$  number of measurements then communication load of the whole network is reduces to

$$C_R(S_{CH} + M) \quad (5)$$

Thus, with correlated cluster and CS, the communication load is significantly reduced.

### 4 Correlation Based on Sensing Range of Node

The proposed correlated clusters are based on the spatial location of sensor nodes hence we present data correlation between them using correlation model. The correlation between sensory data of nodes related to the spatial correlation between them is estimated based on sensory coverage of nodes. In addition, their reading association character can describe the correlation of different sensor nodes, which is covariance. The covariance between two measured values from node  $n_i$  and  $n_j$  at location  $R_i$  and  $R_j$  respectively can be expressed as [29]

$$Cov\{R_i, R_j\} = \sigma_s^2 K_\vartheta(d) \tag{6}$$

Where

$\sigma_s^2$  = variance of sample observation from sensor nodes

$Cov(.)$  = mathematical covariance

$K_\vartheta(.)$  = denotes correlation function

#### 4.1 Correlation Model

Assume two sensor nodes with sensing range  $rs_1$  and  $rs_2$  located  $d$  distance apart as shown in Fig. 2

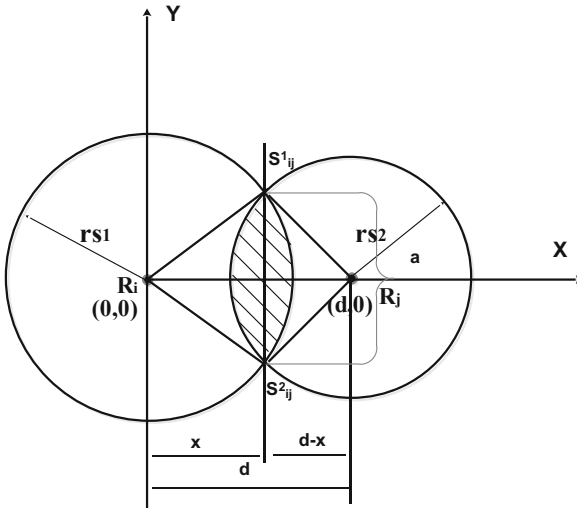


Fig. 2. Correlation model

Using geometry to set up the correlation model with meaning of symbols explained as follows:

$R_i$  and  $R_j$  denotes location of node  $n_i$  and  $n_j$  of disk with radius  $rs_1$  and  $rs_2$  respectively.

$A_i$ : Area  $R_i$  denoting area of  $R_i$

$A_j$ : Area  $R_j$  denoting area of  $R_j$

$R_i^j$ : Region delimitate by the perpendicular bisector of  $R_i$  and  $R_j$  and belongs to  $R_i$

$A_i^j$ : Area  $R_i^j$  denoting the area of  $R_i^j$

$A_j^i$ : Area  $R_j^i$  denoting the area of  $R_j^i$

$R$  denotes the sensing region

$A$  denotes the area of  $R$

$d$  distance between  $R_i$  and  $R_j$

$S_{ij}^1$  and  $S_{ij}^2$  are intersection points of the two nodes

$a$  length of the common chord joining  $S_{ij}^1$  and  $S_{ij}^2$

$$a = \frac{1}{d} \sqrt{4d^2rs_1^2 - (d^2 - rs_2^2 + rs_1^2)} \quad (7)$$

$x$  is the distance between  $R_i$  and chord  $a$

$$x = \frac{d^2 - rs_2^2 + rs_1^2}{2d} \quad (8)$$

If  $d < rs_1 + rs_2$  then  $R_i$  overlaps with  $R_j$  and correlation is defined as

$$K_{\vartheta}(d_{ij}) = \frac{A_i^j + A_j^i}{A} \quad (9)$$

$A_i^j + A_j^i = A^{int}$  is the area of the asymmetry lens which intersect the sensing range of two sensor node and is calculated as using the formula of circle segment of radius  $R'$  and triangle height  $d'$

$$A^{int}(R', d') = R'^2 \arccos\left(\frac{d'}{R'}\right) - d' \sqrt{R'^2 - d'^2} \quad (10)$$

Hence

$$A^{int} = A(rs_1, x) + A(rs_2, d - x) \quad (11)$$

$$A^{int} = rs_1^2 \arccos\left(\frac{d^2 + rs_1^2 - rs_2^2}{2drs_2}\right) + rs_2^2 \arccos\left(\frac{d^2 + rs_1^2 - rs_2^2}{2drs_1}\right) - \frac{1}{2} \sqrt{4d^2rs_1 - (d^2 - rs_2 + rs_1)^2} \quad (12)$$

Hence, from Eq. 9 we obtain

$$K_{\vartheta}(d_{ij}) = \frac{A^{int}}{A} \quad (13)$$

For the case when the sensing range of the two nodes is same i.e.  $rs_1 = rs_2 = r$

$$K_{\vartheta}(d_{ij}) = \frac{2}{\pi} \arccos\left(\frac{d}{2r}\right) - \frac{d}{\pi r^2} \quad (14)$$

It is observe from Eq. 14 that the correlation is a function of distance and the sensing range of the sensors. That is two nodes lying within the sensing range of each other are correlated. In addition for any value,  $1 < d < rs_1 + rs_2$ , correlation exists between nodes with correlation being zero for  $d = rs_1 + rs_2$  while for  $d = 0$  correlation is maximum. Taking this in into consideration we construct a correlated cluster with the radius of the cluster equal to the sensing range of the CH as explained in the next section.

## 5 System Model

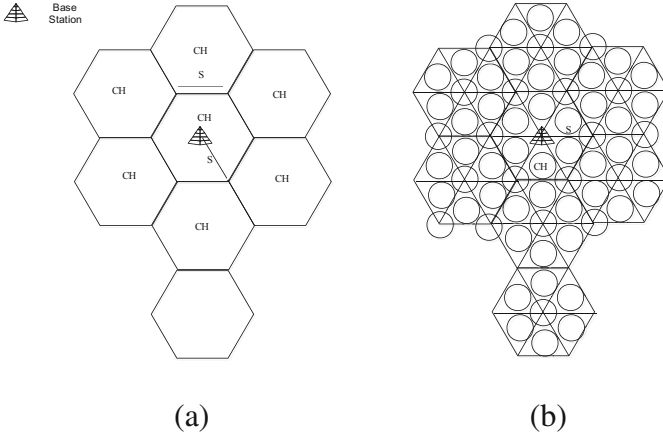
We make following assumptions:

- i. Sensor nodes know the geographic location via attached GPS or other localization techniques.
- ii. The sensing range  $r_s$  is same for each sensor and is half the transmission range  $r_t$ [31], i.e.  $r_t = 2r_s$
- iii. The sensed information is highly correlated
- iv. The nodes are capable of adjusting their transmission power to the desired recipient within  $r_t$ .

In our work, the clustering is BS assisted hence following modules are involved viz: Hexagonal base area division, cluster head selection, subcluster head selection and data transmission.

### 5.1 Hexagonal Deployment

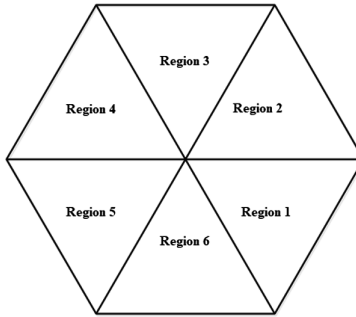
Hexagon being a geometric shape with largest coverage area and resembling the radiation pattern of an omni directional antenna is chosen for sensor deployment. Hexagons can be overlaid without overlapping each other, this has been proven in cellular geometry and is well applicable to WSN also. Hence the area of interest is divided, i.e. sensing field, by tessellating hexagons as shown in Fig. 3b.



**Fig. 3.** (a) Hexagon around Base Station (b) Tessellating Hexagons

Once all the nodes are deployed in the area of interest, they inform their location and energy to the BS. Considering only one part of the network, that is a hexagon, BS divides the area into six regions as triangles as shown in Fig. 4. Each region contains sensor nodes. The formula for dividing the area into six triangle, as shown in Fig. 12, is given in Appendix A

$$Area = \frac{(x_1(y_2 - y_3) + x_2(y_3 - y_1) + x_3(y_1 - y_2))}{2} \quad (15)$$



**Fig. 4.** Hexagon divided into six regions

### 5.1.1 Selection of Cluster Head

Considering BS assisted cluster formation, the BS selects the CH with highest residual energy and appropriate location [31]. The CH selection process is mathematically described by a parameter  $W_{CH}$ , which depends upon the average residual energy of the CH and their position and is expressed as:



$$W_{CH} = w_1 R_{CH}^L + w_2 R_{CH}^E \quad (16)$$

Where  $R_{CH}^L$  is location and  $R_{CH}^E$  is energy factor of CH while  $w_1$  and  $w_2$  indicate the contribution of both the parameters in the expression of  $W_{CH}$ . After dividing the field into six regions the BS calculates geographic center point of each region, this is the value  $R_{CH}^L$ . The center point of the cluster is calculated using the formula:

$$O_x = \frac{A_x + B_x + C_x}{3} \quad O_y = \frac{A_y + B_y + C_y}{3} \quad (17)$$

The sensor nodes do not know who is closest to the central point of a cluster area, in this scenario, cluster of all nodes within the range from the center be the CH candidates of the cluster. The candidate that has smallest distance to the center of cluster becomes the CH. BS geocast the tuple  $(R_{CH}^L, R_{CH}^E)$  into the area. All nodes receive this tuple, but the one with the closest value announced in the message is elected as CH. As shown in Fig. 5.

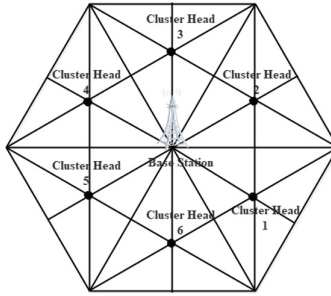


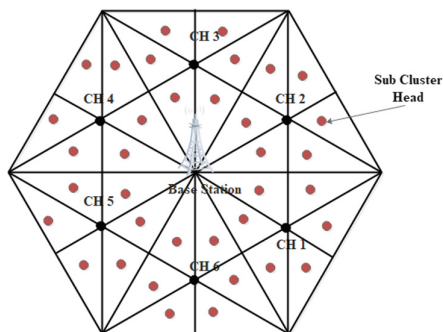
Fig. 5. Location of cluster head in the region of interest

### 5.1.2 Sub Cluster Head Selection

After the identification of CH, the sub cluster heads of each cluster-area has to be elected. Following the same procedure, each region is further subdivided into six sub regions as given by Eq. 14 and then SCH is calculated. Six SCH are elected in each region. These subclusters form the correlated regions; hence only the SCH is required to gather and transmit data for this region to the CH of that region. Figure 6 shows the location of these subcluster heads.

### 5.1.3 Sleep Scheduling

When the SCH becomes the coordinator of the cluster, it sends a beacon frame to schedule the sleep mode of the cluster members. All the sensor nodes in the cluster are asleep, and only the SCH is awake. It senses and sends data to the CH of that region which further sends it to the BS. Thus energy is conserved by data compression, efficient control of transmission power and efficient sleep scheduling of the cluster nodes. The beacon frame structure is as shown in Fig. 7, for IEEE 802.15.4 [32]



**Fig. 6.** Formation of Sub Cluster Heads

In payload field of the beacon, sleep schedule is sent by the SCH, which is not same for all the nodes, it depends on the node that becomes the CH for next round and the subsequent rounds. Next CH for the cluster is determined by CH based on the area of overlap as discussed in next section.

Octets	2	1	4/10	2	Variable	Variable	Variable	2
Frame Control	Sequence Number	Addressing Fields	Super-frame Specification	GTS	Pending addressing fields	Beacon Payload	FCS	
	HGR			MAC protocol		MFR		

**Fig. 7.** Beacon frame structure as defined by IEEE 802.15.4

#### 5.1.4 Determination of CH for Next Round

In a cluster formed by gathering sensor nodes within the sensing range  $r_s$  of the CH, the CH will drain its energy since only it is performing the task of sensing, compressing and transmitting. Also, sensing range of the sensor node changes with remaining energy. Hence, once energy level of the CH reaches a predetermined threshold level say  $E_{th}$ , CH has to change in the next round. Using Eq. 10, CH calculates area of overlap for each MN and decide CHs for the subsequent rounds and accordingly decide the sleep schedule for each node. This schedule is then transmitted in the beacon frame. When the CH changes, the new CH will sense and transmit data in its sensing range so the change in CH will change the cluster position. This is reasonable because after clustering the environment may have changed and the previous cluster may not be valid any more. Even though the position of the cluster changes the membership of the nodes in the cluster will remain the same.

#### 5.1.5 Data Transmission

The CH only receives data from the sub cluster head; it does not perform any data gathering, it only performs CS and generates measurements to be transmitted to the BS.

Let  $CH_i$  denote the CH of the region  $i$ , where  $i = 1$  to  $6$  and  $f_i$  represent the sensor reading obtained by the  $CH_i$ . The  $CH_i$  has  $N_i$  readings which can be denoted as.

$$f_i = [f_1, f_2, \dots, \dots, \dots, f_{N_i}] \tag{18}$$

The CH multiplies this by a random matrix  $\emptyset_i$  and then sends the product  $Y_i$  to the sink.

Thus,  $Y_i = \emptyset_i f_i$  and has  $m_i$  measurements.

The BS collects each measurement from one cluster at a time, and a Block Diagonal Matrix (BDM) as a sensing matrix is built.

$$\begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_M \end{bmatrix}_{M \times 1} = \begin{bmatrix} \emptyset_1 & 0 & 0 & 0 \\ 0 & \emptyset_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \emptyset_M \end{bmatrix}_{M \times N} \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_{N_i} \end{bmatrix}_{N \times 1} \tag{19}$$

This BDM with only one nonzero entry in each row and column is the sparsest measurement matrix. Finally, the BS receives  $Y = \bigcup_{i=1}^C Y$ , the compressed information of all clusters at the BS, the original data can be reconstructed from  $Y$  by using  $l_1$  minimization.

## 6 Experimental Setup and Simulation Results

To evaluate the performance of clustering with CS applied at CH, the dataset used is the real data set obtained by a WSN deployed at Intel Laboratory Berkeley [33], and simulation for this was developed in MATLAB R2015. This data set contains temperature, humidity, light and voltage values periodically collected with 54 distributed Mica2Dot sensor nodes from 25<sup>th</sup> February–5<sup>th</sup> April 2004. Figure 8 shows the distribution of sensor nodes in Berkeley Lab.

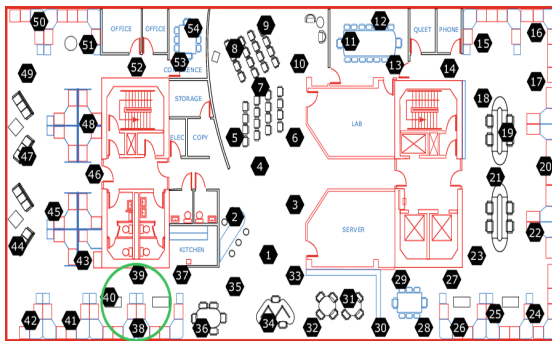
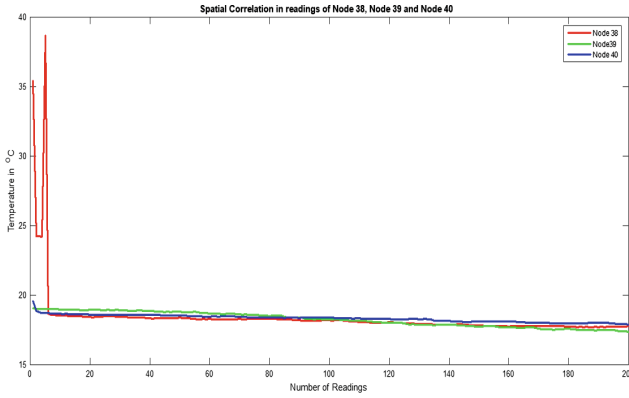


Fig. 8. Intel Berkeley Lab

According to [34], the communication radius of the sensor node in Intel Berkeley Lab is set to 6 m. Following the same, in our work, the sensing radius is 3 m, since sensing radius is half the communication radius [30]. The correlated cluster is formed with Node number 38, 39 and 40 and depicted in the Berkeley lab by a green circle as shown in Fig. 8. To prove that the spatial readings of the nodes are correlated, we tabulate their spatial coordinates, i.e. x and y coordinates (in meters relative to the upper right corner of the lab) in Table 1. and plot a graph of temperature reading at the same time instance in Fig. 9. Table 1 gives the spatial coordinates of sensor Node 38, Node 39 and Node 40.

**Table 1.** Node coordinates

Node	(x location, y location)
38	(30.5,31)
39	(30.5,26)
40	(33.5,28)



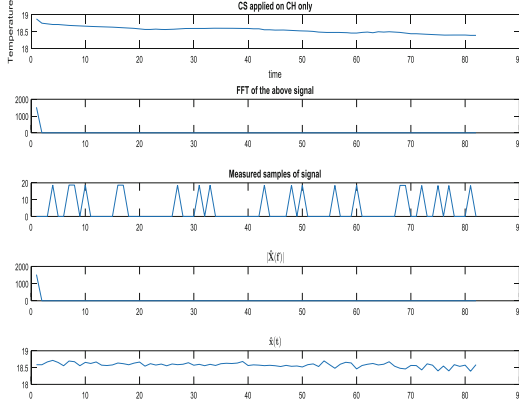
**Fig. 9.** Spatial correlation between readings of Node38, 39 and40

As seen in the graph the readings are highly correlated. Hence instead of sending all the data to the sink we suppress correlated information and save the number of transmissions. Applying CS at the CH at node 40, while keeping node 38, 39 in the sleep mode, the original and reconstructed signal is depicted in Fig. 10.

Like any other compression technique measuring the accuracy of the reconstruction is an important parameter. One of the most popular ways to do it by calculating the root mean square error (RMSE) value. The expression of which is given by:-

$$RMSE = \frac{s - \hat{s}_2}{s_2} \quad (20)$$

Where  $s$  is the original signal,  $\hat{s}$  is the approximated signal and  $s_2 = \left(\sum_{i=1}^n |s_i|^2\right)^{\frac{1}{2}}$  is the 2-norm or Euclidean length of  $s$  [35]. The RMSE is calculated for our proposed method and is **RMSE = 0.004967**.

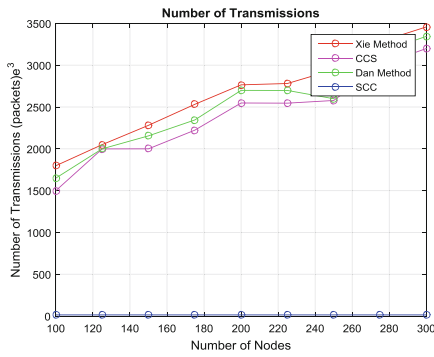


**Fig. 10.** Applying CS on CH of the correlated cluster.

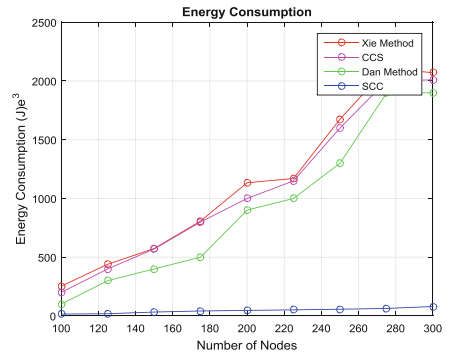
Hence we observe that taking advantage of spatial correlation we can save the number of transmission by only using CH to transmit data to the base station. We compare the performance of the proposed SCC with three state hybrid CS methods viz:-Xie's Method [13], CCS proposed in [11] and Liu's Method [20]. Performance metrics such as the number of transmissions, energy consumption and network lifetime are compared with the existing methods. The scenario is kept same for all of them that is the number of nodes and energy model. The simulation of the proposed correlated cluster is carried out in NS-2 simulation. The simulation parameters are tabulated in Table 2. Simulations were carried out for four different parameters while keeping the scenario same for all the methods and varying the number of nodes. Figure 11a shows that as the number of nodes is increased the number of transmissions is increased but SCC method achieves reduced number of transmissions as compared to existing ones since only the SCHs are the nodes in each correlated cluster that are transmitting and others are in the sleep mode. Also, SCC achieves reduced energy consumption when compared to the existing process as shown in Fig. 11 b when the number of nodes are increased, at the same time network lifetime is improved as the compared to state of the art methods as depicted in Fig. 11c.

**Table 2.** Simulation parameters

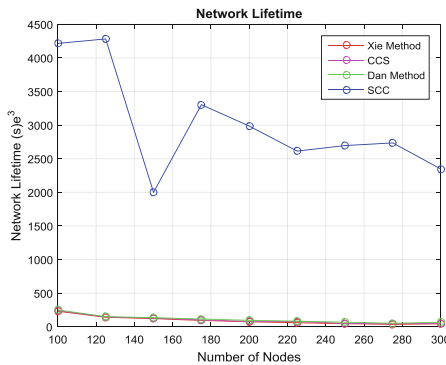
Name	Parameter
Simulator	Network Simulator 2
Topology	Random
Interface type	Phy/WirelessPhy
MAC type	802.11(ad hoc)
Queue type	Drop Tail/Priority Queue
Queue length	100 Packets
Antenna type	Omni Antenna
Propagation type	Two Ray Ground
Routing protocol	AODV
Transport agent	UDP
Application agent	CBR
Network area	600 * 600
Number of nodes	100,120,140,160,180,200,220,240,260,280,300
Simulation time	50 s
Transmission range	60 m
Sensing range	30 m
Initial energy	50 Joules



(a)



(b)



(c)

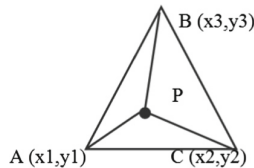
**Fig. 11.** Comparative graph of: (a) number of transmissions (b) energy consumption and (c) network lifetime

## 7 Conclusion

The massive amount of data generated by a dense WSN can be compressed economically with CS. Usually, CS is integrated with clustering while neglecting the inherent spatial correlation in WSN. In this paper, we exploit spatial correlation, which is inherent in the area of interest to be monitored. Instead of using the circular convention shape, hexagonally clustered WSN is designed. The hexagon is further restructured into the spatially correlated cluster by subdividing the hexagon into regions and sub regions. Different from other spatially correlated clusters that are based on spatial distance or similarity in data reading, we propose the use of spatial proximity in the impact area to form the correlated cluster. A derivation of which is presented in this paper. Hence, correlated clusters with the radius equal the sensing range of a sensor node are formed. With appropriate location, at the median of the triangles, CHs and SCHs are selected. Only SCHs are transmitting data to the CH of that region with MN in the cluster scheduled to sleep; no intra-cluster communication cost is incurred in this cluster. NS-2 and MATLAB simulators are used to demonstrate cluster formation and data communication. Comparing our work with existing methods of clustering, where MN transmit data to the CH and CH further transmits it to the base station, transmission efficiency is achieved in this work. Along with saving on the number of transmissions we also conserve energy consumption in the network. A detailed energy analysis of cluster formation and data transmission is carried out in this work. In spite of sending fewer measurements using CS at CH, the original signal is reconstructed at the base station with low RMSE value. Thus we have integrated compressive sensing with spatially correlated cluster avoiding communication overhead and reducing the number of transmissions. We believe the network lifetime is prolonged along with reduced energy consumption which is the main bottleneck for a battery operated sensor network.

## Appendix A

### Appendix A



**Fig. 12.** Calculating area of triangle

Let the node is located at point P. Calculate area of the triangle PAB. It can use the formula

$$Area = \frac{(x_1(y_2 - y_3) + x_2(y_3 - y_1) + x_3(y_1 - y_2))}{2}$$

Let this area be A1.

Calculate area of the triangle PBC. Let this area be A2.

Calculate area of the triangle PAC. Let this area be A3.

If P lies inside the triangle, then A1 + A2 + A3 must be equal to A.

## References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. *Commun. ACM* **38**(4), 393–422 (2002)
2. Dabirmoghaddam, A., Ghaderi, M., Williamson, C.: Cluster-based correlated data gathering in wireless sensor networks. In: 2010 IEEE International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS). IEEE (2010)
3. Rooshenas, A., et al.: Reducing the data transmission in wireless sensor networks using the principal component analysis. In: 2010 Sixth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). IEEE (2010)
4. Gastpar, M., Dragotti, P.L., Vetterli, M.: The distributed Karhunen–Loeve transform. *IEEE Trans. Inf. Theor.* **52**(12), 5177–5196 (2006)
5. Candès, E.J., Wakin, M.B.: An introduction to compressive sampling. *IEEE Sig. Process. Mag.* **25**, 21–30 (2008)
6. Chen, F., Chandrakasan, A.P., Stojanovic, V.M.: Design and analysis of a hardware-efficient compressed sensing architecture for data compression in wireless sensors. *IEEE J. Solid-State Circ.* **47**(3), 744–756 (2012)
7. Donoho, D.L.: Compressed sensing. *IEEE Trans. Inf. Theor.* **52**(4), 1289–1306 (2006)
8. Rabbat, M., Haupt, J., Singh, A., Nowak, R.: Decentralized compression and predistribution via randomized gossiping. In: The Fifth International Conference on Information Processing in Sensor Networks, IPSN 2006, pp. 51–59 (2006)
9. Wang, X., Zhao, Z., Xia, Y., Zhang, H.: Compressed sensing based random routing for multi-hop wireless sensor networks. In: 2010 International Symposium on Communications and Information Technologies (ISCIT), pp. 220–225 (2010)
10. Luo, C., Wu, F., Sun, J., Chen, C.W.: Efficient measurement generation and pervasive sparsity for compressive data gathering (2010)
11. Luo, J., Xiang, L., Rosenberg, C.: Does compressed sensing improve the throughput of wireless sensor networks? In: 2010 IEEE International Conference on Communications (ICC). IEEE (2010)
12. Wu, X., et al.: Sparsest random scheduling for compressive data gathering in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **13**(10), 5867–5877 (2014)
13. Xie, R., Jia, X.: Transmission-efficient clustering method for wireless sensor networks using compressive sensing. *IEEE Trans. Parallel Distrib. Syst.* **25**(3), 806–815 (2014)
14. Nguyen, T.M., Teague, K.A., Rahnavard, N.: Inter-cluster multi-hop routing in wireless sensor networks employing compressive sensing. In: 2014 IEEE Military Communications Conference (MILCOM), IEEE (2014)
15. Duarte, M.F., et al.: Signal compression in wireless sensor networks. *Philos. Trans. R. Soc. A* **370**(1958), 118–135 (2012)
16. Bajwa, W., et al.: Compressive wireless sensing. In: Proceedings of the 5th International Conference on Information Processing in Sensor Networks. ACM (2006)



17. Luo, C., et al.: Compressive data gathering for large-scale wireless sensor networks. In: Proceedings of the 15th Annual International Conference on Mobile Computing and Networking. ACM (2009)
18. Xiang, L., Luo, J., Vasilakos, A.: Compressed data aggregation for energy efficient wireless sensor networks. In: Proceedings of the IEEE Sensor, Mesh, and Ad Hoc Communications and Networks (SECON '11), pp. 46–54, June 2011
19. Nguyen, T.M., Teague, K.A.: Compressive sensing based data gathering in clustered wireless sensor networks. In: 2014 IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS). IEEE (2014)
20. Liu, D., et al.: Cluster-based energy-efficient transmission using a new hybrid compressed sensing in WSN. In: 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE (2016)
21. Lee, S., Pattem, S., Sathiamoorthy, M.: Spatially-localized compressed sensing and routing in multi-hop sensor networks. In: Proceedings of the 3rd International Conference on Geosensor Networks (GSN) (2009)
22. Xiaoronga, C., Mingxuan, L., Suc, L.: Study on clustering of the wireless sensor network in distribution network monitoring system. Phys. Procedia **25**, 1689–1695 (2012)
23. Vuran, M.C., Akyildiz, I.F.: Spatial correlation-based collaborative medium access control in wireless sensor networks. IEEE/ACM Trans. Netw. **14**(2), 316–329 (2006)
24. Yuan, J., Chen, J.: The optimized clustering technique based on spatial-correlation in wireless sensor networks. In: Proceedings of IEEE Youth Conference on Information Computing and Telecommunication, YC-ICT, pp. 411–414, September 2009
25. Liu, C., Wu, K., Pei, J.: An energy-efficient data collection framework for wireless sensor networks by exploiting spatiotemporal correlation. IEEE Trans. Parallel Distrib. Syst. **18**(7), 1010–1023 (2007)
26. Shakya, R.K., Singh, Y.N., Verma, N.K.: Generic correlation model for wireless sensor network applications. IET Wirel. Sens. Syst. **3**(4), 266–276 (2013)
27. Liu, Z., et al.: Distributed spatial correlation-based clustering for approximate data collection in WSNs. In: 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA). IEEE (2013)
28. Ramesh, K., Somasundaram, K.: A comparative study of clusterhead selection algorithms in wireless sensor networks. arXiv preprint [arXiv:1205.1673](https://arxiv.org/abs/1205.1673) (2012)
29. Vuran, M.C., Akan, Ö.B., Akyildiz, I.F.: Spatio-temporal correlation: theory and applications for wireless sensor networks. Comput. Netw. **45**(3), 245–259 (2004)
30. Zhang, H., Hou, J.C.: Maintaining sensing coverage and connectivity in large sensor networks. Ad Hoc Sens. Wirel. Netw. **1**(1–2), 89–124 (2005)
31. Khalid, Zubair, Durrani, Salman: Distance distributions in regular polygons. IEEE Trans. Veh. Technol. **62**(5), 2363–2368 (2013)
32. Ouni, S., Ayoub, Z.T.: Predicting communication delay and energy consumption for IEEE 802.15.4/Zigbee wireless sensor networks. Int. J. Comput. Netw. Commun. **5**(1), 141 (2013)
33. Intel labs berkeley data. <http://db.csul.mit.edu/www.select.cs.cmu.edu/data/labapp3/>
34. Yuan, F., Zhan, Y., Wang, Y.: Data density correlation degree clustering method for data aggregation in WSN. IEEE Sens. J. **14**(4), 1089–1098 (2014)
35. Quer, G., et al.: Sensing, compression, and recovery for WSNs: sparse signal modeling and monitoring framework. IEEE Trans. Wirel. Commun. **11**(10), 3447–3461 (2012)



# Condition Monitoring of Coal Mine Using Ensemble Boosted Tree Regression Model

R. Uma Maheswari<sup>1</sup>(✉), S. Rajalingam<sup>1</sup>, and T. K. Senthilkumar<sup>2</sup>

<sup>1</sup> Department of Electronics and Communication Engineering,  
Rajalakshmi Institute of Technology, Chennai, India  
uma.bhuvan@gmail.com, rajalingvlsi@gmail.com

<sup>2</sup> Manipal Global Education Services, Bengaluru, India  
tkseneeee@gmail.com

**Abstract.** In recent years, Fires and explosion in coal mines imposes number of life threats for mine workers along with a rapid increase in environmental air pollution. By using various risk assessment methodologies, coal miners can easily predict the potential risks of forthcoming hazards in advance. In this work, a novel approach is proposed for monitoring the fire-resistant hydraulic fluids (HFA) contamination level. Fire resistance property of HFA fluids varies with the viscosity. Water content. By monitoring the water content in HFA fluids, fire resistance can be easily predicted. Fire resistance hydraulic fluid properties are trained in Ensemble Boosted Regression Tree (EBRT) to predict the potential risk in coal mines. EBRT is the supervised training algorithm which is proposed for leveraging an efficacious coal mine monitoring into existence. EBRT model estimates stronger prediction by linearly integrating the weaker estimations. Threshold rule-based decision making is adopted for the effective mitigation of risks. EBRT is optimized to minimize the cross-validation loss. Furthermore, Bayesian optimizer is used to minimize the objective function to 7.81 with regularized parameter lambda is chosen as 0.34 to minimize the ensemble trees. The root Mean square error is optimized to 31.68.

**Keywords:** Regression · Ensemble boosted tree · Risk assessment · Condition monitoring

## 1 Introduction

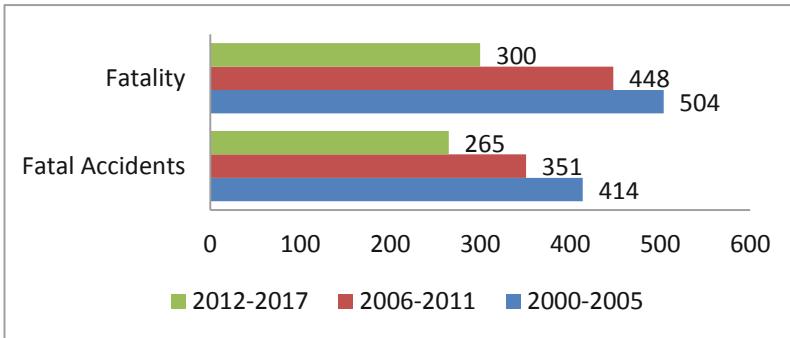
In the recent past, Unscientific way of mining has resulted to subsidence problems and fires in coal mines. Deep underground coal mines initiate a higher risk rate when compared with the other open coal mines. Fire accidents and fatality rates are higher in India than in western countries. Hydraulic fluids are used in mining process and heavy vehicles are pressurized under the harsh operating conditions. Temperature of pressurized hydraulic fluids increases during the mining operations. When these hydraulic fluids are sprayed on the hot surfaces, fire risk rate increases considerably. Hazardous gases like methane, carbon monoxide (CO) emission is considered as the another potential fire risk. 5% to 15% increase in CO concentration in the air poses a high risk for explosion. Table 1 lists the potential ignition sources in underground coal mines

(“Prevention of Fires in Underground Mines — Guideline: Resources Safety” 2013). It was observed from Coal India Ltd statistics, fatal accidents and fatality rates high in underground mines.

**Table 1.** Potential fire ignition sources

Type	Ignition source
Heat energy	Pressurized hydraulic fluids/fuels sprayed on hot surfaces, induction heating.
Electrical energy	Short circuit arc, earth faults, electric discharge in motors.
Mechanical energy	Friction, grinding, cutting.
Chemical reaction	Self-oxidation, auto-ignition, Exothermic reaction.

Indian (Coal India Ltd) coal mine accident statistics (2000–2017) is shown in Fig. 1 (“SAFETY AT A Glance” 2017). Condition monitoring of coal mines is used for early detection of fire and explosion hazards and mitigation strategies could be automated. In recent years, machine learning algorithm plays a crucial role in automation. In this work, a novel approach is proposed for monitoring coal mine hydraulic fluid and hazardous gas emission using an ensemble boosted regression tree model.



**Fig. 1.** Indian coal mines accident statistics

## 2 Related Work

Geothermic information system based hazard assessments and modeling were reviewed in (Suh et al. 2017). Statistical analysis with Bayesian classifiers, decision trees and contingency tables was performed to obtain behavioral patterns of various mining accidents (Sanmiquel and Vintó 2015). Fluid contamination levels predicted from mean, standard deviation, kurtosis of fluid data analysis (Helwig and Schütze 2016). Moving sub window approach is adapted to extract thermal anomalies of different

temperature coal fire risk areas are detected with thresholding techniques (Kuenzer et al. 2007). Thermal image processing method is employed for detection of surface and subsurface coal fires (Mishra et al. 2011). In (Cheng and Yang 2012) rough set theory is used to select best verification indexes and SVM is trained to classify the risk ranks for mine ventilation system. Computational fluid dynamic approach is adapted to handle hazardous gases from diesel emission in underground mine (Kurnia et al. 2014). Cluster tree WSN with REST is proposed for coal mine monitoring (Cheng et al. 2015). Top Down Fixed rule based regression model is proposed for prediction of Methane concentration in coal mines(Kozielski et al. 2015). Electrical resistance tomography (ERT) with interferometry synthetic aperture radar remote sensing technique is proposed to monitor underground coal gasification monitoring (Mellors et al. 2016). Fuzzy TOPSIS model based risk evaluation was proposed in (Mahdevari et al. 2014). Coal burst risk assessment framework based on US mines was presented in (Mark and Gauna 2016). In (Shen et al. 2016) CAN Bus technology is used for real time monitoring and fault diagnosis of hydraulic drilling in coal mines.

Improved Hilbert hung transform (HHT method) with micro seismic interpretation method is proposed to monitor hydraulic fracturing (Zhu et al. 2017). sampling robot approach is proposed to monitor hydraulic fluids in mines (Li et al. 2017). Azure machine learning based Internet of Things system is proposed for underground coal monitoring (Jo et al. 2018).

### 3 Materials and Methods

#### 3.1 Hydraulic Fluids Monitoring

Physical and chemical properties of hydraulic fluids used in coal mines are listed in Table 2 (Givens and Michael 2003; Peter 2004). Under harsh mining operation the pressurized mineral based hydraulic fluids pose fire risks. Fire resistant hydraulic fluids used in underground coal mines are fire-resistant hydraulic fluids soluble in water (HFA-S) and emulsified in water (HFA-E)(Dwuletzki et al. 2010). HFA fluids have low thermal induction than mineral oil-based fluids. Condition monitoring of HFA fluids are essential to avoid serious accidents. Prolonged use of water evaporated HFA fluids leads to adverse secondary effects. Water content and viscosity of fluids are inversely proportional. Variation in viscosity causes variation in fire resistance of fluids. Ensemble Boosted regression tree model is trained with properties of fluids and viscosity is predicted for fire resistance estimation.

#### 3.2 Ensemble Boosted Tree Regression Model

Regression machine learning prediction performance is improved by ensemble approach to reduce the prediction performance measures noise, bias and variance. In gradient ensemble boosting method, the predictors are chosen sequentially. Dataset is divided into simple trees, trees learn one by one. Weights are adjusted sequentially; multiple reweighted prediction estimates are summed to improve prediction performance. Estimated weak predictions are linearly combined to get stronger prediction to

**Table 2.** Fire resistant fluid properties

Fire resistant hydraulic fluids	Anti-wear hydraulic fluids (HM)	Fire resistant water In oil emulsion (45% water content) (HF-B)	Fire resistant water glycol fluid (HF-C)	Fire resistant synthetic phosphate ester fluid (HF-DR)	Fire resistant synthetic polyol ester fluid (HF-DU)
Viscosity at 40° C	32–68	8–100	40	22–100	46–68
Specific Heat Capacity (J/Kg/° K)	–	3350	3300	1270	2310
Thermal Conductivity (W/m/°K)	–	0.52	0.31	0.11	0.15
Vapor Pressure mbar	0.001 at 50°C	–	80 at 50° C	<1 at 150° C	–
Density @ 15°C	0.88	1.0	1.10	1.15	0.93
Specific gravity	0.85–0.88	0.91–0.93	1.05–1.10	1.02–1.16	0.91–0.96
Water content	0.05%	43%	43%	0.05%	0.1%
Heat of combustion (kJ/g)	29.1	16.3	5.3	19.1	21.8
Auto ignition temp °F	650	830	830	>1100	750
Maximum temp °F	130	50	65	150	150

boost the performance (Bühlmann and Hothorn 2007; Natekin and Knoll 2013). Ensemble Gradient Boosted Regression Model is mathematically defined as follows

1. Ensemble estimates

$$\tilde{h}(y) = \sum_{j=1}^N h_j(y) \tag{1}$$

$h_j(y)$  weighted estimates.  $N$  – number of iterations.  $j$ -data samples.

2. To reduce the variance and bias gradient boosting is adapted. Loss function  $\Psi(x, h)$  is defined to adjust the root mean square error of variance and bias. Negative gradient of loss function is defined as

$$\Delta(y) = E_x \left( \frac{\partial \Psi(x, h(y))}{\partial h(y)} \right) \tag{2}$$

Regression gradients

$$\frac{1}{2} [y_i - h(y)]^2 \tag{3}$$

3. Fit the regression tree to fit the target  $\Delta(y)$

$$\Phi = \arg \min \sum_{y_i \in \Delta(y)} \lambda(y_i, h_{m-1}(y_i)) + \gamma \tag{4}$$

$\gamma$  - Regularization parameter.

## 4 Results and Discussion

### 4.1 Dataset

The dataset is synthesized with 73 hydraulic fluid variants used in underground coal mines.  $73 \times 5$  data samples are trained with target as flash point temperature. Viscosity, Fire Point, Auto Ignition Temperature, Boiling Point, Vapor Pressure are used as the predictors. Flash point temperature is estimated using ensemble boosted regression tree. MATLAB 9.4.0 regression learner and Weka 3.8.2 is used to compare the performance of supervised regression learning algorithms. Fivefold cross validation is adapted to reduce the bias and variance. In this Method, entire data set is divided into five subsets and one subset is used for testing and remaining subsets are used for training. This process continues till all subsets are used for training and testing.

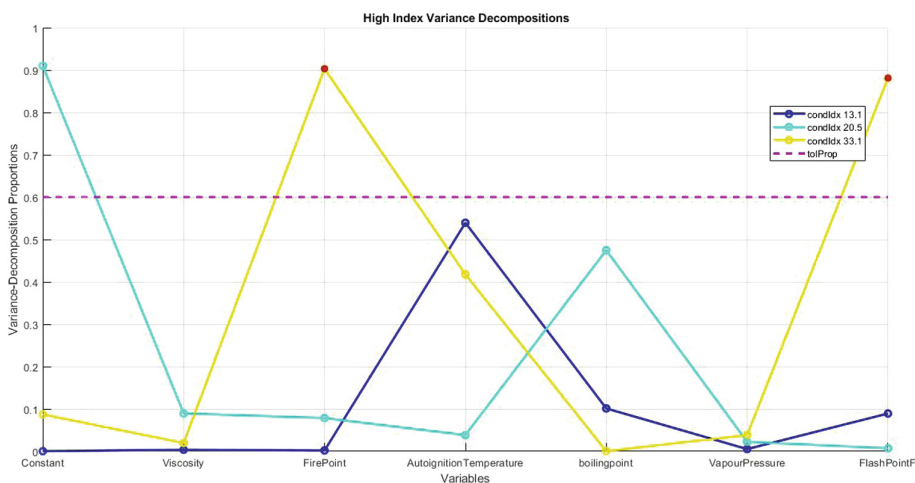
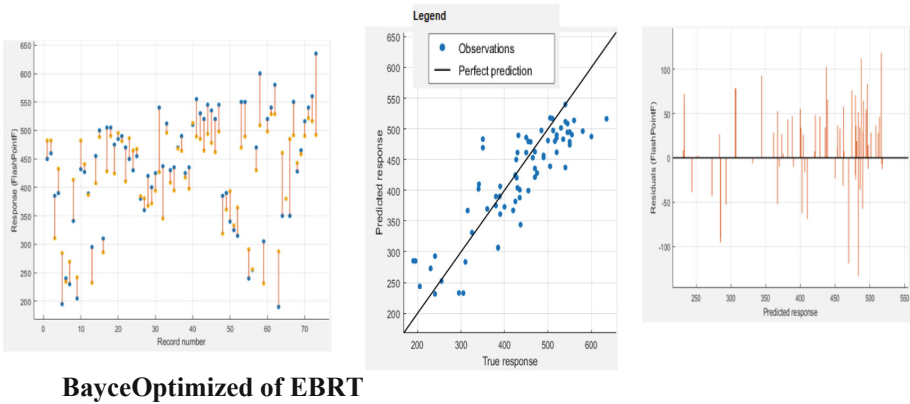


Fig. 2. Variance decomposition table

**Correlation Analysis of Predictors.**

The properties of synthesized predictor data are analyzed by estimator variance. To assess the degree of association with the predictor correlation test is carried out. Dependencies among predictors is evaluated by the measure of the strength of pairwise linear relationships. Figure 2 shows the variance decomposition table. 5–10 condition indices indicates weak dependencies. 30–100 condition indices specify moderate to high dependencies. Fire point predictor with condition Index 33.1 alone shows the proportion above tolerance 0.6. Tolerance is empirically fixed based on mutual dependence. From Fig. 3, it was observed that the significant t statistics (highlighted in red) in predictor pairs show high correlation. Auto ignition temperature, boiling point and flash point scatters widely, that shows the possibility of potentially influenced data subsets. Various regression models are fit into the data. The best training model is chosen based on the root mean squared error and the

The Dataset is trained to Ensemble Boosted Regression Tree (EBRT) model. Regression learner performance is evaluated with Fig. 4. Record number shows the number of observations in cross validation training. In response plot, blue dots represent actual values and yellow dots represents predicted values. Root mean square error measure is used to evaluate the score of EBRT model.



**Fig. 3.** Ensemble boosted regression tree regression model performance (a) Response plot (b) Predicted Vs actual plot (c) Residual plots.

**Bayce Optimized of EBRT**

It was observed from Table 3, EBRT model is the best fit to the data. To improve the performance of EBRT model, generalized error-loss should be reduced. Cross validation (CV) loss of the regression model depends on a number of learning cycles, maximum number of splits and learning rate. To minimize the CV loss the model is optimized by hyper parameters. Table 4 shows the optimized hyper parameters for each iteration. Regularization is used to reduce the number of ensembles with fewer trees to reduce the loss thus it improves the training model’s performance. Minimum number Mean Square Error (MSE) re-substitution required to avoid over fitting. Regularization

parameter  $\lambda$  is chosen optimally to tradeoff between the accuracy and generalization error. Figure 5 (a) shows the CV loss MSE before optimization and (b) shows the minimum objective function. The objective function is to minimize the cross validation loss. After optimization the minimum objective function is estimated at 7.81. Figure 6 shows the  $\lambda$  characteristics.

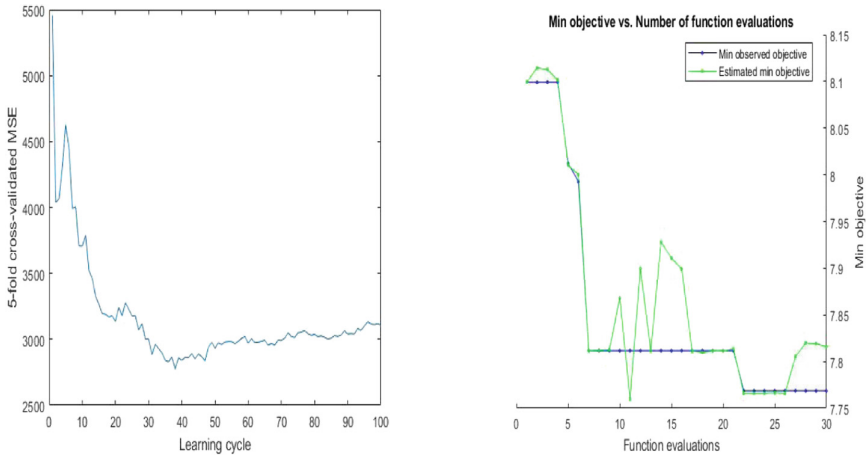


Fig. 4. (a) Cross validation loss (b) Minimum objective function

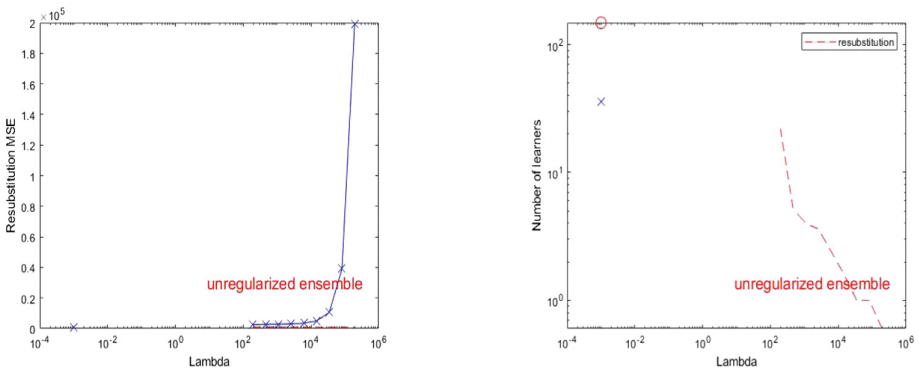
Table 3. Comparison of regression models

Regression model	Correlation coefficient	Mean absolute error	Root mean square error	Relative absolute error	Root relative squared error
Linear regression	0.8121	47.65	59.69	57.35	57.25
Isotonic regression	0.8395	44.35	55.70	53.42	53.43
Additive regression	0.6852	60.06	78.01	72.28	74.82
Multilayer perceptron	0.7392	65.39	82.35	77.24	78.35
Linear SVM	0.71	41.99	56.16	54.55	55.87
Random forest	0.7775	48.04	64.31	57.81	61.69
Bagging tree	0.8391	44.05	55.87	52.03	53.16
<b>Un regularized ensemble boosted tree</b>	<b>0.74</b>	<b>39.06</b>	<b>53.04</b>	<b>48.95</b>	<b>49.75</b>

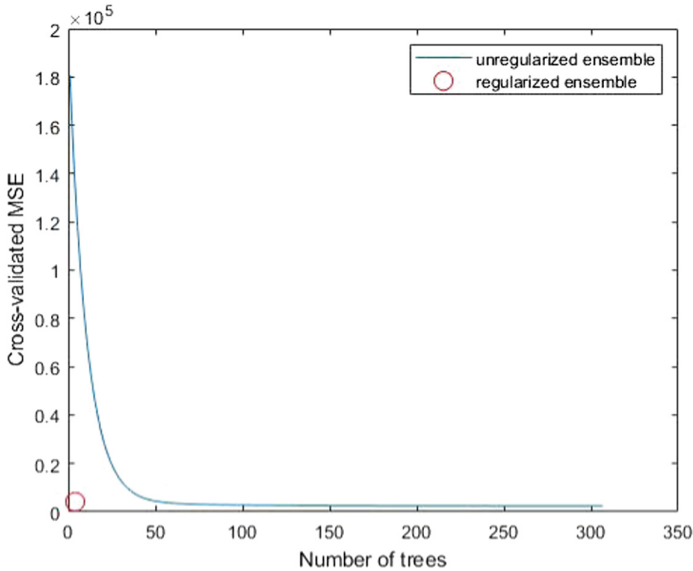


**Table 4.** Optimization results of iterations.

Iteration	Evaluation result	Objective	Objective run time	Best so for (observed)	Best so for (estim)	Number of learning cycles	Learning rate	Max num splits
1	Best	8.0992	24.183	8.0992	8.0992	383	0.51519	4
2	Accept	8.3896	3.2141	8.0992	8.1144	16	0.66503	6
3	Accept	8.2014	3.5583	8.0992	8.1128	33	0.2556	67
4	Accept	12.066	0.86643	8.0992	8.1014	13	0.0053227	5
5	Best	8.0123	0.80496	8.0123	8.0102	13	0.37677	64
6	Best	7.9927	10.571	7.9927	8.0003	319	0.39664	2
7	Best	7.8117	7.6918	7.8117	7.812	312	0.061709	1
8	Accept	8.01	1.1053	7.8117	7.8124	45	0.086639	3
9	Accept	7.9469	10.709	7.8117	7.8127	381	0.04136	13
10	Accept	7.9305	5.2953	7.8117	7.8681	211	0.055123	5
11	Accept	9.264	0.77872	7.8117	7.7601	28	0.05782	1
12	Accept	8.2958	13.01	7.8117	7.8998	499	0.12308	64
13	Accept	8.0616	3.05	7.8117	7.8116	124	0.157	5
14	Accept	8.1821	2.9651	7.8117	7.9281	116	0.093554	22
15	Accept	7.8818	11.345	7.8117	7.9108	497	0.051277	1
16	Accept	8.4626	11.163	7.8117	7.8991	475	0.99568	2
17	Accept	7.8165	11.499	7.8117	7.8111	499	0.04942	1
18	Accept	7.9442	11.695	7.8117	7.8099	498	0.0085616	1
19	Accept	7.9564	1.5085	7.8117	7.8113	62	0.18594	1
20	Accept	7.9717	6.3737	7.8117	7.8114	281	0.018679	1
21	Accept	11.218	11.52	7.8117	7.8136	496	0.0010147	3
22	Best	7.7686	11.347	7.7686	7.766	498	0.019224	1
23	Accept	7.8186	7.8292	7.7686	7.7661	339	0.037172	1
24	Accept	7.9971	3.3185	7.7686	7.766	141	0.92095	1
25	Accept	8.1601	3.8554	7.7686	7.7665	164	0.46496	1
26	Accept	8.1765	0.46726	7.7686	7.7659	10	0.26526	1
27	Accept	7.9076	11.744	7.7686	7.8054	496	0.014218	1
28	Accept	7.9266	11.496	7.7686	7.8199	498	0.026671	1
29	Accept	7.8098	1.4666	7.7686	7.8192	61	0.12043	1
30	Accept	7.8427	7.0878	7.7686	7.8158	307	0.049023	1



**Fig. 5.** Regularization parameter characteristics (a) Lambda Vs MSE (b) Lamda Vs Number of learnes



**Fig. 6.** Optimized cross validated MSE with regularization

## 5 Conclusion

Fire resistive hydraulic fluid resistivity depends on the water content in the fluid. Water evaporation changes viscosity that intern changes the fire resistivity. In this paper a novel approach for hydraulic fluid monitoring is developed by using supervised machine learning ensemble boosted regression tree model. The proposed method shows 31.68 root mean squared error under optimized hyper parameters such as number of maximum splits, number of learning cycles and learning rate. In this work, some of the missing properties of some of the fluids pose challenges. In future, the sensitivity of the method can be improved by using proper missing data handling approaches.

## References

- Bühlmann, P., Hothorn, T.: Boosting algorithms: regularization, prediction and model fitting. *Stat. Sci.* **22**(4), 477–505 (2007). <https://doi.org/10.1214/07-STS242>
- Cheng, B., Cheng, X., Chen, J.: Lightweight monitoring and control system for coal mine safety using REST style. *ISA Trans.* **54**, 229–239 (2015). <https://doi.org/10.1016/j.isatra.2014.07.004>
- Cheng, J., Yang, S.: Data mining applications in evaluating mine ventilation system. *Saf. Sci.* **50**(4), 18–22 (2012). <https://doi.org/10.1016/j.ssci.2011.08.003>
- Dwuletzki, H., Pfaender, B., Niemczyk, K.: New fire-resistant hydraulic fluids type HFA for mining use – critical analysis. In: Dyczko, A.T., Jerzy Kicki, A., Myszkowski, M., Stopa, Z. (eds.) *New Techniques and Technologies in Thin Coal Seam Exploitation*, pp 201–209. CRC Press, BOGDANKA (2010)

- Helwig, N., Schütze, A.: Data-based condition monitoring of a fluid power system with varying oil parameters. In: 10th International Fluid Power Conference (IFK2016), pp. 425–436 (2016)
- Jo, Byungwan, Muhammad, Rana, Khan, Asad: An internet of things system for underground mine air quality pollutant prediction based on Azure machine learning. *Sensors* **18**(4), 930 (2018). <https://doi.org/10.3390/s18040930>
- Kozielski, Stanisaw, Dariusz Mrozek, Pawe Kasprowski, Boena Maysiak-Mrozek, and Daniel Kostrzewa. 2015. “Regression Rule Learning for Methane Forecasting in Coal Mines.” In *Beyond Databases, Architectures and Structures: 11th International Conference, BDAS 2015 Ustro, Poland, May 26 –29, 2015 Proceedings Communications in Computer and Information Science*, 521:495–504. <https://doi.org/10.1007/978-3-319-18422-7>
- Kuenzer, Claudia, Zhang, J., Li, J., Voigt, S., Mehl, H., Wagner, W.: Detecting unknown coal fires: synergy of automated coal fire risk area delineation and improved thermal anomaly extraction. *Int. J. Remote Sens.* **28**(20), 4561–4585 (2007). <https://doi.org/10.1080/01431160701250432>
- Kurnia, J.C., Sasmito, A.P., Wong, W.Y., Mujumdar, A.S.: Prediction and innovative control strategies for oxygen and hazardous gases from diesel emission in underground mines. *Sci. Total Environ.* **481**(1), 317–334 (2014). <https://doi.org/10.1016/j.scitotenv.2014.02.058>
- Li, H., Xu, H., Wang, J., Fu, X., Bai, Z.: Design of automatic control system of coal sampling robot hydraulic system oil temperature. In: *Proceedings - 9th International Conference on Intelligent Human-Machine Systems and Cybernetics, IHMSC 2017*, vol. 1, pp. 38–42 (2017). <https://doi.org/10.1109/IHMSC.2017.16>
- Mahdevari, S., Shahriar, K., Esfahanipour, A.: Human health and safety risks management in underground coal mines using fuzzy TOPSIS. *Sci. Total Environ.* **488-489**(1), 85–99 (2014). <https://doi.org/10.1016/j.scitotenv.2014.04.076>
- Mark, C., Gauna, M.: Evaluating the risk of coal bursts in underground coal mines. *Int. J. Min. Sci. Technol.* **26**(1), 47–52 (2016). <https://doi.org/10.1016/j.ijmst.2015.11.009>
- Mellors, Robert, Yang, X., White, J.A., Ramirez, A., Wagoner, J., Camp, D.W.: Advanced geophysical underground coal gasification monitoring. *Mitig. Adapt. Strat. Glob. Change* **21**(4), 487–500 (2016). <https://doi.org/10.1007/s11027-014-9584-1>
- Mishra, R.K., Bahuguna, P.P., Singh, V.K.: Detection of coal mine fire in Jharia coal field using Landsat-7 ETM+ data. *Int. J. Coal Geol.* **86**(1), 73–78 (2011). <https://doi.org/10.1016/j.coal.2010.12.010>
- Natekin, A., Knoll, A.: Gradient boosting machines, a tutorial. *Front. Neurobot.* **7**, 21 (2013). <https://doi.org/10.3389/fnbot.2013.00021>
- Peter, Hodges: *Hydraulic Fluids*, 1st edn. Wiley, New York (2004)
- Prevention of Fires in Underground Mines — Guideline: Resources Safety. Western Australia (2013). <https://doi.org/ISBN9781921163169>
- SAFETY AT A Glance (2017). [https://www.coalindia.in/DesktopModules/DocumentList/documents/Safety\\_at\\_a\\_Glance\\_03042018.pdf](https://www.coalindia.in/DesktopModules/DocumentList/documents/Safety_at_a_Glance_03042018.pdf)
- Sanmiquel, Lluís, Rossell, Josep M., Vintró, Carla: Study of Spanish mining accidents using data mining techniques. *Saf. Sci.* **75**, 49–55 (2015). <https://doi.org/10.1016/j.ssci.2015.01.016>
- Shen, Z., Dong, H., Yao, N., Li, X.: *Condition Monitoring and Fault Diagnosis System of Fully Hydraulic Drilling in Coal Mine* (2016)
- Suh, J., Kim, S.M., Yi, H., Choi, Y.: An overview of GIS-based modeling and assessment of mining-induced hazards: soil, water, and forest. *Int. J. Environ. Res. Public Health* **14**(12), 1463 (2017). <https://doi.org/10.3390/ijerph14121463>
- Givens, W.A., Michael, P.W.: *Hydraulic fluids*. In: Totten, G.E., Westbrook, S.R., Shah, R. J. (eds.) *Fuels and Lubricants Handbook: Technology, Properties, Performance, and Testing* 225. ASTM International (2003). <https://doi.org/10.1520/MNL37WCD-EB>

Zhu, Q., Yu, F., Cai, M., Liu, J., Wang, H.: Interpretation of the extent of hydraulic fracturing for rockburst prevention using microseismic monitoring data. *J. Nat. Gas Sci. Eng.* **38**, 107–119 (2017). <https://doi.org/10.1016/j.jngse.2016.12.034>



# Performance Analysis of Image Compression Using LPWCF

V. P. Kulalvaimozhi<sup>1</sup>(✉), M. Germanus Alex<sup>2</sup>, and S. John Peter<sup>3</sup>

<sup>1</sup> Manonmaniam Sundaranar University, Tirunelveli, India  
vpkulal@yahoo.com

<sup>2</sup> Department of Computer Science, Government Arts College, Nagercoil, India  
mgalxus@yahoo.com

<sup>3</sup> Department of Computer Science, ST. Xavier's College, Palayamkottai, India  
jaypeeyes@rediffmail.com

**Abstract.** Image compression is the most important feature for achieving an efficient and secure data transfer. One of the main challenges in compression is developing an effective decompression. The input images that is compressed may not be more effectively restored in the decompression process that is based on quantization using Cosine Transformations or Wavelet transformations where the pixel information will be lost. To overcome these challenges, encoding process were employed. In the encoding process the pixel information were well protected but the compression efficiency is not improved. In order to overcome this challenge Lossless Patch Wise Code Formation (LPWCF) is employed. In the patch wise code generation the compression process is based on the pixel grouping and removing the relevant and recurrent pixels. In the proposed method, the images were first reduced in size by combining the current pixel with the previous pixel. The resulting image size is nearly the half of the size of the input image. The resulting image is then divided into small patches. In the patch recurrent pixels and their locations were identified. The identified pixel locations were placed prior to the pixel value and then the process is repeated for the complete image. The result of each patch acts as a code. In the receiver side the same process is reversed in order to obtain a decompressed image. The process is completely reversible and hence the process can be employed in the process of transmission of the images. The performance of the process is measured in terms of the compression ratio, the image quality analysis of the input and the decompressed image based on PSNR, MSE and SSIM.

**Keywords:** Compression · Pixel grouping · Recurrent pixels · Bits per pixel per band (bpppb) · Decompression

## 1 Introduction

A huge amount of memory storage space is created to store and transmit the image raw data in various applications [1]. Compression of hyperspectral images (HSI) is the most important research area for performing the efficient data transfer to analyze the land areas available in the earth. In the compression process, mainly two types of techniques are progressed such as lossy and lossless compression. For lossy process, the redundant data are eliminated, as a result some image information are damaged. In contrast,

lossless compression achieves greater compression ratios than lossy compression without the loss of required information. The redundancy of image data are then represented in terms of spatial, spectral, or temporal redundancy. The main challenge faced in the compression phase is the effective reconstruction of image data onto the minimum loss of pixels. The discussion of various image compression algorithms along with their merits and demerits that are utilized to reduce the image size which then reduces the image quality [2].

They are fractal image compression, discrete cosine transform, coding of wavelet coefficients, lossless compression algorithms, fuzzy compression, hyperspectral compression algorithm, data re-ordering technique, color image compression, and the Hadamard based image decomposition and compression algorithms. The lossy hyperspectral image [3] compression techniques are effectively analyzed in this research area.

The major requirements of HSI compression are to reduce the on-board size, download time, and the communication channels capacity. The main intention of this work is to reduce the transmission overhead and also to evaluate the number of compression algorithms used for processing the onsite HSI data [4].

The comparison of Wavelet based compression techniques of HS image information are as follows: binary embedded zerotree wavelets (BEZW), 3D-Set Partitioning In Hierarchical Trees (SPIHT), and the 3D-Set Partitioning Embedded bloCK (SPECK) [5]. This shows an effective lossless compression technique of hyperspectral image. Hence, the input images that are compressed by using a compression technique have been produced less amount of efficiency. Although using transformations the pixel information was lost. To overcome these issues encoding process is employed. The Lapped Transform and Tucker Decomposition (LT-TD) [6] is used to compress the HSI. In this research, the lapped transform is utilized to decorrelate each band of a HSI. To rearrange the three-dimensional (3D) wavelet sub-band configurations from the diverse frequencies of transformed coefficients and which it is named out as third-order tensors. Finally, the core tensor is formed due to the sub-band disintegration rule and 3-factor matrices by Tucker decomposition. Then, most of the original tensor energy is preserved from the core tensor, and using the bit-plane coding algorithm which encoded the tensor code into the bit-streams. In the encoding process, the pixel information was well preserved but the compression efficiency is not improved. This paper proposes the lossless patch wise code formation (LPWCF) scheme to overcome the issues in the compressing technique.

The following points shows the objectives of the proposed technique illustrate as:

- Pixel grouping → it is employed for removing the recurrent and relevant pixels in the input image based on the compression process.
- LPWCF → it is used to generate the compressed code which reduces the image size to nearly half of their original size.
- proposed method → it is capable of reducing the image size to a greater extent, thus reducing the transmission time and improve the security of the original image.
- decompressed image → it is obtained by using the reversible process.

## 2 Related Works

Recently, significant efforts have been directed towards the hyperspectral image compression algorithms. Therefore, the evolution of the opinions, interests, and comments on the hyperspectral image compression were discussed. Sujithra et al. [7] presented the Walsh Hadamard Transform (WHT) and the Discrete Wavelet Transform (DWT), which is utilized to compress the hyperspectral images based on the spectral and spatial information available in the images. They applied DWT, to split the HSIs into the subband imageries. After that, each transformed block DC value were splitted and low-frequency sub-band of each block was utilized based on the WHT technique. The main purpose of this transformation is to achieve high bit per pixel per band and compression ratio. Cheng and Dill [8] discovered the new dual-tree Binary Embedded Zerotree Wavelet (BEZW) algorithm for compressing the HSI based on the lossless to lossy schemes. They achieved 3-D integer reversible hybrid transforms and decorrelate spectral and spatial data from acclimatizing the Karhunen- Loeve transform and DWT. Then, optimized the discovered performance results due to an asymmetrical dual-tree structure. The large number of spectral bands occupied for image transmission also high. Huber-Lerner, et al. [9] suggested the Principle Component Analysis that surveyed the Discrete Cosine Transform (PCA-DCT) compression technique for reducing hyperspectral images size. It was considered only lossy compression technique on the spectral axis and it represent as a simple and implementation for the fast processing method.

They introduced the widely held Reed-Xiaoli (RX) algorithm and the enhanced quasi-local RX ( $RX_{QLC}$ ) was utilized for detecting the target based method. In this scenario, transmission time and storage space was also high. Du et al. [10] introduced the JPEG2000 with PCA for spectral decorrelation. They retained the PCs and compressed the majority of information about the dataset. Furthermore, the PCA +JPEG2000 has been preserved the valuable HSIs information on avoiding the presence of anomalies, unmixing, and the classification. The compression efficiency was not in an effective range. Amrani, et al. [11] endorsed the lossless principal polynomial analysis (PPA) for evading the issues such as side information, energy compaction property, and the integer mapping. They developed two generalization techniques of PPA was Backwards PPA and the Double-Sided PPA. The redundant and complexity were the major issues in this endorsed model. Narmadha, et al. [12] utilized the DWT with CANDECOM/PARAFAC (DWT-CP)) for compressing the hyperspectral image. Initial process of compression process was performed in each spectral band by utilizing the (9/7) bi-orthogonal wavelet based on the 2DWT technique. Therefore, reached high compression ratio due to the CP in the 4-wavelet sub-band HSIs. Finally, the elements of the core tensors were coded by exploiting the Adaptive Arithmetic Coding (AAC) algorithm. The redundant information was the major issues in the utilized model. Wu et al. [13] recommended the high-order lossless compressing technique for HSIs based on the clustered Differential Pulse Code Modulation with Removal of Local Spectral Outliers (C-DPCM-RLSO) methods. The special effects of spectral outliers were removed mainly by a multiple linear regression twice processes. In this research work, clustered all the spectral lines and employed linear regression for evaluating the prediction coefficients. For each band of each class, the values were predicted and

sorted the difference between predicted values and actual values. Then, identified and removed the spectral outliers and the resulting spectral lines were utilized to take away the regression for estimating the predicted values and the ending prediction coefficients. Lastly, the entropy coded were performed in between the original and the predicted image residuals.

The major drawbacks of the recommended method were slower and lower average bit-rate. Nahavandi et al. [14] introduced new adaptive compression method like Extended New Lossless Compression Method (ENLCM) for hyperspectral data. This technique was comprised of three different approaches:

Based on the histogram evaluation, separated the corrupted bands of the other bands.

Utilized Binary Hybrid Genetic Algorithm with Particle Swarm Optimization (BHGPSO) to optimize the uncorrupted bands and finding the group of bands of minimum correlation between each other.

Finally, the suggested visually lossless compression method utilized to code the remaining bands.

In conclusion, the compressed bit-stream was created based on the above mentioned three compression steps due to the addition the three compression process results and this process was utilized to storage or transmission sections.

Zhang et al. [15] presented a multi-dimensional or tensor data processing approach for compressing and reconstructing the hyperspectral image (HSI). They received core tensor which multiplied by a matrix factor beside an individual mode from the decompression of original tensor information based on the developed tensor decomposition technology, and it was represented from the observed hyperspectral image. After compressing the HSI to the core tensor, the multi-linear projection through the factor matrices utilized to reconstruct the data. Shahriyar et al. [16] aimed to compress the hyperspectral image without loss of image information. This paper invented the binary tree of lossless predictive HS coding scheme was employed to assemble the integer residual bitmap from the residual frame. After creating the large homogeneous blocks of adaptive size from utilizing the high spatial correlation in HS residual frame and also utilized the context-based arithmetic coding method to create a code that was represented as a unit. Amrani et al. [17] employed the regression wavelet analysis (RWA) for lossless coding of remote-sensing data. They utilized the multivariate regression with the wavelet-transformed components relationships. This analysis suggested three regression models evade the issues was accuracy, component scalability and computational complexity. But the estimation accuracy was the major drawbacks in this recommended analysis.

Zhang et al. [18] focused on the hyperspectral un-mixing compressive sensing model (HUCSM) problems. They have developed three main aspects in this research for solving the issues in the reconstruction process and identifying the end members from an HS image:

Created novel constraints for representing the spatial local similarity and spectral sparsity of the profusion matrix.

Locally similar sparsity-based hyperspectral un-mixing compressive sensing (LSSHUCS) method to improve the reconstruction accuracy.

Lagrangian algorithm to solve the problem of HUCSM.



But, the un-mixing model cannot reveal that reconstruction accuracy accurately. Fu et al. [19] suggested the spectral–spatial adaptive, sparse representation (SSASR) to efficiently compress the hyperspectral image (HSI). Primarily, constructed the super pixel and then designed the spectral signatures for each super pixel. Lastly, Huffman coding was performed to achieve the bit stream without considered the contextual arrangement in the sparse quantities from the sparse coefficients. Therefore, the major consideration implemented on the contextual arrangement of the sparse quantities. Shen et al. [20] utilized the new lossless compression algorithm on arbitrarily shaped the region of interests (ROIs) in the hyperspectral images. First of all, decorrelate the hyperspectral image spatially and spectrally by a two-stage prediction method. Secondly, the prediction residuals were encoded based on the Golomb Rice (GR) coding method. After that, several grouping of full context pixels and boundary pixels with the connected residuals were represented from the mixture geometric model. The data overload was the major problem that limits the accuracy of the image. The loss of image pixels, large memory storage space, and the transmission time were considered as the major drawbacks to achieving the better performance in the proposing technique.

### 3 Implementation of LPWCF

LPWCF implementation is mainly for reducing the memory storage space and improving the security of the original image data. Figure 1 represents the proposed HSI compression and decompression process flow diagram.

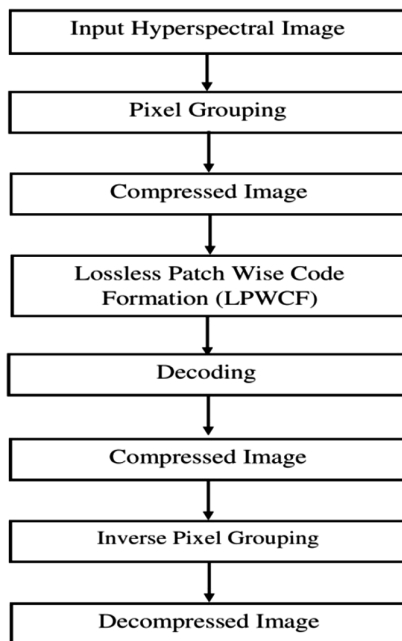


Fig. 1. Workflow of the proposed system.

The major processes in proposed work to reduce the transmission time consumption without reducing the quality of the image are listed as follows:

- Pixel Grouping
- Code Generation
- Image Decompression

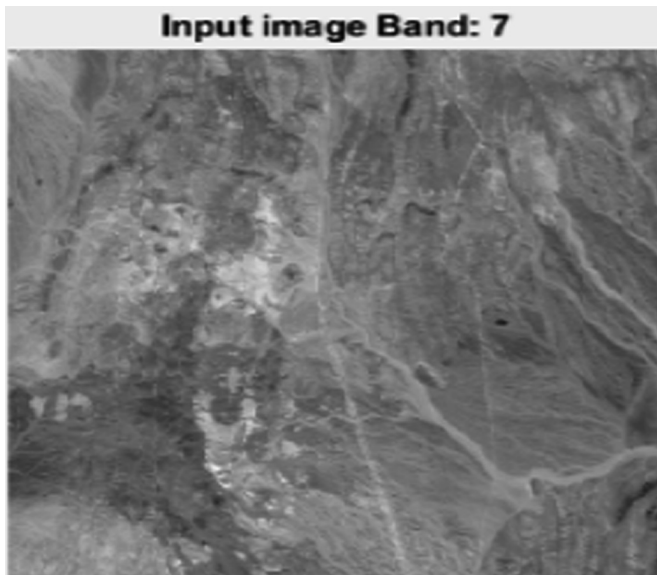
The detailed description of each process in the proposed work is presented in next sub-sections. Table 1 present the variables used in the proposed algorithm.

**Table 1.** Symbols and Descriptions

List of variables	Description
R, C	Corresponding row and the column of the image pixel
Z	Compressed code
MSB	Most Significant Bit
LSB	Least Significant Bit
i, j	Length and size of the patch
$P_k$	Compressed image patches
$V_{pk}$	Unique patches

### ***Hyperspectral Image.***

In conventional color image, the light spectrum is split into three broad overlapping image slices such as Red, Green, and Blue bands. While a hyperspectral image splits the spectrum into numerous tinny image slices. The HSI consists of hundreds of spectrum bands and that bands mainly depends the hyperspectral camera. Figure 2 represents the input hyperspectral Image.



**Fig. 2.** Hyperspectral Input Image

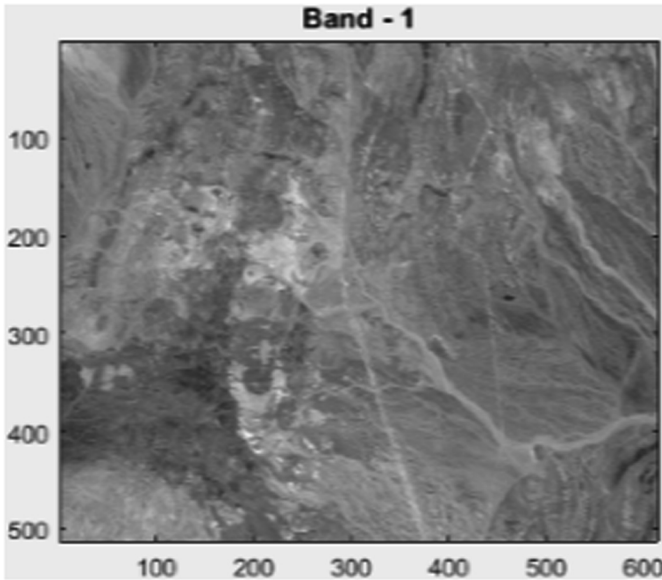
**Pixel Grouping.**

The current and previous band of all using the causal pixels which represent the current pixel row and column of the image. If a current pixel value is equal to the neighboring value then assign neighboring pixel value. Otherwise, assign the previous pixel value to the current pixel. The group of pixel vectors represent  $n$  and consider the hyperspectral input image as,

$$X = \{x_i \in R^B\} \quad (1)$$

Here  $j = 1, 2, 3, \dots, n$  and  $B$  represent the number of spectral bands. The spatial location (coordinates) and vector of spectral values are characterized in each pixel of the HSI. The main objective of the pixel grouping is the significant reduction of the redundant information and improve the compressed image quality. The two main steps involved in the pixel grouping as (Fig. 3),

- Removing the relevant and recurrent pixels
- Grouping the pixel



**Fig. 3.** Pixel Grouping Image

**Code Generation**

After applying, Lossless patch Wise Code Formation (LPWCF) method to derive the code for the compressed image. The major advantage of using this proposed method illustrates as,

- Preserved the pixel information
- Reduced the image size
- Low transmission time
- Improved security of the original image
- Low computational complexity with high compression efficiency

The LPWCF code generation scheme is performed based on the compressed image as the required source of the system. Initially, reduced the image size by combining the previous pixel value with current pixel value. Then the compressed image is divided into number of small patches and identifies the frequent pixel value and their corresponding positions in an image. The identified pixel locations are located in the current pixel value, and the progression is repetitive for the complete image. The outcome of each patch acts by means of the code is the required code.

The proposed algorithm to generate the compressed code is listed as follows:

---

Lossless patch wise code formation algorithm

---

Input; Raw Hyperspectral Image

Output; Compressed Code

---

Step-1:

[R C] = Image;

Step-2:

Initialize Code Z=1

Step-2:

for i=1 to R

Step-3:

LSB ( $C_p$ ) =  $N_p$ ;

end for loop

//  $C_p$  → Current Pixel;

$N_p$  → Neighbouring Pixel

Step-4:

*Compressed\_image* = LSB ( $C_p$ );

// LSB → Least Significant Bit

Step-5:

$P_k$  = Patches (*Compressed\_image*);

// k → 1,2,3,..., Total number of Patches

Step-6:

$V_{P_k}$  = *unique* ( $P_k$ );

Step-7:

for i=1 to length ( $V_{P_k}$ )

Step-8:

for j= 1 to size ( $P_k$ )

Step-9:

if  $V_{P_k}(i) == P_k(j)$

Step-10:

Count = Count + 1; end if

Step-11:

if Count > 1

Step-12:

Z = Z + 1;

end if;

end for loops

---

***Image Decompression.***

Image decompression is the reverse process of compression technique. It decompresses the compressed image into the large volume of hyperspectral image. In order to achieve the high quality of the hyperspectral image. The image decompression is performed under the following process are,

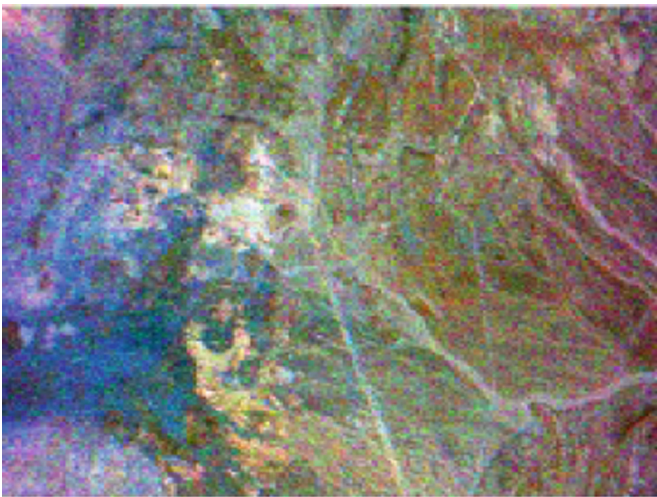
Decoding

Inverse Pixel Grouping

The decoding is the reverse process of encoding technique. To break the compressed image code and identify the repeated pixels in the hyperspectral image. Then, identify the recurrent pixel locations and generate the patches. Applying lossless decompressing technique to decompress the image which is nearly half of the original size of the image. Again, perform the pixel grouping in an inverse mode to recover the original image. The image pixel which is split into MSB and LSB value. The MSB pixel value placed in the current row while LSB value placed in the next row. Then, go for next pixel image further continue the process until complete all the pixel in the compressed hyperspectral image. Finally, recover the decompressed image.

Thus, the overall algorithm for decompression is the reversible process to that of LPWCF method. Therefore, the proposed LPWCF method is capable of reducing the image size to a greater extent and thus leads to reduce the transmission time.

Finally, reconstruct the original hyperspectral image with minimized size. Figure 4 shows the reconstructed HIS image.



**Fig. 4.** Reconstructed HS image

## 4 Performance Analysis

### *Dataset.*

The Airborne Visible/Infrared Imaging Spectrometer (AVIRIS) was developed in 1997 for collecting the hyperspectral images that are used for various research process. The four main datasets are taken such as Jasper Ridge, Moffett Field, Lunar Lake, and the Cuprite. This AVIRIS database was discovered in 1987 by the NASA Jet Propulsion Laboratory.

### *Lossless results (Bits per Pixel per Band).*

The lossless results of predictive coding methods, compressing the whole hyperspectral images is illustrates in Table 2. The proposed LPWCF methods is compared with the existing methods such as C-DPCM, LUT, JPEG-LS, LAIS-LUT, M-CALIC, 3D-BEZW.

**Table 2.** Lossless results

Coding method	Jasper	Lunar	Cuprite	Moffett
JPEG-LS	8.38	7.48	7.66	8.04
C-DPCM-20	4.62	4.75	4.68	4.62
M-CALIC	5	4.91	4.89	4.92
LUT	4.95	4.71	4.66	5.05
LAIS-LUT	4.68	4.53	4.47	4.76
3D-BEZW	4.75	4.62	4.52	4.51
LPWCF	–	4.9	1.0331	4.9554

Among the predicting coding methods, the proposed LPWCF method acheives greater performance over other methods.

### *PSNR.*

The proportion of the maximum power value in the signal to the total amount of power required for processing of noise signals is defined as the peak signal-to-noise ratio (PSNR). Dynamic range values have occurred in the signals. The higher reconstruction quality of the image depends on the larger PSNR value. Hence PSNR value is expressed in the logarithmic scale of decibels (dB). Therefore PSNR value is expressed in the mean - squared error (MSE) that have the maximum possible pixel value of HSI dimensions. For hyperspectral image, the PSNR of the reconstructed result as,

$$PSNR = 20 \log_{10} \frac{255^2}{MSE} \quad (2)$$

and

$$MSE = \frac{1}{pq} \sum_{i=1}^p \sum_{j=1}^q [c(i,j) - \hat{c}(i,j)]^2 \quad (3)$$

Where,  $c(i, j)$  represents the components of the HSI and  $\hat{c}(i, j)$  represents the reconstructed image components.

The proposed PSNR value is compared with the traditional methods such as Stagewise Orthogonal Matching Pursuit (StOMP), Least Angle regression (LASSO), HYperspectral Coded Aperture (HYCA), hyperspectral Unmixing Compressive Sensing (UCS), and the Locally Similar Sparsity based Hyperspectral Unmixing Compressive Sensing (LSSHUCS), LSSHUCS\_nts1 [18].

From the figure, shows that the proposed LPWCF method compared with the traditional methods of urban dataset under. Hence, the proposed LPWCF method achieve higher PSNRs.

### SNR.

The SNRs is defined as the logarithmic proportion of the original image to the difference between the original image and the reconstructed images. This calculation is mainly used to estimate the hyperspectral image distortion ratio. The mathematical form of SNR is illustrated as,

$$SNR = 10 \log_{10} \frac{\|R\|_F^2}{\|R - \hat{R}\|_F^2} \quad (4)$$

Where  $\hat{R}$  represents the reconstructed hyperspectral data. The ranges are derived from 0.1db and enumerate the rates by a bppb.

## 5 Conclusion

Forecasting the relevant compression technique to compress the hyperspectral image without any loss of pixel information is the critical task in the proposed work. In this paper, the LPWCF scheme is proposed to generate the code for transmitting a large amount of image data. The pixel grouping method is employed to remove the noise and also reduce the recurrent and relevant image data. Then, generate the compressed code for transmitting the image data. After, applying the decoding process to which retrieve the compressed image. Finally, inverse pixel grouping process is performed to recover the original image without any loss of pixel in the image. The comparative analysis between the proposed LPWCF with the existing techniques is performed for analyzing the LPWCF performance. Hence, the proposed LPWCF method achieves greater results than the existing in terms of PSNR, SNR, and the lossless compression results.

## References

1. Saxena, L., Armstrong, L.: A survey of image processing techniques for agriculture (2014)
2. Rehman, M., Sharif, M., Raza, M.: Image compression: A survey. Res. J. Appl. Sci. Eng. Technol. **7**, 656–672 (2014)
3. Ramesh, S., Bharat, P., Anand, J., Selvan, J.A.: Analysis of lossy hyperspectral image compression techniques. Int. J. Comput. Sci. Mob. Comput. **3**, 302–307 (2014)

4. Babu, K.S., Ramachandran, V., Thyagarajan, K., Santhosh, G.: Hyperspectral image compression algorithms—a review. In: *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*. Springer, pp. 127–138 (2015)
5. Puri, A., Sharifahmadian, E., Latifi, S.: A comparison of hyperspectral image compression methods. *Int. J. Comput. Electr. Eng.* **6**, 493 (2014)
6. Wang, L., Bai, J., Wu, J., Jeon, G.: Hyperspectral image compression based on Lapped transform and Tucker decomposition. *Sig. Process. Image Commun.* **36**, 63–69 (2015)
7. Sujithra, D., Manickam, T., Sudheer, D.: Compression of hyperspectral image using discrete wavelet transform and Walsh Hadamard transform. *Int. J. Adv. Res. Electron. Commun. Eng. (IJARECE)* **2**, 314–319 (2013)
8. Cheng, K.-J., Dill, J.: Lossless to lossy dual-tree BEZW compression for hyperspectral images. *IEEE Trans. Geosci. Remote Sens.* **52**, 5765–5770 (2014)
9. Huber-Lerner, M., Hadar, O., Rotman, S.R., Huber-Shalem, R.: Compression of hyperspectral images containing a subpixel target. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **7**, 2246–2255 (2014)
10. Du, Q., Ly, N., Fowler, J.E.: An operational approach to PCA+JPEG2000 compression of hyperspectral imagery. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **7**, 2237–2245 (2014)
11. Amrani, N., Laparra, V., Camps-Valls, G., Serra-Sagrìstà, J., Malo, J.: Lossless coding of hyperspectral images with principal polynomial analysis. In: *2014 IEEE International Conference on Image Processing (ICIP)*, pp. 4023–4026 (2014)
12. Narmadha, D., Gayathri, K., Thilagavathi, K., Basha, N.: An optimal HSI image compression using DWT and CP. *Int. J. Electr. Comput. Eng.* **4**, 411 (2014)
13. Wu, J., Kong, W., Mielikainen, J., Huang, B.: Lossless compression of hyperspectral imagery via clustered differential pulse code modulation with removal of local spectral outliers. *IEEE Sig. Process. Lett.* **22**, 2194–2198 (2015)
14. Nahavandi, S.K., Ghamisi, P., Kumar, L., Couceiro, M.: A novel adaptive compression technique for dealing with corrupt bands and high levels of band correlations in hyperspectral images based on binary hybrid GA-PSO for big data compression. *Int. J. Comput. Appl.* **109**, 18–25 (2015)
15. Zhang, L., Zhang, L., Tao, D., Huang, X., Du, B.: Compression of hyperspectral remote sensing images by tensor approach. *Neurocomputing* **147**, 358–363 (2015)
16. Shahriyar, S., Paul, M., Murshed, M., Ali, M.: Lossless hyperspectral image compression using binary tree based decomposition. In: *2016 International Conference on Digital Image Computing: Techniques and Applications (DICTA)*, pp. 1–8 (2016)
17. Amrani, N., Serra-Sagrìstà, J., Laparra, V., Marcellin, M.W., Malo, J.: Regression wavelet analysis for lossless coding of remote-sensing data. *IEEE Trans. Geosci. Remote Sens.* **54**, 5616–5627 (2016)
18. Zhang, L., Wei, W., Zhang, Y., Yan, H., Li, F., Tian, C.: Locally similar sparsity-based hyperspectral compressive sensing using unmixing. *IEEE Trans. Comput. Imaging* **2**, 86–100 (2016)
19. Fu, W., Li, S., Fang, L., Benediktsson, J.A.: Adaptive spectral-spatial compression of hyperspectral image with sparse representation. *IEEE Trans. Geosci. Remote Sens.* **55**, 671–682 (2017)
20. Shen, H., Pan, W.D., Wu, D.: Predictive lossless compression of regions of interest in hyperspectral images with no-data regions. *IEEE Trans. Geosci. Remote Sens.* **55**, 173–182 (2017)





# Facial Analysis Using Deep Learning

Priyanka More<sup>(✉)</sup>, Poonam Desale<sup>(✉)</sup>, Mayuri S. Gothwal<sup>(✉)</sup>,  
Pradnya S. Sahajrao<sup>(✉)</sup>, and Aarzoo A. Shaikh<sup>(✉)</sup>

Genba Sopanrao Moze COE, Pune, India

morepriyankad@gmail.com, poonam.195@gmail.com,  
mayurigothwal@gmail.com, ranisahajrao@gmail.com,  
sarzo0860@gmail.com

**Abstract.** A face search system which merges a live search strategy along with a state-of-the-art commercial-off the shelf (COTS) matcher, one cascaded framework. In this first sort massive album of photos, to figure out the top-k most alike faces. The k retrieved prospect is re-ranked by emerging equalities depending on deep features and those results by the COTS matcher. The software based technique is complex and large. It analysis unique shape, pattern and positioning to the respective facial features. It estimates with the records consists of images present in central or local database, the deep network representation combines with a state-of-the-art as well as COTS face matcher in large-scale face search system. According to study on the face datasets leads to complexity: LFW dataset (consist of face detectable). In this project Viola-Jones face detector algorithm is used. The Viola-Jones Technique use to perform feature extraction and evaluation the Rectangular features measures with a new image representation their calculation is very fast.

## 1 Introduction

In this generation, many faces, images get captured, saved and posted over the internet. Interesting challenge in this is quick image retrieval, which intends to search various face images of interest from large database collection of face images of interest from bunch of images present in the large database. Face recognition methods, a structure matching is studied and then rank faces in the dataset (gallery) as per the query generation it. The scope of model based schema is scalability at social media as the recognize model need to measures the query images with the face image present in large dataset like social media. As providing a face image as a query. The aim is to retrieve images having faces of that particular person is visible in the query image, from a online image database just like social media presenting tens of millions of face images. Many applications of face search system consist of face image search on name-based, tagging of image and videos based on face, etc. Previously the state of art image retrieval system used whereas bag-of-visual-words representation use to decrease the performance applied on face. We propose a face search system which ensures a fast search procedure, and also retrieve the information about the query face using deep learning algorithms.

## 2 Motivation

In this paper we propose system which detects face image of target person during the test phase. The challenge addressed here is to resolve ambiguity in person identification and recognition once the face gets detected. In order to learn a classifier from public dataset, we need to address issues such as lighting conditions, pose, and alignments inclinations in the face image. One can address them using the face detector (Viola jones algorithm). Hence retrieving a video of similar faces for face recognition.

## 3 Literature Survey

### 3.1 Scalable Face Image Retrieval with Identity-Based Quantization and Multi-reference Re-ranking

**Abstract:** By giving a face image as an input query, our objective is to achieve the retrieval of images presenting faces of the person occurs in the query as an input image, from an image database that is social network including tens millions of images. Common face retrieval system has many applications, includes face image search using name, tag in images and videos, etc. In the state of art image retrieval system which was previously used where bag-of-visual words representation was use to decrease the performance when applying on face images. Now-a-days scalable face representation uses local and global features to develop a scalable face image retrieval system

1. The local features based on component are not only concealing geometric limit and also more effective within different poses and variations.
2. A typical quantization scheme based on identity is to judge local features into distinct visual words is occurred, permitting to index face images for scalability.

### 3.2 Scalable Face Image Retrieval Using Attribute-Enhanced Sparse Code-Words

Users are mainly interested in photos with people (family, friends, celebrities). Thus with the increasing of images a content based image retrieval (CBIR) is used for many applications. Here content refers to colours, shapes, textures, tags/descriptions associated with the image. Suppose we query a face image given CBIR tries to find image from a large database. Its applications are

1. Automatic Face Annotation
2. Crime investigation.

The facial attributes help in differentiating the face into male/female. In the conventional methods we used low level features which absence of semantic meanings (only the eyes/nose). But face image also contains (face expression, posing) so results

were not satisfactory. With integrating high level attributes (hairstyle, gender) in feature representation better decisions are made for image retrieval. To handle this, use of two methods are as follows:

1. Identity-Based Quantization
2. Identity contained Sparse Coding.

## 4 Face Retrieval: Pre-filtering the Gallery via Deep Neural Network

In the modern era of computers and internet many operation are performed like capturing, storing and sharing of images over the internet. One of interesting and challenging application of computer vision is retrieval of faces automatically, is intended to search many or particular face images in which we are interested from the large dataset. Technique of face identification, a copy of facial identity is studied and then faces are get ranked in the database (i.e. gallery) with respect to the query. One disadvantage of schemas based on model is scalability in large galleries to the identify the model. By comparing the query images with all face image in database (i.e. gallery). In this paper, we introduce method which filters the database (i.e. gallery). The learning of facial feature is the solution to the problem of scalability. Face image entitled the feature vectors which get indexed, searching and ranking in the feature space. Additionally mention the face retrieval system that is combination of both COTS matcher and k-NN search. First phase, deep learning is used based on facial representation to pre-filter gallery set and search top k-most related faces to input query face image. Rank the top k-most related face by joining the equalities from deep facial features gives the output. Last stages; use a manifold ranking algorithm to fully face images:

- Cascade schemas for large scale face retrieval problem, consider performance and scalability.
- Retrieval result compared either unconstraint i.e. web download images. And constraint large scale facial images database.

## 5 Face Recognition Vendor Test

Urbanization means more than half of all people in Asia will be living cities. The global scale changes and increasing demand for solution will be enable to live safe. Our goal is to use our cutting edge technology to help and create countries and cities. Where people can live in peace with identifying the each person. Everyday action are increasing and handle electronically, despite of pencil, paper or face to face. The increase in electronic activity results very large demand offering robust and appropriate user identification and verification. Facial age evaluation is a part of research to the Face Recognition test. The facial recognition algorithm that we entered in the 2013 test was only one to achieve the accuracy of 99.9%. It is 1:1 verification using headshot.

Comparing them with the photo in their different ages. Example: How u look in age of 20’s and 30’s and 40’s. The software is able to correctly identifying them as all the same person. This also guesses our age by recognizing of photo. The comparison are categorized in two types:

1. Verification: The given individual gets compared with whom they say and gives Yes or No.
2. Identification: The comparison is between the given individual with the other individual in the database and a ranked list matches.

## 6 System Architecture

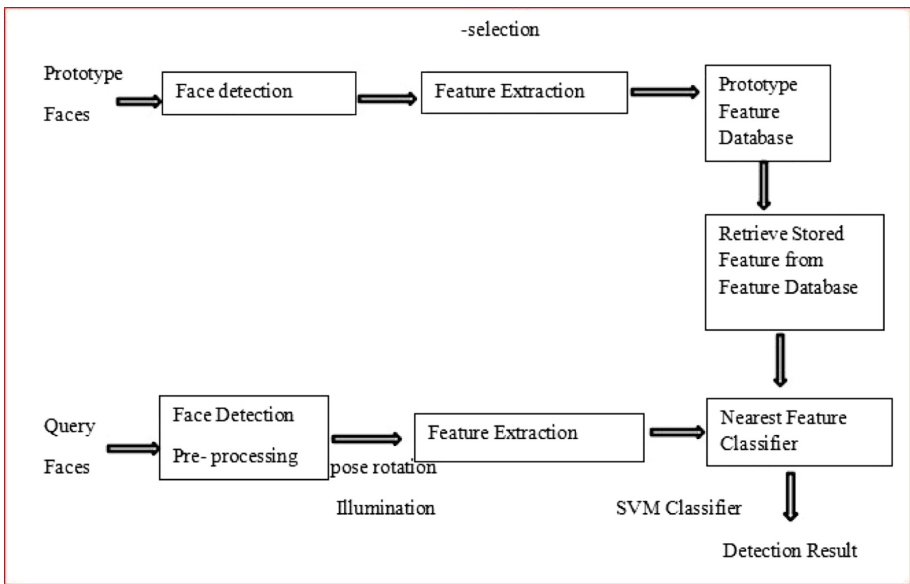


Figure: Working of System Architecture

**Algorithm Used:** Viola Jones face detection algorithm, A “paradigmatic” method for real-time face detection. Training is slow, but detection is very fast.

The algorithm has four stages:

1. Haar Feature Selection.
2. Creating an Integral Image.
3. Ad boost Training.
4. Cascading Classifiers.

## 1. Haar Feature Selection

**Edge detection:** Edge detection includes convolution kernels which are rectangular boxes containing low values and high values can also be denoted as lighter and darker regions of boxes respectively. Suppose we create a kernel that is similar to what is to be extracted from the face image, it looks like horizontal line. So kernel is applied all over the test image. The output of it is what will be extracted from the image, the high value areas where that pattern matches the image. Haar features are similar these convolutional kernels. They are of different types, the way we apply them on our test image. We apply these kernels to our image, few properties common to human face are: say to detect the eyes, so the eyes region will show higher value than the nose. The gap bridge of the nose will be lighter than eyes. The cheeks area fairer than the nose. Accordingly kernels are adjusted and classifiers are learnt. Composition of properties forming match able facial features:

Location and size: eyes, mouth, bridge of nose. Value: oriented gradients of pixel intensities. Value of feature =  $\sum$  (pixels in white area) -  $\sum$  (pixels in black area) each feature results in single value calculated. All we understand is they have resemblance to characteristics of face. Considering all features, we end up calculating 60,000+features, so we have to evaluate huge set of features. This is difficult for real time face detection. Basic idea is to eliminate the redundant features. This is done by ADABOOST.

## 2. Creating an Integral Image

In an integral image the value at pixel(x,y) is some of pixels above and to left to (x, y). It's used for areas which are not useful some being computationally difficult for 10,000 features we need not sum up all pixels all the time. We use value of patch. Approximately 16000+features values are detected for 24\*24 base resolution, which needs to be, calculated but only few set are useful to identify a face. Some non-relevant features are removed, the useful features are used to build a weak classifier or features use to detect a face is a weak classifier.

## 3. Adaboost Training

ADABOOST is a combination of all these weak classifiers which gives a strong classifier  $F(x) = w1f1(x) + w2f2(x) + w3f3(x)$ . Where,  $f(x) =$  strong classifier,  $w1f1(x) =$  weak classifier,  $w2f2(x) =$  weak classifier,  $w3f3(x) =$  weak classifier.

The output of this weak classifier will be either 0/1 showing presence of pattern in input image. All the outputs of these weak classifiers are either positive or negative. Even if one of them is negative it shows absence of feature hence not a face. 25,000 features are used to generate a strong classifier.

## 4. Cascading

In this first all the non-face regions are removed so that it can concentrate on facial features to detect the face.

**Applications:**

1. Security purposes in shops or organizations, starting from small scale applications to wider scope of face recognition in law enforcement.
2. To counter terrorism by recognizing faces at terminals airports during immigration, person Identification, etc.
3. It can be used to mark attendance in org or even provide discounts in shops for customers based on number of times particular customer has occurred keeping them.

on number of times particular customer has occurred keeping them.

**7 Conclusions and Future Work**

This research work discussed the challenging issue in image processing like identification of person from the image sets and proposed a new technique to overcome the issue. The proposed technique helps to resolve the identification and recognition of images. To address the problem of ambiguity in face recognition we have used a principled max-margin framework where the person to be identified is treated as a latent parameter. The evaluation of our method on the public dataset created by us suggests that while the problem is hard, we can make progress. Though our method gives high localization accuracies we will try in future to build more robust methods to identify identical twins also.

**References**

- Chen, B., Chen, Y., Kuo, Y., Hsu, W.: Scalable face image retrieval using attribute-enhanced sparse code-words. *IEEE Trans. Multimedia* **15**(5), 1163–1173 (2012)
- Wu, Z., Ke, Q., Sun, J., Shum, H.Y.: Scalable face image retrieval with identity-based quantization and multi-reference re-ranking
- Grother, P., Ngan, M.: Face recognition vendor test (FRVT): Performance of face identification algorithms. NIST Interagency, Gaithersburg, Rep. 8009 (2014)
- Wang, D., Jain, A.K.: Face retriever: pre-filtering the gallery via deep neural net. In: *Proceedings of the International Conference on Biometrics* pp. 473–480 (2015)



# Detection of Primary Glaucoma Using ANN with the Help of Back Propagation Algo in Bio-medical Image Processing

G. Pavithra<sup>1</sup>, T. C. Manjunath<sup>2(✉)</sup>, and Dharmanna Lamani<sup>3</sup>

<sup>1</sup> VTU, RRC, Belagavi, Karnataka, India

<sup>2</sup> ECE, DSCE, Bangalore, Karnataka, India

dr.manjunath.phd@ieee.org

<sup>3</sup> ISE, SDMIT, Ujire, South Kanara, Karnataka, India

**Abstract.** One of the dreaded diseases that adversely affects human eye in the world is the Glaucoma. It should be remembered that without eyes, nothing is possible in this world. Further, as per the WHO, it is a well-known fact that the glaucoma is determined as the second largest disease across the globe. Proper care should be taken to avoid this at an early stage, as this would later result in the loss of human vision. The glaucoma disease occurs in the human eyes because of the increase in the intraocular pressure of the fluid flow in the drainage canal of human eyes. To reduce the glaucoma treatment expenses, we are devising a low cost module method for detecting the primary glaucoma in the humans using their fundus images. The images of the infected eye will be captured by the fundus camera, analyzed & a info is given to the patient that he/she is affected with the glaucoma disease. Once the person comes to know that they are affected, then proper diagnosis can be done by gathering consultations from the medical experts. The method of detecting the primary glaucoma is being presented in this section using a revised artificial neural network along with a back propagation algorithm concepts. The morphological operators concepts are being used for the processing the cup and the disc & finally the region of interest, i.e., the cup and the disc areas are detected from which the infected ratio is computed. Using a revised feature extraction process, the features of the captured disc & the cup can be efficiently detected with a concept of CDR detection and the result will declare whether the input test image is glaucomatic or not. Simulations have been done in the Matlab environment. Databases have been taken from the hospitals & online. The simulation results have shown the effectivity of the method proposed in this extensive research work.

**Keywords:** Modelsim · Matlab · Glaucoma · Eye · Disease · Normal · Affected · Blocks · Pressure · Tool · Hardware · Implementation · FPGA · Xilinx · Modelsim · Matlab · Histogram equalization · Intensity transformation · Database

## 1 Introduction

Developments in bio-medical image processing and digital imaging has laid more emphasis on the quality of the captured image along with a number of features embedded into it to make a better understanding on how to use the digital images to its maximum capacity. Bio-medical image processing is vast raised in the medical field which can be diagnosed with the help of a computer. The Fig. 1 shows a comparison of normal eye & a glaucomatic eye.



Fig. 1. Enlarged view of normal & affected eye with glaucoma

## 2 Literature Survey

A number of researchers have worked on the diagnosis & detection of *primary & secondary glaucoma* with a consideration on the number of fundus image types using automated image analysis concepts till date (*both at the investigation level & at the hospital levels*). In this paragraph, a conceptual view of the background info w.r.t. the related literature on the detection of *primary glaucoma* is being presented. Madhusudhan *et al.* [1, 2] proposed a method in which fundus color images are used for calculating cup to disk ratio which were affected with *primary glaucoma* & used for glaucoma detection using some IP techniques. Narasimhan and Vijyreka [3] worked on the increase in cup to disc ratio in their research paper w.r.t. the early detection of *primary glaucoma* in humans & used the Open CV for detection purposes.

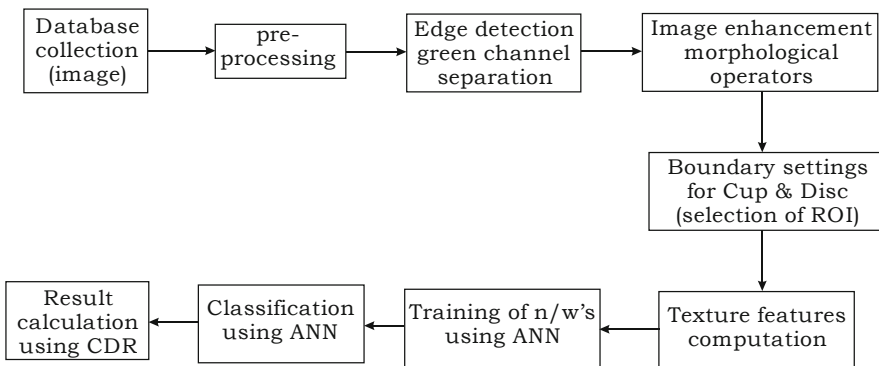
Muramatsu, *et al.* [4–6] did extensive work on the determining the CDR [7] of the optic nerve for detection of *primary glaucoma* on stereo type fundus images in pairs from fundus camera & used retinal images. Li and Chutatape developed novel algorithms for the automatically locating the position of the OC & OD in retinal images in [8] & also developed a model-based approach for automated feature extraction in fundus images in [9]. Morales *et al.* [10] researched upon the automatic detection of OD based on the PCA & Mathematical Morphology, which is used for detection of primary glaucoma. Joshi, Sivaswamy and Krishnadas developed a novel method for OD & OC segmentation from the monocular color retinal images for *glaucoma (primary)* assessment in [11].



### 3 Proposed Block Diagram

In this fusion, we are able to develop computational and mathematical methods for solving clinical and biomedical research problems. The recent developments in the computation process along with the new discoveries in the technological areas such as x-rays, fundamental physics, natural & material science, digital radiography, computed tomography, MRI, CT Scans & other optical imaging techniques have given impetus to the automatic detection of the intact 3D bodies of the glaucoma disease w/o harming any parts of the human eye. The recent 21st century's computerized digital images have grown in multi & in interdisciplinary works giving rise the scope and importance of the innovations in the development of algos which are computationally fast, effective & lesser in cost [12–14].

The input to the proposed algo is the images taken from the database (block-1). Then, the input image is pre-processed (block-2) & further the edges are detected using green channel separation technique (block-3). Image enhancement is carried out next using the morphological operators (block-4). Segmentation process is carried out next to extract the cup & disc (block-5), i.e., the boundary settings for cup & disc are done here. Texture features of the ROI (cup & disc) is extracted & computed (block-6). Training of the database is carried out next using artificial neural networks (block-7), finally the classification process is carried again using ANN (block-8). Finally, the results are computed using the cup to disc ratio (block-9), from which it can be detected whether the patient is affected with glaucoma or not using the value of CDR. Figure 2 [15–17].



**Fig. 2.** Block-diagram of glaucoma detection using ANN method with the help of BPA & training classification using neural nets

### 4 Collection of Database (DB Survey)

In order to build the glaucoma detection algo, first & foremost step is to gather a large number of healthy & unhealthy images, which could be clubbed under a single as a 'Database'. In this paper we have considered 50 fundus images collected from various

databases around the world out of which, 30 are from Hospitals, 10 are from High Resolution Fundus (HRF) & the remaining are from the online databases from [www.optic-disc.org](http://www.optic-disc.org) database images and rest of them were taken from online database DROINS & others from IIT-drishti site, couple of the images were taken from the eye hospitals also.

## 5 Pre-processing of Fundus Images

The pre-processing is a technique which suppresses the unwanted distortions or improves some of the image features that are important for further processing. In the work considered, the fundus color image is taken first from the image database, the ROI, i.e., the optic disc & the optic cup (pink or light orange color) are to be extracted. OD & OC extraction when done on the complete image, then the focussing has to be done on the region of interest (ROI) and has to be computationally fast & cost-effective with an increase in the accuracy during the segmentation process in order to produce the final result. The ROI from all images from the DB is cropped down & resized to  $(512 \times 512)$  [18–20]. To start with, the pre-processing of the retinal fundus images is done first. Gray scale conversion is done next. Then, MO's (dilation & erosion) are used next for cropping the images to get the OC & OD, which is being used for further processing in order to detect the nature of the disease (normal or moderate or severe). Intensity equalization, thresholding is done to obtain the ROI, i.e., the cup & the disc.

## 6 Softwares Employed in the Research Work

The software tool that is employed for developing the code is Matlab<sup>(R)</sup> & the different tool boxes such as IP tool box, DSP tool box, etc.... Coding (programs) are developed as .m files, the developed codes are run after giving the fundus image as the input and the results are observed from which the glaucoma detection can be traced, i.e., whether the patient is affected with glaucoma or not.

## 7 Concepts of ANN

Glaucoma detection can also be done using artificial neural networks, which is being presented in this section. By screening of the patients, glaucoma can be potentially reduces risk of permanent blindness by 50%, once the patient comes to know about the disease, he/she can take further decision about the post-glaucoma treatment. Here, neural network is trained in such a way that it the ANN can detect many glaucoma parameters @ different levels using the training process. The neuron model has been developed with the help of feed forward back propagation network in the neural network domain, which is explained in the subsequent section.

Neural network approach is one of the powerful method which is used for the analysis & detection of the primary glaucoma, whether the disease is present or not. The block-diagram of the proposed methodology for this contribution was presented in

Sect. 2 (Fig. 2) along with the brief description of each & every blocks. It has to be noted in this context that the database (i/p to the algo) & the pre-processing concepts that are used in the starting stage of the algorithm are similar to that explained in the Sect. 4 & DRIONS HR RGB fundus image DB along with HRD data base (*which consists of healthy & un-healthy images*) has been used for the pre-processing of the fundus images for glaucoma detection. The various processes used in the glaucoma detection are explained under various sub-headings one after the other as mentioned below.

ANNs are computing systems that are inspired by the biological neural networks which forms the anatomical neural network structure of the human brain. Such learning systems “learn” to perform different types of tasks by considering a number of learning examples, generally w/o being programmed (once programmed-behaves like self-learning mechanisms) with performing any type of complicated task using a set of learned specific rules. For ex., in image recognition, they might learn to identify images using a proper training algorithms consisting of a definite number of neurons/nerve cells. The neural network topology used for diagnosing the eye diseases contains attribute informations of 22 signs and symptoms with an i/p, hidden & o/p layer (all of which can be categorized as nodes). It is to be noted that hidden layers can be more also as such the training weights will be more effective. Each neuron in the input layer represents a particular sign or symptom. The neurons in the output layer represent the eye disease. The structure of a typical ANN is shown in the Fig. 3 with 4 inputs, 4 outputs & 3 hidden layers. Typically, many such input/target pairs are needed to train a network and to get a perfect matched output. In the work considered, a BPA (BP algo) is being used to train the ANN on a pre-determined set of i/p & target pairs, which is shown in the Fig. 4 and to get good results after the training process is over.

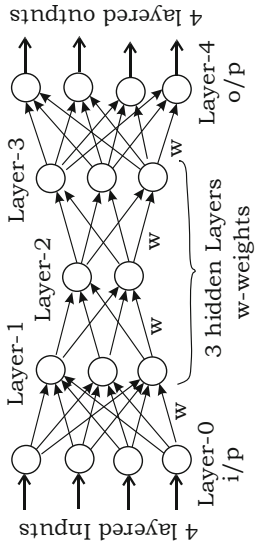


Fig. 3. A typical ANN structure

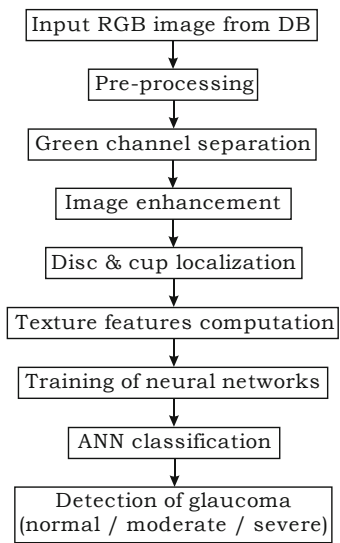


Fig. 4. Flow diagram of proposed methods

Generally, four steps are used in the process of training the ANN. They are – assembling of the training data, creating the n/w object, training the neural n/w & simulating the n/w response to different new inputs.

## 8 Parameters Used for Training

IOP, RNFL, CDR, Thickness of nasal region, Thickness of superior region, Thickness of inferior region.... which are given as i/p parameters to the training algo.

## 9 Simulation Results

Codes are developed in the Matlab environment & are run for different fundus images & the results are observed for various cases of glaucoma, viz., normal (case-1), moderate (case-2) & severe (case-3). To start with, the fundus images, viz., image\_1.jpg, image\_4.jpg & image\_5.jpg are given as inputs to the developed algo one after the other & the results are observed as normal (Figs. 5, 6, 7, 8, 9 and 10), moderate (Figs. 11, 12, 13, 14, 15 and 16) & severe (Figs. 17 and 23) respectively. A 2 layer back propagation network is employed for the classification of the disease. The transfer function used was log sigmoid transfer function. The network was trained using parameters of 20 patients. The training data was used to teach the network to classify the disease as normal, mild or severe (3 separate cases are shown in the simulation results section). Testing was done with parameters of 50 patients (whose nature of disease to be decided by the proposed algorithm). Similarly, the analysis is carried out for the remaining 47 images present in the database and finally the quantitative results are tabulated as shown in the Table 1. After getting extraction of optic cup and disc from the segmentation process, the ANN concepts are used for detection of the glaucoma disease (classification method). From the database of 50 images, the performance values, gradient values & the Mu values obtained is shown in the Table 1. From this table, it can be inferred that out of 50 images taken from the database, 16 were normal, 18 were moderate & the rest 16 were severe case of glaucoma, thus resulting in 68% glaucoma affectedness.

In the 1<sup>st</sup> case considered, when the image\_1.jpg is given as the input to the developed algo, the result obtained is a normal case of glaucoma as shown in the Fig. 5, the results being shown in the command window in the Fig. 10. Other plots related to the case\_1 are also obtained as mentioned next. Performance plot indicates the MSE and epochs values based on which presence of glaucoma is checked. Based on training regression, plots are shown with different values of 'R' means regression value. The graphs of neural network trained values window & the regression plots are shown in the Figs. 6 and 7 respectively. Also, the plots of performance & the training plots at different epochs are shown in the Figs. 8 and 9 respectively.

Case 1 : Normal-Image\_1.jpg

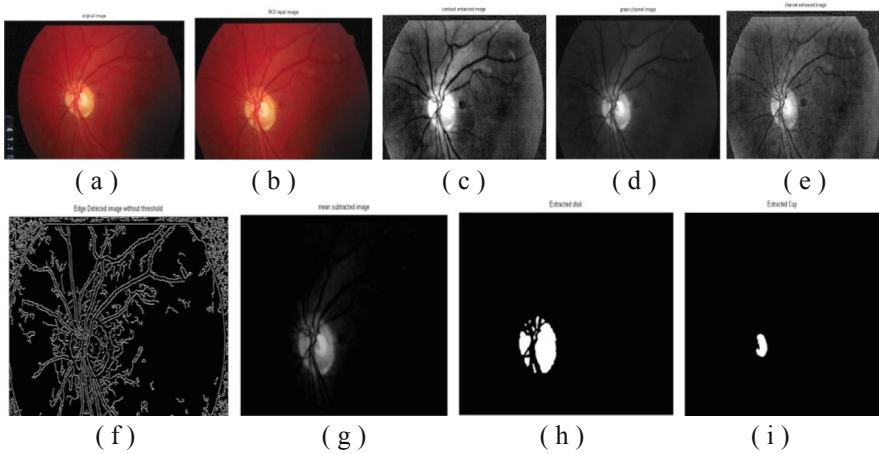


Fig. 5. Matlab results of simulation; normal case of glaucoma (a) i/p query image\_1 (b) Realized image (c) Green channel (d) & (e) Channel enhanced image (f) Edge detected image (g) Mean Subtracted (h) Extraction of Disc (i) Extraction of Cup

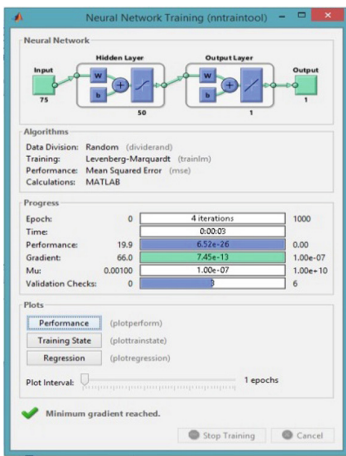


Fig. 6. Neural network trained values window

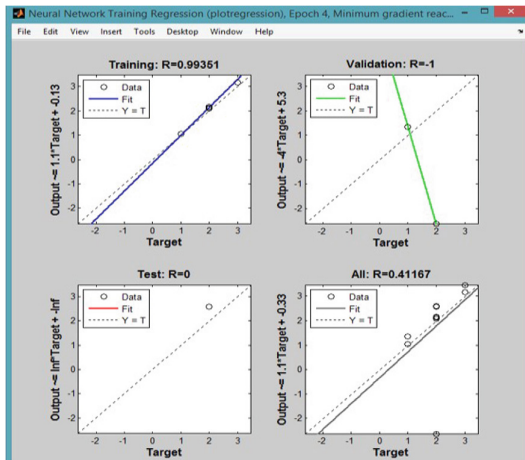


Fig. 7. Regression plot

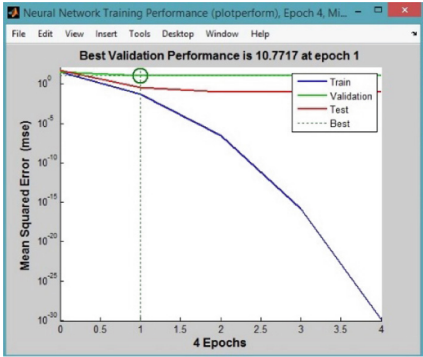


Fig. 8. Performance plot

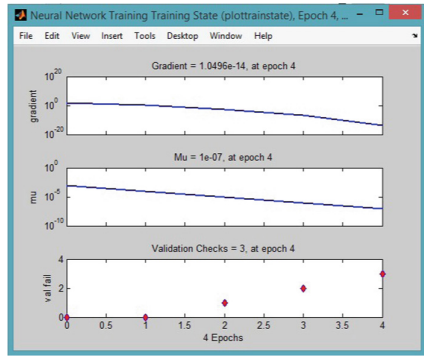


Fig. 9. Training plot

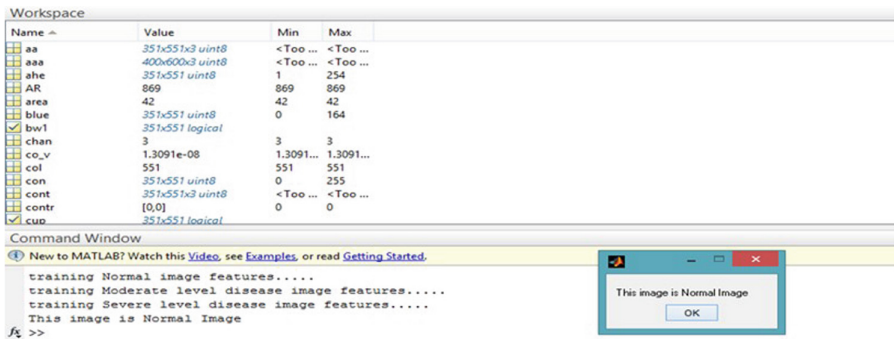


Fig. 10. CDR output at command window with cup & disc area for the case 1 showing normal case

In the 2<sup>nd</sup> case considered, when the image\_4.jpg is given as the input to the developed algo, the result obtained is a moderate case of glaucoma as shown in the Fig. 1, the results being shown in the command window in the Fig. 2. Other plots related to the case\_2 are also obtained as mentioned next. Performance plot indicates the MSE and epochs values based on which presence of glaucoma is checked. Based on training regression, plots are shown with different values of ‘R’ means regression value. The graphs of neural network trained values window & the regression plots are shown in the Figs. 13 and 14 respectively. Also, the plots of performance & the training plots at different epochs are shown in the Figs. 15 and 16 respectively.

Case 2 : Moderate-Image\_4

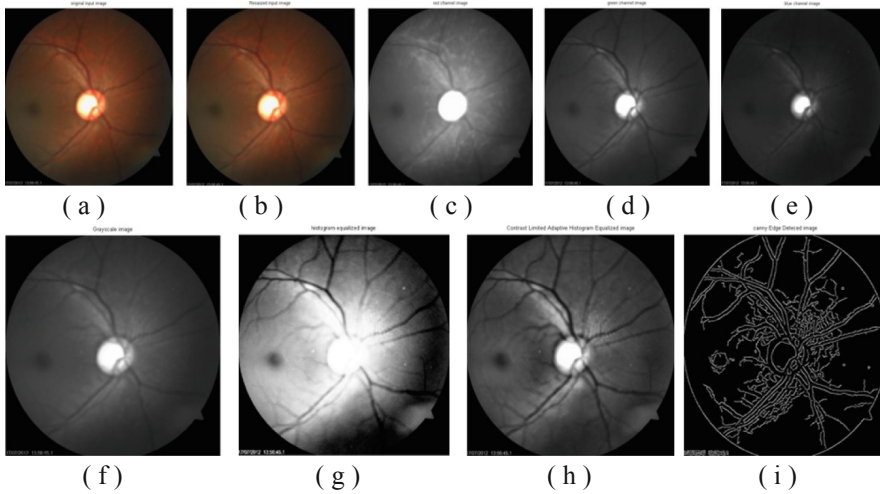


Fig. 11. Matlab results of simulation; moderate case of glaucoma (a) i/p query image\_1 (b) Resized image (c) Red channel (d) Green channel (e) Image-Blue Channel (f) Gray scale image (g) Histogram equalized image (h) CLAHE image (i) Contrast edge detected image

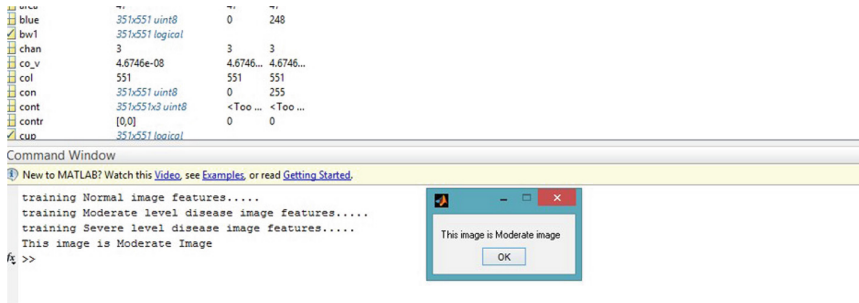


Fig. 12. CDR output at command window with cup & disc area for case 2 showing moderate case

In the 3<sup>rd</sup> case considered, when the image\_5.jpg is given as the input to the developed algo, the result obtained is a severe case of glaucoma as shown in the Fig. 17, the results being shown in the command window in the Fig. 18. Other plots related to the case\_3 are also obtained as mentioned next. Performance plot indicates the MSE

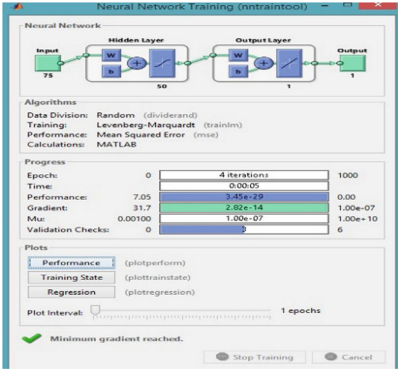


Fig. 13. Neural network trained value

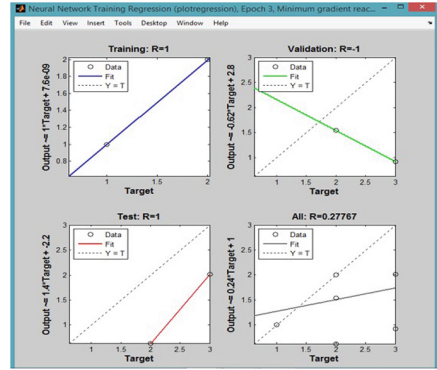


Fig. 14. Regression plot

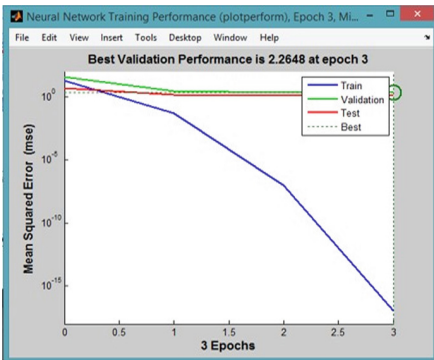


Fig. 15. Performance plot

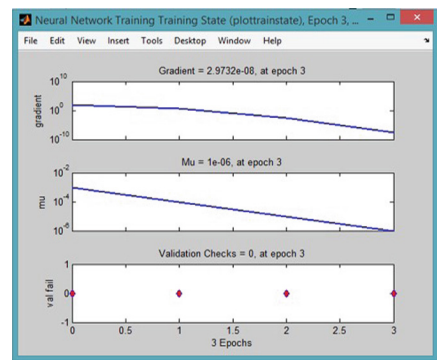
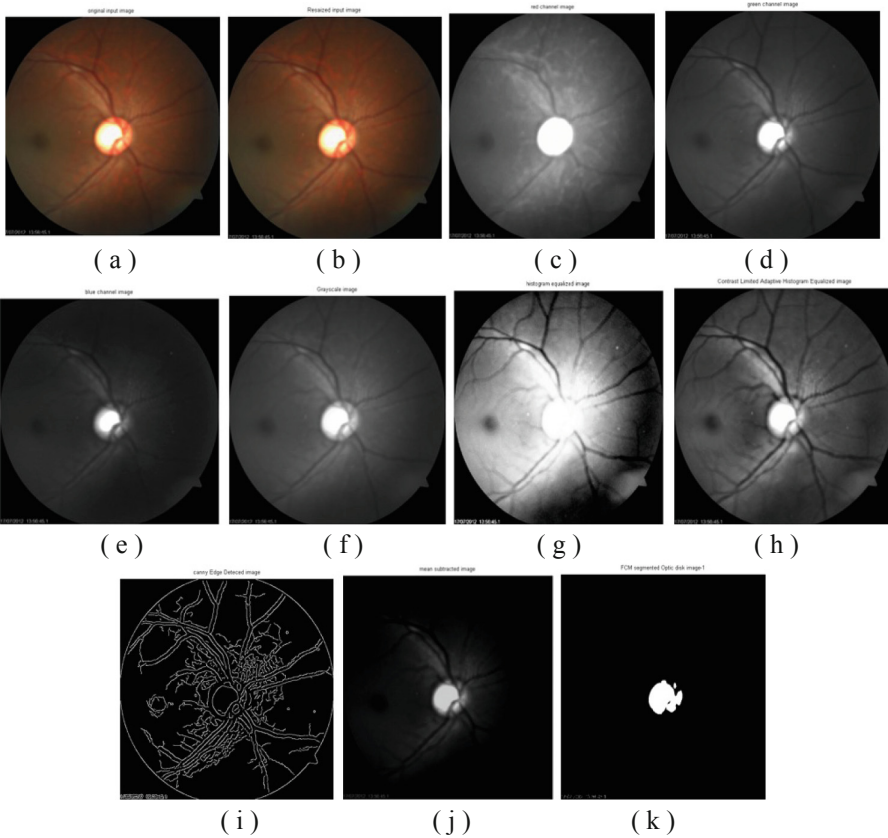


Fig. 16. Training plot

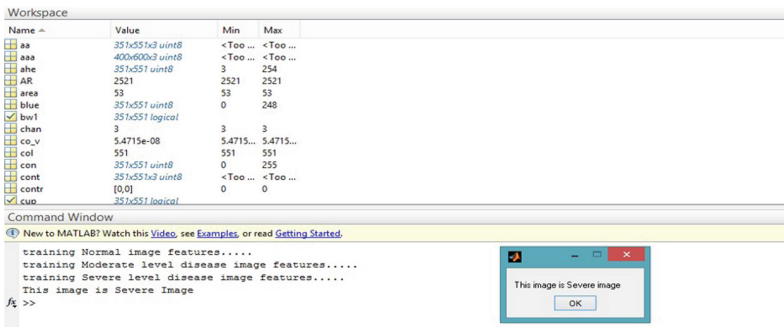
and epochs values based on which presence of glaucoma is checked. Based on training regression, plots are shown with different values of 'R' means regression value. The graphs of neural network trained values window & the regression plots are shown in the Figs. 19 and 20 respectively. Also, the plots of performance & the training plots at different epochs are shown in the Figs. 22 and 23 respectively. The Fig. 21 showing the training process in the display window.



**Case 3 : Sever Glaucoma(>0.6) - Image\_5**



**Fig. 17.** Matlab results of simulation; severe case (a) i/p query image (b) realized input image (c) red channel (d) green channel (e) blue channel (f) GS image, (g) histogram equal image (h) CLAHE (i) canny edge detection (j) means subtraction (k) FCM OD self-image



**Fig. 18.** CDR output at command window with cup and disc area for the case 3 showing severe case

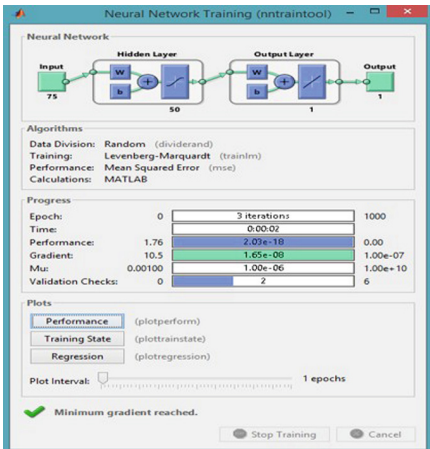
**Table 1.** Training values by artificial neural networks

No.	Image Name	Performance	Gradient	Mu	Status
1.	Image 1 (Normal case)	6.52e-28	7.45-13	1.00e-05	Normal
2.	Image 2	2.26e-19	5.15e-09	1.00e-05	Normal
3.	Image 3	1.12e-30	1.05e-14	1.00e-07	Severe
4.	Image 4 (Moderate case)	3.45-29	2.8e-14	1.00e-06	Moderate
5.	Image 5 (Severe case)	2.03-25	1.16-08	1.00e-07	Severe
6.	Image 6	2.76e-22	4.54e-14	1.00e-05	Normal
7.	Image 7	4.13e-17	5.68e-08	1.00e-06	Moderate
8.	Image 8	1.76e-29	1.77e-14	1.00e-07	Severe
9.	Image 9	1.34e-29	2.33e-14	1.00e-06	Moderate
10.	Image 10	4.49e-29	3.44e-15	1.00e-07	Severe
11.	Image 11	4.37e-28	1.32e-13	1.00e-05	Normal
12.	Image 12	2.26e-19	5.25e-09	1.00e-07	Severe
13.	Image 13	1.13e-30	1.15e-14	1.00e-06	Moderate
14.	Image 14	9.14e-18	2.8e-08	1.00e-06	Moderate
15.	Image 15	1.09e-25	3.42e-12	1.00e-05	Normal
16.	Image 16	2.77e-22	4.64e-14	1.00e-07	Severe
17.	Image 17	4.14e-17	5.78e-08	1.00e-06	Moderate
18.	Image 18	1.77e-29	1.87e-14	1.00e-05	Normal
19.	Image 19	1.35e-29	2.43e-14	1.00e-06	Moderate
20.	Image 20	4.40e-29	3.54e-15	1.00e-07	Severe
21.	Image 21	4.35e-28	1.31e-13	1.00e-05	Normal
22.	Image 22	2.24e-19	5.24e-09	1.00e-07	Severe
23.	Image 23	1.23e-30	1.14e-14	1.00e-06	Moderate
24.	Image 24	9.24e-18	2.8e-08	1.00e-06	Moderate
25.	Image 25	1.19e-25	3.41e-12	1.00e-05	Normal
26.	Image 26	2.87e-22	4.65e-14	1.00e-07	Severe
27.	Image 27	4.24e-17	5.77e-08	1.00e-06	Moderate
28.	Image 28	1.87e-29	1.86e-14	1.00e-05	Normal
29.	Image 29	1.45e-29	2.44e-14	1.00e-06	Moderate
30.	Image 30	4.50e-29	3.55e-15	1.00e-07	Severe
31.	Image 31	3.35e-28	1.31e-13	1.00e-05	Normal
32.	Image 32	1.24e-19	5.24e-09	1.00e-07	Severe
33.	Image 33	2.23e-30	2.14e-14	1.00e-06	Moderate
34.	Image 34	8.24e-18	3.8e-08	1.00e-05	Normal
35.	Image 35	2.19e-25	4.41e-12	1.00e-05	Normal
36.	Image 36	3.87e-22	5.65e-14	1.00e-07	Severe
37.	Image 37	5.24e-17	6.77e-08	1.00e-06	Moderate
38.	Image 38	2.87e-29	2.86e-14	1.00e-05	Normal
39.	Image 39	1.45e-29	3.44e-14	1.00e-06	Moderate
40.	Image 40	3.50e-29	4.55e-15	1.00e-07	Severe

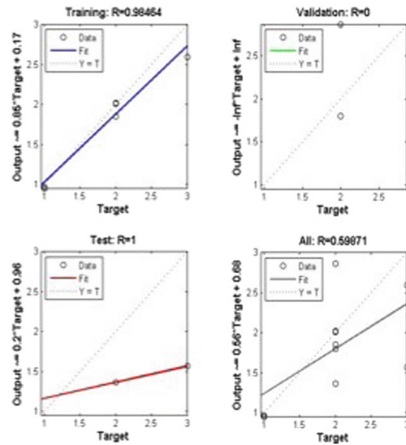
*(continued)*

**Table 1.** (continued)

No.	Image Name	Performance	Gradient	Mu	Status
41.	Image 41	3.25e-28	1.33e-13	1.00e-06	Moderate
42.	Image 42	1.14e-19	5.23e-09	1.00e-05	Normal
43.	Image 43	2.13e-30	2.15e-14	1.00e-07	Severe
44.	Image 44	8.14e-18	3.85e-08	1.00e-05	Normal
45.	Image 45	2.19e-25	4.45e-12	1.00e-07	Severe
46.	Image 46	3.27e-22	5.66e-14	1.00e-06	Moderate
47.	Image 47	5.24e-17	6.76e-08	1.00e-06	Moderate
48.	Image 48	2.27e-29	2.87e-14	1.00e-05	Normal
49.	Image 49	1.25e-29	3.47e-14	1.00e-06	Moderate
50.	Image 50	3.20e-29	4.58e-15	1.00e-07	Severe



**Fig. 19.** Neural network trained values window



**Fig. 20.** Plot of regression



Fig. 21. Display window showing the training process

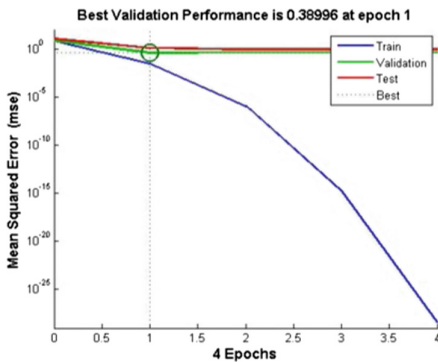


Fig. 22. Plot performance

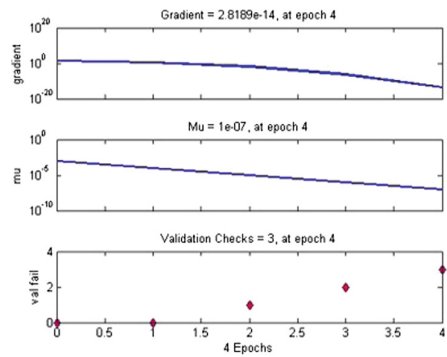


Fig. 23. Plot of the train state

## 10 Conclusions of the Research Work

Detection of primary glaucoma using ANN with the help of back propagation algo in bio-medical image processing was presented in this research paper. In this research article, ANN is being used for the detection of primary glaucoma using the back propagation algorithm. A pre-defined set of images are being trained, first & when the query image is being given as the input, the o/p, i.e., whether the query image is being affected with glaucoma or not is being produced. The simulation was run for all the

fundus images considered in the database. In this section, only 3 cases from the database, viz., one from normal, one from moderate & one from severe case of glaucoma were considered for the simulation purposes. The  $\mu$  parameter was obtained in each case from which it was justified that the patient was normal, moderate & severe, which is also depicted in the quantitative results table. The performance values & the gradient values are used to calculate the  $\mu$  parameter from which the status of the disease could be determined. The simulation results shown in the results section shows the effectivity of the methodology developed by us. Similarly, the results are observed for the remaining set of images present in the database & is not shown here for sake of convenience. One of the major drawback of the proposed method is the CDR value cannot be determined, but the  $\mu$  parameter could be used for the detection of the glaucoma.

## References

1. Madhusudhan, M., Malay, N., Nirmala, S.R., Samerendra, D.: Image processing techniques for glaucoma detection. In: International Conference on Advances in Computing & Communications, pp. 365–373, 22 July 2011. Springer, Heidelberg (2011)
2. Madhusudan, M., Nath, M.K., Dandapat, S.: Glaucoma detection from color fundus images. *Int. J. Comput. Commun. Tech. (IJCCT)* **2**(6), 7–10 (2011)
3. Rathod, D.D., Manza, R.R., Rajput, Y.M., Patwari, M.B., Saswade, M., Deshpande, N.: Localization of optic disc and macula using multilevel 2-D wavelet decomposition based on haar wavelet transform. *Int. J. Eng. Res. Tech. (IJERT)* **3**(7), 474–478 (2014). ISSN: 2278-0181
4. Hatanaka, Y., Noudo, A., Muramatsu, C., Sawada, A., Hara, T., Yamamoto, T., Fujita, H.: Automatic measurement of cup to disc ratio based on line profile analysis in retinal images. In: 33rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society, Boston, MA, USA, 30 August–3 September 2011, pp. 3387–3390 (2011)
5. Muramatsu, C., Nakagawa, T., Sawada, A., Hatanaka, Y., Yamamoto, T., Fujita, H.: Automated determination of cup-to-disc ratio for classification of glaucomatous and normal eyes on stereo retinal fundus images. *J. Biomed. Opt.* **16**(9), 096009-1–096009-7 (2011)
6. Hatanaka, Y., Nagahata, Y., Muramatsu, C., Okumura, S., Ogohara, K., Sawada, A., Ishida, K., Yamamoto, T., Fujita, H.: Improved automated optic cup segmentation based on detection of blood vessel bends in retinal fundus images. In: 36th Annual International Conference of the IEEE Engineering in Medicine & Biology Society, Chicago, IL, USA, 26–30 August 2014, p. 126–129 (2014)
7. Ahmad, H., Yamin, A., Shakeel, A., Gillani, S.O., Ansari, U.: Detection of glaucoma using retinal fundus images. In: International Conference on Robotics & Emerging Allied Technologies in Engineering, Islamabad, Pakistan, 22–24 April 2014, pp. 321–324 (2014)
8. Li, H., Chutatape, O.: A model-based approach for automated feature extraction in fundus images. In: 9th IEEE International Conference on Computer Vision (ICCV 2003), Nice, France, 2nd Volume Set, 13–16 October 2003, vol. 1, pp. 394–399. IEEE Computer Society (2003)
9. Li, H., Chutatape, O.: Automatic location of optic disc in retinal images. In: 7th IEEE International Conference on Image Processing, Thessaloniki, Greece, 7–10 October 2001, vol. 2, pp. 837–840 (2001)

10. Morales, S., Naranjo, V., Angulo, J., Alcañiz, M.: Automatic detection of optic disc based on PCA and mathematical morphology. *IEEE Trans. Med. Imaging* **32**(4), 786–796 (2013)
11. Joshi, G.D., Sivaswamy, J., Krishnadas, S.R.: Optic disc and cup segmentation from monocular color retinal images for glaucoma assessment. *IEEE Trans. Med. Imaging* **30**(6), 1192–1205 (2011)
12. Khan, F., Khan, S.A., Yasin, U.U., ul Haq, I., Qamar, U.: Detection of glaucoma using retinal fundus images. In: 6th IEEE Conference on Biomedical Engineering (BMEiCON), AmphurMuang, Thailand, 23–25 October 2013, pp. 1–5 (2013)
13. Kavitha, S., Karthikeyan, S., Duraiswamy, K.: Early detection of glaucoma in retinal images using cup to disc ratio. In: IEEE International Conference on Computing Communication and Networking Technologies (ICCCNT), Tamil Nadu, 29–31 July 2010, pp. 1–5 (2010)
14. Lamani, D., Manjunath, T.C.: Diagnosis of glaucoma disease through image feature fractal dimension. Ph.D. Thesis, VTU, Belagavi, February 2016
15. Pavithra, G., Manjunath, T.C.: Different clinical parameters to diagnose glaucoma disease: a review. *Int. J. Comput. Appl. (IJCA)*, **116**(23), 42–46 (2015). IF 3.546, ISSN 0975–8887
16. Pavithra, G., Manjunath, T.C.: Automated diagnose of neo-vascular glaucoma disease using advance image analysis technique. *Int. J. Appl. Inf. Syst. (IJAS)* **9**(6), 1–6 (2015). Published by Foundation of Computer Science (FCS), NY, USA, ISSN 2249-0868
17. Pavithra, G., Manjunath, T.C.: A novel approach for diagnosis of glaucoma through optic nerve head (ONH) analysis using fractal dimension technique. *Int. J. Mod. Educ. Comput. Sci. (IJMECS) ICV*, 55–61 (2016)
18. Pavithra, G., Manjunath, T.C.: A novel approach for diagnosis of glaucoma through optic nerve head (ONH) analysis using fractal dimension technique. *Int. J. Mod. Educ. Comput. Sci. (IJMECS)* **8**(1), 55–61 (2016)
19. Pavithra, G., Manjunath, T.C.: A novel method of digitization & noise elimination of digital signals using image processing concepts. *Int. J. Eng. Res. Electron. Commun. Eng. (IJERECE)*, **3**(11), 38–44 (2016). ISSN (Online) 2394-6849, Impact Factor 3.689, paper id 8
20. Pavithra, G., Manjunath, T.C.: Design of algorithms for diagnosis of primary glaucoma through estimation of CDR in different types of fundus images using IP techniques. *Int. J. Innov. Res. Inf. Secur. (IJIRIS)*, **4**(5), 12–19 (2017). Paper id MYISSP 10135



# RTMDC for Effective Cloud Data Security

Pankaj Verma<sup>1(✉)</sup>, Nilima Dongre<sup>1(✉)</sup>, and Vijaylaxmi Bittal<sup>2(✉)</sup>

<sup>1</sup> Department of IT, RAIT, Nerul, Navi Mumbai, India  
vermapankaj2497@gmail.com, nilimarj@gmail.com

<sup>2</sup> Department of CSc, RAIT, Nerul, Navi Mumbai, India  
vijaylaxmi.bittal@gmail.com

**Abstract.** In today's world, almost everything has been digitised and hence the cloud computing is emerging as a boom in its field. But the most disturbing fact is that the cloud computing also appears as a vulnerable platform and therefore the security becomes the most important aspect in the cloud computing applications. Security issues are mainly dealt with known and unknown threats, malware and network access by unknown or unauthorised users. Hence, it has become a fundamental feature to create a secure platform for the cloud computing technologies. In this scenario, we proposed a RTMDC (Reputation based Trust Management system with Data Colouring) systems, which builds and tests a secure platform using Reputation Based Trust Management technique. Reputation based trust factor is then calculated using the collective reviews given by the users. This research work focuses on the images that has been related to the cloud users.

**Keywords:** RBTMS · Data Colouring · ACPC · TABE · RTMDC · DDOS

## 1 Introduction

Sharing the resources e.g. computer networks, servers, storage, applications and services is known as cloud computing. Individuals and organisations put up their data onto the cloud at free storage space or at a very low storage cost. It also provides value-added services e.g. lowering down the companies' data storage and maintenance costs.

### Cloud Computing Security

The cloud adoption is the main concern for ensuring security in maintaining sensitive business information. As the public cloud has multiple users, the basic hardware framework is shared with a number of cloud customers. This habitat needs abundant solitude among logical computing resources. Simultaneously, account login authorisation guards the access to public cloud storage and computing resources. Numberless organisations are confined by complex regulatory liabilities and governance standards but they are scared to put up data in the public cloud due to panic of disruption, loss or theft. But this fear is going down now because logical isolation has proven trustworthy and inclusion of data encryption and distinct identity and access management tools has enhanced the security inside the public cloud.

## 2 Literature Review

### A. Aspects of Cloud Security:

Security plays a crucial role in the adoption of cloud computing technologies. If the humongous amount of individual data and likely safe data that is stored by people in the personal computers are ported to cloud, some safety steps should be taken to safeguard the data. Clouds are dependent upon the conventional data confidentiality, availability, integrity and concealment issues, also few more attacks until now.

Few security issues are as follows:

- Confidentiality: The scare of whether the delicate data is still safe when it has been ported to the cloud. Whether the CSP would be trustworthy and snooping wont happen in the data?
- Integrity: The clients recognition that cloud provider is performing the calculations rightly will be in what way? How the clients will recognise that information is saved without altering it?
- Availability: What would happen if the cloud givers runs out of trade? What would happen if cloud givers are invaded by a denial of service attack?
- Privacy issues Privacy is the significant concern when a vast amount of data is to be stored by cloud.
- Additional attacks Bodies out of the company can save and calculate the information so raiders can conveniently aim the connection link among the cloud givers and the user.

### B. Security Services in Cloud Computing:

The following services in CC provides the security [12]:

- Virtualisation: Each user is allocated an entirely secluded virtual habitat to accomplish the task.
- Virtual Private Network (VPN): Using the VPN, the exchange of data among cloud giver and client may be safe.
- Federated Identity: It is the capability to transmit information beyond safety territory with the help of requests and affirmations from a digitally signed identification giver. Consumers who earlier validated themselves in the company's web must be certified to the assistances of company which would be functioning above the cloud. This is given by federated identity service, that binds management of identities of the company and cloud assistance giver combined.
- Policy Services: Describes policies which form judgement to determine which cloud service giver to appoint depending on factors like security, reliability, etc.

### C. Security Measure:

Virtualisation: Fundamental to enable a Cloud Computing habitat is known as Virtualisation. In a multi-rental habitat it is very important to have seclusion among processes indulging for distinct companies. An error in application or OS results in



seclusion violation. The quick fix to this type of issues is to help various companies, is either by allotting individual physical machines or virtual machines [12]. As the whole accessible resources are not required, therefore the virtualisation happens to be the cost effective result for this because may be we use only a chunk of assets in the given system. Besides seclusion, virtualisation in cloud do have more benefits. The foremost requirements of cloud giver is brisk elasticity, so that we can join the resources else delete them based on present request by user company. Portability is second benefit of virtualisation. The movement of virtual machine from one physical system to another is easier when maintenance work is going on.

### 3 Related Work

#### A. ACPC:

Normally, cloud customers and cloud servers exist out of the information owners loyal domain. The P2P cloud depository makes new threats concerning the control to access and the information safety whereas the information owner generally saves the crucial data for dividing them in the loyal domain of cloud depository. Yet, in P2P depository cloud, no such procedure feasible for access control [1]. By joining CC and P2P computing, a P2P depository cloud can be made to present vastly accessible depository services, cutting back the commercial expenditure by abusing the depository area of competing consumers. Additionally, there are no procedures for control in access in P2P cloud storage.

ACPC allows information holders to authorise maximum of the hard customer cancellation tasks to cloud hosts and renowned peers in the system. The efficiency calculation states that ACPC is greatly productive under possible framework, and this considerably decreases the calculations induced to data holders and cloud host during client revocation, in comparison with different state-of-the-art revocable ABE designs [2].

#### B. TABE:

In trust attribute based encryption, we recognise the trust of the attributes in web site at first and secondly, depending on trust attribute we make the access policy to cipher text [3].

In key policy attribute based approach, guidelines are linked with keys and attribute are linked with cipher text. Cipher text attribute based encryption policies are liked with cipher text and attribute are linked with keys. Information holder catches the trust attributes in websites by deploying Trust Attribute Detection Techniques, then encodes the file depending on the trust attributes uploads the file in cloud. Client decodes the file from the cloud by deploying trust attributes based decryption.

The conduct of TABE depends upon the number of attribute and time taken to encode and decode the file. The accomplishment time of TABE is lower than the CP-ABE and KPABE. Safety of TABE is much more than the CP-ABE and KP-ABE is based on trust attributes. The information holder can produce and describe

new access policy dependent upon the actions of client and past of the client. Close access control is gained based on access policy. Client access benefits and privacy is won by TAFE. Client secret key is obliged and won by TAFE and save the key exploiters. Data secrecy is won through TAFE. Accomplishment time of TAFE is limited compare to CPABE and KP-ABE. Data confidently is achieved through TAFE. Trust based attribute revocation is fast compare to other attribute based encryption techniques.

### C. RBTMS:

Along these lines shown up in the system of online business structure, e.g. eBay. In scattered settings, notoriety based ways have been proposed for dealing with confide in P2P frameworks, in versatile impromptu systems, open key testaments, and, recently, in the Semantic Web. The emphasis here is on trust calculation models fit to evaluate the level of assume that can be put resources into a specific gathering in light of the historical backdrop of its past conduct. The fundamental issues describing the notoriety frameworks are the put stock in metric (how to display and register the trust) and the administration of notoriety information (how to safely and effectively recover the information required by the confided in calculation). Swamp made one of the early endeavours at formalising trust utilising basic trust measurements in view of direct conditions. Various notoriety components for P2P frameworks, for example, took after comparable trust and notoriety models. Ordinarily, notoriety based trust is utilised as a part of appropriated systems where a framework just has a constrained perspective of the data in the entire system. New trust connections are induced in light of the accessible data (following abusing world's data). In these situations, the accessible data depends on the proposals and the encounters of different customers, and it is commonly not marked by accreditation specialists but rather (conceivably) self-marked by the wellspring of the announcement. This approach bolsters trust gauges with a wide, continuum go and permits the proliferation of trust (e.g., transitive engendering) along the system and also weighting of qualities (e.g., fresher data versus more seasoned data) [4].

## 4 Problem Statement

Cloud has become the most important aspect when we are operating in the digital world and is vulnerable to thefts and malicious attacks which ultimately results in loss of data. The resources shared and utilised in cloud environment needs security at all times, be it the physical infrastructure, virtualisation layer or application layer. In absence of security measures in these levels, the data is vulnerable to different attacks. Thus there is a requirement of secured cloud platform so that our data is safe.

## 5 Proposed Approach

Notoriety is a focal idea in different circumstances that incorporate cooperation among commonly doubting gatherings. In trust based methodology common exertion between hubs can be utilised by creating trust among a troop of associates which are envisioned to be reliable towards the beginning and after that the rest arrange is quickened by those companions. Each plan can be utilised as a part of different application situations.

In the RTMDC for P2P systems, the resultants of past exchanges are spared in the trust vectors, proceeded by the associates. Each associate keeps a trust vector for each other companion it has exchanged with before. In this outline, the reactions are masterminded and estimated by the appraisals of unwavering quality the responders with a specific end goal to procure the most reliable associate to download.

### A. Reputation based Trust Management using Data Colouring

Among the most difficult issues for the reception and ascent of distributed computing is Trust Management. The exceedingly evolving, conveyed, and hazy nature of cloud administrations offers different testing issues, for example, protection, accessibility and security. Sparing buyers’ protection is a troublesome undertaking because of the fragile information associated with the connections amongst clients and the trust administration benefit. Moderating cloud administrations against their terrible clients (e.g., associated clients may give equivocal criticism to hurt a specific cloud benefit) is an intense issue. Guaranteeing the accessibility of the trust administration benefit is second noteworthy issue due to the changing idea of cloud conditions.

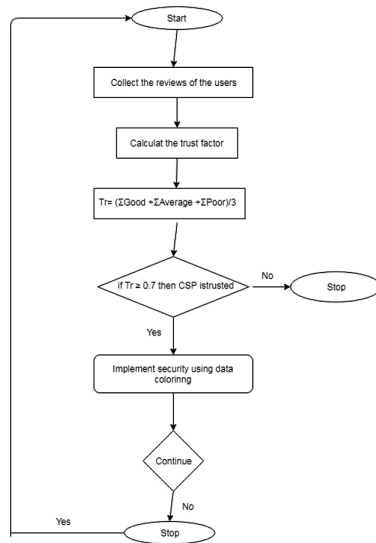
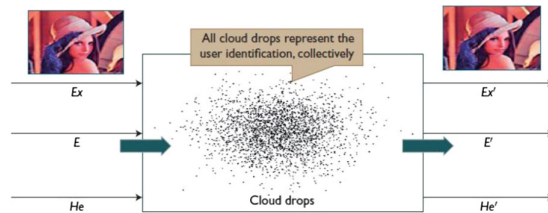


Fig. 1. Working of RTMDC.

Client's input is a decent starting point to decide the general reliability of cloud administrations. Unequivocally, we separate the accompanying key difficulties of the trust administration in cloud situations: Trust Management Service's Availability, Consumer's Privacy, Cloud Services Protection (Fig. 1).

### B. Data Colouring

Forward cloud generator is needed to make a pinch of each component of a pixel matrix, and a fresh pigment will be appeared after crossing the matrix. The pigment acquiring the form of a component could be fixed into any part of data. Furthermore, all clients information is fixed with cloud components of end client's watermarks that displays the expectation, entropy, and hyper entropy of the water-4 mark data. Amusingly, no such typical encoding and decoding is there in the procedure of colouring of data. The procedure of data colouring consists of, the area of the watermark to be installed and the design for installing is determined by an end clients appealed strength of security and admissible rate. Strength of security will tell added space for storage, and design complexity will elect time cost of information accessing (Fig. 2).



**Fig. 2.** Forward and backward data colouring processes by adding or removing unique cloud drops (colours) in data objects [11].

### C. Algorithm for converting image into negative:

1. Get the RGB value of the pixel.
2. Calculate the new RGB value as shown

$$\text{below. } R=255-R, G=255-G, B=255-B.$$

3. Save the new RGB value in the pixel.

Note! We don't have to change the alpha value because it only controls the transparency of the pixel.

D. Algorithm for converting an image into grayscale:

1. Get the RGB value of the pixel.
2. Find the average of RGB i.e.

$$\text{Avg.} = (R+G+B)/3.$$

3. Replace the R, G and B value of the pixel with average (Avg.) calculated in step 2.

Note! We don't have to change the alpha value because it only controls the transparency of the pixel. Hence, for a grayscale image the RED, GREEN and BLUE component of a given pixel is same.

E. System design (Fig. 3):

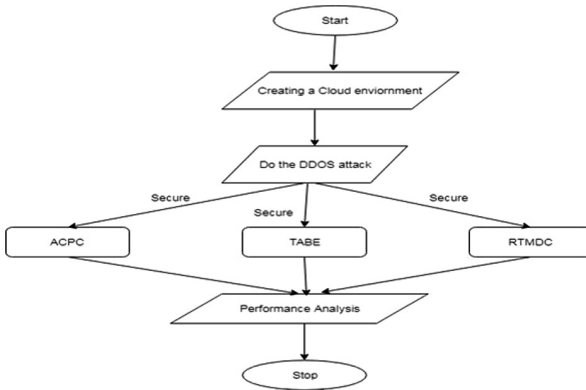


Fig. 3. Flowchart for system design.

## 6 Comparative Analysis

Here we will compare the RTMDC and other techniques with some parameters to know the kind of performance the RTMDC can give us to safeguard our cloud from malicious and unauthorised users (Fig. 4).

S.No	ALGORITHM	KP-ABE	CPABE	NON-MONOTONIC	HABE	MABE	RTMDC
1.	Component	Data is associated with an access policy	CT is associated with an access policy	Represent negative constraints	Hierarchical generation of key	Multiple authorities	Data color identification on w.r.t. sensitivity
2.	Efficiency	Average	Average	High	Better	Scalable	High
3.	Secured Access Control	Low	Average	Average	High	Average	High
4.	Computational Overhead	High	Average	More	More	More	More
5.	Data Confidentiality	No	Yes	Yes	Yes	Yes	Yes
6.	User Accountability	No	No	Yes	No	Yes	Yes
7.	Scalability	No	Yes	No	No	Yes	Yes
8.	User Revocation	No	No	Yes	Yes	Yes	Yes
9.	Collusion Resistant	Yes	Yes	Yes	Yes	Yes	Yes
10.	Limitation	It cannot decide who can encrypt data	Decrypt key only support user attribute that are organized logically	Insufficient and complex	Unsuitable to implement	Each authority attribute set should be disjoint	If reputation is compromised then the trust will be gone

Fig. 4. Comparison of ABE techniques with RTMDC.

## 7 Performance Analysis

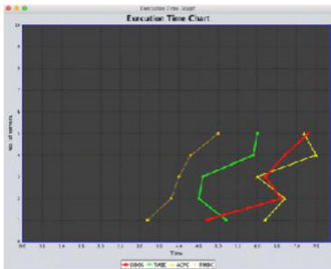


Fig. 5. Graph for lowest set of values.

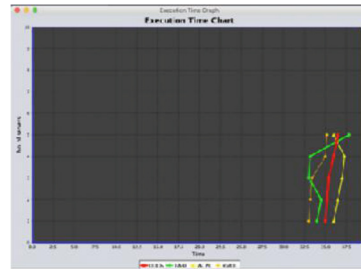


Fig. 6. Graph for high set of values.

The above Fig. 5 represents the execution time taken by different techniques to execute data. The particular graph is taken for the lowest values possible for execution. The time taken to execute a file is the time taken by different techniques to encrypt the file. As a result, when the file size increases, the time to execute a file also increases. The values are as follows:

- No of Data centre: 2
- No of VM: 2
- No of Cloudlets: 1
- MIPS: 256
- RAM: 256

The above Fig. 6 represents the execution time taken by different techniques for very high set of values for execution. The values are as follows:

- No of Data centre: 100
- No of VM: 500
- No of Cloudlets: 2500
- MIPS: 25000
- RAM: 2048

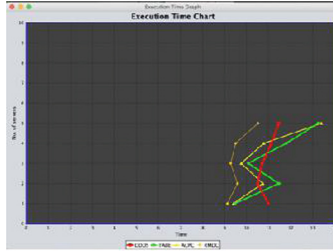


Fig. 7. Graph for any set of values.

The above Fig. 7 represents the execution time taken by different techniques to execute data for any set of values. The values are as follows:

- No of Data centre: 10
- No of VM: 20
- No of Cloudlets: 50
- MIPS: 5000
- RAM: 1024

## 8 Conclusion

The main aim of the our approach is to protect the data which has been stored on cloud from the malicious users and activities. We, here analysed and compared the different techniques to check whether the encryption and decryption of data on cloud is secure and only the authorised user can access the data. The RTMDC technique has come out to be the most reliable technique to save the data from malicious attacks and preventing the data from being modified and wrongly used.

## References

1. Shaik Hussain, S.I., Yuvaraj, V.: A secure data access control method using AES for P2P storage cloud. *IEEE* (2015)
2. He, H., Li, R., Dong, X., Zhang, Z.: Secure, efficient and fine-grained data access control mechanism for P2P storage cloud. *IEEE* (2014)
3. Manjusha, R., Ramachandran, R.: Sharing data in cloud based on Trust Attribute Based Encryption (TABE). *ARNP J. Eng. Appl. Sci.* **10**(9), 3 (2015)
4. Bonatti, P., Duma, C., Olmedilla, D., Shahmehri, N.: An integration of reputation-based and policy based trust management
5. Liu, Y.-C., Ma, Y.-T., Zhang, H.-S., Li, D.-Y., Chen, G.-S.: A method for trust management in cloud computing: data coloring by cloud watermarking. *Int. J. Autom. Comput.* **8**(3), 280 (2011)
6. Banerjee, A., Neogy, S., Chowdhury, C.: Reputation based trust management system for MANET. In: *Third International Conference on Emerging Applications of Information Technology (EAIT)* (2012)
7. Selcuk, A.A., Uzun, E., Pariente, M.R.: A reputation-based trust management system for P2P networks. *Int. J. Netw. Secur.* **6**(3), 235–245 (2008)
8. Noor, T.H., Sheng, Q.Z., Yao, L., Dustdar, S., Ngu, A.H.H.: CloudArmor: supporting reputation-based trust management for cloud services. *IEEE Trans. Parallel Distrib. Syst.* **27**(2), 367–380 (2015)
9. Nitya Lakshmi, R., Laavanya, R., Meenakshi, M., Suresh Gana Dhas, C.: Analysis of attribute based encryption schemes. *Int. J. Comput. Sci. Eng. Commun.* **3**(3), 1076–1081 (2015)
10. Saravana Kumar, N., Rajya Lakshmi, G.V., Balamurugan, B.: Enhanced attribute based encryption for cloud computing. In: *International Conference on Information and Communication Technologies (ICICT 2014)* (2014)
11. Hwang, K., Li, D.: Trusted cloud computing with secure resources and data coloring. *IEEE* (2010)
12. Chadha, K., Bajpai, A.: Security aspects of cloud computing. *Int. J. Comput. Appl.* **40**(8), 43–47 (2012)
13. *Security for Cloud Computing Ten Steps to Ensure Success: Cloud Standards Customer Council* (2017)





# Human Tracking Using Wigner Distribution and Rule-Based System in RGB Video

J. R. Mahajan<sup>1</sup>(✉) and C. S. Rawat<sup>2</sup>

<sup>1</sup> Department of ETE, Pacific University, Udaipur, India  
mahjayant@gmail.com

<sup>2</sup> Department of ETE, Vivekanand Institute of Technology,  
Chembur, Mumbai, India  
csrawat3@gmail.com

**Abstract.** In recent times, human tracking plays a crucial role in several applications like surveillance, free biometry, realistic world etc. In this research work, we suggest a new method to track the objects like humans using the motion obtained from color images. This algorithm does not use the object characteristics which is tracked and hence it resembles human eyes that uses the process of tracking in all the available images in RGB. Spatial and temporal association of motions are considered for motion association, which is the proposed plan of action to decrease the undesired selection process. Furthermore, for different images the Wigner distribution has been used which is less dependent on the fluctuation in threshold frame and thus reduces the untrue object detections. The results acquired with this algorithm is identical and consistent which in turn provides the reduction in computational complexity of this algorithm.

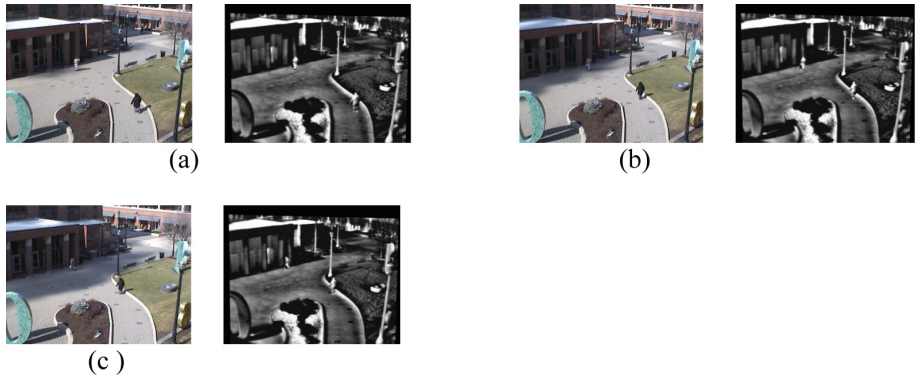
**Keywords:** Human tracking · Wigner distribution

## 1 Introduction

The objective of this line of work is to explore the approach for tracking of human motion using only color imaging. In this motion tracking system only RGB imaging using popular and easily available CCTV cameras. Recently, the color imaging and applications based on it like to track the motion; facial recognition has attracted the researcher's attraction especially from image processing and vision community [1]. There are already lot of attempts which includes the visible imagination in application like facial identification and in addition to track motion into the gray scale and thermal cameras, which also called as data fusion system. As color cameras available at cheaper cost due to mass demand, it becomes effective to track the humans for various applications in color camera images.

In use-cases like non-cooperative surveillance outside, where the background is so cluttered and here, RGB imaging can play vital role in identifying the person using color property of every object tracking in each case. This concept has mainly encouraged to use color camera image to track motion of human beings. The one issue about visible imaging is that it is sensitive to darkness or low-density condition, generally which is the problem in almost all of the motion based tracking on seeable

camera, see Fig. 1. This fact makes human tracking in visible images more appropriate for outdoor motion tracking situations in daylight as well as nighttime, where shadowing conditions and variation in the lights are dominating a factor which makes tracking more difficult. Thus, having intelligent algorithm to handle these issues faced by visible tracking algorithm is very important to make system more robust [15, 16].



**Fig. 1.** Shadow effects dominant in visible camera images [2].

We propose here a new technique for tracking of human using Color Imaging. This algorithm does not use characteristic of object which is tracked and hence it is just like a human eyes that uses the process of tracking in much available RGB images, especially using cues obtained from motion of object. In the proposed approach, different types of data association like spatial, temporal data association, is used reduce the undesired selection. Additionally, for different images the Wigner distribution has been used which is less depends on the fluctuation in threshold frame and thus reduces the untrue object detections.

The remaining part of this paper is designed as follows. Next Sect. 2, explains the state of art of tracking of human. Section 3 elaborates about methodology of proposed human tracking method in visible cameras. The observation and discourse are presented in Sect. 4. Lastly, the paper is completed to focus on the uniqueness as well as observation of the proposed method.

## 2 Motion Tracking: State of the Art

The general understanding for tracking of human is to be determining the human position across the video frames. Depending upon the image position, there are two types of object tracking, called as, Static and Active Camera Tracking as well as Motion Tracking. Also, depends on the motion, motion sensors used along with object, they are divided into two classes called as, With Markers and Marker-less (considered in this work). Based on the methods used for motion tracking, two types of algorithms are used for motion tracking, these are tracking based on Recognition and motion based tracking.

Another criterion to classify the techniques based on the motion type which is nothing but tracking of human in motion. Thus, the tracking of human use-cases is divided in two types which are Motion based Articulated and Moving Motion. In most of the application like surveillance the multiple object tracking is used. Different motion tracking technologies are described in literature which are as follows Kalman Filter, Extended Kalman Filter, Particle filter, Unscented Kalman Filter, Hidden Markov model, affine transform, Gabor Transform etc.

The Performance Measures used in motion tracking research are error calculation (RMS/MSE/PSNR), Motion Curve Matching which includes Matching coordinates, processing speed important in Real-time applications, calculation of False Positive and False Negative.

Figure 2 shows, the typical system of tracking of object or motion, which is basically a combination of video acquisition system, image analysis algorithm which yields object coordinates and display of the device which shows the object path and/or logically generation of signal to event detection.

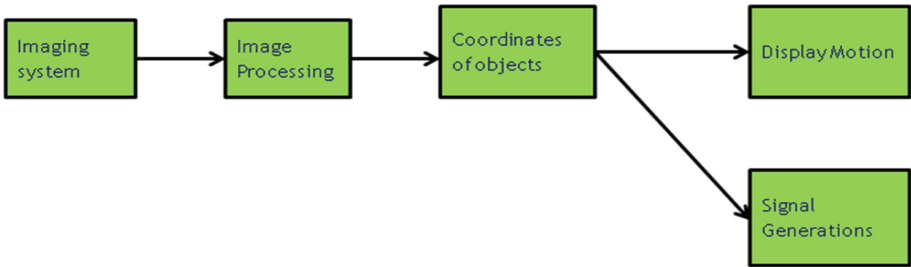


Fig. 2. Motion tracking system

Being tracking the object is critical task in any human tracking based applications, our work focused on development of human tracking technique which is applied to the images taken from thermal camera. The basic tracking algorithm for object is shown in Fig. 3.

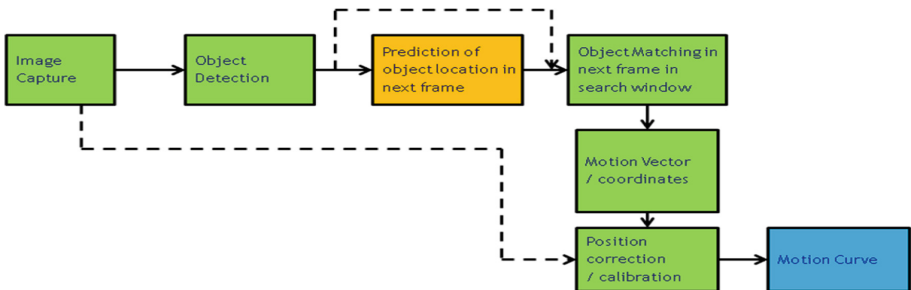
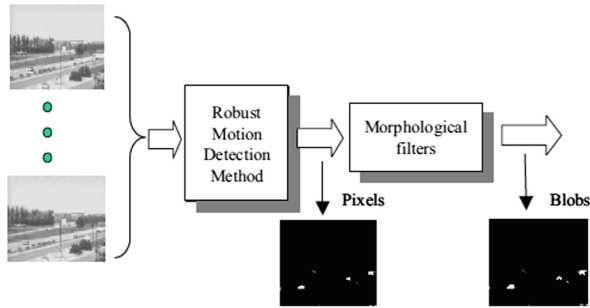


Fig. 3. Typical tracking algorithm for object

The detection of Object can be achieved from the following steps [2]. Figure 4, shows the difference image.

- The easiest approach is Image subtraction between successive frames.
- If morphological operators are required, then they are used.
- Requirement of Segmentation.



**Fig. 4.** Human detection

Using estimation of Motion, the matching of moving object in surrounding of next frame uses the motion tracking. For finding the best matching unit, there are many approaches available Refs. [3–5], which is based on

- Pixel (Pel) (complex computationally)
- Block
- Region
- Mesh or shape (triangle, hexagonal, content based)

Best matching unit can be obtained with similarity criterion as mentioned below

- MAD (Mean absolute difference)
- MSE (Minimum Mean Square Error)
- SSE (Sum of Squared Error)
- MAD (Mean Absolute Difference)
- MAE (Mean Absolute Error)

The good matching procedure to calculate the motion vector which included the similar criteria for search based for closeness of pixels in next frame. Typically this search frame is in the rate of  $15 \times 15$  pixels, and then it required the high computational power. To avoid those computational complexities, various optimization techniques are available in literature. Following are some approaches along with their references.

- 2-D logarithm search [6]
- TSS [7]
- NTSS [8]
- FSS [9]
- Based on Two step multiple local winners [10]
- Search based on Conjugate Direction [11]

In the field of tracking of motion, there are two popular techniques available for visible camera based on motion tracking [12] are Kalman filter and Particle filter which are very popularly used and particle Filter [13].

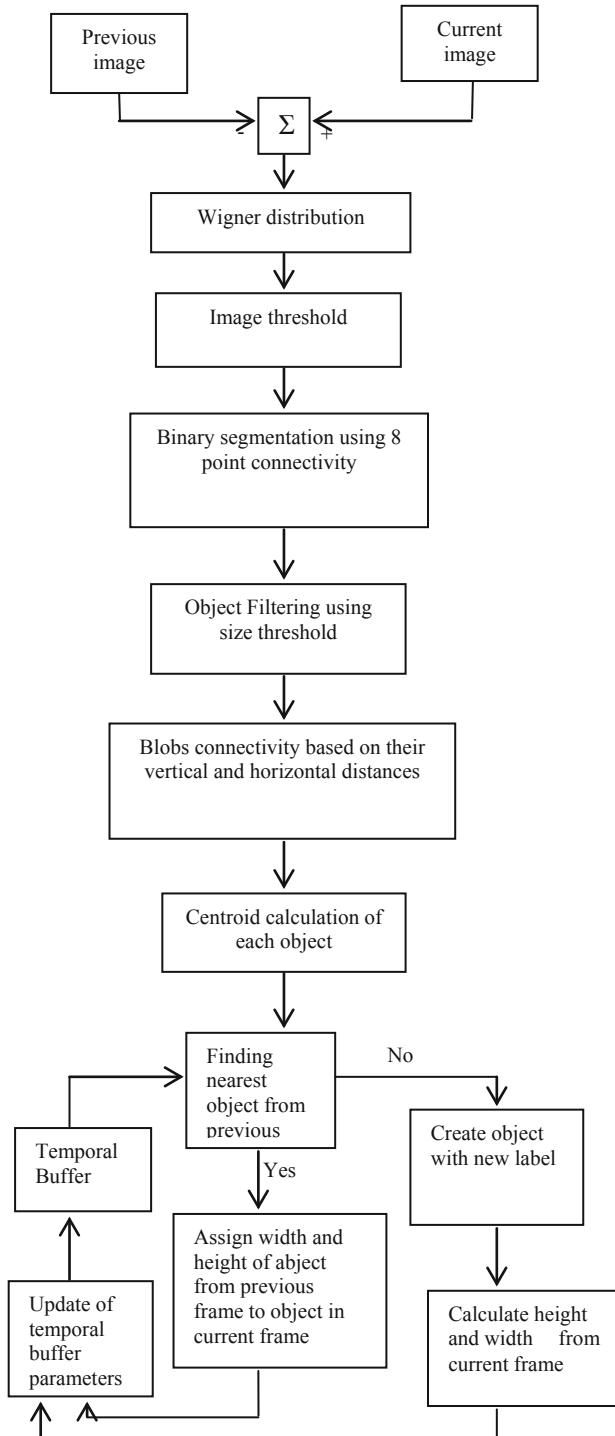
### 3 Methodology

Based on the tracking done by natural eyes, this work has been uses in visible camera images as more focus is on the motion of object. The motion cues are paramount for eyes to decide whether object is moving or not. For this purpose, we have made a use of the various data associations processes. Basically there are two types of motion association, considered in the proposed technique. These techniques however was used for thermal images earlier [18].

- Spatial Data association
- Temporal Data Association

As frames become available, the difference of images is calculated in each of RGB plane of color frames. This difference is between current frame and previous frame. The subtraction takes place between three planes of respective frames and then difference from each was added to have single difference image. This differential image is then passed through the calculation of Wigner distribution for dc frequency [14]. The DC frequency basis function is able to pull the missed part of the motion components observed between two frames. For the difference images without applying the Wigner distribution, it has been observed that thresholding is not effective to separate out motion from noisy fluctuations due to winds and varying illumination in the scene. The difference image obtained after Wigner distribution is thresholded to separate the motion points from noisy points and this gives a binary image. Using 8-neighbourhood connectivity, the foreground object points are located and grouped to FG label. Depending on the earlier discussed clutters which exists in RGB images, the large number of untrue negative objects are available in binary image. The filtering based on the criteria of minimum size is applied on the objects founds in binary image. This criteria is consistent with the objective of application where human is to be detected and they are sufficiently large in the frame. The previous step yields the group of connected pixels (region) which are moving and sufficiently significant in size. If there are two sub regions of motion exists due to noise, algorithm connect these blobs by using vertical and horizontal threshold of distances between two nearby blobs. Vertical threshold kept larger than horizontal one when the person move in vertical shape. This is useful to separate out two persons are close and moves in same direction. The outputs in step shows that the same label to close by spot are indicating close spot of same person.

Another motion association way, we used in this technique is temporal and it is realized by employing a temporal buffer such that temporal motion if exists in previous time frame is more likely to be carried in next frame in close vicinity of next frame. With respect to centroid, each object motion regions are evaluated. The existing objects in previous frames are compared with centroid for their closeness are tested. The nearest object with distance less than threshold is found from the previous frame, then the labelling is given to the object from the current frame shows the previous frame object is



**Fig. 5.** Data flow for proposed method

now at its new position which gives its centroid. The height and width of object of current frame is allocated from previous frame (In future, the history of objects like height and width will be averaged and created to all the current frame objects height and width). With this new object location, the temporal buffer gets updated.

In case, if the nearest object has a distance greater than pre-defined threshold, then object create the new entry of new person with new label. Its width and height are calculated from current frame. Thus with this new object parameters, temporal buffer is updated. All the objects in current frames are stored in temporal buffer. The data flow chart for tracking of motion algorithm are shown in Fig. 5.

## 4 Experimental Results and Discussion

With the help of MATLAB, we develop the algorithm which is applied to OTCBVS website [17], where the database is available. The database is called as thermal and color database. It contains the of six image sequences where, each image sequence contain approximate 2500 frames. The numbers of frames vary from sequence to sequence. For a given location with pedestrians, first three sequences are taken. From different location, second image sequence was taken. Wigner image have a threshold of 0.30. For filtering out the false objects, the threshold size is of 15 pixels is kept. Temporal buffer has a depth of four. The distance of thresholds in vertical and horizontal are 20 and 10 respectively. In any direction the object present in next frame as a same object is 5 pixels which is a minimum distance. For all the sequences, these threshold parameters are kept constant. For every frame, the color resolution is 24 bits with three planes of RGB. Based on experimental results we get, following discussion will be carried out for different sequences. It is easily observed that our proposed algorithm can detect object in situations where human eye fails to detect.

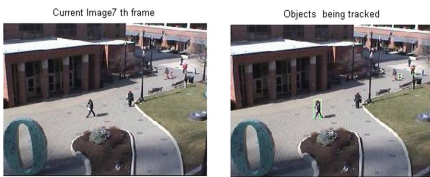
The proposed technique is used on all six sequences available in database. The result obtained for first frame sequence is shown in Fig. 6. In this frame, one person moving and another person is still. The moving person is being tracked. There is a person far away from the camera appearing at upper side of frame and because of low contrast between person and background, is missed by the tracking system. This happens as the third person is beyond the resolution range of camera. Even if this person is tracked the results obtained are unsatisfactory.

In Fig. 7, most of the persons including small kid and dog have been captured by tracking system as they are moving as shown in figure. In different environment, two persons have been tracked by system which is shown in Fig. 8. Figure 9 shows the person coming behind tree has also been located by the system. The same person is being located further in coming frames as shown in Fig. 10. Figure 11 shows that as person enters in scene, he is been located instantly by tracking system, this shows the consistency of our algorithm. Figure 12 shows that even female is been located and thus our system is gender independent. The Fig. 13 shows the 4 frames with same person at different time points. It can be seen that with varying background, still person is being located, this proves the robustness of proposed algorithm.

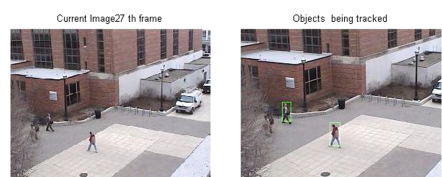
Thus the results obtained from this algorithm shows the error less and efficient performance of tracking the person in thermal images. In the upcoming work, by considering the perspective parameters of camera, the location of the objects obtained by the threshold are automatically and/or making adaptive thresholding.



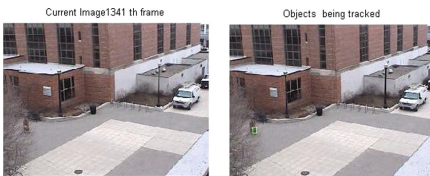
**Fig. 6.** Results for first frame sequence of database



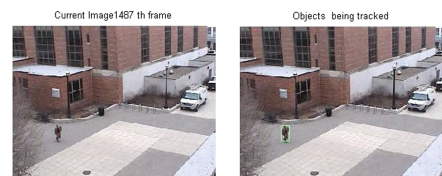
**Fig. 7.** Multiple moving object tracking



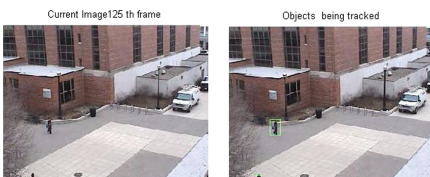
**Fig. 8.** Multiple object tracking in different environment



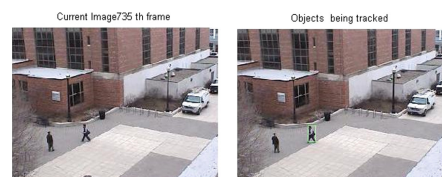
**Fig. 9.** Occlusion based object tracking



**Fig. 10.** Continue of Fig. 9 in next frame

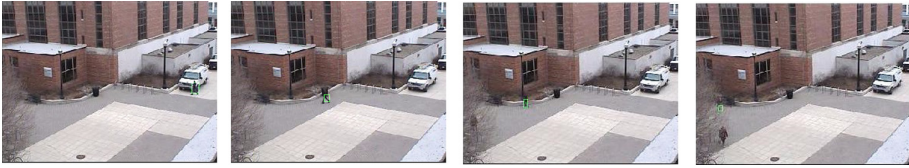


**Fig. 11.** Instant object location using tracking system



**Fig. 12.** Gender independent system





**Fig. 13.** Tracking using different frames at different background

## 5 Conclusion

We propose a new method for person tracking using thermal images in this paper. This method depends on Wigner distribution modeling of the inter-frame difference image and the conjunction of spatial and temporal data associations. The proposed algorithm has small computational complexity and is thus quite fast when compared to methods that use object features. We presented results on several image frames from dataset. The results obtained with this technique shows that consistency and robustness achieved with proposed algorithm.

## References

1. Wolff, L.B., Socolinsky, D.A., Eveland, C.K.: Chapter 6, Face recognition in the thermal infrared
2. Herrero, E., Orrite, C., Alcolea, A., Roy, A., Guerrero, J.J., Sagüés, C.: Video-sensor for detection and tracking of moving objects. In: Perales, F.J., Campilho, A.J.C., de la Blanca, N.P., Sanfeliu, A. (eds.) *IbPRIA, Pattern Recognition and Image Analysis. LNCS*, vol. 2652, pp. 346–353. Springer, Heidelberg (2003)
3. Van Beek, P.J.L., Tekalp, A.M., Puri, A.: 2-D mesh geometry and motion compression for efficient object-based video representation. In: *Proceedings of the International Conference on Image Processing*, vol. 3, pp. 440–443 (1997)
4. Altunbasak, Y., Murat Tekalp, A., Bozdagi, G.: Two-dimensional object-based coding using a content-based mesh and affine motion parameterization. In: *Proceedings of the International Conference on Image Processing*, vol. 2, pp. 394–397 (1995)
5. Badawy, W., Bayoumi, M.: A mesh based motion tracking architecture. In: *The 2001 IEEE International Symposium on Circuits and Systems, ISCAS 2001*, vol. 4, pp. 262–265 (2001)
6. Jain, J., Jain, A.: Displacement measurement and its application in interframe image coding. *IEEE Trans. Commun.* **29**(12), 1799–1808 (1981)
7. [http://www.ece.cmu.edu/~ee899/project/deepak\\_mid.htm](http://www.ece.cmu.edu/~ee899/project/deepak_mid.htm)
8. Li, R., Zeng, B., Liou, M.L.: A new three-step search algorithm for block motion estimation. *IEEE Trans. Circuits Syst. Video Technol.* **4**(4), 438–442 (1994)
9. Po, L.-M., Ma, W.-C.: A novel four-step search algorithm for fast block motion estimation. *IEEE Trans. Circuits Syst. Video Technol.* **6**(3), 313–317 (1996)
10. Hsieh, H.-H., Lai, Y.-K.: A novel fast motion estimation algorithm using fixed subsampling pattern and multiple local winners search. In: *The 2001 IEEE International Symposium on Circuits and Systems, ISCAS 2001*, vol. 2, pp. 241–244 (2001)
11. Srinivasan, R., Rao, K.: Predictive coding based on efficient motion estimation. *IEEE Trans. Commun.* **33**(8), 888–896 (1985)

12. Stauffer, C., Grimson, W.E.L.: Learning patterns of activity using real-time tracking. *IEEE Trans. Pattern Anal. Mach. Intell.* **22**(8), 747–757 (2000)
13. Isard, M., Blake, A.: CONDENSATION—conditional density propagation for visual tracking. *Int. J. Comput. Vision* **29**(1), 5–28 (1998)
14. Wigner, E.: On the quantum correction of thermodynamic equilibrium. *Phys. Rev.* **40**, 749–759 (1932)
15. Padole, C.N., Vaidya, V.G.: Image restoration using Wigner distribution for night vision system. In: 9th International Conference on Signal Processing, ICSP 2008, pp. 844–848 (2008)
16. Vaidya, V.G., Padole, C.N.: Night vision enhancement using Wigner distribution. In: 3rd International Symposium on Communications, Control and Signal Processing, ISCCSP 2008, pp. 1268–1272 (2008)
17. <http://www.cse.ohio-state.edu/otcbvs-bench/>
18. Padole, C.N., Alexandre, L.A.: Wigner distribution based motion tracking of human beings using thermal imaging. In: 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition - Workshops, San Francisco, CA, pp. 9–14 (2010)



# Agent Technology Based Resource Allocation for Fog Enhanced Vehicular Services

Daneshwari I. Hatti<sup>1</sup>(✉) and Ashok V. Sutagundar<sup>2</sup>

<sup>1</sup> Department of Electronics and Communication, BLDEA's V.P. Dr. P.G. Halakatti College of Engineering and Tehnology, Vijayapur, Karnataka, India  
daneshwari\_hatti@yahoo.co.in

<sup>2</sup> Department of Electronics and Communication, Basveshwar Engineering College, Bagalkot, Karnataka, India  
sutagundar@gmail.com

**Abstract.** IoT comprising heterogenous devices with varied and constrained resources imposes challenge in managing the available network resources. The new technology raised to solve these challenges is fog computing. In this research work, Agent technology for Fog enhanced vehicular services model is proposed. For managing the resources at the edge of the network fog is used and cloud agency is used for providing services to the tasks that are not given by the fog. The proposed work is designed and simulated using cloudsim tool and analysed using cloud analyst tool. Performance measures such as resource utilization, allocation time and congestion rate is measured and resulted with better resource utilization, less allocation time and reduced congestion rate.

**Keywords:** Agent · Cloud agency · Fog agency · Game theory · Resource allocation

## 1 Introduction

Due to increase in demand of resources for the devices in Internet of Things (IoT), to manage the scarcity of resources in devices, cloud computing provides required services to perform the operation in devices. Since every user request to the cloud for providing services resulting in increased latency and congestion. Hence Fog Computing (FC) [1, 2] is introduced to minimize and provide services such as memory, connectivity and computing at the edge of network. Fog is situated between cloud and edge devices or Internet of Things (IoT). FC acts as intermediate layer for providing the Cloud services virtually at the edge of network in managing the IoT devices [3]. The fog constitute switches, routers, servers etc. The resources available in fog nodes is comparatively less than cloud, hence management of resources is essential for providing services to the devices with guaranteed Quality of Service (QoS). The objective of the paper is to incorporate software agents for computing the computational and communication resources, estimate the amount of resources required for the IoT. The agencies manage the devices, allocate resources using game theory approach and provide the service with reduced resource allocation time and congestion.

The organization of this paper is as follows. Few works on amalgamation of cloud, IoT and fog computing for managing resources is highlighted in Sect. 2, Sect. 3 proposes the work and discusses agencies. In Sect. 4, results are discussed. Section 5 concludes the paper.

## 2 Related Work

In [4] fog computing, communication between fog and cloud and between fog and edge devices are reviewed in detail. In [5] smart combination of Fog and Cloud Computing is addressed for building an adaptable and scalable platform for IoT. In [6] IoT is integrated with cloud computing and Smart Gateway with Fog Computing is discussed. The overhead of cloud network is reduced by incorporating fog computing. In [7] seamless fog (sFog) is proposed that supports congestion control and handover schemes. In [8] authors integrated fog computation and Medical Cyber-Physical System (MCPS) to build fog computing supported MCPS (FC-MCPS). In particular they investigated base station association, task distribution and virtual machine placement toward cost-efficient FC-MCPS. In [9] authors explained the agent technology for aggregating data. In [10] authors proposed model for predicting the resources, estimating and reserving resources based on customer type, resource pricing for present and new customers. In [11] authors proposed resource allocation mechanism based on game theory approach for providing fairness among users in resources utilization. In [12] a noncooperative game model for resource allocation and calculating Nash equilibrium (NE) an algorithm is proposed. In [13] an auction-based method is proposed for allocation of resources among the users with incomplete information in a non-cooperative environment. In this work fog residing between IoT and cloud reduces the traffic towards cloud and manages devices. Agencies estimate, predict and allocate services to the vehicles efficiently.

## 3 Proposed Work

Proposed work incorporates fog computing for providing the services to the edge devices. Agencies have been employed in cloud and fog for utilizing the services offered and allocate resource efficiently to the devices diverted to it. Resource prediction and estimation is performed in the fog agency using game theory approach. Communication within fog network through fog agencies and Communication with cloud and fog network is discussed using fog and cloud agencies. In this section network environment, agencies and algorithm are discussed.

### 3.1 Network Scenario

Network model is illustrated in Fig. 1. It constitutes of three layers. The bottom layer depicts the IoT or edge devices, middle layer constitutes fog layer comprising of fog instances and top layer is Cloud.

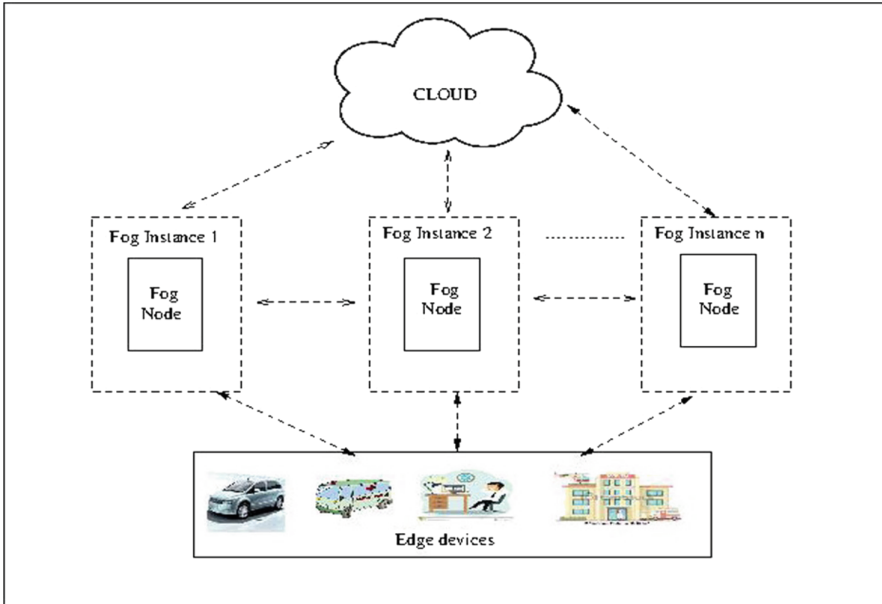


Fig. 1. Network model

Figure 1 shows the network environment for communication among fog instances and between fog – cloud network is illustrated.

- Communication among fog instances: The edge devices request services to fog instance 1. The fog instance 1 perform the resource allocation to the devices based on priority of the job or tasks. The fog agency computes the resources and allocates to devices if requirement is less than available resources.
- Communication between fog and Cloud network: If available resources is less than the required, fog diverts the traffic towards cloud. Cloud agency allocates the required resources to the job through fog agency by job migration agents.

### 3.2 Agencies

Agents [14] are software program residing in the network, collects resource information, performs resource estimation and updates resource repository and allocates resources using game theory approach. In the proposed work two agencies namely cloud agency and fog agency are framed for providing the service to job or edge devices by managing the resources in fog.

1. **Cloud Agency (CA):** CA is shown in Fig. 2. CA consists of static and mobile agents. It constitutes of Cloud Manager agent (CMA), Cloud Resource Repository (CRR) and Cloud Resource Broker Agent (CRBA).

- Cloud Manager Agent (CMA): It is static agent, creates CRR and CRBA. It monitors the resources available in cloud and updates CRR.

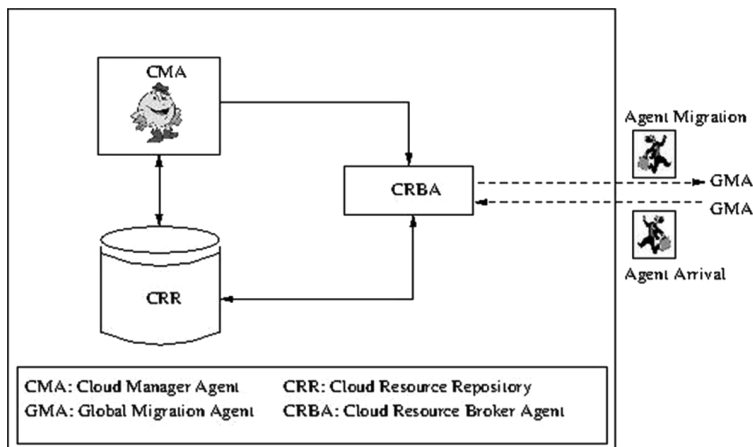


Fig. 2. Cloud agency

- Cloud Resource Repository (CRR): It is static agent. It computes the resources utilized and updates the repository.
  - Cloud Resource Broker Agent (CRBA): It is mobile agent. It computes the amount of resources required and fetches from CRR sends to Fog Agency (FA) through GMA. FA allocates to the devices.
2. **Fog Agency (FA):** FA is shown in Fig. 3. FA consists of static and mobile agents. It constitutes Fog Resource Manager Agent (FRMA), Fog Resource Repository (FRR), Fog Computational Agent (FCA), Fog Resource Broker Agent (FRBA), Global Migration Agent (GMA) and Job Agent (JA).
- Fog Resource Manager Agent (FRMA): It is static agent. It creates FRR, FCA, FRBA, GMA and JA. It monitors the devices entering in to fog instance for service request. It collects the resources available in fog nodes.
  - Job Agent (JA): It is mobile agent resides in fog node carries job/task from the edge devices and forwards to FRR. The fog resources are represented by Virtual Machine (VM). VM provides resources to the devices by JA through Road Side Unit (RSU).
  - Fog Resource Repository (FRR): It is static agent. It consists of VM1, VM2.... VMn, having varied resources. It is updated as the resources are utilized by the edge devices. The status of resources available in VM is sent to FRBA.
  - Fog Resource Broker Agent (FRBA): It allocates the resources by using game theory approach discussed in algorithm in Sect. 3.4.
  - Global Migration Agent (GMA): It is mobile agent moves from FA to CRBA for fetching the required resources to the tasks that are not having sufficient resources in the FA.
  - Fog Computational Agent (FCA): It performs the resource estimation of resources available in VM's. The resources include memory, bandwidth and CPU.

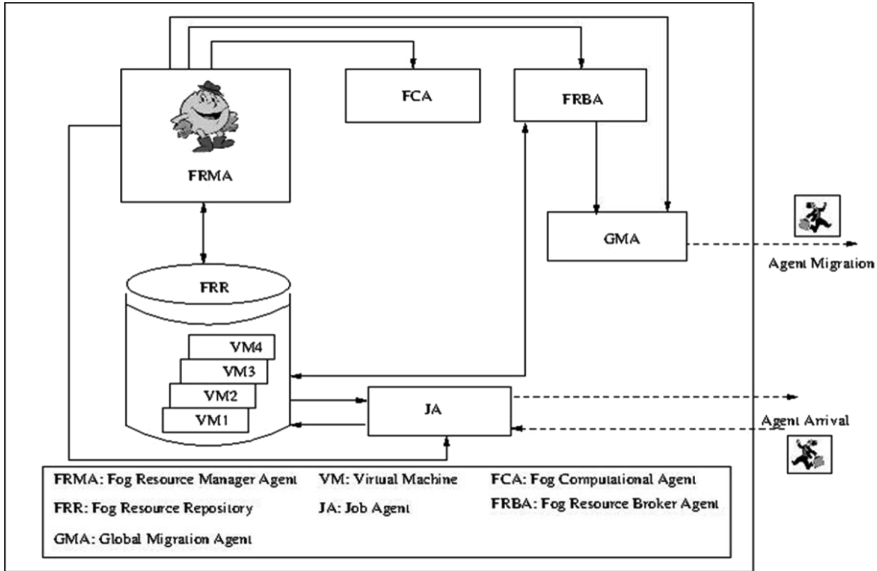


Fig. 3. Fog agency

### 3.3 Algorithm – Proposed Work

1. **Begin**
  - i. Communication between Fog instances
  2. Communication between user and fog instance 1
  3. User sends message to Fog 1
  4. Fog 1 will monitor tasks details.
    - If**(fog instance 1 is having resources)
      - forward the resources to user.
    - else** (insufficient resources)
      - send request to next Fog instance
    - end if**
  - ii. Communication Using Cloud agency
  5. Communication between user and cloud
  6. User sends job to Fog instance 1
    - If**(Fog instance schedules message)
      - {
        - Forward message to Cloud
        - Cloud agency will check requirement
        - Forward the availability details to Fog 1 instance
        - Forward Same from Fog 2 to user
      - }
    - else**
  7. Wait till the fog instance schedules
    - end if**
8. **END**

### 3.4 Algorithm- Resource Allocation Using Fog and Cloud Agency

**Nomenclature-** VM -Virtual Machine, cloudlets-Tasks/Jobs, JA- Job Agent, FCA- Fog Computational agent, FRBA- Fog Resource Broker agent, GMA – Global Migration Agent, CA- Cloud Agency, CRBA- Cloud Resource Broker Agent, FRR- Fog Resource Repository,  $R_{cpu}$  - “CPU Resource”,  $R_{memory}$  - “Memory Resource”,  $R_{BW}$  -“Bandwidth Resource”

**Input** - tasks/jobs

**Output**- tasks are assigned to VMs based on priority

**1. Begin**

**2. for** i-1 to n

accept tasks/jobs from JA represented as cloudlets in cloudsim and ID are assigned

**end for**

**3. for** i-1 to m

FRR creates the VMs and assigns the ID

**end for**

**4.** FRR submits VMs and tasks (cloudlets) to the FRBA

**5.** FRBA creates the VMs priority list (using Game theory) and updates

**5.1 for**(i=1 to m)

FCA calculates resource availability using equation 1 [15] and updates to FRBA

$$\frac{R_{CPU(i)}R_{CPU}}{R_{CPU(i)} + R_{CPU(-i)}}; \frac{R_{memory(i)}R_{memory}}{R_{memory(i)} + R_{memory(-i)}}; \frac{R_{BW(i)}R_{BW}}{R_{BW(i)} + R_{BW(-i)}} [15]$$

**end for**

**5.2 for** (i-1 to m)

FCA calculates the utility function or payoff of each VM using equation 2 [15]

$$U\left(R_{CPU(i)}R_{memory(i)}R_{BW(i)}\right) = \frac{\alpha_i R_{CPU(i)}R_{CPU}}{R_{CPU(i)} + R_{CPU(-i)}} + \frac{\beta_i R_{memory(i)}R_{memory}}{R_{memory(i)} + R_{memory(-i)}} + \frac{\Gamma_i R_{BW(i)}R_{BW}}{R_{BW(i)} + R_{BW(-i)}} [15]$$

**end for**

**5.3 if** (available resource of i-th VM > required resources)

individual VM is assigned

**else**(available resource of i-th VM < required resources)

sharing of VM & scaling of resource

**else if** (available of resource in shared VM < required resources)

send request to CA through GMA

fetches resource availability from CRBA and forward to FRBA

**end if**

**6. for** i-1 to m

6.1 FRR updates the priority list and sends to FRBA

**6.2** repeat the steps 5.1 to 5.3 till the completion of all tasks

**end for**

**7. End**



## 4 Results and Discussion

### 4.1 Simulation

The network model is designed, simulated, and measured some performance parameters such as resource allocation time that is latency, Congestion rate, number of tasks and resource utilization.

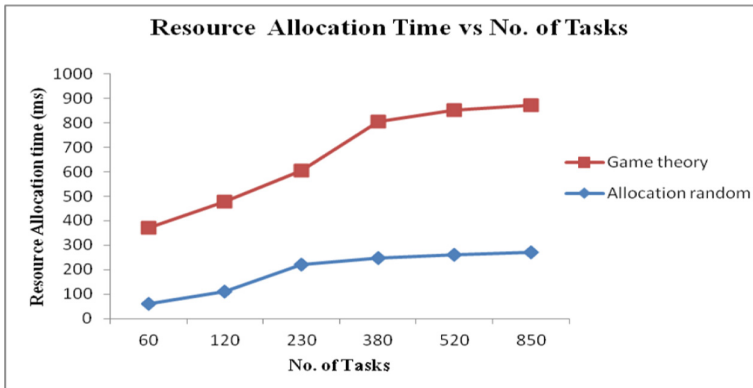
#### Algorithm : Simulation steps

**Begin**

1. The network environment is created.
2. Parameters and inputs are configured.
3. The proposed scheme is applied.
4. The performance parameters of the network are computed and analysed.

**End**

Figure 4 shows the Resource allocation time (ms) obtained for the number of tasks performed using cloud agency and fog agency. Resource allocation time is less for less number of tasks for both as the number of tasks increases the allocation time rises for the cloud agency and reduced in fog agency. Agencies manage the tasks and allocate the resources through fog and cloud with reduced allocation time. Allocation time rises for both the cases in increased number of tasks but comparatively fog agency provides with less allocation time compared to cloud agency.



**Fig. 4.** Resource allocation time vs No. of tasks

Figure 5 shows the resource utilization in % vs number of tasks graph. In normal allocation the amount of resources used is less compared to proposed approach. Game theory approach is used by the agent for allocating resources optimally to the tasks with increased resource utilization percentage. If required resources are less than available, the utilization is normal and with increased requirement then available resources,

utilization rate decreases and if both levels are equal then utilization rate is attained maximum level. Resource utilization for the proposed algorithm is more compared to the normal allocation.

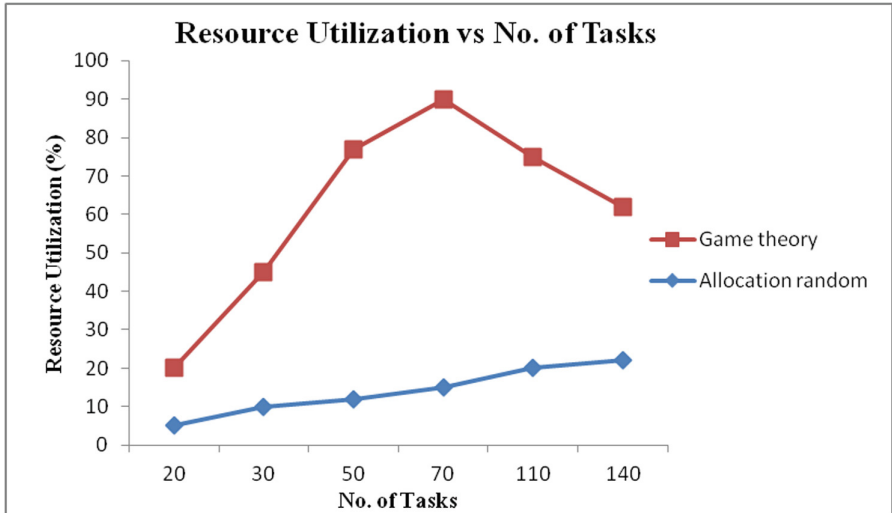


Fig. 5. Resource utilization vs No. of tasks

Figure 6 depicts the congestion rate in % for the tasks scheduled by fog and cloud agencies. The tasks processed with less congestion rate is by fog agency as it routes the high resource cost tasks to cloud through GMA.

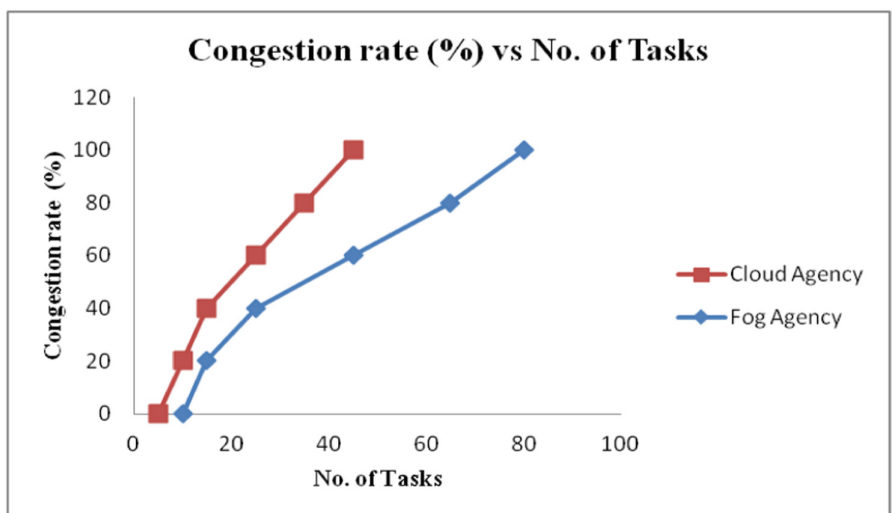


Fig. 6. Congestion rate in % vs No. of tasks

## 5 Conclusion

In this paper the devices/vehicles are provided with services through fog and cloud agency. The resources are managed by considering the fog instances comprising VM. VM are allocated through agencies by using game theory approach to reduce congestion rate and resource allocation time with increased resource utilization.

**Acknowledgements.** The authors are thankful for the college and AICTE for the support in doing the work. The work is funded by AICTE grant for carrying out the project “Resource Management in Internet of Things” Ref. No. File No. 8-40/RIFD/RPS/POLICY-1/2016-17 dated August 02, 2017.

## References

1. Dastjerdi, A.V., Buyya, R.: Fog computing: helping the Internet of Things realize its potential. *Computer* **49**(8), 112–116 (2016)
2. Yi, S., Li, C., Li, Q.: A survey of fog computing: concepts, applications and issues. In: *Proceedings of the 2015 Workshop on Mobile Big Data*, New York, NY, USA, pp. 37–42 (2015)
3. Ketel, M.: Fog-cloud services for IoT. In: *Proceedings of the SouthEast Conference*, New York, NY, USA, pp. 262–264 (2017)
4. Luan, T.H., Gao, L., Li, Z., Xiang, Y., Wei, G., Sun, L.: Fog computing: focusing on mobile users at the edge. [arXiv:1502.01815](https://arxiv.org/abs/1502.01815) Cs, February 2015
5. Yannuzzi, M., Milito, R., Serral-Gracià, R., Montero, D., Nemirovsky, M.: Key ingredients in an IoT recipe: fog computing, cloud computing, and more fog computing. In: *2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pp. 325–329 (2014)
6. Aazam, M., Huh, E.: Fog computing and smart gateway based communication for cloud of things. In: *2014 International Conference on Future Internet of Things and Cloud*, pp. 464–470 (2014)
7. Bao, W., et al.: sFog: seamless fog computing environment for mobile IoT applications. In: *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems - MSWIM 2018*, Montreal, QC, Canada, pp. 127–136 (2018)
8. Gu, L., Zeng, D., Guo, S., Barnawi, A., Xiang, Y.: Cost efficient resource management in fog computing supported medical cyber-physical system. *IEEE Trans. Emerg. Top. Comput.* **5**(1), 108–119 (2017)
9. Sutagundar, A.V., Manvi, S.S.: Wheel based event triggered data aggregation and routing in wireless sensor networks: agent based approach. *Wirel. Pers. Commun.* **71**(1), 491–517 (2013)
10. Aazam, M., Huh, E.: Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT. In: *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*, pp. 687–694 (2015)
11. Xu, X., Yu, H.: A game theory approach to fair and efficient resource allocation in cloud computing. *Math. Probl. Eng.* (2014). <https://www.hindawi.com/journals/mpe/2014/915878/>. Accessed 02 Nov 2018

12. Wang, Z., Xu, W., Yang, J., Peng, J.: A game theoretic approach for resource allocation based on ant colony optimization in emergency management. In: 2009 International Conference on Information Engineering and Computer Science, pp. 1–4 (2009)
13. Nezarat, A., Dastghaibifard, G.: Efficient Nash equilibrium resource allocation based on game theory mechanism in cloud computing by using auction. In: 2015 1st International Conference on Next Generation Computing Technologies (NGCT), pp. 1–5 (2015)
14. Sutagundar, A.V., Manvi, S.S.: Fish bone structure based data aggregation and routing in wireless sensor network: multi-agent based approach. *Telecommun. Syst.* **56**(4), 493–508 (2014)
15. Sutagundar, A.V., Attar, A.H., Hatti, D.I.: Resource allocation for fog enhanced vehicular services. *Wireless Pers. Commun.* 1–19 (2018). <https://doi.org/10.1007/s11277-018-6094-6>



# Various Face Annotation Techniques: Survey

Bhavini N. Tandel and Urmi Desai<sup>(✉)</sup>

Computer Engineering Department,  
Sarvajanik College of Engineering and Technology, Surat, India  
btandell1995@gmail.com, urmi.desai@scet.ac.in

**Abstract.** Basic idea behind the Face Annotation is to detect the facial expression and process further on it for various applications. Techniques of face annotation are used to give an appropriate name to the face image. In this research work, first the face notations are saved in the database and it can be retrieved any time for further processing and then it compares two different images of a same person and finds out whether those images belongs to the same person only. In this paper we described various techniques of face annotation such as Content based, Retrieval based, Search Based, Cluster Based and Caption Based face annotation. Based on the study we present the parametric evaluation of existing techniques.

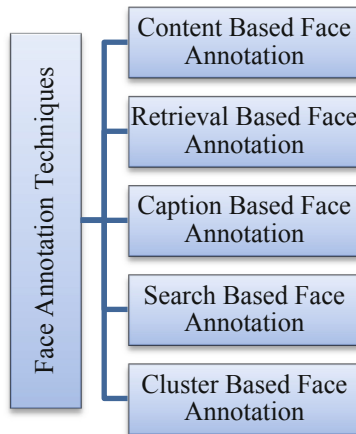
**Keywords:** Face annotation · Face detection · Feature extraction

## 1 Introduction

Now a day's digital data is widely use all over the place and due to the popularity of advances in the web large amount of visual data are created and stored. To extract some useful information or to improve an image, Image first converted to digital form and some image processing operations are performed on it. Digital image Processing techniques help in manipulation of the digital images by using computers. Digital cameras and handheld devices such as phone sticks and mobile phones are growing violently in the present world. Peoples can upload billions amount of pictures in the social sites such as Facebook, Flickr, Picasa web and etc. Most of the images available on the web have practically zero metadata associated with it portraying the semantic idea associated with the image. Metadata include caption, title and other words associated with image which describe the information about the image which used in indexing for image retrieval. To give some caption to the particular image is called Image annotation [1]. Annotation is giving some linguistic information about one or more prospects of image. Huge amount of data i.e. Collection of face images can be managed and organized in the face annotation. On the internet there are many images which are labeled but some of them are not labeled correctly which is called weak labels. On the social media, SBFA perform annotation on weak labeled face images.

The fame of digital cameras and the quick growth of photo sharing social network tools show the number of digital pictures shared by users on the social network via Flickr, Facebook, Icloud, Photo bucket, Google+ and so on. The huge amount of these shared data is human face images. In this shared data some face images are tagged and

some are tagged incorrectly. The automatic face annotation can annotate the face images automatically [2]. In automatic face annotation can automatically detect the face from the photo and give the correct name to the photo which is called face annotation or face tagging. In many applications face annotation is beneficial such as auto face annotation techniques, online photo album management, new video summarization, personal photos, person identification in news videos and family photos etc. [2, 5]. There are various techniques in face annotation such as To get the top most common face images is done in CBIR for a query facial image. In the task of annotation, efficiency and scalability can be improved by the cluster based face annotation. The set of related face images can be regained from the huge database and label them with related name is the main purpose of the RBFA. Assign captions to more than one face image which comprises several names and several faces is done by the caption based face annotation technique. Who is appeared on an image can be find by the captions normally. Achieve relativity high performance without user interaction (Fig. 1).



**Fig. 1.** Various face annotation techniques

Without user interface high performance can be achieved.

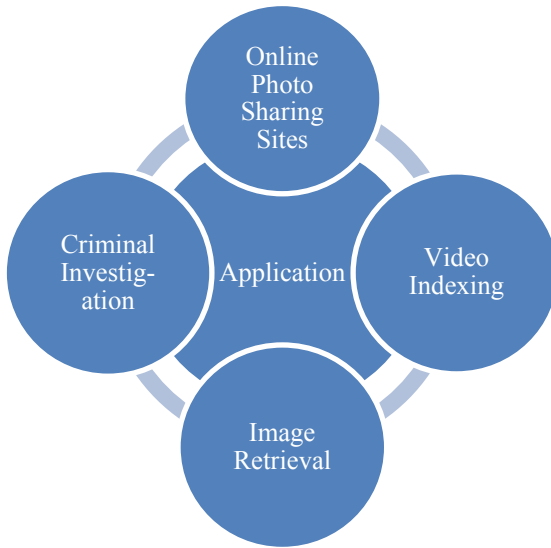
- Annotation of face can be completed at micro and macro scale.
- Face annotation of wild landmark.
- Also used for video domain and online management of photo album.

There are many tasks available on the weak labeled face images by the search based face annotation (SBFA) on the internet. Many marked face photos compared with the traditional datasets are freely offered which is used for search based framework from the internet. The main objective of the face annotation based on the search is to assign the correct label to the query image given. From the database of weak label, top most related face images can be retrieved first to identify the new one image and annotate new face image by taking vote of attendant similar images with label in this framework. In the database many face images are marked as wrong labels are referred as weakly

labeled face image database [4]. One of the challenges faced by SBFA is how to competently feat the shortlisted candidate faces image and their weak labels for the task of annotation [2]. Face Annotation by searching huge scale web face images (FANs) is the one of the example of automated SBFA system. In this system for the given query image, First we get a shortlist of most related face images from the face image dataset and then annotate the query image using sparse representation techniques by extracting the top ranked face images with their corresponding labels [3].

**Application of SBFA**

The following paper is including abstract, introduction, various existing techniques related to face annotation, parametric evaluation of various methods, conclusion of the paper and references (Fig. 2).



**Fig. 2.** Application of SBFA

**2 Existing Methods**

To create face acknowledgment and connected them with facial images face annotation is used. This acknowledgment includes things for example place, person name, date etc. There are various methods are available for face annotations which are discussed below:

**2.1 Search Based Face Annotation**

In [3] search-based face annotation system is presented which is FANs: Face Annotation by Searching huge scale web face images. In this system first we get the top k face images from the large scale web face images from the database and annotate the query image by labels which are associated with top k similar face images. Main challenges of

SBFA are (i) From large facial image database how to efficiently get the most similar top k facial images for a query image and (ii) How to effectively use the shortlist of candidate face images and their weak labels automatically name the faces [3].

The Fig. 3 shows the framework of the FANS system. This framework consists of four modules are which are as follow: (1) The database construction module by collecting web face images. (2) The database indexing module to quickly get the high-dimensional features of faces (3) Retrieval module of content-based facial image to search for the query face images (4) The automated annotation module to name the query image by retrieved similar top k facial images and their equivalent weak labels.

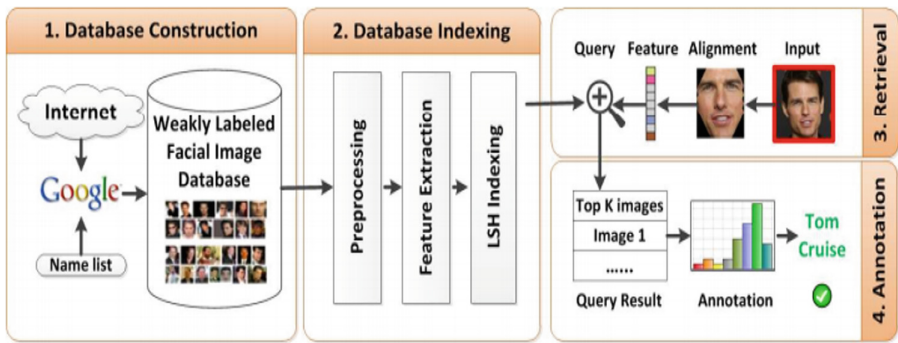


Fig. 3. Framework of FANS system [3]

In the first module, the large set of facial images should be collected from internet which is freely available and some facial images databases are also available on the internet such as LFW and Pubfig. In this system they created their own database because the already available database images are too small in size. In the second module, preprocessing and indexing of image should be carried out. Preprocessing steps include face detection, alignment, representation of facial features and high dimensional indexing. Here for face detection the Viola-Jones algorithm is used to detect face regions. After detection image indexing should be done using DLK algorithm that aligned all the face images to a reliable position in accordance of the positions of feature of face. Extract the GIST descriptor as a facial feature for feature representation. Then, Locality-Sensitive Hashing (LSH) is used for indexing the face features. These two modules are made before you can annotate a facial query image and another two modules are related to the annotation of the query images [3]. In this system they adopt the algorithm of sparse reconstruction, WRLCC [6] to deal with the task of automated annotation of face. To maximize the annotation effectiveness, the query face image is annotated by operating both information of weakly labels and visual contents of top-ranked face images [3].

In [2], they present search based face annotation framework with mining face images that are weakly labeled which can be easily available on the internet. One of the important problems in SBFA performs annotations efficiently by manipulating the list of most related facial images and their weak, often noisy labels. To solve that issue,



they proposed unsupervised label refinement (ULR) machine learning method that corrects the labels of facial images. In order to solve the convex optimization problem they develop effective optimization algorithm. To improve the scalability clustering based approximation algorithm is used [2].

### 2.2 Content Based Face Annotation

The approach of Content Based Image Retrieval (CBIR) can be used to search for and get the more similar images for the input image given in database. This approach indexes images using color, shape and texture. Jiang et al. [7] proposed an approach for automatic face detection using color analysis. In this approach regions of face are detected by adaptive boosting algorithm and for enhancing the confidence in face detection to reduce false positive problem color based face classifier combined with classifier of haar cascade as shown in Figs. 5, 6 and 7.

For AdaBoost haar classifier, it can be classified in three types such as, center-surround, edge and line features. For classifier training, Technique of integral image applied to extract Haar-like features. Face regions are detected by their facial features such as shape, lips, ears, nostril, eye areas and distance between the ellipse and the shape of the region, eyebrows is computed using the Hausdorff distance measure. In the

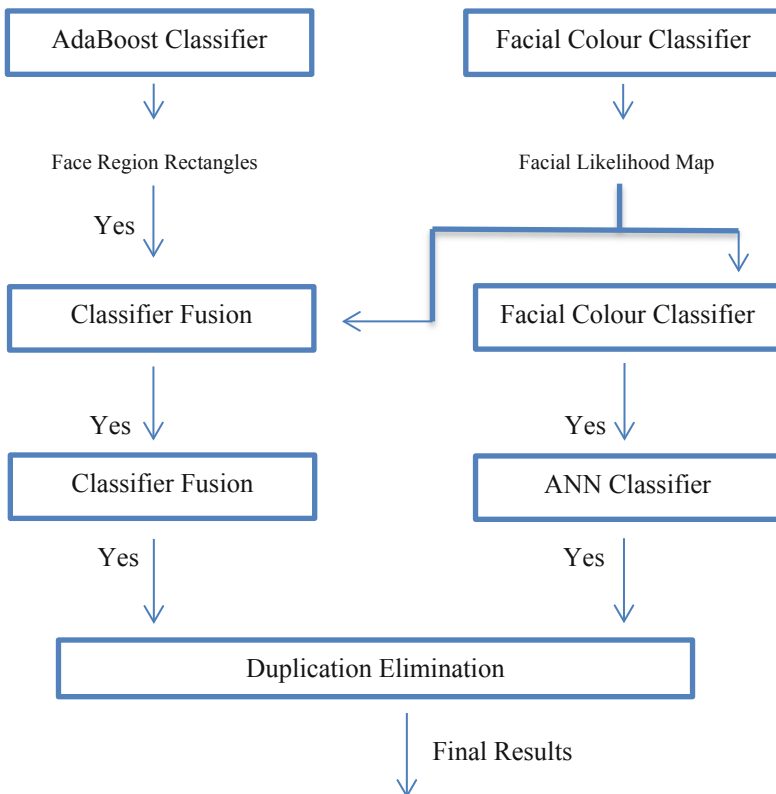
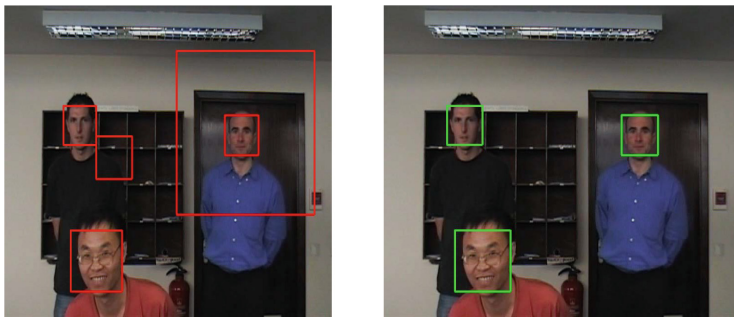


Fig. 4. Face classification scheme [7]

fusion scheme of face detection, The AdaBoost classifier reexamine the detected regions in accordance with the face probability map at level of feature and image. Some areas of the face that are not detected by the AdaBoost classifier are sent to an ANN classifier to check if it is a profile. The classification scheme shown in the Fig. 4.



**Fig. 5.** Colour filtering of face [7]



**Fig. 6.** Detection of false positive [7]



**Fig. 7.** Face detection of side view [7]

### 2.3 Retrieval Based Face Annotation

The RBFA is an effective system for annotation of facial image. Mainly it can be used to extract the huge collection of weakly labeled face images. Wang et al. [6] presented weak label regularized local coordinate coding (WLRCC) annotation method. This framework is applied for retrieval process and face alignment and detection using DLK algorithm. GIST facial feature is extraction for learning and then for performing annotation WLRCC method is applied. Wang et al. [8] presented the scheme of unifying transductive and inductive learning (UTIL) which is the mixture of transductive and inductive learning technique. Classifiers in this framework are trained using weak label laplacian SVM algorithm from weakly labeled data. This frame can correct the UTIL framework. Framework of Retrieval Based Face Annotation (RBFA) consist the following steps: (1) Face images are collected from WWW. (2) Pre-processing and indexing of high-dimensional feature of face images (3) content-based facial image retrieval for a query facial image (4) and WLRCC algorithm for face annotation.

To boost the performance of annotation WLRCC algorithm is used by unified learning scheme to exploits the local coordinate coding (LCC) principle for additional discriminative features to learn and make use of the graph-based regularization for simultaneously enhancing the weak labels [8] (Fig. 8).

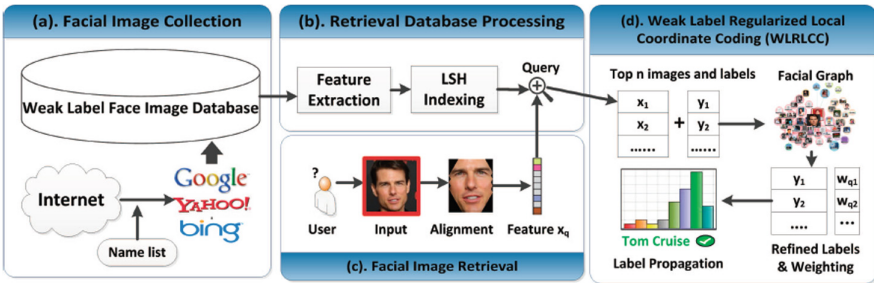


Fig. 8. RBFA framework [8]

### 2.4 Cluster Based Face Annotation

The procedure of grouping a set of examples such a way that examples are more related to each other in the same group than to those in other is generally known as cluster based face annotation. It can be applied in two different levels, such as the image level, which groups all the associated face images in the associated cluster set. The second step is the name level, groups the names into a set of groups in this level.

Adams et al. [9] present a method i.e. Grouper which opens the collection of facial binding frames that can be used to test the framework of annotation. We define a new evaluation metric based on the consistency of this gold standard set to describe the attributes of successful and unsuccessful annotations. This metric takes into account the size, shape and location of the box and false positives and false negatives. Compared to

this gold standard, they examine best methods for consolidating disparate user annotations into a single, accurate bounding box for each face in the image. This method is evaluated based scores for several features of bounding box annotations presented and predict consolidation performance using information gathered from crowd sourced annotations. Grouper can determine that similarity to gold standard and predict recognition performance.

## 2.5 Caption Based Face Annotation

This type of face annotation is mainly used to mention suitable human names to equivalent faces detected in image collection. Guillaumin et al. [10] proposed approaches for labeling the person in the news images with captions. In the first step the similar faces for the queried image person are retrieved from large dataset. In the second step, All persons appearing in pictures are attached with names and using SIFT descriptors feature vectors are calculated and then for finding similarity between the facial features euclidean distance metric is used. Xiao et al. [11] presented a method for naming the images. In this, the method of regularized low rank representation (RLRR) is used to calculate the matrix then supervised structural metric learning (ASML) method is used to create the distance metric and then annotation is obtained using fused affinity matrix (Table 1).

**Table 1.** Comparison of existing face annotation methods

Annotation methods	Preprocessing	Feature Extraction	Which Classifier is used?	Dataset used
Content based method	For face detection Color based Gaussian and for face region Hausdorff distance	AdaBoost and rectangular Haar features	Artificial Neural Network (ANN)	AT & T, 20 side view images, database QMUL for color images Caption
Caption based method	Face and eye detector	Gaussian method & SIFT descriptors	Euclidean	Yahoo! News dataset
Retrieval based method	For face alignment DLK is used	Gabor and GIST	KNN with L2 distance	ADB, WDB, WDB-040K, PubFig
Search based method	For face alignment DLK is used	GIST	KNN	Naming images from IMDB and Images collected WWW
Cluster based method	–	Bounding box, Threshold Parameter	Grouper consolidation	LFW

### 3 Parametric Evaluation

The above table described parametric evaluation of the various face annotation techniques based on the following parameters such as preprocessing of each method, which features are extracted and classifiers used by each technique and databases used by different techniques.

### 4 Conclusion

In this paper we studied the various annotation frameworks for different face annotation techniques which enhance the quality of labels and discover the solution of annotation algorithms. Preprocessing stage can enhanced the accuracy of the methods. Among all the existing techniques, Content based method are giving good result as they implement the multiple features.

### References

1. Zhang, D., Islam, Md.M., Lu, G.: A review on automatic image annotation techniques. *Pattern Recogn.* **45**(1), 346–362 (2012)
2. Wang, D., et al.: Mining weakly labeled web facial images for search-based face annotation. *IEEE Trans. Knowl. Data Eng.* **26**(1), 166 (2014)
3. Hoi, S.C.H., et al.: Fans: face annotation by searching large-scale web facial images. In: *Proceedings of the 22nd International Conference on World Wide Web.* ACM (2013)
4. Sun, Y.-Y., Zhang, Y., Zhou, Z.-H.: Multi-label learning with weak label. In: *Twenty-Fourth AAAI Conference on Artificial Intelligence* (2010)
5. Chang, J.-R., Juang, H.-C.: An effective machine learning approach for refining the labels of web facial images. ACM (2015)
6. Wang, D., Hoi, S.C.H., He, Y., Zhu, J., Mei, T., Luo, J.: Retrieval-based face annotation by weak label regularized local coordinate coding. *IEEE Trans. Pattern Anal. Mach. Intell.* **36**(2), 550–563 (2014)
7. Jiang, R.M., Sadka, A.H., Zhou, H.: Automatic human face detection for content-based image annotation. IEEE (2013)
8. Wang, D., Hoi, S.C.H., He, Y.: A unified learning framework for auto face annotation by mining web facial images. In: *Proceedings of the 21st ACM International Conference on Information and Knowledge Management.* ACM (2012)
9. Adams, J.C., Allen, K.C., Miller, T., Kalka, N.D., Jain, A.K.: Grouper: optimizing crowdsourced face annotations. IEEE (2016)
10. Guillaumin, M., et al.: Automatic face naming with caption-based supervision. In: *IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2008.* IEEE (2008)
11. Xiao, S., Xu, D., Wu, J.: Automatic face naming by learning discriminative affinity matrices from weakly labeled images. *IEEE Trans. neural Netw. Learn. Syst.* **26**(10), 2440–2452 (2015)
12. Pise, B., Pathan, N., Dube, S.: Correct name labelled for search based face annotation. *Int. J. Eng. Comput. Sci.* **5**(12) (2016)



# Cyber Security: A New Approach of Secure Data Through Attentiveness in Cyber Space

Kumar Parasuraman<sup>(✉)</sup> and A. Anbarasa Kumar

Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamil Nadu, India  
kumarcite@gmail.com, anbumtech08@gmail.com

**Abstract.** Cyber Security assumes a critical job in the field of Information and Communication Technology [ICT]. Securing the information has become one of the greatest difficulties in the present day. When we consider cyber security, the main aspect that strikes in our mind is ‘cyber crimes’ which are expanding enormously day by day. Different Governments and organizations are taking numerous measures so as to keep these cyber crimes. Other than different measures cyber security is as yet a big concern to many. This paper for the most part centers around difficulties looked by cyber security on the most recent technologies. It also focuses around most recent about the cyber security methods, ethics and the trends changing the appearance of cyber security. Governments, military, associations, budgetary foundations, colleges and different organizations gather, process and store a great deal of private data on PCs and transmit that data over systems to various PCs. With the tenacious quick advancement of volume and enhancement of cyberattacks, incite attempts are required to anchor touchy business and individual data, and to anchor national security. The paper talk with respect to the idea of the internet and shows how the web is unbound to transmit the mystery and budgetary data. We demonstrate that hacking is as of now typical and dangerous for overall economy and security and exhibited the diverse techniques for Cyber attacks in India and around the globe.

**Keywords:** Cyber security · Cybercrime · Cyberspace · Cyber attacks

## 1 Introduction

Cyber security is the wellbeing of PCs and PC system against unapproved attacks or interruption. Cyber security is described as advances and procedures worked to guarantee PCs, PC equipment, programming, systems and information or data from unapproved get to, vulnerabilities gave through Internet by cyber culprits, gatherings of fear based cyber terrorist and hackers. At home, at work, and at school, our creating reliance on innovation asks for increasingly unmistakable security on the web [1]. Individuals are our country’s first line of insurance in guarding against online dangers. Thus, cybersecurity is a common duty, requiring care and watchfulness from every resident, network, and country.

Cyber security is related to guaranteeing your web and system based mechanized equipment and information from unapproved access and adjustment [3]. Web is by and by not just the wellspring of data and in addition has developed as a medium through which we cooperate, to advance and move our things in various structures, talk with our customers and retailers and do our cash related trades. The Internet offers heaps of favorable circumstances and gives us opportunity to advance our business over the globe in minimum charges and in less human endeavors in constrained capacity to center time.

As Internet was never worked to track and follow the conduct of users. In this paper examined about the issues of cyber security dangers and gathers the current security models. Figure 1 speaks to the principle issues checked on in this paper, which incorporate cyber security workforce, powerlessness examining, email infection sifting, individual data insurance, aversion of cyber wellbeing, and firewall administrations.

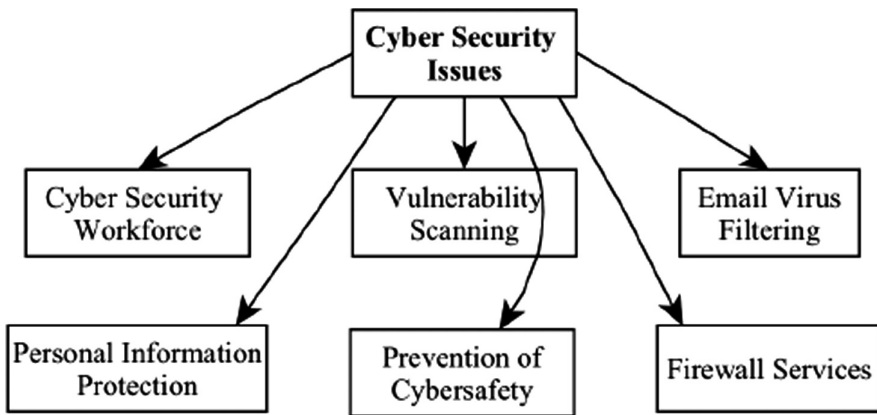


Fig. 1. Issues of cyber security

The Internet was truly worked to interface self-administering PCs for asset sharing and to give a typical stage to network of researchers. As Internet offers from one hand enormous number of favorable circumstances and afterward other hand it likewise gives meet opportunities to cyber-terrorists and hackers. Terrorist affiliations and their supporters are using web for a wide extent of purposes, for instance, gathering information and scattering of it for Terrorist militant reason, enlisting crisp Terrorist, financing attacks and to persuade demonstrations of Cyber Terrorist. Generally used to energize correspondence inside Terrorist gatherings and get-togethers and scattering of data for fear based Terrorist purposes.

## 2 Problem Statement

### 2.1 Importance of Cyber Security

**Who:** Harmful performing artists hope to cause hurt in the internet, for instance, a hacker taking individual information. Liberal performers circumstantially cause mischief to a system, network, or the Internet, for instance, a laborer who unintentionally downloads malware onto their association's system.

**What:** Harmful performing artists abuse the obscurity and vulnerabilities of the Internet using methods that keep running in multifaceted nature from botnets to infections. Kindhearted performers present dangers through basic exercises that can go from tapping on an obscure connect to utilizing a USB drive.

**When:** It is hard to expect when a cyber incidence will occur.

**Where:** Cyberspace, consistently traded with "the Internet," is made by and accessible through PC masterminds that share information and empower correspondence. As opposed to the physical world, the internet has no restrictions crosswise over air, land, sea, and space.

**Why:** Benign performers surprisingly and frequently unknowingly cause hurt while malignant on-screen characters may have an extent of points of view, including searching for classified data or private information, money, credit, renown, or retribution.

There are such huge numbers of dangers in the Internet, some more veritable than others. The dominant part of Cyber criminals is eccentric; they target unprotected PC frameworks at any rate whether they are a piece of an administration organization office, Fortune 500 association, a little private business, or have a place with a home user.

### 2.2 Methodology to Avoid from Cyber Attacks

No citizen, network, or nation is safe to digital hazard, yet there are steps you can take to constrain your risks of an incidence:

1. Set hard passwords, change them consistently or as often as possible, and don't share them to anyone.
2. Keep your OS, program, and other basic programming redesigned by introducing refreshes
3. Maintain an open discourse with your companions, family, and others about Internet security.
4. Use security settings and limit the measure of individual information you post on the web.
5. Be watchful about offers on the web.



**2.3 Cyber Crime Terms and Requirements**

1.	Quick Actions	<ul style="list-style-type: none"> <li>• Check to guarantee the product on the larger part of your frameworks is a la mode</li> <li>• Run an output to guarantee your framework isn't tainted or acting suspiciously</li> <li>• If you find an issue, disengage your gadget from the Internet and play out a full framework reestablish</li> </ul>
2.	In House	<ul style="list-style-type: none"> <li>• Disconnect your device (PC, Play station, tablet, etc.) from the Internet. By impairing the association from Internet, you shield an attacker or infection from having the ability to get to your PC and perform undertakings, for instance, discovering individual in-arrangement or individual information, controlling or eradicating records, or using your device to attack others</li> <li>• If you have hostile to infection programming introduced on your device, refresh the infection definitions and play out a manual output of your entire systems. Introduce the majority of the appropriate patches to settle known vulnerabilities</li> </ul>
3.	In Office	<ul style="list-style-type: none"> <li>• If you approach an IT division, connect with them expeditiously. The sooner they can investigate and clean your PC, the less harm to your PC and diverse PCs on the systems</li> <li>• If you believe you may have uncovered touchy data or information about your association, report it to the best possible people inside the association, including framework administrator. They can be alarm for any suspicious or unusual development</li> </ul>
4.	Institutions, college, etc.	<ul style="list-style-type: none"> <li>• Immediately educate an, instructor, or workforce or staff in control. On the off chance that they approach an IT department, contact them immediately</li> </ul>

**2.4 Nature of Cyberspace**

Cyber space is an interactive area comprised of digital networks that is utilized to store, adjust and communicate data. It incorporates the internet, yet additionally the other information system that help our organizations, infrastructure and services. The internet is virtual space that use equipment and electric currents or fields range to store, trade and exchange information utilizing sorted out system and concerned physical structure. It is unimportant where communication and web related activities happen [11]. The internet is nonexistent where means to contain things is either existing or depiction of world. That is completely virtual condition wherein information exchange and correspondence happens that partners about 2.8 billion people far and wide to give a typical stage to share considerations, points of view, organizations and fellowship. It is stretch and no limit in nature and growing mightily without consider any political periphery.

Cyberspace is widespread, interconnected digital technology. The term entered the mainstream culture from science fiction and expressions of the human experience however is presently utilized by technology strategists, security experts, government, military and industry developers and business visionaries to portray the area of the

worldwide environment. Others view the cyberspace as only a notional situation in which communication over PC systems happens. At the point when the employments of the Internet, networking, and digital communication were all developing significantly and the expression “cyberspace” had the capacity to express to the numerous new thoughts and wonders that were rising.

### 3 Objectives of Cyber Security

Cybersecurity is by and by considered as indispensable bit of individuals and families, and furthermore associations, governments, instructive establishments and our business. It is fundamental for families and watchmen to security the youths and relatives from online extortion [4]. To the extent cash related security, it is critical to anchor our money related information that can impact our very own budgetary status. Web is crucial and gainful for workforce, understudy, staff and instructive organizations, has gave loads of learning openings with number of online dangers. There is fundamental requirement for web clients to perceive how to insurance themselves from online extortion and data fraud. Appropriate getting some answers concerning the online conduct and System assurance results decline in vulnerabilities and increasingly secure online condition. Little and medium-sized associations in like manner practice distinctive security related challenges due to limited assets and legitimate Cyber security aptitudes [8]. The brisk improvement of progressions is also making and making the Cyber security even more troublesome as we don't present perpetual answers for concerned issue [9].

Despite the fact that, we are successfully battling and acquainting diverse systems or advances with secure our System and information yet these giving assurance for transient as it were. Regardless, better security understanding and reasonable methodology can assist us with ensuring protected innovation and competitive advantages and decrease budgetary and notoriety misfortune.

The state and adjacent governments hold sweeping proportion of data and private records online in computerized frame that breezes up fundamental concentration for a Cyber attack. The greater part of time governments confront troubles on account of unacceptable foundation, nonattendance of mindfulness and adequate financing. It is fundamental for the legislature to give reliable organizations to society, keep up resident to-government correspondences and security of mystery information or data.

In the course of recent years, pros and policymakers have conveyed extending stresses over shielding ICT Systems from Cyber attacks—deliberate endeavors by unapproved people to get to ICT System, as a rule with the objective of robbery, disturbance, harm, or other unlawful activities. A few specialists expect the number and earnestness of Cyber attacks to increase all through the accompanying a couple of years. The Performance of securing ICT System and their substance has come to be known as cybersecurity. A wide and potentially to some fluffy idea, cybersecurity can be a profitable term anyway will all in all restrict correct definition. It ordinarily alludes to one of three things:

A ton of exercises and diverse appraisals wanted to anchor—from attack, disturbance, or distinctive dangers—PCs, PC Systems, related equipment gear and gadgets

programming and the information they contain and convey, Including programming and other data, furthermore unique segments of the internet.

1. The state or nature of being shielded from such dangers.
2. The wide field of undertaking went for actualizing and upgrading those exercises and quality.
3. It is related to anyway not generally saw as indistinguishable to the idea of data security.

The ensuring data or information and data System from unapproved get to, use, divulgence, disturbance, change, or decimation so as to give:

**(a) Integrity**

Which includes guarding against ill-advised information change or obliteration, and consolidates guaranteeing data non-denial and genuineness.

**(b) Confidentiality**

Which includes safeguarding approved limitations on access and exposure, including recommends for anchoring singular insurance and elite information.

**(c) Accessibility**

Which includes anchoring reasonable and dependable access to and utilization of information.

Cybersecurity is in like manner now and again conflated inappropriately out in the open exchange with various thoughts, for instance, security, information sharing, insight get-together, and observation. Protection is connected with the limit of a person to control access by others to information about that distinct individual. Consequently, great cybersecurity can help secure assurance in an electronic domain, yet information that is shared to help cybersecurity exercises may every so often contain singular information that likely a few onlookers would view as private. Cybersecurity can be a technique for anchoring against undesired observation of and social occasion of insight from a data System. However, when gone for potential wellsprings of Cyber attacks, such occasions can in like manner be important to help affect cybersecurity. Likewise, surveillance through checking of data stream inside a system can imperative segment of cybersecurity.

## 4 Internet Usage in India

The statistics given data how many of them are using internet in India from 2015 onwards. In the year of 2018, India had 500 million people using internet in Mobile, Smart Phones, Laptop, Tablets etc. The anticipated to develop to 635.8 million web clients in 2021. In spite of the vast base of web clients in India, only 36% of the Indian populace got to internet in 2015. This is a huge increment in the comparison to the past years, considering the web infiltration rate in India remained at around 10% in 2011. Furthermore, men overwhelmed web utilization with 71% to womens 29%. India as of now is the second-biggest online market around the world. The dominant part of India's web clients are cell phone web clients, who exploit modest options in contrast to costly landline associations that require work area PCs and foundation.

## 5 Importance of Cyber Crime

Cybercrime implies criminal exercises including web, PCs or some other between associated framework. The term that covers wrongdoings like phishing, charge card fakes, illicit downloading, modern undercover work, tyke sex entertainment, tricks, digital fear based oppression, creation and additionally dissemination of infections, Spam, etc. Cybercrime amazingly influences people, organizations, and national security because of the commonness of the Internet [2]. Numerous nations should cooperate and utilize legitimate, authoritative, and mechanical strategies to battle cybercrime. To diminish the harm to basic foundations. To anchor the Internet from being mishandled [5]. “The modern thief can steal more with a personal computer than with a gun. Tomorrow’s terrorist may be capable to do more damage with a keyboard than with a bomb”.

### 5.1 The Main Causes of Cyber Crime

#### 5.1.1 Cyber Stalking

It is using the Internet to bug another person; the term is used in this reaction to allude to the usage of the Internet, email, or other electronic specialized gadgets to stalk someone else. Stalking as a rule incorporates badgering or compromising conduct that an individual takes part in monotonously, for instance, following an individual, execution at an individual home or place of business, making provocation phone calls, leaving created messages or questions, or vandalizing an individual’s property. If someone uses the Internet to irritate, undermine, or threaten someone else, the offender is liable of Cyber stalking [6]. The most evident precedent is sending compromising email. Regardless, a great rule is that email’s substance would be seen as compromising in ordinary discourse, it will probably be seen as a danger at whatever point sent electronically. Distinctive instances of Cyber stalking are less clear. In case you request that someone quit messaging you, yet they continue doing all things considered. Unfortunately, there is no sensible answer on that issue. Actually it might possibly be consider as a wrongdoing, contingent on such factors as the substance of the messages, the recurrence, the earlier connection among you and the sender, and your purview.

#### 5.1.2 Intellectual Property Theft

The Intellectual property is depicted as an advancement, new research, technique, model and equation that have a financial esteem. Licensed innovation is secured with having licenses and trademarks and with the copyright on recordings, accounts and music too. It is solid that showcase confidences and inside business data are amazingly attacked assets for any association [13]. This business information might be in various structures, for instance, future thing plan, client records and value records and so forth the web is the as often as possible used medium to energize the Intellectual property robbery since it is definitely not hard to cover the personality on system.

#### 5.1.3 Salami Attack

In the salami Cyber attack, Cyber culprits and aggressors take money little sum from many ledgers to make an immense sum. The change ends up being unimportant to the

point that in a solitary case it is hard to take note. Expect, a bank representative makes a program into keeping money programming, that diminishes an inconsequential measure of money (state Rs. 2 consistently) from the record of each client [14]. It is general regard that no client will no doubt see this unapproved conclusion, anyway it will be valuable to digital offenders that benefit.

#### **5.1.4 E-Mail Bombing**

It is sending of huge measure of messages to a concentrated on distinctive individual. A great deal of messages fundamentally top off the beneficiary's inbox on the server or, sometimes, server advances toward getting to be neglect to get such huge sum information and quits working. There are various ways to deal with make an email bomb like "zombie" or "robot" which are fit to send persistent thousands or even a huge number of messages to beneficiaries' email address. Email is attacking and email flooding, both the terms are used conversely and speak to similar marvels. It is said email bombarding as the beneficiary's inbox gets topped off with huge number of undesired sends and the concentrated on unique individual does not end up ready to get extra vital messages.

#### **5.1.5 Phishing**

One of the more typical ways to deal with achieve wholesale fraud is through a technique called phishing, which is the path toward endeavoring to provoke the target to give you singular information. For instance, the aggressor may pass on an email demonstrating to be from a bank, and telling beneficiaries that there is an issue with their ledger. The email at that guides them to tap on a connection to the bank site where they can login and check their record. Regardless, the connection really goes to a phony sites set up by the aggressor [12]. Right when the target goes to that site and enters his information, he will have quite recently given his username and secret word to the aggressor. Many end clients today think about these sorts of systems and abstain from tapping on email joins. Be that as it may, not every person is so sensible, and this attack still is viable. It is also the circumstance that the assailants have thought of methodologies for phishing. One of these techniques is called cross-site scripting. If a site enables clients to post content that diverse client can see, the aggressor at that point posts, yet rather than posting an audit or other genuine substance, they post a content. By and by when diverse clients visit that site page, instead of stacking a survey or remark, it will stack the aggressor's content. That content may do any number of things, anyway for the most part for the content to divert the end client to a phishing site. On the off chance that the assailant is shrewd, the phishing site is by all accounts indistinguishable to the certifiable one, and end clients don't realize they have been diverted. Cross-webpage scripting can be anticipated by web designers clearing up all client input.

#### **5.1.6 Identity Theft**

Identity Theft is a creating issue and a to a great degree exasperating one. The thought is so basic, anyway the procedure can be intricate, and the ramifications for the unfortunate casualty can be exceptionally outrageous. The musing is only for one distinct individual to go up against the character of another. This is normally endeavored to make purchases;

in any case, misrepresentation ought to be feasible for various reasons, for instance, getting charge card's in the unfortunate casualty name, or considerably driver's licenses. If the culprit gets a charge card in someone else's name, he can purchase items and the casualty of this extortion is left with commitments she didn't think about and did not approve. Because of getting a driver's permit in the unfortunate casualty's name, this extortion might be endeavored to shield the culprit from the outcomes of his or her own poor driving record. For instance, a unique individual may move your driving information to make a permit with his or her own image. Possibly the criminal for this circumstance has a terrible driving record and even warrants out for speedy capture. Should the distinctive individual be ceased by law authorization officers, the individual would then have the capacity to exhibit the phony permit. Right when the cop checks the permit, it is genuine and has no excellent warrants. Nevertheless, the ticket the criminal gets will go on your driving record, since it is your data on the driver's permit. It is likewise impossible that the culprit of that extortion will truly pay the ticket, so prior or later you—whose personality was stolen—will get see that your permit has been dropped for inability to pay a ticket. But in the event that you would, have the capacity to demonstrate, with observers, that you were not at the region the ticket was given at the time it was given, you may have no reaction yet to pay the ticket, in order to reestablish your driving benefits.

### **5.1.7 Spoofing**

It demonstrates to a system to have unapproved access to PCs, whereby culprit sends messages to a sorted out PC with an IP address. At the beneficiary end it gives the idea that messages are being transmitted from a mindful source. To lead IP satirizing, a programmer first makes endeavor to find a trusted in host IP address and after that change and alteration of parcels are done to exhibit that the bundles are being made shape unique host.

### **5.1.8 Worms, Trojan Horses, Virus**

A PC infection needs another medium to transmit. Further, the PC infection turns out to be incredible exactly when it joins itself with a pernicious program or executable archives. When we run or execute these strong records then infection leaves its disease. In the field of software engineering, the degree that we know the infection age isn't trademark wonders. It for each situation needs human exercises to get augmentation. The nearness of infection in your framework does not hurt PC until its related executable documents or program run. A worm and infection both the terms used proportionally however there is physical contrast as worm don't require solid connected documents while infection requires. Nearness of worm in framework alone can influence the execution of your framework. It requires no human activity. The Trojan Horse, at first look shows up as valuable programming anyway harm PC and its item as it gets introduced on. A couple of Trojans make auxiliary entry for noxious clients to control your PC remotely, approving private and individual data Theft.

### **5.1.9 DoS and DDoS**

A denial of service (DoS) attack alludes an endeavor to make PC, server or system assets out of reach to its affirmed clients typically by using briefly interference or

suspension of administrations. A Distributed Denial of Service (DDoS) attacks recommends a DoS attacks that spreads from more than one infected systems. With pernicious programming meanwhile [10]. These infected systems are overall called as “botnets” that control the goal infected systems.

### 5.1.10 Pornography

The pornography is very difficult and it doesn't have any correct depiction according to law as each nation has their very own customs and tradition. The action of pornography in a few nations is legal however in some it is illegal and punishable. It is characterized as the demonstration of utilizing the internet to make, show, circulate, import, or distribute erotic entertainment or indecent materials. With the methodology of the internet, customary explicit substance has now been to a great extent supplanted by online/Cyber pornographic content. Pornography has no legal or steady definition. The pornography depends how the society, norms and their values are responding to the pornographic content.

## 5.2 Growth in Cyber Crime

Countless by and by have been motorized and now less requesting to manage the help of data innovation. By and by, scarcely any piece of society remains unaffected. Prior to the complete of 2018, over 2.8 billion people are using web worldwide while 4.5 billion still ought to be associated. By and by, our lives look defective without web, mobiles and PCs. Records are kept up cautiously and traded on correspondence lines. Banks and other budgetary organizations in like manner use web and associated system to finish cash related trades [7]. So it winds up vital to anchor our system from treats and hacking. As shown by report around 1,00,000 infections/worms are educated for to be dynamic consistently and out of which 10,000 are distinguished as new and one of a kind. Insights spoke to in the Table 1. demonstrate that Cyber crime cases developing step by step in our day by day life.

**Table 1.** Rises in cyber crimes

Cyber crime	2018	2017
Online Banking	2095	1343
Facebook Related	316	151
Email Hacking	125	97
Lottery Fraud	42	15
Data Theft	47	43
Job fraud	49	40
Twitter Related	12	4
<b>Total cases</b>	<b>3474</b>	<b>2402</b>

Internet Security Thread Report include 2018 as the time of Mega Breach. In this year add up to number of ruptures was around 64% which was greater than in 2017 with 257 breaks. So also, more noteworthy than in 2016 with 207 ruptures. Regardless of whether, 2018 was the year in which eight ruptures uncovered more noteworthy than 12 million personalities however in 2017 only a one break was gifted to uncover about a comparative number of characters. In 2018, around 557 million characters were broken that has exchanged monetary and charge card data, date of birth, contact number and IDs into criminal hands. Commonly, Cyber attackers search for helplessness in valid sites to have control to malevolent programming.

### 5.3 Cyber Crimes in India

By virtue of cybercrime, huge number of appropriate targets may ascend through extending time spent on the web, and the use of online administrations, for instance, keeping money, shopping and document sharing making clients slanted to phishing attacks or extortion. The major Cyber crime declared in India are denial of web service, hacking of websites, PC virus and worms, Pornography, Cyber squatting, Cyber stalking and phishing. Right around 71% of data robbery is finished by current and ex-workers and 29% by programmers. India needs to go far in anchoring the imperative data [15]. As demonstrated by Symantec’s (American Global Computer Security Software Corporation) web security danger report, India has seen a 280% development in bot diseases that is continuing to spread to a greater number of rising urban territories in India. India has the most noteworthy proportion in the realm of active spam or garbage mail of around 282 million consistently around the globe. India’s home PC proprietors are the most centered around region of Cyber attacks. Mumbai and Delhi ascending as the primary two urban regions for Cybercrime.

1. Continuous Hacking website by cyber criminals
2. Stealing the Data and Information
3. Growing phishing attacks on Ecommerce and Financial Websites
4. Cybercriminals directing Social and Expert Systems
5. Dangers are directed at Mobile Platform: Smartphones and Tablets.

**Table 2.** Cyber crime growth in India

Year	Cases registered under IT Act	Person arrested
2014	966	799
2015	1791	1184
2016	2876	1522
2017	4356	2098

Rate of Cyber Crimes (Information Technology Act + Indian Penal Code Sections) expanded by 59.1% in 2018 when contrasted with 2017 (from 2,213 of every 2017 to 3,477 out of 2018). Cyber Fraud represented 47.9% (292 out of 621) and Cyber Forgery represented 43.1% (269 out of 621) were the primary cases under IPC



classification for Cyber Crimes. 64.0% of the guilty parties under Information Technology Act were in the age group 18–30 years (958 out of 1,633) and 58.2% of the guilty parties under Indian Penal Code Sections were additionally in the age groups 18–30 years (258 out of 589). As indicated by Indian Ministry of Communications and Information Technology, around 79 government websites were hacked and 17,021 security occurrences scanning, spam, malware infection, denial of service and system break-in including that of Government, Defense and public sector undertakings were reported up to June, 2014.

The number of security breach incidents remained at 14,023 of every 2017 and 23,789 out of 2018. As per Indian Computer Response Team (CERT-In) a total number of 312, 371 and 79 government websites were hacked within the years 2017 and 2018 (up to June). Statistics represented in the Table 2 show that cyber crimes are promptly growing in numbers and difficulty as well. We still need a method or procedure to control cyber crimes. As the statistics of the arrested people show that there is a huge gap between cases recorded and the person arrested. It means we are not success and arresting all the criminals who commit such kinds of cybercrimes.

## 6 Conclusion

In this paper, we have illuminated about the idea of the internet and described the Cyber security with its necessities everywhere throughout the world. Vital insights exhibit that India stays on third position in the utilizing of web and besides encountering the issues of Cyber security. We have furthermore illuminated distinctive methods for Cyber attacks and showed how the sites hacking occasions are ordinary and creating with time the world over. From the audit, it was uncovered that larger piece of the examinations has been directed on the Cyber Stalking, Intellectual Property Theft, Salami Attack, E-Mail Bombing, Phishing, Identity Theft, Spoofing, Worms, Trojan Horses, Virus, DoS and DDoS and Pornography. Nonetheless, not very many examinations from the perspective of secret phrase security. There are general suggestions on the most ideal approach to anchor the secret key yet no confirmed convention to anchor the framework normally. Along these lines, there is a need for more examinations to the extent techniques and models from this point of view to affirm that passwords are secured.

## References

1. Aggarwal, P., Arora, P., Neha, Poonam: Review on cyber crime and security. *IJREAS* **02**(01), 48–51 (2014)
2. Yassir, A., Nayak, S.: Cybercrime: a threat to network security. *IJCSNS Int. J. Comput. Sci. Netw. Secur.* **12**(2), 84 (2012)
3. Tonge, A.M., Kasture, S.S., Chaudhari, S.R.: Cyber security: challenges for society-literature review. *IOSR J. Comput. Eng. (IOSR-JCE)* **12**(2), 67–75 (2013)
4. Catlett, C. (ed.): A scientific research and development approach to cyber security. Report submitted to the U.S. Department of Energy, December 2008

5. Rane, S.V., Choudhary, P.A.: Cyber crime and cyber law in India. *Cyber Times Int. J. Technol. Manage.* **5**(2) (2012)
6. U.S. Department of Justice: Cyberstalking: a new challenge for law enforcement and industry — a report from the Attorney General to the Vice President. U.S. Department of Justice, Washington, D.C., pp. 2, 6, August 1999
7. Richards, J.: Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators, pp. 21–54. CRC Press, Boca Raton (1999)
8. Sharma, R.: Study of latest emerging trends on cyber security and its challenges to society. *Int. J. Sci. Eng. Res.* **3**(6), 1 (2012). ISSN 2229-5518 IJSER © 2012
9. Saxena, P., Kotiyal, B., Goudar, R.H.: A cyber era approach for building awareness in cyber security for educational system in India. *IACSIT Int. J. Inf. Educ. Technol.* **2**(2), 167 (2012)
10. Jaideep, G., Battula, B.P.: Detection of spoofed and non-spoofed DDoS attacks and discriminating them from flash crowds. *EURASIP J. Inf. Secur.* **9** (2018). <https://doi.org/10.1186/s13635-018-0079-6>
11. Casey, E.: *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, pp. 5–19. Academic Press, London (2011)
12. Khonji, M., Iraqi, Y.: Phishing detection: a literature survey. *IEEE Commun. Surv. Tutor.* **15** (4), 2091–2121 (2013)
13. Dalla, Er.H.S., Geeta, Ms.: Cyber crime – a threat to persons, property, government and societies. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **3**(5), 997–1002 (2013)
14. Raiyn, J.: A survey of the cyber attack detection strategies. *Int. J. Secur. Appl.* **8**(1), 247–256 (2014)
15. Kandpa, V., Singh, R.K.: Latest face of cyber crime and its prevention in India. *Int. J. Basic Appl. Sci.* **2**(4), 150–156 (2013)



# Algo\_Seer: System for Extracting and Searching Algorithms in Scholarly Big Data

M. Biradar Sangam<sup>1</sup>, R. Shekhar<sup>1</sup>, and Pranayanath Reddy<sup>2</sup>(✉)

<sup>1</sup> Department of Computer Science and Engineering,  
Alliance University, Bangalore, India  
smbiradar14@gmail.com, shekhar.r@alliance.edu.in

<sup>2</sup> Department of Computer Science Engineering,  
KLH University, Hyderabad, India  
pranay\_taj@yahoo.co.in

**Abstract.** Algorithms are the crucial and important part for any research and developments. Algorithms are usually published in the scientific publications, journals, conference papers or thesis. Algorithms plays important role especially in the computational and research areas where the researchers and developers look for the innovations. Therefore there is need for a search system which automatically searches for algorithms from the scholarly big data. Algo\_Seer is been proposed as part of CiteSeer system which automatically searches for pseudo codes and algorithmic procedures and performs indexing, analysis and ranking to extract the algorithms. This work proposes a search system Algo\_Seer which utilizes a novel arrangement of procedures such as rule based method, machine learning methods to recognize, separate and extract the calculated algorithms from the academic reports. Particularly mixture troupe machine learning systems are utilized to obtain the efficient results.

**Keywords:** CiteSeer · Algo\_Seer · Pseudo codes · Algorithmic procedures · Troupe machine learning · Rule based method

## 1 Introduction

Algorithms are used in most of the research and computational fields for modeling and implementing various research works. Algorithms are the integral part for the new developments. Algorithms are published in the scholarly big data by scholars especially in computational sciences and related fields. These algorithms are used by the developers and researchers for their work. Therefore searching such algorithm for the research and development and extracting them is crucial task. To enable the searching and extraction of such algorithms from increasingly large collection of data and digital documents; indexing, searching and analysis of algorithms is used. Indexing is nothing but a procedure to systematically arrange the documents extracted from the scholarly articles, journals and publications and also indexing is done for the various language algorithm and pseudo code extraction like C, C++ and other languages. Then the ranking is done for prioritizing the documents for the easy extraction of the relevant

algorithms for the researches and developments. For indexing process Apache SOLR indexing method can be used.

Algo\_Seer is an efficient search engine which is been introduced as a part of CiteSeer with the motive to investigate the large and effective set of algorithms from the scholarly big data in order to provide the researchers a large algorithm data base. The work proposes inform all set of scalable techniques and approaches used by the Algo\_Seer to search and extract the algorithms from heterogeneous pool of big data. Also a hybrid machine learning approach is used to discover the algorithm representation from scholarly articles and digital documents. An essential number of scholarly articles in computer science and related research areas developed by the researcher contain high-quality algorithms.

This work also represents an efficient survey of the various search engines used for searching, extracting and analyzing the algorithms such as Tab\_Seer, Ack\_Seer, Collab\_Seer, Algorithm\_Seer, and Chem\_Seer. These search engines are introduced as a part of the CiteSeer engine which is an efficient search engine used for extraction and annotation of the algorithms from the digitally published documents.

## **2 Related Work**

In this work two major sections have been discussed which are document element extraction from the scholarly big data and search engines used to extract the information from the scholarly documents.

### **2.1 Document Element Extraction from the Documents**

This work extensively studies about the searching and extraction of the document elements such as tables, figures, formulae, algorithms expressions from the scholarly big data. Image processing and Optical character recognitions methods can also be used for extraction of data elements and text blocks from the two dimensional image [9].

Therefore to make search for such data elements from the documents several methods are also been discussed in this work such as rule based methods, machine learning methods and the hybrid methods to extract the pseudo codes and the algorithmic procedures from the documents. Documents elements are identified to extract the Pseudo codes and Algorithmic procedure by the presence of captions in the documents and using the set of regular expressions.

### **2.2 Search Engines for the Scholarly Information**

This work also discusses the different search engines used for searching, extracting and analyzing the documents entities such as chemical formulae, expressions, algorithms, pseudo codes, mathematical formulae, tables and figures etc. these search engines could be Algorithm\_Seer, Tab\_Seer, Chem\_Seer and many. These search systems are being implemented as part of Cite\_Seer system which is an efficient search engine for the search and extracting the documents from the scholarly big data. These search engines

used the methodologies like indexing, similarity measurements, ranking of algorithms to extract the documents entities.

### 3 Need of Search Engine for Algorithms

Computational science and related disciplines are into developing, analyzing, applying the algorithms to their work. Thus such field needs an efficient algorithm to implement their work. There are also certain ways to extract the algorithm such as either developer will write the algorithm or search for algorithms in unrelated engines thus there is need to provide an efficient search engine which will allow the searcher to extract the algorithm from the scholarly bug data.

Advanced problems in different disciplines even non-computational engineering which need efficient solutions require transforming the problems into algorithmic solutions on which the standard algorithms can be applied. Thus the standard algorithms are collected from the different sources such as text books, encyclopedias, Wikipedia's and websites which provide the references for the algorithms for their research work. It is found that roughly 1,765 standard algorithms were cataloged when the Wikipedia were parsed for algorithm pages published in 2010.

There for searching for such algorithms manually is a trivial task for the developers. Researches, developers and others who goals to discover the efficient and appropriate algorithms would have continuously make search and keep eye on relevant publications in their related fields of study to keep themselves updated to the new releases. This problem of searching algorithms in big data is worst for the new developers, who are inexperienced in the fields and not aware of documents to be searched. Therefore there is ideally need for one search engine which automatically search for the algorithms of request and extract them from the huge set of scholarly documents and also from the new publications. Such a system could prove to support algorithm indexing, searching, and a wide range of potential knowledge discovery applications and studies of the algorithm evolution, and presumably increase the productivity of scientists.

### 4 Types of Algorithm Representation

The algorithms published in the various publications and the digital documents can be represented in two ways, which allow the researchers and the developers to extract the algorithms easily from the big data [7].

1. Pseudo Codes (PC's)
2. Algorithmic Procedures (AP's)

Identifying and extracting the algorithms from scholarly big data is an active area of research for the researchers. For algorithm discovery in digital documents, Bhatia, et al., have described a method for automatic detection of pseudocodes (PCs) in Computer Science publications [1].

Each of the pseudo codes are searched from the documents with the help of captions they are accompanied. The pseudo codes accompanied by the caption are

identified by set of regular expressions. However this approach is limited coverage due to reliance of captions in the documents for the pseudo codes and wide variations in the writing format followed by various journals and authors. It is found that in most of the documents and journals the pseudo codes were seen not accompanied by the caption remain undetected by the approaches and also even though pseudo codes are commonly used in scientific documents to represent algorithms [5]. Majority of algorithms are represented as algorithmic procedures which are published in the journals and publications but vary in their presentation in following ways.

- **Writing Style:** Pseudo codes found in the documents are written in programming style, with no details of the algorithms. Symbols, Greek letters, method names, programming keywords are used write the pseudo codes in the documents. On the other way round algorithm procedures are written in a listing style, in descriptive manner. Every step for algorithm procedure is written in step by step either in points or as numbers. Algorithmic Procedures have limited power to express critical nested loops and are less concise than Pseudo Codes, but they are easier to express and understand by common people who lack in programming knowledge and not aware of technical aspects.
- **Location in the document:** pseudo codes may appear anywhere in the documents, they are not part of running text. Therefore most pseudo codes have identifiers to refer to the pseudo codes. These identifiers may be captions, function names, method names used in the pseudo codes and name of the algorithms directly. Algorithmic procedures on other hand appears as a part of running text and do not have and identifiers hence they require different techniques to identify them in the documents.

## 5 Literature Survey

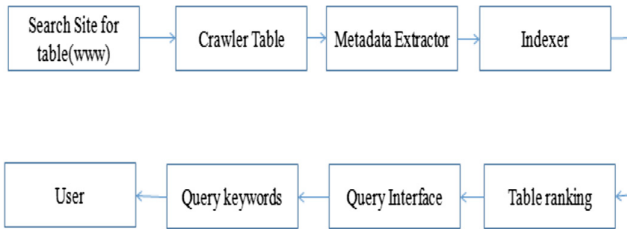
The process of building and analysis of algorithms and data structures is a basic and very important part of modern computational environments. Therefore extraction and searching of related and efficient algorithm is needed in all the research fields. To extract such algorithms many search engines have been studied and implemented for various fields such as

- Hirschberg's algorithm broadly used algorithm in bioinformatics, it is used find maximal global alignments of DNA and protein sequences [11].
- In stock portfolio optimization algorithms are used for diversifying search results in information retrieval systems.
- In the industrial design disciplines, the Latent Dirichlet Allocation is effectively used to identify notable product features [2].

Several search systems are used to search for the algorithms and pseudo code from the scholarly big data. This scholarly big data contain the documents, articles, conference papers, books, thesis and journal published for the recent researches.

## 5.1 TAB\_Seer

TAB\_Seer is a search system used to search for the different tables in the documents. Tables usually contain the test results. This search engine will extract the table's metadata, indexes and ranks the table data [10]. The following figure shows the architecture for the TAB\_Seer system (Fig. 1).



**Fig. 1.** Architecture of TAB\_Seer

The table crawler will search for the documents with tables to extract the result table for algorithms. Then the metadata extractor will extract those tables which consists of three parts text information stripper which strips out text information from PDF source and others are table box detector, table environment metadata, table frame metadata, table affiliated metadata, table layout metadata, table type metadata, table cell-content metadata are the six categories of the Table metadata [10]. The table metadata contains the information for where the table is located in the document. Table affiliated data includes table caption, table caption position, table footnote, table reference text. The table layout meta data helps to capture the correct table from the document for the algorithm search.

## 5.2 Collab\_Seer

Collab\_Seer searches for collaborators based on co-author network. It uses three vertex similarity measures they are jaccard similarity, cosine similarity and relation strength similarity. This method uses the social network strength to identify the various collaborators using the strength similarity matrix [3]. Lexical similarity is used to identify the researcher's interests for the different research work. The system consists of five components they are co-author information analyzer which retrieves data from Cite-Seerx dataset, get a co-author network, vertex similarity to analyze the network structure, key phrase extractor to extract key phrases of each article, lexical similarity integrates authors to the key phrases and the similarity integrator concatenates indexed vertex similarity score and indexed lexical similarity score to calculate collaborate recommendation (Fig. 2).

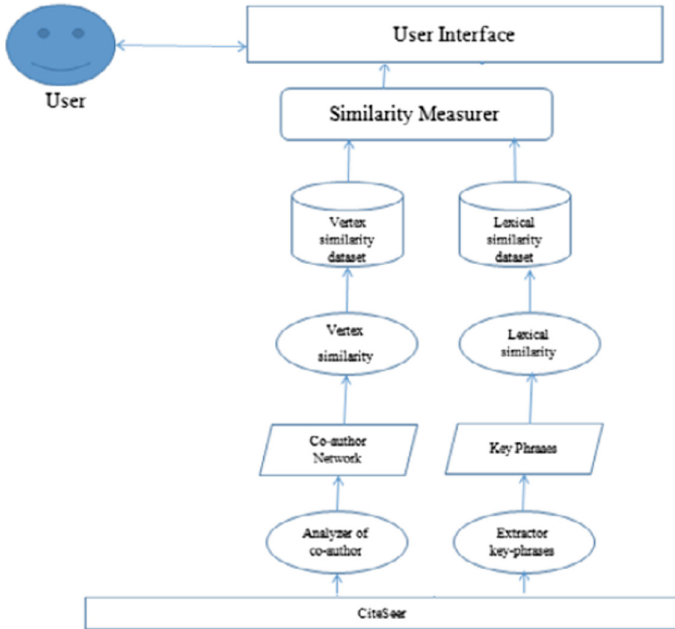


Fig. 2. Collab\_Seer architecture

### 5.3 Ack\_Seer

Ack\_Seer is used to extract the acknowledgements from documents and thesis. Acknowledgements are rich in providing the information about the contributors to the research work, collaborators, author for the various research works. Named Entity Recognition (NER) method is used to extract the acknowledged people from the documents. Open Calais can be used as the NER tool for the extraction. The number of passages from document are passed through the NER and the result is then merged to search for the appropriate acknowledgements. Merging process removes the duplication from the documents for the efficient result.

With Ack\_Seer search engine acknowledgements are extracted by extracting the passages and entities, next the disambiguation is done and the acknowledgement are extracted from the documents. Initially dictionaries are used to extract and merge the documents to extract the acknowledgements from the documents. Open Calais method extract the acknowledgements from the documents by categorizing them into three parts as person, company and institutes. Once the documents is been searched the next step will be indexing and ranking the documents to search for the appropriate names.

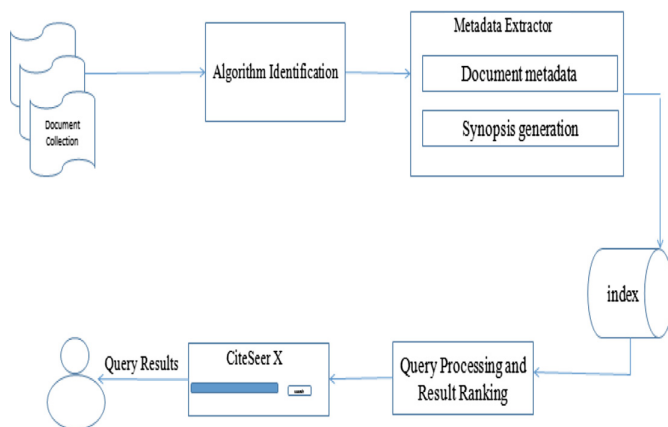


## 5.4 Chem\_Seer

Chem\_Seer is also a part of Cite\_Seer which is specially designed for the chemical field to extract the chemical formulae, figures and table search for the medical fields. It is type of search is engine which extract the chemical entities from the text then the indexing is done with the text in order to support the chemical formulae and names from the text and it also supports the various query models to model the document for the entity tagging. An algorithm of independent frequent subsequence mining (IFSM) is used to extract the sub-terms of chemical names and approximate probabilities of their occurrence [6]. Then at the end algorithm ranking is done and the formulae are extracted.

## 6 Architecture of the System Algo\_Seer

The present work discusses the prototype of the search engine is been discussed which is Algo\_Seer. This system is designed as part of the CiteSeer search engine which is specifically designed for the documents elements search and extraction of the document elements from the scholarly big data. Algo\_Seer is used to search for the pseudo codes and algorithmic procedures from the scholarly documents, publications and journals. The following show this architecture of the Algo\_Seer search system (Fig. 3).



**Fig. 3.** Architecture of the Algo\_Seer

The methods presented in this work are rule based method, machine learning methods and hybrid methods, these methods can also be generalized for other searches such as search for algorithms from the html and figure extraction from the documents. Though there are similarities when searches are made for algorithms in text data and webpages, but they differ in their presentation style. Usually the algorithms in webpage are written in html form where in text document contain the algorithms written in the readable manner which can be extracted easily from the huge set of data. These methods presented in this work can also be used for the other search such as table search, figure search, expressions search etc.

### ***Problem Statement***

The problem is to extract the algorithms in the increasingly vast collection of scholarly digital documents which would require algorithm indexing, searching, discovery and analysis.

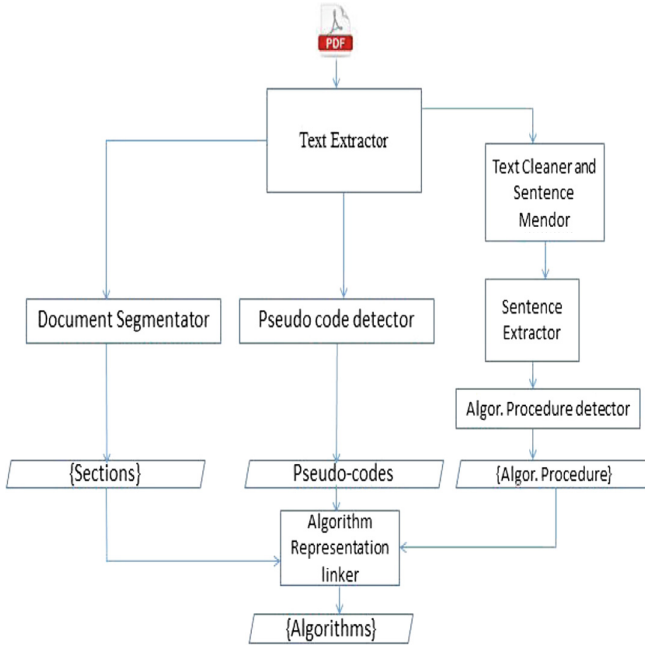
In this work as solution to the above problem, rule based and machine learning methods are used. These are the set of hybrid methods based on the ensemble machine learning approach used to extract both pseudo codes and algorithmic procedure from the scholarly data. These techniques involve indexing, ranking and analyzing the documents for searching and extracting the algorithms.

It also discussed that the documents which contain the captions and direct naming conventions for the documents can be easily searched for the pseudo codes and also documents which contain the direct representation of algorithms are easily extracted for Algorithmic Procedures, which is inadequate for effective retrieval, synopsis generation, meta data generation, indexing and analyses of the Pseudo codes and Algorithmic Procedures.

## **7 Algorithm Identification**

Algorithm identification includes efficient search of the algorithms from scholarly data. This identification involves automatic search of the PC's and AP's from the huge documents. The following diagram shows the high level design of the system.

The current system discussed search for the PDF documents, this is because most of the documents, articles, publications are published in PDF format. The documents published in Cite\_Seer are also found in PDF format [12]. First the plain text is taken as the input, then the document is segmented for the pseudo code detection, sentence extractor is used to search and extract for the sentences from the documents containing the keywords for the PC's and AP's. AP detector first performs the cleaning of the text and sentences, then it identifies for the Algorithmic Procedures. Once the AP and PC are been detected then they are combined and linked together to form the required algorithm (Fig. 4).



**Fig. 4.** High level design

## 7.1 Detecting Pseudo Codes

It is found that most of the documents use the pseudo codes for the efficient and effective representation of the algorithms in the documents. PC's are usually present as separate part from the running text in the documents. And these can be found with the help of identifier which they are accompanied with such as captions, function names or algorithm names. Rule based method (PC-RB), an group of machine learning based method (PC-ML), and a combined method (PC-CB) are the three methods discussed.

### A. Rule Based Method

Rule based method extracts for the pseudo code from the documents using the grammar identification and caption attached to the document. The approach use by the rule based method forms the basis for the pseudo code search.

The proposed PC-RB extends the baseline by adding the following rules to improve coverage and reduce false positive rate:

- A Pseudo Code caption should contain minimum of one algorithm keyword, It could be pseudo-code, algorithm, and procedure.
- Captions in which the algorithm keywords appear after prepositions are discarded, as these are not similar to caption of PCs.

### **B. Machine Learning Method**

The documents in the scholarly data which does not contain the captions will remain undetected by the rule based method. Thus the machine learning method is used to effectively search for the algorithm which lack of captions in the documents. This method will search for the contents of the PC, and this is motivated by the observation that most of the document contains the pseudo codes in sparse manner.

### **C. Combined Method**

Though Machine Learning method will detect for the pseudo codes which do not accompanied with captions but the documents which are not captured in first sparse box will also remain undetected. This may be due to the reason that such documents are written in figure format or in descriptive manner.

**STEP1:** when document is given, first run both Pseudo Codes-Rule Based and Pseudo Codes-Machine Learning methods.

**STEP2:** For every PC box searched by PC-ML, if a caption is detected for PC by PC-RB is in proximity, then the PC box and the caption are merged.

### **Detecting Algorithmic Procedures**

Algorithmic procedures are the elaborated way of writing the algorithms in the scholarly documents. These are written in descriptive manner and used to represent relatively simpler algorithms when compare to pseudo codes. Algorithmic procedures are expressed by loops, recursion, and function name. Again the two methods are used to detect the AP's in documents.

#### **A. Rule Based Method**

APs in the sentence can be identified by certain properties which allow easy extraction of the algorithms are,

- The sentences usually end with follows:, steps:, algorithm:, follows:, following:, follows., steps:, below:.
- he sentences usually contain at least an algorithm keyword.

#### **B. Machine Learning Method**

Some of the algorithms in the documents do not facilitates to the rules defined by the rule based method thus machine learning method is used. In machine leaning method it adopts the approach of feature selection and classification to search for the algorithms in the scholarly documents.

## **8 Advantages**

CiteSeerx is autonomous, requiring no manual effort during indexing. CiteSeerx allows easy browse of contents of citation as fast as possible. CiteSeerx can display the context paper in the way it is cited in subsequent publications.

## 9 Conclusion

In this work it has been discussed the different methods used for searching, extracting and analyzing the algorithms from the scholarly big data. Also a brief survey of various search system used for different fields for the algorithms searches and other search are been discussed.

This work also represents the advantages of the search engines used for searching the algorithms and other document elements form the scholarly big data and facilitates that these search engines are analyzed as part of Cite\_Seer search system for the documents.

## References

1. Wang, J.: Mean-variance analysis: a new document ranking theory in information retrieval. In: Proceedings of the 31st European Conference IR Research on Advances in Information Retrieval, pp. 4–16 (2009)
2. Blei, D.M., Ng, A.Y., Jordan, M.I.: Latent Dirichlet allocation. *J. Mach. Learn. Res.* **3**, 993–1022 (2003)
3. Tuarob, S., Tucker, C.S.: Fad or here to stay: predicting product market adoption and longevity using large scale, social media data. In: Proceedings of the ASME International Design Engineering Technical Conferences & Computers and Information in Engineering Conference (2013)
4. Tuarob, S., Tucker, C.S.: Quantifying product favorability and extracting notable product features using large scale social media data. *J. Comput. Inform. Sci. Eng.* **15**(3) (2015). <http://computingengineering.asmedigitalcollection.asme.org/article.aspx?articleid=2090327>
5. Hirschberg, D.S.: A linear space algorithm for computing maximal common subsequences. *Commun. ACM* **18**(6), 341–343 (1975)
6. Guha, S., Koudas, N.: Approximating a data stream for querying and estimation: algorithms and performance evaluation. In: Proceedings of the 18th International Conference on Data Engineering, pp. 567–576 (2002)
7. Kataria, S., Browner, W., Mitra, P., Giles, C.L.: Automatic extraction of data points and text blocks from two-dimensional plots in digital documents. In: Proceedings of the 23rd National Conference on Artificial Intelligence, vol. 2, pp. 1169–1174 (2008)
8. Sojka, P., Liska, M.: The art of mathematics retrieval. In: Proceedings of the ACM Symposium on Document Engineering, pp. 57–60 (2011)
9. Bhatia, S., Mitra, P.: Summarizing figures, tables, and algorithms in scientific publications to augment search results. *ACM Trans. Inf. Syst.* **30**(1), 3:1–3:24 (2012)
10. Liu, Y., Bai, K., Mitra, P., Giles, C.L.: TableSeer: automatic table metadata extraction and searching in digital libraries. In: Proceedings of the 7th ACM/IEEE-CS Joint Conference on Digital Libraries, pp. 91–100 (2007)
11. Hearst, M.A., Divoli, A., Guturu, H., Ksikes, A., Nakov, P., Wooldridge, M.A., Ye, J.: BioText search engine: beyond abstract search. *Bioinformatics* **23**(16), 2196–2197 (2007)
12. Hassan, T.: Object-level document analysis of PDF files. In: Proceedings of the 9th ACM Symposium on Document Engineering, pp. 47–55 (2009)



# A Review on Infrared and Visible Image Fusion Techniques

Ami Patel and Jayesh Chaudhary<sup>(✉)</sup>

Computer Engineering Department,  
Sarvajanik College of Engineering and Technology, Surat, Gujarat, India  
412amipatel@gmail.com, jayesh.chaudhary@scet.ac.in

**Abstract.** The term fusion means in moderate approach to extract the information acquired in several domains. The term infrared and visible image fusion has been intended to find compatible fused image with detailed textures of visible images and an impressive infrared object area. We therefore combine infrared and visible images to create solitary image. Current real - time applications that encourage image fusion including military surveillance, automate agricultural, object recognition, remote sensing, and medical applications. The concept of merging two or more than two images using the various image fusion schemes. This paper begins with the background information on the image fusion. Secondly, infrared and visible image fusion rest on multi-scale transformation of existing techniques are reviewed with all the merits and demerits of the same table lists. Further section elaborates fusion strategies and fusion performance evaluation metrics are summarized.

**Keywords:** Infrared image · Visible image · Image fusion · Infrared and visible image fusion

## 1 Introduction

Image fusion is a vital part of computer vision and image processing. Fusion aims to combine multiple images obtained into single (fused) images from different types of multi-sensor. The fusion procedure can extract valuable information from source images and add to the fused image without any artifacts being presented [1]. The fusion procedure has the advantage of taking information from multiple images of the similar scene containing relevant information in single image, so as to human can easily visualize the better understanding of scene. Herein, relevant information as visible images contain scene background and infrared images contain background of target objects. In image fusion, images from various sensors including visible (VI), infrared (IR), images with the same scene with different focal lengths, images with the same scene at different times, images with different viewpoints, computed tomography (CT) and magnetic resonance imaging (MRI) [1] exist decent sources used for fusion. In many aspects, combination of infrared (IR) and visible (VI) image fusion is important. Visible images exhibit high spatial resolution, scene texture details and chiaroscuro, making them more appropriate for the visual perception of humans. However, serious conditions such as sunlight, smog and other bad weather conditions

influence images [2]. Meanwhile, Infrared images can illustrate the thermal radiation of targets from their backgrounds. Low spatial resolution of infrared images reduce the impact of external environment [2]. The multidisciplinary infrared and visible image fusion scheme used as military surveillance [1, 2], medical [1, 2], agricultural automation [2], remote sensing [3], and object recognition [1–3]. Image fusion can be understood on three levels namely pixel-level, feature-level, and decision-level [3]. Pixel level image fusion, which can be referred to as a fusion type wherein all new pixels of the merged image achieves dissimilar value when all image pixels are grouped together. Image fusion at feature level, the significant features are first extracted on each source images, after compiled for certain exact resolves. Image fusion at decision level is a fusion based on judgment and also referred to as fusion at symbol level. All the levels are brief describe in next section. Fusion process can be developed with different schemes as multi-scale transform in pyramid transform (PT) [4–6], wavelet transform [7–11], curvelet transform [12], contourlet transform [13], and edge-preserving filter [14–18]. The concept of pyramid, transforms source images into sub-images and performs decomposition, initial image formation for re-composition and re-composition steps. The pyramid transformation has less memory space and low computational complexity [2]. PT cannot however introduce spatial information and block phenomena [2]. Wavelet transform, curvelet transform, and contourlet transform seem to be present multi-scale geometrical analysis in image fusion process. Wavelet transform cannot represent the directional information. Contourlet transformation is a multi- directional multi-resolution imaging method for overcome above problem [1]. Edge-preserving filter takes two or more input images to decompose into smooth base layer as well as detail layer capable of preserving multi-level information. The structure of this paper is follows as: Sect. 2 provides the theoretical background of image fusion. Section 3 existing infrared and visible image fusion methodology as well as fusion rules are examine in detail. Section 4 Comparative analysis of image fusion techniques, Sect. 5 describe performance evaluation metrics for image fusion. Finally, image fusion can concluded within future direction in Sect. 6.

## 2 Background of Image Fusion

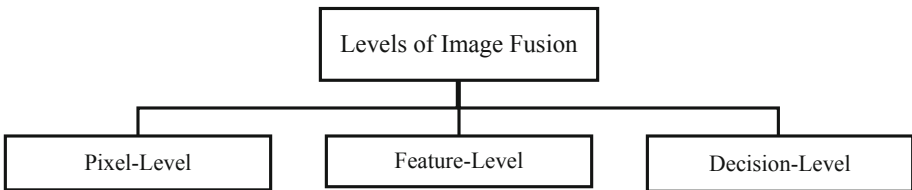
Image fusion process combines two or more images into a single output image that better describes the scene than any single input image. The fusion image provides detailed information on the scene that is more convenient for the human vision perception and machine perception. The image fusion requires improved lighting conditions in the scene and improved image qualities to facilitate the detection of different moving objects. Image fusion process for high - quality images that allows a proper understanding of the scenery that can be useful for surveillance and target recognition. The illustration of infrared and visible image fusion is shown in Fig. 1.



**Fig. 1.** Example of image fusion

## 2.1 Levels of Image Fusion

The Image fusion can be understood at three levels namely Pixel-Level Fusion, Feature-Level Fusion, and Decision-Level Fusion are describe as below (Fig. 2).



**Fig. 2.** Levels of image fusion

Image fusion at pixel level, which can be referred to as a fusion type wherein all new pixels of the merged image achieves dissimilar value when all image pixels are grouped together. Basic requirements [17] are exact on the fused result such as (i) all salient information can be preserved in the fusion process; (ii) artifacts or inconstancies cannot be introduced; (iii) shift invariant. Image fusion at feature-level, the relevant features are taken out on each source image, after compiled for certain exact purposes. The features including size, shape, contrast and texture are identified [18]. Fusion information at the decision level is taken out separately on every source images and decisions are formerly taken for each input or source channel. The decision-level fusion is also referred to as a symbol-level fusion, which combines information at the highest abstraction level [18] (Fig. 3).



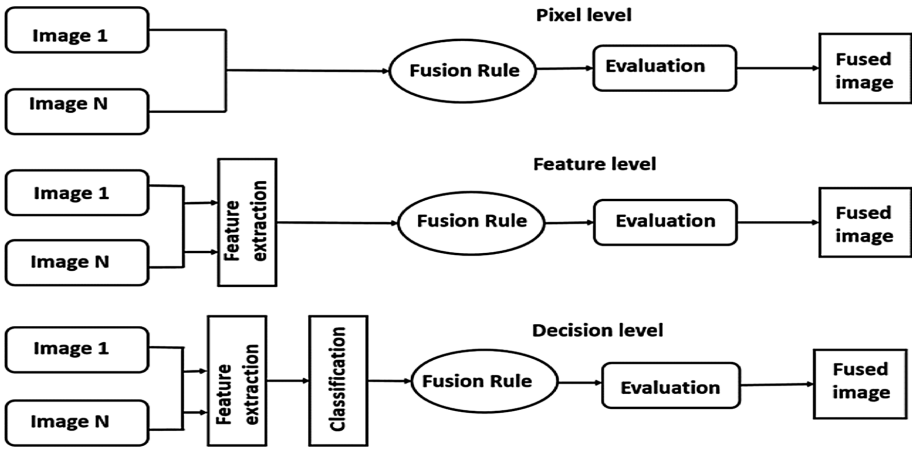


Fig. 3. Procedure for level of image fusion [21]

### 2.2 Types of Image Fusion

Image fusion schemes are generally categorized as single-sensor and multi-sensor image fusion schemes. In single sensor scheme, the series of images with the same scene is captured using a single sensor and relevant information on such a few images is incorporated into a digital image through the fusion process. Even in rowdy environments and in too many lighting conditions, human may not be able to track the target of interest which might easily be originate as of the merged images of the target scene. Applications for digital photography such as multi-focus imaging or even multi-exposure imaging are share of single sensor scheme. Moreover, such fusion schemes still have their drawbacks. Perhaps they just rely on circumstances including lighting and the sensor’s latency. For instance, VI sensors such as digital camera capture good pictures visually under high lighting conditions. They do not indeed to capture good images in low light conditions including night, mist and gales. Single sensor image fusion shown in Fig. 4.

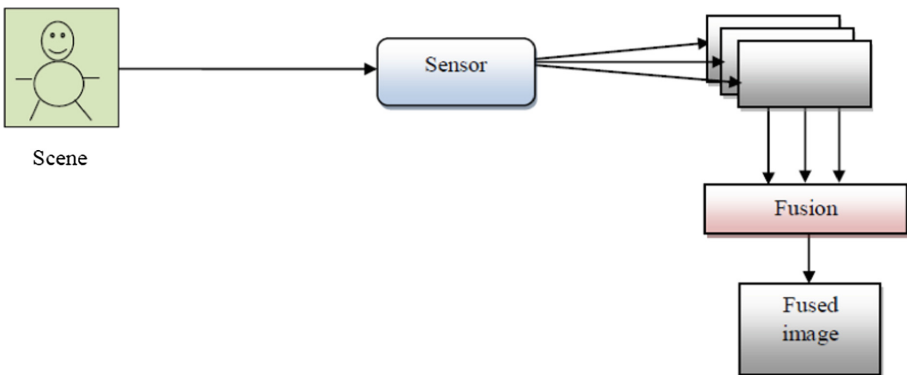


Fig. 4. Single sensor image fusion [28]

Multi-sensor image fusion schemes are initiated to take pictures under adversative environmental conditions in order to resolve the difficulties of single-sensor scheme. Various images of a certain scene are captured in multi-sensor image fusion using different sensors of altered modalities to obtain federal information. For illustration, VI sensors are decent in high illumination circumstances. Yet, IR sensors are capable to capture images in low lighting environments. The fusion process merged the essential and needed information on these images into one image. Multi-sensor image fusion shown in Fig. 5.

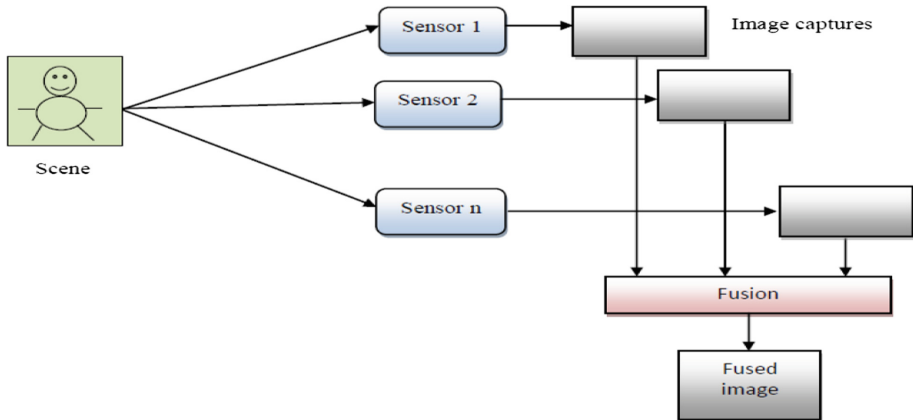


Fig. 5. Multi sensor image fusion [28]

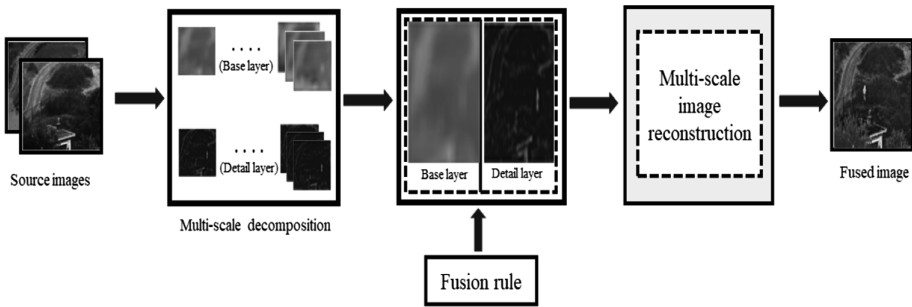
### 2.3 Applications

- **Military Surveillance** [1, 2]: Infrared and visible image fusion should be gives to complementary information about target scene. Visible images provide contextual information such as foliage, field of battle, texture and topsoil. Infrared images, on the other hand, contain object (person), enemy and vehicle movements in the foreground. To retrieve the information about the target and improve the image quality, information from both IR and VI images must be merged into a single image, the resulting final fused image.
- **Agricultural automation** [2]: Image processing has been used in agriculture to sort fruits and foods because expectations arise in food quality and safety standards and the detection of certain defects such as dark spots, cracks and bruises on fresh fruits. Many researchers using different image fusion methods should explore such concepts in agriculture.
- **Remote sensing** [2, 3]: Image fusion in remote sensing must be a constantly growing market, such as vegetation mapping or environmental observation. In applications to improve the quality of images with improved computing power and the demand for greater precision in the geoscience information system, the spatial and spectral resolution of remotely sensed images needs to be improved. These requirements must be met by the use of imaging fusion techniques.

- **Object recognition [1–3]:** Object recognition means the target object is identified. Both types are infrared and visible fusion of images in the object recognition system. In the first stage, the fusion and recognition with the fused effect and fusion algorithm can be integrated into the recognition process in which it is difficult to define the two processes [1]. Secondly, use decomposition methods or fusion rules to make a certain scene visible.
- **Medical [1, 2]:** Different modalities of medical imaging, such as Positron Emission Tomography (PET), Single Photon Emission Tomography (SPECT), Computer Tomography (CT) and MRI, are used to capture complementary information. The individual images do not provide the all the necessary details. Consequently, information from various captures must be included in a single image.

## 2.4 Infrared and Visible Image Fusion Framework

In fusion framework, fusion scheme depend on multi-level transforms that consist of the following steps as shown in Fig. 6.



**Fig. 6.** Infrared and visible image fusion framework

These steps are described in brief as: first, we taken infrared and visible images as source images. Each source images are decomposed into base layers (high-frequency) and detail layers (low-frequency) of sub-images at different levels which has different significances, carrying on different types of information such as global/local information, grayscale or average grayscale and so forth. The base layer contain detail information about scene such as vegetation, soil, texture, lines, and etc. The detail layer reflects the target object or person. These two layers of sub-images are then merged using various fusion rules. Finally, we involves inverse transformation on fused representation and we get the final fused image.

### 3 Infrared and Visible Image Fusion Methodology

#### 3.1 Pyramid Transform

The aim of the pyramid is to decompose input images into a number of sub-images on different scales. In general, every pyramid transform needs to perform the following steps:

- i. Decomposition: Pyramid is produced at each level of the combination and number of combination levels are predefined depending on the size of the image. The original images are convolved to the low pass channel and the pyramid is created for input images as well as for a large portion of their size.
- ii. Formation of the initial image for re-composition: After decomposition process, the input images are combined. The final decimated images produced by selecting either the minimum or the maximum average decimated image.
- iii. Re-composition: The resulting image is finally created in this process by pyramids formed at each decomposition level. This stage is repeated  $n$  times when the filter used in the decomposition stage is not decimated to the level of re-composition and then convolved with the transpose of the filter. The filter matrix is combined with the pyramid formed by the process of adding the pixel intensity to the decomposition level. The resulting image acts as the next level input. The final level of the merged image is the resulting fused image.

The well-known existing pyramid transform techniques are mentioned as: Laplacian pyramid [4], Steerable pyramid [5], and Contrast pyramid [6]. The Laplacian pyramid is constructed by distorting, sampling, interposing and differentiating from its lower level [1]. For instance, Yu et al. [4] represent Laplacian pyramid to decomposed source images for false color image fusion. In steerable method, two steps are to be required: first, input images are decomposed into low and high-pass subbands. Second, low-pass subbands are further separated into set oriented bandpass subbands and low-pass subbands. The advantage of this method is self-inverting, translation, and rotation invariant [1]. Xu et al. [6] projected infrared and visible image fusion based on contrast pyramid which can be highlight contrast information to achieve the good visual effect.

#### 3.2 Wavelet Transform

The idea of wavelet transformation is a geometric analysis of multiple dimensions. It is the decomposition of spatial frequencies that can be used for the multi-resolution image analysis. A separate filtering and sampling process in horizontal and vertical directions is included. It also provides four subbands with vertical, horizontal and diagonal frequencies on each transformation scale. All subbands contain additional coefficients show the basic and detail components of the input images. These coefficients are fused based on some fusion strategies like coefficient combination rule, region based rule has been used. After that, the reconstruction part is sampled. This scheme is intended to reconstruct the fused image by improving the quality of the fused image (Fig. 7).

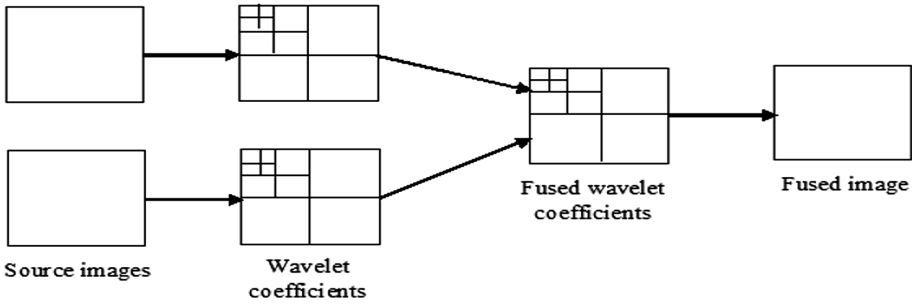
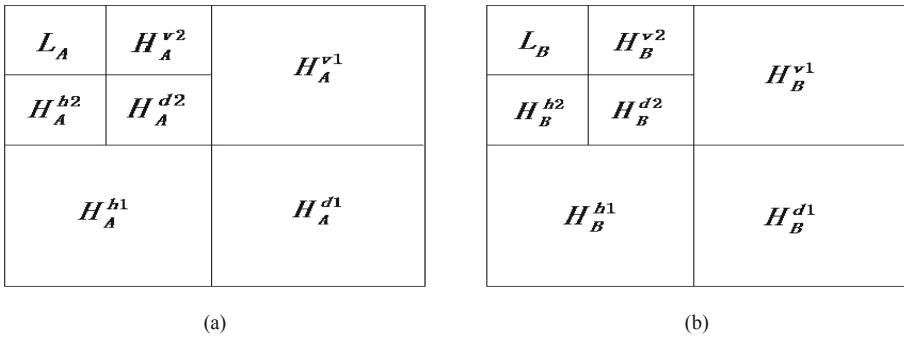


Fig. 7. Wavelet transform based image decomposition

The well-known existing wavelet transform techniques are mentioned as: discrete wavelet transform (DWT) [7], dual-tree discrete wavelet transform (DT-DWT) [8], lifting wavelet transform (LWT) [9], spectral graph wavelet transform (SGWT) [10], and quaternion wavelet transform (QWT) [11]. In Discrete Wavelet Transform (DWT), input images can decompose into low and high-pass subbands that can be generated via bank of filters. The DWT decomposition diagram shown below (Fig. 8).



(a) Decomposition diagram of image A  
 (b) Decomposition diagram of image B

Fig. 8. DWT of image A and B [7]

The high-frequency and low-frequency coefficients of source images A and B are merged with different fusion rules. For low-frequency coefficients, the result is determined by the regional energy. The low frequency coefficient of regional energy is calculated, then the fusion result of the low frequency coefficient is obtained according to the regional energy and the corresponding correlation value. For high frequency coefficients, the difference in the adjacent coefficients is calculated first, then the weighted sum of the difference is obtained. If the weighted sum of image B is less than that of image A, the result of the fusion is high-frequency coefficient of image A, otherwise the high frequency coefficient of image B should be selected. In the end, the fused image will be found by inverse DWT. The dual-tree discrete wavelet transform

[8] can be carried out separable filter bank. It also has merits of invariance, computational reliability and discontinuous discernment over discrete wavelet transformation [1]. Lifting wavelet transform can be worked on a fully spatial transforming method that has merits of intuitive design, improper sampling as well as essential transformation over the traditional wavelet transformation [1].

### 3.3 Curvelet Transform

Curvelet transform is designed to represent the images in different scales and angles and to generalize the wavelet transform in higher dimensions. It is more accurate to expressive the edges and symmetrical (geometric) image structure than wavelet transform. The curvelet transform is decomposed source images into different sub-bands. It is used to fuse infrared and visible images. The difficulty with the curvelet transformation has block artifacts and lower contrast. After multi-resolution decomposition, images are obtained at different resolutions, and different resolution has different meanings, carrying different types of information. These information are separated to allow image fusion during decomposition. The more corresponding information is located and detailed in higher resolution. This coefficients of decomposition are known as high-frequency coefficients. The lower resolution, more comprehensive information is. This coefficients are called coefficients of low frequency. Weighted average fusion rule is used to find the coefficients of low-frequency. It contains image contour information as well as image energy. The high-frequency contain the detail information of the scene, to find the coefficients of high-frequency by grater absolute fusion rule. At last, inverse curvelet transform should be applied on fused coefficients to obtained final fused image.

### 3.4 Contourlet Transform

The contourlet transform can be reconstructed in two steps: laplacian pyramid (LP) and directional filter bank (DFB) [10]. First, the input images can be decompose into one low-pass subband and one band-pass subband by laplacian pyramid. Afterwards, band-pass subband decompose into different direction subbands via directional filter bank. This process continues until the low-pass subband achieves multi-resolution image decomposition in multi-directional form. The contourlet transform can not only be multi-scale as well as time-frequency local, it also has directional characteristics. Due to this, the image edges can be precisely identified in different scales and frequency subbands. After decomposition, find the coefficients of high-frequency and low-frequency. High-frequency coefficients are find using mean gradient fusion which reflect the details and textures of the source images. Contourlet transform cannot be only has multi-scale and time frequency local characteristics, it has directional characteristics. Because of, it can accurately identify the image edges into different scales and different frequency sub-bands (Fig. 9).

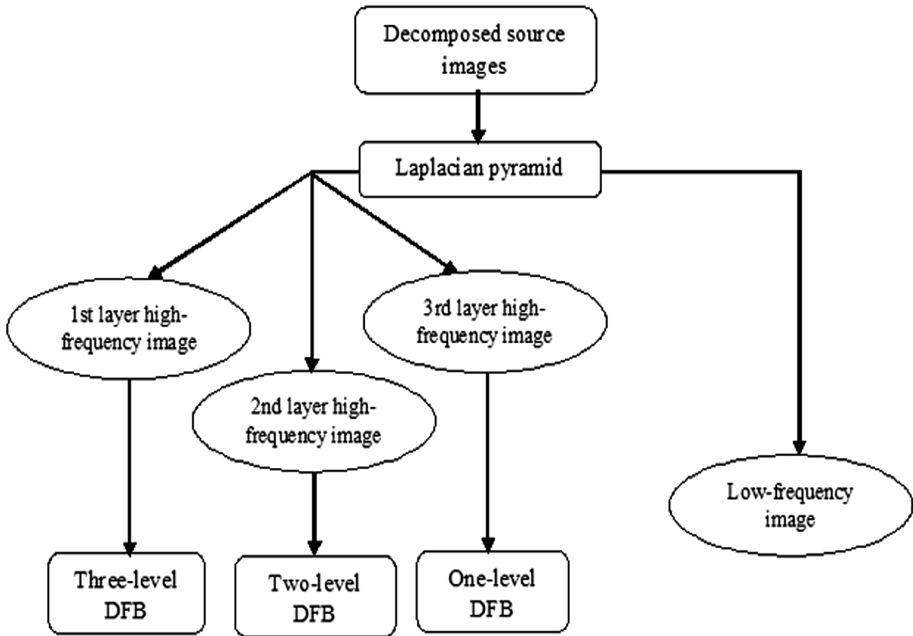


Fig. 9. Contourlet transform [13]

### 3.5 Edge-Preserving Filter

The edge preserving filter decomposition scheme is designed for source images to decompose into smooth base layer and detail layer. It can be used to maintain the spatial consistency of the structure and to decrease halo artifacts nearby the borders [1]. Base layer contain different intensity changes on large scale which is computed by edge preserving filter of the images. Detail layer can be fined by subtracting original images from base layers. Herein, well-known existing edge preserving filter techniques are mentioned as: mean filter [14], nonlocal mean [15], anisotropic diffusion [16], bilateral filter [15], guided filter [18]. The edge-preserving filter process are shown in Fig. 10.

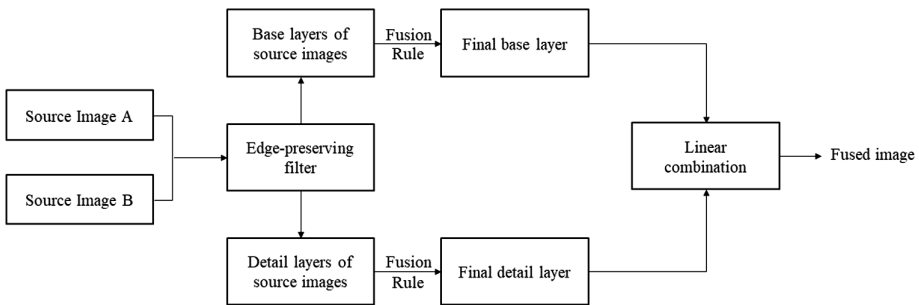


Fig. 10. Edge-preserving based image fusion

In figure, source images A and B are decompose into base layers and detail layers of source images using different edge-preserving filter. Base layer contain large scale variation as well as detail layer contain small scale variation. Base layers and detail layers should be fused on the basis of fusion strategies. The final merged image is then obtained as of the linear combination of the base layer and detail layer. The existing edge-preserving filter i.e. mean filter is simply to displace every pixel value in a picture with neighbouring mean value. This results in the elimination of pixel values that are not representative of their environment. Mean filter can be used to decompose input images into sub-images. It is easy to implement. Yan et al. [15] represent local methods as well as frequency domain filters have the notion of noise reduction when the major geometric specifications are reconstructed. However, the structure, detail and texture cannot be preserved. The non - local middle filter to solve this problem. It is similar to mean filter. Furthermore, it clean the edges without losing too many fine structure and details. The idea is to be calculating each mean value of the pixels in a given image and associated with target pixel to obtain the corresponding values. Bavirisetti et al. [16] proposed anisotropic diffusion process is smooth certain image on homogeneous regions whereas non-homogeneous regions are preserved. It should be based on partial differential equation (PDE) [1]. This method defeats the shortcomings of isotropic diffusion. Most information from source images can be transferred to a fused image. It cannot only smooth an image in the region, but it also retains its borders, contours and position. Bilateral filter is non-linear, and local technique which can smooth image while preserving edges that means of non-linear combination of nearby pixel values [17]. It is also preserving the edges. Guided filter is a linear local model based translation variant filter and computational efficient. The guided image filter including input image, guidance image  $G$ , and output image. The first requirement is that there is a local linear model between the guide image and the filter output. Secondly, the filter output should be as similar to the source image as possible. Toet et al. [18] represent iterative guided filtering, which can be applied to decompose the source images into base layers and detail layers. The base and detail layers are then fused with a guided weighted filtering average for each source image comprising the large-scale intensity variants of base layer and small-scale detail layer. The merged image is carried out to combine final base layer with the detail layer.

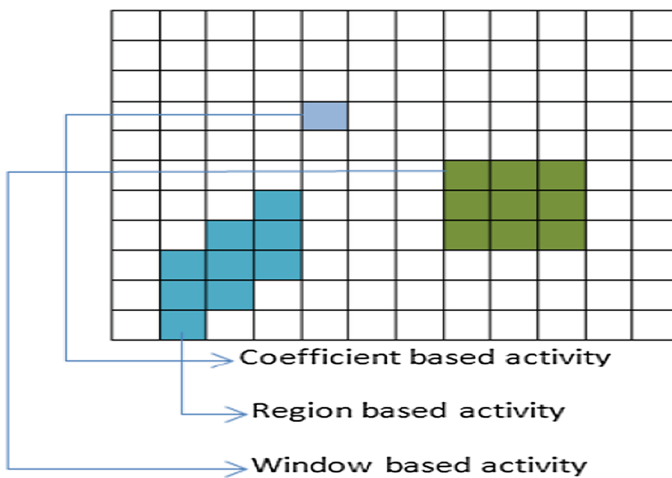
Other multi-scale transform approaches can be applied in infrared and visible image fusion scheme. These includes as, Non-subsampled Contourlet Transform (NSCT) [22], Non-subsampled Shearlet Transform (NSST) [23], Discrete Cosine Transform (DCT) [24], top-hat transform [25], and Singular Value Decomposition (SVD) [26]. NSCT has selves of shift-invariance as well as similar size between each subband image that describes shapes and directional texture of the source images. Yet, the problem with NSCT comprising uncertain object region, poor image factor, and visual artifacts in fused image [22]. NSST decompose the source images into a sequence of high-frequency sub-images and low-frequency sub-images. The advantage of NSST is that it has low computational cost as well as good image performance. Paramanandham et al. [24] presented DCT-based infrared and visible image fusion to decompose input images into sub-images, and particle swarm intelligence can be used to obtain optimized weighting. The top hat transform is a multi-scale morphological transformation. SVD is a transformation of multi-resolution, which decompose input images into smooth and detail sub-images.



### 3.6 Fusion Rules

Fusion rules can be used to find the coefficients of the base layer and detail layer. The familiar existing fusion rules are listed as: choose-max [3], choose-min [3], coefficient combination method [1], coefficient grouping method [3, 27], activity-level measurement [9], region based [1], principle component analysis [1], and brief description of common fusion rules are shown in below:

- Coefficient combination method [1]: It can merged two schemes as per (i) choose-max which can be choose maximum coefficient of the sub-images. (ii) weighted average that can be merging the coefficients of sub-images by weighting.
- Activity-level measurement [8]: It also evaluates regional energy with a particular part of multi-scale images. It can be divided into three parts: measurement based on the window, measurement based on the coefficient and measurement based on the region. In a window-based measurement, a rectangular window is located on the image with a coefficient in center. Activity-based coefficient measures to quantify each and every coefficient independently. The region with strange shapes is based on measurements of the activity level. Activity level measurements methods can be shown in Fig. 11 below,



**Fig. 11.** Activity-level measurement [3]

- Choose-max [3]: This rule as, pixels with the greatest intensity is selected as of two related pixels of input images and placed in resulting fused image at the specific positions.
- Choose-min [3]: It is identical to choose-max, in which the least pixel intensity is selected from the two related pixels of input images and placed in resulting fused image at exact positions.

- Coefficient grouping method [3, 19]: We create a multi-scale depiction of two source image coefficients, one that can be set to every of the multi-scale source image coefficients on the other. The coefficients should be linked to the identical position of the pixels in low pass filtered image.
- Principle component analysis [1]: It can be used to store brightness information of original images for low - frequency images. It is already abridged the dimension, i.e. high-dimensional space is plotted into low-dimensional space with preserving highest information of the source evidence.
- Average fusion rule [3]: This rule, as pixels with average intensity, is selected from the two related pixels of source images and placed in resulting fused image at particular position.
- Region based rule [1]: This rule focuses on objects in image at region level. It is based on a salience province, extraction of features, region of interest, and segmentation of regions.

#### 4 Comparative Analysis of Infrared and Visible Image Fusion Techniques

See Table 1.

**Table 1.** Comparasion table of infrared and visible image fusion techniques

Techniques	Advantages	Scope of improvements	Fusion rules	Datasets
Laplacian Pyramid [4]	<ul style="list-style-type: none"> <li>• It is achieved the fused image with less artifacts</li> <li>• Its computational complexity is low</li> </ul>	<ul style="list-style-type: none"> <li>• It increases the gray or color intensity range and the corresponding intensity</li> </ul>	<ul style="list-style-type: none"> <li>• Pattern selective fusion rule for high frequency</li> <li>• Priority average method for low frequency</li> </ul>	TNO Human Factors
Steerable Pyramid [5]	<ul style="list-style-type: none"> <li>• It is self-reversible and rotation invariant.</li> <li>• It also enables the blending of geometrical and thematic characteristics from source images efficiently</li> </ul>	<ul style="list-style-type: none"> <li>• The representation is an invariant of translation and rotation, but the representation is completed by a factor of <math>4k/3</math> where k is no. orientation bands</li> </ul>	<ul style="list-style-type: none"> <li>• Absolute value maximum selection</li> </ul>	–

(continued)

**Table 1.** (continued)

Techniques	Advantages	Scope of improvements	Fusion rules	Datasets
Contrast Pyramid [6]	<ul style="list-style-type: none"> <li>• The fusion image also contain target, back-ground information</li> <li>• Target can be high-lighted and position can be precisely</li> </ul>	<ul style="list-style-type: none"> <li>• Less time consuming</li> <li>• Less some detail loss</li> </ul>	<ul style="list-style-type: none"> <li>• Otsu method for low-frequency</li> <li>• Absolute maximum combine with morphological operation</li> </ul>	Infrared and multi-type images, multi-focus images
Discrete Wavelet Transform [7]	<ul style="list-style-type: none"> <li>• It is increased directional information, less blocking artifacts, better signal-to-noise ratios</li> </ul>	<ul style="list-style-type: none"> <li>• It can extend to capture the salient features</li> <li>• It can still improve the capture of curves and edges of images</li> </ul>	<ul style="list-style-type: none"> <li>• Regional energy based fusion rule for low-frequency</li> <li>• Weighted sum based fusion rule for high-frequency</li> </ul>	Infrared and visible images
Curvelet Transform [12]	<ul style="list-style-type: none"> <li>• It is more accurate to representing the edges &amp; geometric structure of images</li> </ul>	<ul style="list-style-type: none"> <li>• It improve less block artifacts and efficient represent the detailed spatial information</li> </ul>	<ul style="list-style-type: none"> <li>• Weighted average method for low-frequency</li> <li>• Absolute fusion rule high-frequency</li> </ul>	UN camp series images in TNO images set
Contourlet Transform [13]	<ul style="list-style-type: none"> <li>• It describes the shapes and directional texture of the image</li> <li>• It also captures the image edges' geometry well</li> </ul>	<ul style="list-style-type: none"> <li>• It make to lead good shift-invariance property</li> </ul>	<ul style="list-style-type: none"> <li>• Mean gradient fusion for high-frequency</li> <li>• PCA for low-frequency</li> </ul>	Infrared and visible images
Mean filter [14]	<ul style="list-style-type: none"> <li>• It aims to eliminate noise from every pixel using its neighbour mean value</li> <li>• It is easy to implement</li> </ul>	<ul style="list-style-type: none"> <li>• Single pixel with unrepresentative value can significantly affect the mean value of all the pixels in its neighbours</li> </ul>	<ul style="list-style-type: none"> <li>• Average fusion rule for high-frequency</li> </ul>	Battle field, tree, forest, industry, kayak, and house images
Bilateral filter [17]	<ul style="list-style-type: none"> <li>• It removes noise from each pixels</li> <li>• It can smooth image and preserve details</li> </ul>	<ul style="list-style-type: none"> <li>• It improve sharpness of fused image</li> <li>• Less time consumption</li> </ul>	<ul style="list-style-type: none"> <li>• Choose-max fusion rule for directional subbands</li> <li>• Average method for approximation subbands</li> </ul>	UN camp, Gun, Tropical, Medical images

(continued)

**Table 1.** (continued)

Techniques	Advantages	Scope of improvements	Fusion rules	Datasets
Nonlocal mean filter [15]	<ul style="list-style-type: none"> <li>• It benefits as of preserves the structure, details and texture of the images as well as high redundancy of natural images to smooth images</li> </ul>	<ul style="list-style-type: none"> <li>• In some cases, noise is increase so the make performance of this filter, image suffers from less blurring and loss of image details</li> </ul>	<ul style="list-style-type: none"> <li>• Local neighbourhood gradient weighted fusion rule for approximation subbands</li> <li>• Local eight-order correlation fusion rule for detail subbands</li> </ul>	UN camp, Dune, Flower, City images
Anisotropic diffusion [16]	<ul style="list-style-type: none"> <li>• The majority of the information is transferred from the source image to the merged image.</li> <li>• The fusion loss is much less</li> <li>• Fusion artifacts are insignificant</li> </ul>	–	<ul style="list-style-type: none"> <li>• KL-Transform for detail layer</li> <li>• Weighted superposition for base layer</li> </ul>	IR-visible, MMW-visible images
Guided Filter [18]	<ul style="list-style-type: none"> <li>• It is computationally efficient, translation variant based on local linear model</li> </ul>	<ul style="list-style-type: none"> <li>• It may have halos near some edges</li> </ul>	<ul style="list-style-type: none"> <li>• Weighted recombination for detail layers</li> </ul>	TNO Human Factors

## 5 Performance Evaluation Metrics for Image Fusion

The fusion performance of different approaches should be familiar to estimate the involvement of the reference images also in the fused image, which ensures quality of the fused image according to visual perception of human. The fusion strategies can be quantitatively and qualitatively evaluated. The fusion performance techniques can be evaluated and identified as subjective and objective evaluation approaches in numerous quality fields. Subjective methods can access quality of the fused image according to the visual system of human, which is the direct process of image quality assessment. The objective methods can be measure the fused image quantitatively. Objective evaluation including different metrics based on Entropy (E), Mutual Information (MI), Structural Similarity Index Measure (SSIM), Root Mean Square Error (RMSE), Visual Information Fidelity (VIF),  $Q^{AB/F}$ . Herein, A, B, and F signifies as infrared, visible, and fused image. X denotes source image variable. Evaluation metrics are described as below:

1. **Entropy:** It can be used to compute the richness of the information delimited in fused images. The greater value specifies the more details in fused image.

Entropy is usually used as an auxiliary measurements [1]. Entropy is mathematically expressed as [1],

$$EN = - \sum_{l=0}^{L-1} p_l \log_2 p_l \quad (1)$$

where L signifies no. of grey levels,  $p_l$  defined the corresponding gray level normalized histogram in the fused image [1].

2. **Mutual Information:** Quality measurement shows how much data in fused image transmits as of the input images. Mutual information expressed as [1],

$$MI = MI_{A,F} + MI_{B,F} \quad (2)$$

where  $MI_{A,F}$  and  $MI_{B,F}$  gives the quantity information that transfer as of source images into fused image [1]. The MI can be calculated in two random variables as,

$$MI_{A,F} = \sum_{x,f} P_{X,F} \log \frac{P_{X,F}}{P_X P_F} \quad (3)$$

where,  $P_X$  and  $P_F$  indicated the peripheral histogram of the source image X and the fused image F,  $P_{X,F}$  defined the input image X joint histogram and the fused image F [1].

3. **Structural Similarity Index Measure (SSIM):** It measures the structural similarity between two images and the misrepresentation of the image as a combination of luminance, loss disparity and contrast perversion [2]. SSIM mathematically defined as,

$$SSIM_{X,F} = \frac{\sigma_{XF}}{\sigma_X \sigma_F} \frac{2\mu_X \mu_F}{\mu_X^2 \mu_F^2} \frac{2\sigma_X \sigma_F}{\sigma_X^2 \sigma_F^2} \quad (4)$$

where  $\mu_X$ ,  $\mu_F$  denotes mean intensities and  $\sigma_X$ ,  $\sigma_F$ ,  $\sigma_{XF}$  are the variances and covariance.

4. **Root Mean Square Error (RMSE):** It is an error similar to mean square. It refers to the changes between fused image and source image. It indicates that fused image has small error [1].

$$RMSE = \frac{RMSE_{AF} + RMSE_{BF}}{2} \quad (5)$$

5. **Visual Information Fidelity:** The objective of VIF is to create a model to calculate image distortions that include noise additives, blurs and changes in global or local contrast [2]. The VIF procedure can be executed in four steps [1]: source and fused images can be filtered and further broken down into different blocks. After that, each block must be evaluated with and without distortion. Third, VIF is calculated for each subband. VIF is finally calculated.

6.  $Q^{AB/F}$ : It measures the similarity of the edge transferred from source images to the fused image.  $Q^{AB/F}$  is mathematically defined as [1],

$$Q^{AB/F} = \frac{\sum_{i=1}^N \sum_{j=1}^M Q^{AF} w^A + Q^{BF} w^B}{\sum_{i=1}^N \sum_{j=1}^M (w^A + w^B)} \quad (6)$$

## 6 Conclusion

Now a days, infrared and visible image fusion is trendy topic in several domain. Thus, we present a comprehensive survey on existing infrared and visible image fusion techniques as well as we also define the pros and cons of these techniques. Each methods can be briefly summarized with the fusion strategies to find the coefficients of the sub-images. At last, we describe the performance evaluation metrics for the result of infrared and visible image fusion that depict (calculate) information about how much fusion gain, fusion loss, fusion artifacts and, some other information in fused image. Furthermore, future work has to be improve the existing infrared and visible image fusion methods of evaluation for human perception as well as how to develop the system with high efficiency and less time consumption. Infrared images have high noise so degrades target objects to be improve the anti-noise performance with the salience analysis of infrared and visible image fusion. Thus, researchers and developers of image fusion are given a new direction to tackle these complications.

## References

1. Ma, J., Ma, Y., Li, C.: Infrared and visible image fusion methods and applications: a survey. *Inf. Fusion* **45**, 153–178 (2018)
2. Jin, X., Jiang, Q., Yao, S., Zhou, D., Nie, R., Hai, J., He, K.: A survey of infrared and visual image fusion methods. *Infrared Phys. Technol.* **85**, 478–501 (2017)
3. Dogra, A., Goyal, B., Agrawal, S.: From multi-scale decomposition to non-multi-scale decomposition methods: a comprehensive survey of image fusion techniques and its applications. *IEEE Access* **5**, 16040–16067 (2017)
4. Yu, X., Ren, J., Chen, Q., Sui, X.: A false color image fusion method based on multi-resolution color transfer in normalization YCBCR space. *Optik – Int. J. Light Electron Opt.* **125**(20), 6010–6016 (2014)
5. Liu, Z., Tsukada, K., Hanasaki, K., Ho, Y., Dai, Y.: Image fusion by using steerable pyramid. *Pattern Recogn. Lett.* **22**(9), 929–939 (2001)
6. Xu, H., Wang, Y., Wu, Y., Qian, Y.: Infrared and multi-type images fusion algorithm based on contrast pyramid transform. *Infrared Phys. Technol.* **78**, 133–146 (2016)
7. Zhan, L., Zhuang, Y., Huang, L.: Infrared and visible images fusion method based on discrete wavelet transform. *J. Comput.* **28**, 57–71 (2017)
8. Madheswari, K., Venkateswaran, N.: Swarm intelligence based optimisation in thermal image fusion using dual tree discrete wavelet transform. *Quant. InfraRed Thermography J.* **14** (1), 24–43 (2016)

9. Zou, Y., Liang, X., Wang, T.: Visible and infrared image fusion using the lifting wavelet. *TELKOMNIKA Indonesian J. Electr. Eng.* **11** (2013)
10. Yan, X., Qin, H., Li, J., Zhou, H., Zong, J.-G.: Infrared and visible image fusion with spectral graph wavelet transform. *J. Opt. Soc. Am. A* **32**, 1643 (2015)
11. Chai, P., Luo, X., Zhang, Z.: Image fusion using quaternion wavelet transform and multiple features. *IEEE Access* **5**, 6724–6734 (2017)
12. Quan, S., Qian, W., Guo, J., Zhao, H.: Visible and infrared image fusion based on curvelet transform. In: *International Conference on Systems and Informatics (ICSAI)* (2014)
13. Li, H., Liu, L., Huang, W., Yue, C.: An improved fusion algorithm for infrared and visible images based on multi-scale transform. *Infrared Phys. Technol.* **74**, 28–37 (2016)
14. Bavirisetti, D.P., Dhuli, R.: Two-scale image fusion of visible and infrared images using saliency detection. *Infrared Phys. Technol.* **76**, 52–64 (2016)
15. Yan, X., Qin, H., Li, J., Zhou, H., Zong, J.-G., Zeng, Q.: Infrared and visible image fusion using multiscale directional nonlocal means filter. *Appl. Opt.* **54**(13), 4299 (2015)
16. Bavirisetti, D.P., Dhuli, R.: Fusion of infrared and visible sensor images based on anisotropic diffusion and Karhunen-Loeve transform. *IEEE Sens. J.* **16**(1), 203–209 (2016)
17. Hu, J., Li, S.: The multiscale directional bilateral filter and its application to multisensor image fusion. *Inf. Fusion* **13**(3), 196–206 (2012)
18. Toet, A., Hogervorst, M.A.: Multiscale image fusion through guided filtering. In: *Target and Background Signatures II* (2016)
19. Yang, B., Jing, Z.-L., Zhao, H.-T.: Review of pixel-level image fusion. *J. Shanghai Jiaotong Univ. (Sci.)* **15**(1), 6–12 (2010)
20. Piella, G.: A general framework for multiresolution image fusion: from pixels to regions. *Inf. Fusion* **4**(4), 259–280 (2003)
21. Kalaivani, K., Phamila, Y.A.V.: Analysis of image fusion techniques based on quality assessment metrics. *Indian J. Sci. Technol.* **9**(31), 1–8 (2016)
22. Meng, F., Song, M., Guo, B., Shi, R., Shan, D.: Image fusion based on object region detection and non-subsampled contourlet transform. *Comput. Electr. Eng.* **62**, 375–383 (2017)
23. Wu, W., Qiu, Z., Zhao, M., Huang, Q., Lei, Y.: Visible and infrared image fusion using NSST and deep Boltzmann machine. *Optik* **157**, 334–342 (2018)
24. Paramanandham, N., Rajendiran, K.: Infrared and visible image fusion using discrete cosine transform and swarm intelligence for surveillance applications. *Infrared Phys. Technol.* **88**, 13–22 (2018)
25. Bai, X., Zhou, F., Xue, B.: Fusion of infrared and visual images through region extraction by using multi scale center-surround top-hat transform. *Opt. Express* **19**(9), 8444 (2011)
26. Song, Y., Xiao, J., Yang, J., Chai, Z., Wu, Y.: Research on MR-SVD based visual and infrared image fusion. In: *Infrared Technology and Applications, and Robot Sensing and Advanced Control* (2016)
27. Falk, H.H.: Prolog to a categorization of multiscale-decomposition-based image fusion schemes with a performance study for a digital camera application. *Proc. IEEE* **87**(8), 1313–1314 (1999)
28. [Shodhganga.inflibnet.ac.in/jspui/bitstream/10603/151753/9/09\\_chapter%201.pdf](http://Shodhganga.inflibnet.ac.in/jspui/bitstream/10603/151753/9/09_chapter%201.pdf)



# Implementation of the Standard Floating Point DWT Using IEEE 754 Floating Point MAC

R. Prakash Rao<sup>(✉)</sup>, P. Hara Gopal Mani, K. Ashok Kumar,  
and B. Indira Priyadarshini

Electronics and Communication Engineering, Matrusri Engineering College,  
Saidabad, Hyderabad, India

prakashiiits@gmail.com, gopalmaniph@yahoo.com,  
kashok483@gmail.com, priyadarshini414@gmail.com,

**Abstract.** This work concentrates mainly for the implementation of Standard DWT using IEEE 754 floating point format. Currently, in the signal processing, for audio purpose the fixed point DWT is used as audio CODEC [1]. The main bottleneck of the fixed point DWT or the traditional DWT is the speed because at the input of the fixed point DWT the over-sampled ADC which is the Sigma-Delta ADC is used. The Sigma-Delta ADC can't give the speed more than 1 MHz because as the sampling rate increases, the step size decreases so that it takes more time to follow the analog signal which causes the limitation of the speed. Due to the speed limitation of ADC, the whole audio CODEC system which was designed by the fixed point DWT becomes slow even it has the capability to operate with a better speed. Hence, to optimize the system the FIR filters which are used to constitute the standard floating point DWT have been implemented in VLSI.

**Keywords:** DWT · IEEE 754 floating point · Audio CODEC · Sigma-Delta ADC

## 1 Introduction

To overcome the limitation of the speed of Sigma-Delta ADC, it has to be replaced by the logical connection instead of the physically connected Sigma-Delta ADC between the audio source and the fixed point DWT. The logical connection is provided through the development of user defined float point package using IEEE 754 standard and compile with IEEE standard library of digitally define tool. DWT designed in this manner is called Standard floating point DWT. To such floating point DWT, the audio source which is in the form of analog is converted into IEEE 754 standard and applied at the input using a test-bench. This floating point DWT be designed with floating point FIR filters. The floating point FIR filters are designed by floating point MAC [1]. Such MAC is designed by the floating point adder and floating point multiplier along with shifter. These floating point arithmetic operators are designed by the user defined



floating point library package [2]. With all such topics, this chapter explains the complete implementation issues of the Standard floating point DWT using IEEE 754 format. At the end of the work, various results of the standard floating point DWT are also illustrated.

## 2 Traditional 3-Stage DWT and Its Limitations

Traditional fixed point DWT functions with fixed-point MAC and its MAC has been designed through fixed point adder and multiplier along with a shifter. Because, it operates along with the sigma-delta analog to digital converter and digital to analog converter at the input side and output side of the fixed point DWT correspondingly, the first drawback of the traditional DWT is speed [3]. The sigma-delta analog to digital converter is used to alter the analog signal to the digital signal. Sigma-delta operates with oversampling rate which means that the sampling rate is more than twice to that of the maximum frequency component of the signal. When it is oversampled, the number of step sizes are more which will take more time to follow the analog signal. Likewise the speed will be less [4].

The second bottleneck of the traditional DWT is, db4 co-efficients are actually in floating point hence these should be transformed into the fixed point using various scale parameters before and after the computation. At the end the results are scaled down by the same parameter [5], due to which the system may obey the non-linear property and hence there may be a chance to decrease the system stability.

## 3 Realization of Standard Floating Point DWT for 3 Stage Using Filter Bank Approach

The primary objective of this research is to design the 3-stage floating point audio CODEC using floating point DWT. As the floating point DWT is constituted by the filter bank and it has been implemented by the sub-band coding advance as given in the following sections [6].

### 3.1 Sub-Band Coding

Sub-band coding can be explained with the successive decomposition of input signal through filter bank. The discrete wavelet transform crumbles a signal to a set of dissimilar resolution sub-signals correspond to the different frequency bands. It results in a multi-resolution representation of signals with localization in both the spatial and frequency domains [7]. It is attractive in the case of signal compression, but it is not possible in the case of Fourier Transform which gives good localization in one domain at the expense of other. Sub-band coding is a process in which the input signal is divided into various frequency bands. The filter bank is a compilation of filters which are having a similar node either at output or input. If filters have a common node (N) at the output, they form the synthesis bank and when they share a common node (N) at the input, they form the analysis bank which is shown in Fig. 1. The fundamental concept of filter bank is divide a signal equally at the frequency domain [8, 9].

### 3.2 Perfect Reconstruction Filters

The above Fig. 1 shows the two-band analysis cum synthesis filter bank system. In the analysis bank  $H_0(z)$  and  $H_1(z)$  are the low pass and high pass FIR filters respectively. Similarly, in the synthesis filter bank  $F_0(z)$  and  $F_1(z)$  are the low pass and high pass FIR filters respectively. From the above Fig. 1 the final output  $X(Z)$  is given by

$$X(Z) = 1/2[H_0(Z)F_0(Z) + H_1(Z)F_1(Z)]X(Z) + 1/2[H_0(-Z)F_0(Z) + H_1(Z)F_1(Z)]X(-Z) \tag{1}$$

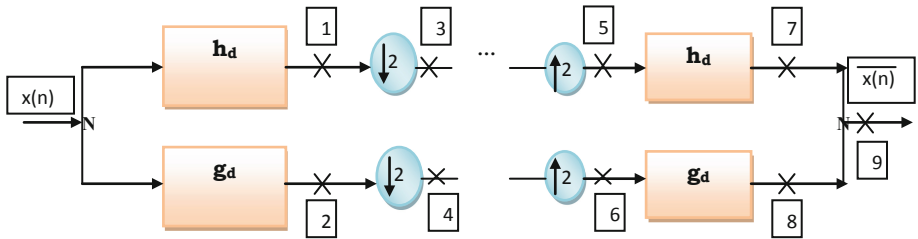


Fig. 1. A two band analysis cum synthesis filter bank system

Alias can be cancelled by choosing the filters such that the quantity in Eq. 6.9,  $H_0(-Z) F_0(Z) + H_1(-Z) F_1(Z)$  is zero [9].

Thus the following choice cancels aliasing.

$$\begin{aligned} F_0(Z) &= H_1(-Z) \\ F_1(Z) &= -H_1(-Z) \end{aligned} \tag{2}$$

For the  $H_0(z)$  and  $H_1(z)$  it is possible to completely cancel the aliasing by the choice of synthesis filters [10].

In the matrix form expression 1 can be written as –

$$z. \widehat{x(z)} = [x(z) \cdot x(-z)] \underbrace{\begin{bmatrix} H_0(Z) & H_1(Z) \\ H_0(-Z) & H_1(-Z) \end{bmatrix}}_{H(z) = \text{Alias component matrix}} \begin{bmatrix} F_0(Z) \\ F_1(Z) \end{bmatrix}$$

The matrix  $H(Z)$  is called the aliasing component (A.C) matrix. The term which contains  $X(-Z)$  originates because of the decimation. On top of the unit circle,  $X(-z) = X(e^{j(w-\pi)})$  which is a right shifted version of  $X(e^{jw})$  by an amount of  $\pi$ . This term takes into account aliasing due to the decimators and imaging due to the expanders [11]. It could be referred this just as the alias term or alias component.

### 3.3 Elimination of Aliasing Effect

When the input signal to the decimator is not band-limited, then the spectrum of decimated signal has aliasing. Hence, the input signal should be band-limited to  $\pi/D$ , where  $D$  is the decimator.

### 3.4 FIR Filters

For the multi-rate signal processing, FIR filters are chosen than IIR filters because

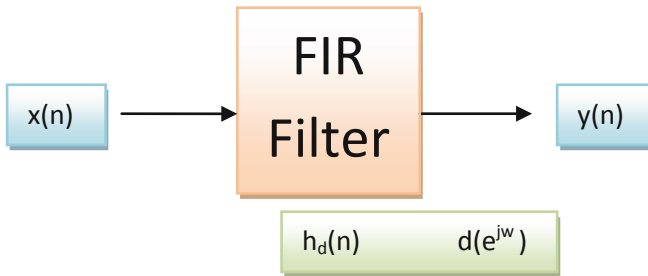
- (1) FIR filters are stable
- (2) FIR filters can be designed with exactly linear phase
- (3) Limit cycles are not produced in the FIR filters since these filters are not having feedback [12].

FIR filters can be designed using three techniques i.e.,

- (1) Fourier series technique
- (2) Frequency sampling technique
- (3) Window technique

Because, in this research Daubechies-4 window which is suitable for audio applications is used, the design of FIR filter using window technique is illustrated here.

#### 3.4.1 FIR Filter Using Window Technique



**Fig. 2.** FIR filter

The above Fig. 2 shows the FIR filter. In Fig. 2

$$\begin{aligned}
 h_d(n) &= \text{Fourier coefficients having infinite length} \\
 &= 1/2\pi \int_{-\pi}^{\pi} H(e^{jw}) \cdot e^{jwn} dw
 \end{aligned} \tag{3}$$

$$\begin{aligned}
 H_d(n) &= \text{Fourier series representation of } h_d(n) \\
 &= \sum_{n=-\infty}^{\infty} h_d(n) \cdot e^{jn}
 \end{aligned} \tag{4}$$

### 3.4.2 Daubechies Wavelet Co-efficients

Because of the 3-stage Standard floating point audio CODEC is to be implemented by DWT using multi-rate analysis, the window size is not fixed which means that analysis is to be done for different frequency bands by the high pass and low pass filters with the different resolutions by the decimators. As the specifications are changed window to window, a superior exercise is required to find the resultant filter co-efficients. After a lot of exercise, Prof. Ingrid Daubechies, had invented the low pass and high pass filter co-efficients for various applications and released for the public domain. It is important to note that the objective of this research is not to introduce the wavelet concepts starting from the scratch, but to present the application of wavelet in the field of signal compression such as in audio applications. But, in general to find the order of the filter (N); the transition frequency ( $\Delta f$ ), sampling rate (fs), pass band attenuation ( $\square_p$ ), stop band attenuation ( $\square_s$ ) are required. If the response of the low pass filter is considered with various specifications as given below,

- $f_s$  = sampling rate
- $\Delta f$  = transition frequency
- $\square_p$  = pass band attenuation
- $\square_s$  = stop band attenuation

The order of the filter (N) could be found with the empirical relation as given below:

$$\begin{aligned}
 \Delta f_{\min} &= f_s/N \text{ or} \\
 \Delta f &\approx f_s/N * [\text{Atten}(\text{db}) - 8]/14 \text{ or} \\
 N &= f_s/\Delta f * [\text{Atten}(\text{db}) - 8]/14
 \end{aligned} \tag{5}$$

There are different mother wavelets like db2, db4 and db6 etc., which are invented by Prof. Ingrid Daubechies and for each one, there is a specific application. Some of the basic wavelets are explained as given below.

#### db2 Wavelet

db2 wavelet is also called Haar wavelet. It has 2 vanishing movements.

**db4 Wavelet**

As the name itself, db4 is having the four vanishing movements. It is specified for the audio applications. The filter co-efficients are extracted from the Matlab command as given below:

```
?[L.H] = orthfilt(dbwavf('db4'))
```

$$L = -0.1294 \quad 0.2241 \quad 0.8365 \quad 0.4830$$

$$H = -0.4830 \quad 0.8365 \quad -0.2241 \quad -0.1294$$

**db6 Wavelet**

It has 6 vanishing movements. It is used for C.T scan to identify the tumors by EEG and ECG.

**3.4.3 Stage Standard Floating Point DWT Implementation**

This section illustrates the implementation of the Standard floating point DWT decomposer and the DWT re-constructor.

**Standard DWT Decomposer and Re-structor**

Figures 3 and 4 show the 16 bit floating point Standard DWT decomposer and re-structor respectively. Its operation is explained in the below sub-sections.

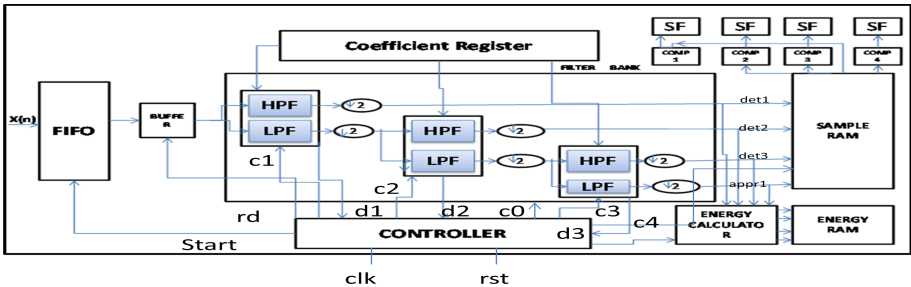


Fig. 3. 16-bit floating-point decomposer

The proposed 16-bit Standard floating-point DWT consists of various modules [5]. Each module can be explained in the below sub-sections.

**FIFO**

This module takes the signal sample and stores in the memory location. Once the FIFO module gets filled up the stored data is approved to the input buffer module. The FIFO module accepts the data when start signal goes high and passes data out to the input buffer module under read signal going high. The FIFO consists of 16 locations and passes out parallely 16 samples of data at a time to the buffer module.

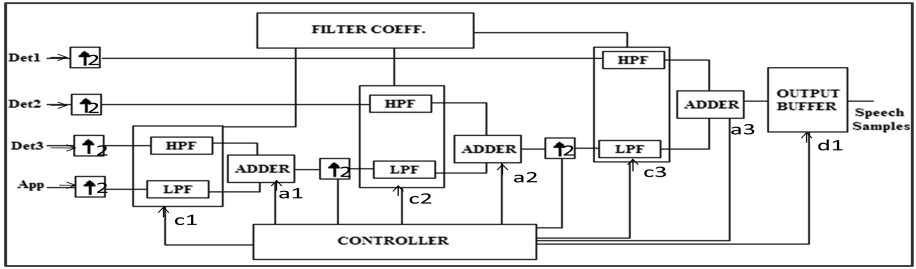


Fig. 4. 16 bit floating point re-constructor

### Input Buffer

The module takes the data from the FIFO unit and packetizes the data and passes to the filter bank module. On every system clock the module passes out four samples each to the data transfer to attain synchronization between the data received and the filter bank operation.

### Filter Bank

The Standard floating point DWT design consists of the core unit as the filter bank, which contains three banks of high-pass and low-pass filters. The filters decompose the input-signal samples into various sub bands depend upon the filter co-efficients sent to it.

### Filter Stack

The filter stacks are the sub-modules of the filter bank where a pair of high-pass and low-pass filters are embedded into it. The high pass filter performs convolution operation between the input signal and the filter co-efficient passed from the co-efficient register. The convolution operation is carried out by the implementation of a floating point multiplier and a floating point adder module followed by shifting operation.

The high pass filter extracts the upper frequency components from the signal that get decimated by 2. The obtained samples are then passed down to SRAM unit where the samples get stored into the memory unit. The high pass unit gives the detail co-efficients and the low pass filter gives the approximate co-efficients which get further decomposed into its individual components. The low pass filter carries out the operation similar to high pass filter.

### Controller

The controller is the control unit of the standard DWT design. It generates the control signals to different modules for its proper functionality. The controller reads the status of the filter stack as d1, d2 and d3 signal and generates appropriate control signals to the filter stack for its proper functioning. The controller gives the start signal to the FIFO unit when the system is reset and on the completion of FIFO filling generates a control signal to energy RAM and sample RAM to store the obtained samples and their energy.

### Co-efficient Register

This unit holds the filter co-efficients for the filter unit and passes the co efficient to the filter bank for its operation.

### Sample RAM

The detail and approximate co-efficients obtained from the filter bank are stored into the sample RAM unit. Sample RAM unit consists of  $9 \times 4$  memory location to store the sub band samples. Each band is stored separately in sequence in the memory location.

### Energy RAM

This module calculates the energy of each sample unit. The energy of a sample is calculated as square of the magnitude sample.

### Comparator

The comparator module compares the obtained detail co-efficients and approximate co efficient elements in each sub band and finds the highest value in every sub band. The obtained value is the scale-factor for that sub band stored as Sfac1, Sfac2, Sfac3 and Sfac4.

### Operation

The samples of the speech or audio whichever is to be processed that should be applied at the input of the FIFO of Fig. 3. As soon as controller sends the start signal to FIFO, it commences to accept the samples from the input. Because, FIFO length is  $16 \times 16$ , it stores the maximum of sixteen samples with the 16-bit length of each. Whenever FIFO is filled by the 16 samples it sends the first 4 samples to the buffer. From the buffer, the four samples are applied to the first section of the high pass filter and low pass filter of the filter bank. The low-pass and high-pass filters perform convolution operation between the input samples which come from the buffer and the high pass filter co-efficients from the co-efficient register. After convolution, HPF sends its output to the decimator. The decimator reduces the number of samples by 2 and then sends its output to the sample RAM. The components stored in this manner in sample RAM through the first section of the HPF are called detail1 components or det1. In the similar way, the convolution operation is carried out by the first section of the LPF between the samples come from the buffer and the low pass co-efficients from the co-efficients register. The output of the LPF is sent to the decimator for the decimation process. It reduces the number of samples to the half and sends its output to both HPF and LPF of the second section. After convolution, the outputs of the HPF which are called detail2 (det2) components, stored in the sample RAM and the outputs of the LPF are applied to the decimator. After decimation process, these will be applied to the third section of the HPF and LPF. The HPF performs the convolution operation and sends the detail3 (det3) components to sample RAM and the output of the LPF which are approximate components (appr1) are also sent to store in sample RAM at the end.

The comparator (comp) compares the respective detail and approximate components and sends the maximum component to the scale factor (SF) section. The reconstructor reads the detail components and approximate component from the scale factor section of the 16-bit floating point decomposer of Fig. 4. In the reconstructor side interpolators are used to obtain the samples which were dropped by the decimator during transmission. In the same way, adders are used to reconstruct the high pass and low pass filters' output. The reconstructor operation is exactly vice-versa to the decimator operation. At the output of reconstructor, the same signal of  $x(n)$  which was applied near the input of decomposer could be observed.

## 4 Results

This part presents the simulation and synthesis outcome of Standard floating point DWT.

### Standard Floating-Point DWT

The simulation for the Standard-floating point DWT design is carried-out by the Modelsim 10.3cl. Since, the Modelsim has not the floating point packages, the customer defined floating point library packages are implemented and added with the standard library of the Modelsim tool. Now by porting the 16-bit floating point values using the testbench, the output would be obtained as shown in Fig. 5.

### Simulation Results

Table 1 shows the simulation results of the Fig. 5 at particular instant of time t1 in binary. For easy understanding the same Table 1 was shown in Table 2 in decimal which states that the error is zero between the transmitted (input) and the received (output) values.

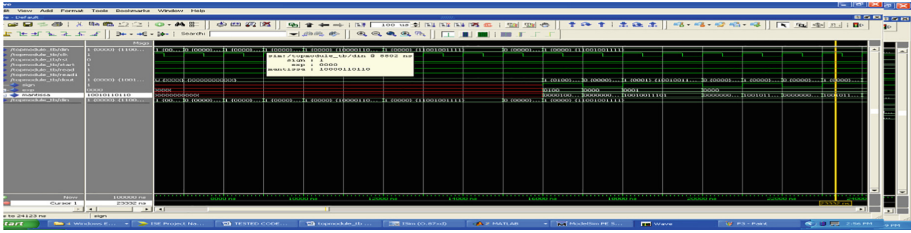
**Table 1.** Using floating-point binary values

Figure	At time	Input value (Binary)	Output value (Binary)	Error
5	t1	1000010000110110	1000010010110110	Zero

**Table 2.** Using floating point decimal values

Figure	At Time	Input value (Decimal)	Output value (Decimal)	Error
5	t1	$-7.6444 * 10^{-06}$	$-7.6444 * 10^{-06}$	Zero





**Fig. 5.** The input and output values of the standard floating point DWT at particular instant of time say t1

**Synthesis Results**

The synthesis is developed by Xilinx Synthesis Technology (XST) tool. The chosen hardware device is Xc2s50e-ft256-6. The speed rating is -6. In this machine, the maximum number of IOs are 182 and the maximum number of BELs are 1728.

Figure 6a shows the top module of the Standard floating point DWT with pins from 0 to 15 among which 0 to 10 range is for the mantissa, 0 to 3 range is for exponent and 1-bit for sign. Figure 6b shows that internal RTL structure between FIFO and buffer. Figure 6c–d show the overall RTL diagrams of the Standard floating point DWT.

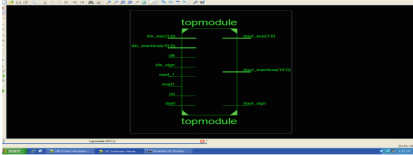


Figure 6.15(a)

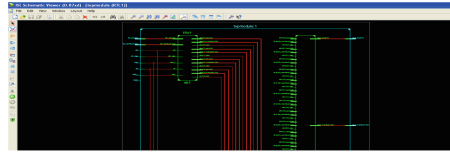


Figure 6.15(b)

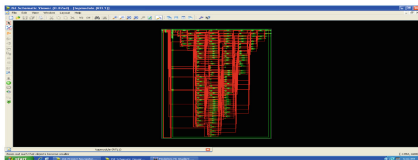


Figure 6.15(c)

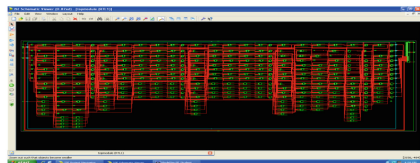


Figure 6.15(d)

**Fig. 6.** RTL diagrams of standard-floating-point DWT

**Synthesis Details**

By the Table 3, it is known that the attained speed of the Standard floating-point DWT is 377.501 MHz through the power utilization and delay of 38.64 mw plus 2.649 ns respectively. The hardware resources that were taken by the Standard floating point DWT be 57% of IOs and 11.8% of BELs.

**Table 3.** Synthesis results for Standard floating-point DWT

Hardware parameters	Standard DWT
No. of IOs	105 out of 182 (57%)
No. of BELs	205 out of 1728 (11.8%)
Min. period	2.649 ns
Maximum speed	377.501 MHz
Power utilization	38.46 mW

## 5 Conclusion

The Standard floating-point DWT had been realized here is by the consumer defined floating-point – library-package with IEEE 754 standard. In the fixed-point DWT, the ADC and DAC need to be used physically but by develop the user defined floating-point package, a logical link had been given between source and DWT instead of physically connected data converters. To the Standard floating point DWT half precision is used; in which 1 bit is used for sign, 4-bits are used for the exponential and 11 bits are allotted for the mantissa.

## References

1. Bishop, S.L., Rai, S., Gunturk, B., Trahan, J.L., Vaidyanathan, R.: Reconfigurable implementation of wavelet integer lifting transforms for image compression, 1-4244-0690-0/06/\$20.00 ©2006 IEEE
2. Grzeszczak, A., Mandal, M.K., Panchanathan, S.: VLSI implementation of discrete wavelet transform. *IEEE Trans. VLSI Syst.* **4**, 421–433 (1996)
3. Rioul, O., Duhamel, P.: Fast algorithms for discrete and continuous wavelet transforms. *IEEE Trans. Inf. Theory* **38**(2), 569–586 (1992)
4. Mahmoud, M.I., Dessouky, M.I.M., Deyab, S., Elfouly, F.H.: Comparison between haar and Daubechies wavelet transformations on FPGA technology. In: *Proceedings of World Academy Of Science*
5. Vaidyanathan, P.P., Nguyen, T.Q., Doganata, Z., Saramaki, T.: Improved technique for design of perfect reconstruction FIR QMF banks with lossless polyphase matrices. *IEEE Trans. Acoust. Speech Signal Process.* **37**, 1042–1056 (1989)
6. Leong, M.H., A'ain, A.K.: Simple analogue active filter testing using digital modelling. In: *2003 Proceedings of Student Conference on Research and Development (SCORED)*, Putrajaya, Malaysia (2003)
7. Kotteri, K.A., Bell, A.E., Carletta, J.E.: Polyphase Structures for Multiplierless Biorthogonal Filter Banks”, 0-7803-8484-9/04/\$20.00 ©2004 IEEE, ICASSP (2004)
8. Malah, D., Crochiere, R.E., Cox, R.V.: Performance of transform and subband coding systems combined with harmonic scaling of speech. *IEEE Trans. Acoust. Speech Signal Process.* **29**(2), 273–283 (1981)

9. Barbedo, J.G.A., Lopes, A.: On the vectorization of fir filterbanks. *EURASIP J. Adv. Signal Process*, 10 pages (2007). <https://doi.org/10.1155/2007/91741>. Article ID 91741
10. Dempster, A.G., Murphy, N.P.: Efficient interpolators and filter banks using multiplier blocks. *IEEE Trans. Signals Process.* **48**(1), 257–261 (2000)
11. Schafer, R.W., Rabiner, L.R., Herrmann, O.: FIR Digital Filter banks for speech analysis. *BEL Syst. Tech. J.* **54**(3), 531–544 (1975)
12. Aswale, M.M., Patil, R.B.: VHDL implementation of multiplier less, high performance DWT filter bank. In: *Proceedings of the World Congress on Engineering, WCE 2007*, vol. I, 2–4 July 2007, London, U.K (2007)



# A Novel for Analytical Healthcare Using Message Queue Telemetry Transfer

C. Anna Palagan<sup>1(✉)</sup> and K. Soundara Rajan<sup>2</sup>

<sup>1</sup> Department of Electronics and Communication Engineering, Teegala Krishna Reddy Engineering College, Medbowli, Hyderabad, India  
annapalagan7467@gmail.com

<sup>2</sup> Teegala Krishna Reddy Engineering College, Medbowli, Hyderabad, India  
rector.jntua@gmail.com

**Abstract.** IoT evolution plays an important role in healthcare applications for data sharing and patient monitoring systems. Patient related information is to be stored securely in health care data management system. By using this database management systems, patient status can be estimated. To identify the quality of analytical data, which is collected from healthcare sensors based on the trail sets. In our proposed system, we used a PI sensor for better results and it will continuously update the information about the patient to the server by using Message Queue Telemetry Transfer (MQTT) protocol. Massive sensors receives the condition of both current health conditions and previous health condition and that will be compared. If any changes found, it will immediately give the alert to the doctor and to the care taker. Machine to Machine (M2M) communication has been established to transfer the data with very high speed. Due to high speed connectivity, the result of patient monitoring will be very accurate and the patient's life can be saved without any delay.

**Keywords:** Internet on Things · Message Queue Telemetry Transfer · Machine to Machine (M2M) transfer · Passive infrared sensor · Health monitoring system

## 1 Introduction

In past years the death rate of human being in the remote areas is increased due to unavailability of habitual treatment as a result of non-availability of modern monitoring system of health and doctors not having proper resources for the treatment of patients in the remote areas. For monitoring health there are many updating systems are available in urban area, but in most of the places due to high cost of machines used for measuring human health the doctors not used the modern machines. According to the survey of World Health Organization (WHO), due to the above mentioned reasons the death rate of human beings is increased everyday at a ratio of both genders is nearly 250/169 in the age ranges from 15 to 60 years of age. From the world population nearly 15% peoples having any one disability, because of the changes in environment created by human beings which causes many diseases like stroke in heart, diabetes, cancer etc., introduced in the modern world. The proposed system avoiding this kind of problems

by using MQTT health based analytical device that monitoring the patient endlessly in all parameters with low cost. For adult's heart disease, diabetes and cancer are the diseases are the most frequent health issues. For these kind of diseases it is not possible to monitor and taking treatment in the remote area due to unavailability of health service which has some limitations of not have sufficient data of the health condition of the concern person and the treatment also taken more cost. So we need the best database of the patient which consists of the complete set health care at anywhere with portable devices and common internet services.

The inspiration to obtain up this development is the humanity is characterized by elevated expenses for its healthiness scheme and reduction effort energy outstanding to healthiness reasons and an aging people. We preserve realize a enormous existence with superior knowledge equipment's in health check discipline and analytical centers and pleasing hale and hearty diet. These aspects position a massive force on the wealth and the common arrangement. Individual way of life and ecological collision factors are the majority momentous hazard factors influencing healthiness standing. For dropping these types of diseases hospital/physicians require to get good quality and appropriate information on fitness monitoring diseases.

### 1.1 Problem Definition

As we be acquainted with massive consequence of doctors nowadays, if we interrelate together internet and health center jointly after that on a regular basis updating of patient can with no trouble complete and monitoring too will be trouble-free. At this time if any dangerous situation is raised then without delay based precedence handling will be completed. Although in this arrangement MQTT place most important responsibility by occupying a smaller amount data package, data centric, fast communication of data and absolute set of connections can be transportable one.

### 1.2 Objectives

At the present time, the biomedical instrumentation holds a well-known location with medicine. Subsequent the tendency, the BPM (Beat Per Minute) has turn into an significant instrument to clarify regarding the implementation of the human being and come around for anomalies by monitoring the heartbeat in the human being body. These strategy are more often than not used hospitals and clinics but are slowly decision their method into domestic use. This manuscript demonstrates on an come within reach to plan a inexpensive, precise and dependable mechanism which can with no trouble calculate the heart rate of a human being body physical condition monitoring arrangement. This apparatus employs a uncomplicated Opto electronic sensor, impecunious on the finger, to give nonstop signal of the pulse digits. The pulse monitors workings together on battery and mains supply. It is superlative for unremitting monitoring in process theatres, ICUs, biomedical/human being engineering studies and sports medicine. In this organization we contain worn high presentation PI which is incessantly updating to server by using MQTT (Message Queue Telemetry Transfer) protocol [1] anywhere we know how to see far above the ground speed data transfer with best M2M connection. To propose a scheme which enables uninterrupted health

monitoring of patient and recurrent updating to hospital server, this notifies the care taker and doctor to take essential action. In addition it provides massive sensor verification to measure up to present and earlier health condition.

## 2 Literature Review of Existing Work

Akram et al. [1, 3] described a sensor containing small device which measures the heart beat and finding health problem which sends message to the doctor and care taker by using http protocol. The speed of this protocol is slow and efficiency also not good for the supervisory control. The server and client elements are mismatched due to not delivering of messages properly. Distribute/subscribe protocols assemble improved the IOT necessities than demand/response because clients do not contain to apply for updates therefore, the network bandwidth is falling and the requirement for using computational resources is reducing by Liu [2].

Niewolny [4], recommended a statement concerning In the Internet of Things (IoT), devices get together and split information in a straight line with every additional and the cloud, creation it likely to assemble, record and examine novel information streams quicker and extra perfectly. Now a day the healthcare systems based on IoT having important determination as a system of devices that unite unswervingly through each other to confine and contribute to vital data from beginning to end a secure service layer (SSL) that connects to a middle command and control server in the cloud.

Rahane et al. [5] presents the system design for elegant Healthcare by means of Wireless Sensor Network (WSN) with GSM Module and Microcontroller. The controller node has emotionally involved on body of patients for collecting the signal from wireless sensors. The wireless sensors propel this signal to base station or control room of medical doctor. This wireless sensors form wireless body sensor network (WBSN). Node of every WSN collected of health care sensors and RF transceivers which propel data to rear end sever. Sensors can decide in the variety of WSNs, while RF transceivers are implemented as a controller which manages WSN additional than frontwards data. The sensing data of every patient are stored in back-end server by means of everyone have its individual ID. The data investigation, database examination, data manning and the system organization are processed on the web page of server. The system can notice irregular situation of patients and launch the SMS or e-mail to the medical doctor.

Ullah et al. [6] demonstrate a representation named as “k-Healthcare” makes apply of four layers, internet layer, service layer, sensor layer and network layer. There are number of sensor worn similar to pulse oximetry, Aurduino, Raspberry Pi, RTX-4100 and smart phone sensors. Communication stuck between layers is completed from end to end IEEE 802.15.4, 802.15.6, IEEE 802.11/b/g/n, Zigbee etc. For data storage space organization the system use cloud storage. The anticipated scheme sustains dissimilar protocols and similar to HTTP, HTTPs, RESTful and Javascript web services. Malokar et al. [7] proposed a system which contains temperature detector which is used to detect the temperature and covert the analog form of temperature into digital form by using ADC. By means of python based pulse oxymetry detectors calculate pulses as fine as oxygen dispersion echelon in the blood. From patient body the blood pressure range

calculated by one detector used as blood pressure detector which gives the diastolic as well as systolic level of body blood pressure. By using Python these information will be send to the Personal Computer through TCP/IP protocol. By using AES algorithm for 128 bits the above data's are encrypted. By computer all these information's are decrypted and the final information is stored in the data set. By using PHP and HTML anyone can browse these information and it will be shown on web page.

Ukil et al. [8] introduces a new method that detects the anomaly detection of the healthcare analytics. From the Biomedical signal the anomalous parts of the entire region will be taken for analysis. This region holds the practical parameters of the human health condition in the medical professionals. In this method it used to minimize the diagnosis error and it maximize the diseases detection and find out the diseases at very early stage. Al-Fuqaha [1] introduce innovative techniques with neat objects along through their hypothetical responsibilities comprise domain exact applications even as everywhere computing and investigative services form application area autonomous services. Howitt et al. [9], converse several key issues approaching up in wireless meadow bus and wireless manufacturing message systems: (i) essential troubles similar to achieving appropriate and steadfast broadcast although channel errors; (ii) the custom of obtainable wireless technologies for this exact pasture of applications, and (iii) the conception of mixture systems in which wireless stations are incorporated into obtainable wired systems. Lin [10], In the planned wireless system, the ECG monitoring function is developed based on the communications manner, which requires a permanent base station (BS) to be associated to an reputable permanent network infrastructure. This BS provides a announcement gateway for wireless ECG sensors worn by patients inside its variety. The data composed from the ECG sensors shabby by numerous patients is transmitted wirelessly to a close at hand BS.

Krishna et al. [12], proposed a system which discuss about the implementation of the protocol MQTT which having less number of sensor node and the sensor network node used for embedded systems. Production with IoT, data gathering is the main goal and this is completed throughout wireless sensor node network and the gateways, these function on near to the ground handing out rate footprints and short bandwidth wireless communication channels, smooth the gateways which are worn as servers have to be charge efficient. [Asiandatasience.com](http://Asiandatasience.com) [13], describes the most important principle of IoT platforms is to diminish the complexities for IoT developers, examine providers, and implementers. Consider of an iceberg; the majority of the ice accumulation is flooded under the waterline.

### 3 Proposed System

In our proposed system an analytical model is available to monitoring the healthcare of the patient for analyzing the health condition of the patient. It consists of computer with single board which used Raspberry pi version 3 has an processor speed 1.2 GHz with ARMv4 BCM2837 and System On Chip processor that includes built in Bluetooth Low Energy and Wi-Fi with RAM of 1 GB. From the sensor all parameters are taken these parameter values updated on the server through Raspberry pi beginning anywhere through MQTT it resolve to be available to the [cloudmqtt.com](http://cloudmqtt.com) which force proceed as

the agent and the client i.e. MQTTLENS App will accept survive situation of the patient and according to several irregularity and captivating care of the critical situation of the patient it will be sent all the way through SMS to the Doctor, Nurse or care taker consequently using the Twilio API. Also a neighboring authenticated server is completed anywhere all the patient physical condition values will be modernized, which can only be authenticated by the Doctor. MQTT is a standardized distribute/subscribe messaging protocol. It was designed in 1999 for make use of on satellites and as such is extremely heart-weight through low down bandwidth necessities creation it perfect for M2M or IoT applications. As such, it has developed into single of the majority frequent protocols for those situations. When it comes to devices communicating more than TCP/IP, there is no lack of protocols. The key is choosing the right one. Accepting the protocol is division of choosing it intended for your application. For message brokering us can use another one protocol but using MQTT in most IoT devices makes the right one produce perfect result in heart weight protocol. Appropriate application of wireless technology has the probable to amplify usefulness, reduce costs, and usually get better the excellence of healthcare. Wireless devices are supposed to be considered and shaped in a method that ensures so as to the device will not conciliation the clinical condition or safety of a patient, or the safety and health of the client or any additional person, at what time the device is second-hand on a patient.

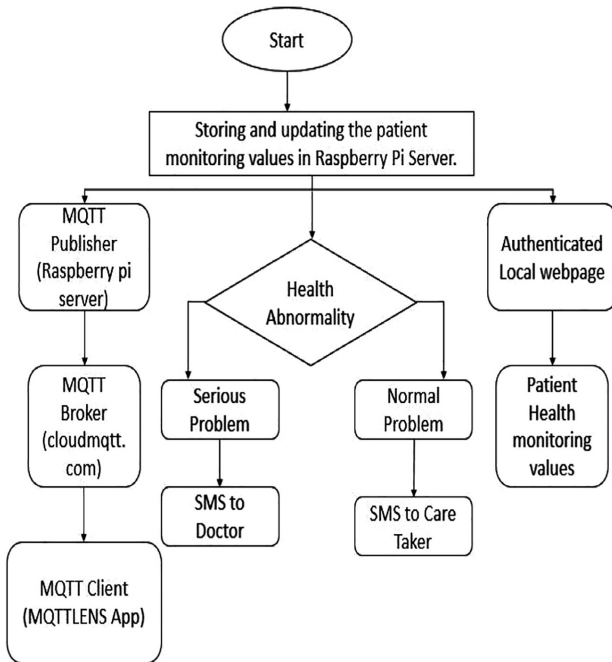
By using the device it should accept the risks when the intended benefits of the patient weight associated with the risky level and the level of protection is compactable compared to the safety and the health of the patient. Wireless Communication Systems plays a major role in the healthcare applications which includes for managing the health condition of the patient effectively with the constant flow of information given to the servers. In the last some decades, this information could include be deliver to every ward through a single computer station, which is unwieldy, protracted, and takes precious time missing from monitoring and caring for patients. But by using wireless devices the monitoring of patient charts, medical histories and laboratory results in real time is possible as simple and low cost. There are also profit in dropping paperwork and unnecessary human interchange. A lesser amount of time is necessary inputting remarks and additional time presented to spend with patients. Connecting patients to monitors and monitors to local area networks requires a huge quantity of cables. This cabling is usually not convenient and predominantly difficult if a patient requirement to be movable or a patient is motionless but the arrangement of equipment (operating table, anaesthesia equipment and monitors) is rearranged.

### 3.1 Methodology

The methodology designed by PYTHON i.e. High level programming is represented by flow chart given below. According to the flow chart the program starts with collecting all parameters from the sensors and updating the same to the server of the Raspberry pi first and the updating is continued. The operations performed in Message Queue Telemetry Transfer have three major steps that include first PUBLISHER, second



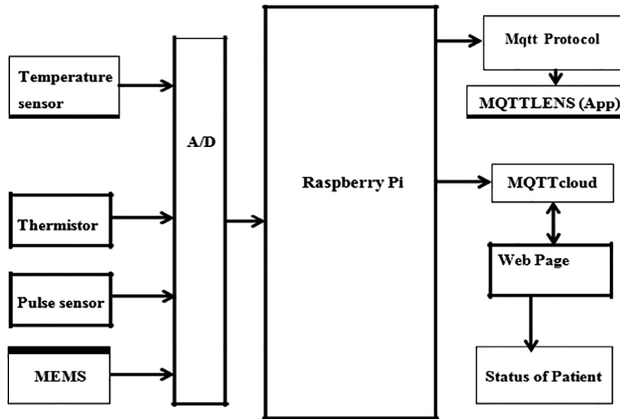
BROKER and third is CIENT. The sensor parameters updating in Raspberry pi is PUBLISHER which keep the values and send to BROKER through cloudmqtt.com. The authentication is done in this by Authentication SID and one Token is inserted into the program. Now for CLIENT we can go with number of apps here MQTTLEN which is a Google app is used to get the patient health situation by means of the theme specified in the program. At the similar instance a local authentication web page is developed using HTML and PHP commencing wherever only doctor can observe the patient condition. And in addition if any irregularity in patient situation according to the critically situation a SMS will be sent to the Doctor, nurse or care taker (Fig. 1).



**Fig. 1.** Flow chart of the proposed method

### 3.2 Block Diagram

The block diagram for Human monitoring system is shown in Fig. 2 below. Initially it measure the parameters from the human body like Pulse counting sensor, motion of the body, temperature of body and room temperature. The patient pulse is counted by the pulse counting sensor and the body temperature sensor thermistor gives the temperature value of patient. The room temperature is measured by temperature sensor.



**Fig. 2.** Block diagram of proposed method

The hardware component Raspberry Pi version 3 is used as an processor which has an specification of 1.2 GHz operating speed with the ARM processor ARMv8 BCM2837 associated with System On Chip which includes built in BLE and Wi-Fi which has an range of 1 GB RAM. The temperature sensor used is LM35 which sense the room temperature. The thermistor LM370 is used to measure the body temperature of the human being. Pulse sensor and MEMS sensors are used to measure the heart beat and motion of the patient and then these values in analog forms is converted into digital form by using Analog to Digital Convertor finally the digital values taken from the ADC output is connected to the servers containing patient monitoring health system. Now this system shows the present condition of the patient. By using MQTT protocol all the above mentioned parameters are sending to the client from the server at the same time all values are updated in the local web page that is authenticated by the user. In this system the monitoring of the human body health condition measures the heart rate of the patient and it gives very reliable and accurate outputs. This system is very much cheaper than other health system because we are using very low price devices that make all parameter very accurate. These plans are regularly second-hand in hospitals and clinics excluding are slowly commences to their way into domestic use. In the block al the sensors from input stage is connected to raspberry pi in order to monitor the input region and all the output stages is controlled by sever. In first phase all sensors are attached to analog to digital convertor which gives digital data as input to raspberry pi. In the second stage present in Raspberry Pi it use ARM which contains SoC that plays a major role of monitoring the entire process done in the input stage. In the output end the Raspberry Pi act as an server by using the protocol MQTT and the output is monitored in the visual output medias like laptop or mobile phones by accessing only one particular host name. The usage of high speed and performance Raspberry Pi that updating the server values continuously by using MQTT protocol. For this continuous updation we need M2M connection which gives high speed data communication. To design scheme which enables uninterrupted health monitoring of patient and regular updating to hospital server, this notifies the care taker and doctor to

take essential action. It also provides massive sensor evidence to match up to current and earlier health condition. For example, visualize an easy system with three clients and a central broker. All three clients release TCP connections with the broker. Clients B and C subscribe to the topic temperature (Fig. 3).

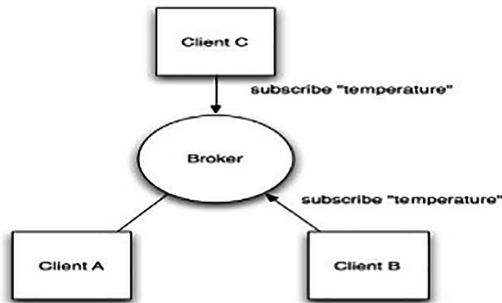


Fig. 3. MQTT architecture Example - I

At a afterward instance, Client A publishes a significance of 22.5 for topic temperature. The broker ahead the message to all subscribed clients (Fig. 4).

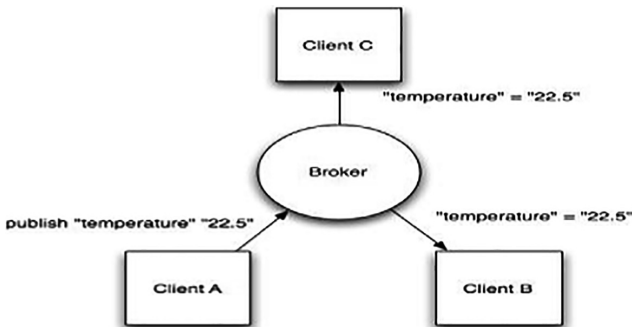


Fig. 4. MQTT architecture example - II

The publisher, subscriber representation allows MQTT clients to communicate one-to-one, one-to-many. This subsequent contented provides a client class which allow applications to unite to an MQTT broker to distribute messages, and to provide the topics and collect published messages. It also provides several assistant functions to create publishing one off messages to an MQTT server much uncomplicated. It supports Python 2.7 or 3.x, with incomplete hold up for Python 2.6. The MQTT protocol is a machine-to-machine (M2M)/“Internet of Things” connectivity protocol. Designed as a tremendously heartweight distribute/subscribe messaging convey, it is functional for

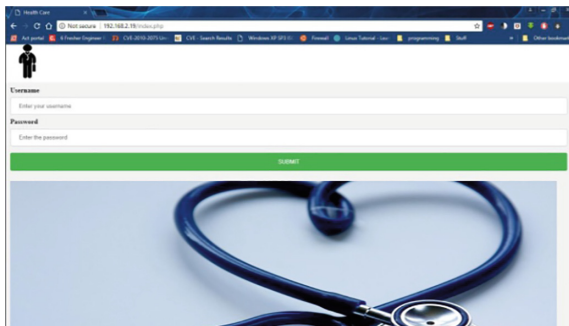
relations with isolated locations where a minute code footprint is compulsory and/or network bandwidth is at a quality.

## 4 Results and Discussions

In above Fig. 5 illustrates regarding the full hardware setup of scheme, wherever all sensors such as temperature, thermistor, pulse counting, mems sensors are linked to Raspberry Pi. In reality the web page will be evident through login information wherever login necessary compulsorily. If we not remember the password afterward also we can make new password by means of registered mail id. exhibit of webpage is shown in below Fig. 6.



**Fig. 5.** Hardware setup



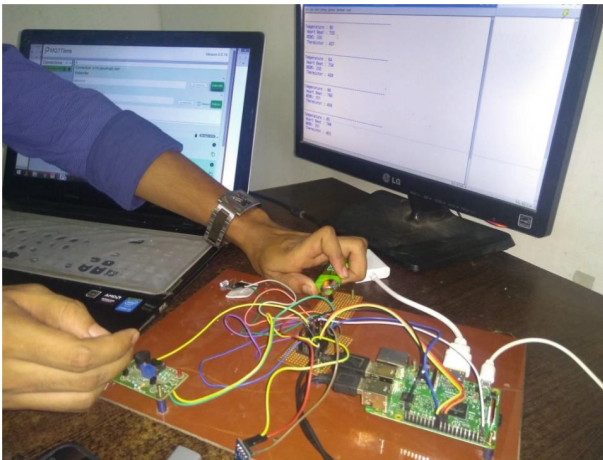
**Fig. 6.** Login page of patient

After POWER ON, it displays some chance values. In above figure we can as well see web page through login particulars. On webpage following login it exposed parameters of patient as

Heartbeat = \$\$\$ bpm  
 Temperature = \$\$ C  
 Thermistor = \$\$\$.\$ K  
 MEMS = \$\$

At any time a Patient is associated with sensors then raspberry reads digital data which will published to broker (i.e., server) and displayed on web page which will be acts as subscriber. As in lower Fig. 6 sensors are associated to patient body then, we can see a number of values of patient are regularly updating on page. In Fig. 6 we be able to see modify in only temperature collection only and thermistor only due to difference is applied to those sensors only. It shows as follows

Heartbeat = 80 bpm  
Temperature = 51 C  
Thermistor = 309.7 K  
MEMS = FITS



**Fig. 7.** Connecting all sensors to patient body variation in TEMPERTURE and THERMISTOR



**Fig. 8.** Connecting all sensors to Patient body variation in HEARTBEAT and MEMS

In Fig. 7 we can see modify in only temperature variety merely and thermistor only due to difference is functional to individuals sensors only. It shows as follows (Fig. 8)

Heartbeat = 69 bpm  
 Temperature = 51 C  
 Thermistor = 309.7 K  
 MEMS = NORMAL

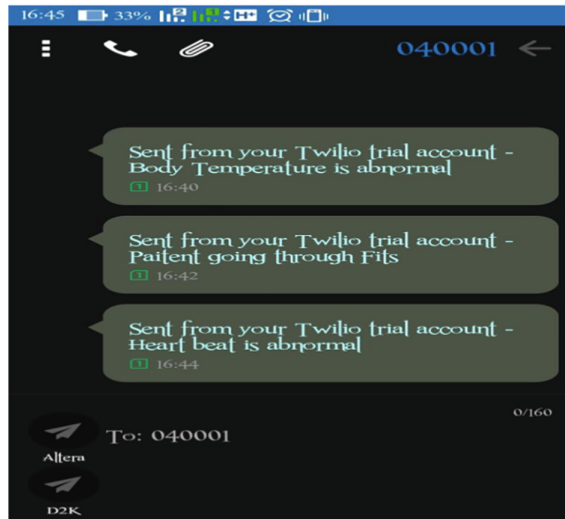


Fig. 9. In abnormality condition we can send SMS using Twilio

Above Fig. 9 illustrates whenever abnormality situation rises in any parameters, immediately message can be send to particular caretaker/doctor/nurse.

## 5 Conclusion and Future Work

In many of the existing system they used ARM-11 processors as hardware model having less number of integrated feature when compared to the Raspberry Pi processor. In our proposed work the ARM processor is replaced by Raspberry Pi processor which increases the speed of operation and cost effective. The MQTT used as protocol to transfer messages from the servers to the clients and M2M connection is made in between the systems. The occurrence of every component has been consistent out and located circumspectly. Using extremely sophisticated IC's like Broadcom BCM2387 chips.et, 1.2 GHz Quad-core ARM cortex-A53 (64 Bit) processor, Linux OS technology with the lend a hand of increasing knowledge. Thus the scheme has been effectively premeditated experienced. In future the implement is done by reducing complexity in circuitry design and manufacturing all sensors on one board.

## References

1. Al-Fuqaha, A., Guizani, M.: Internet of Things: a survey on enabling technologies, protocols, and applications. *IEEE Wirel. Commun.* **17**(4), 2347–2375 (2015)
2. Liu, Y.: The design and implementation of a virtual medical centre for patient home care. In: 20th IEEE Annual International Conference of Engineering in Medicine and Biology Society, Hong Kong, vol. 3, pp. 1163–1165 (1998)
3. Akram, A., Alam, K.M.: A survey on MQTT protocol for the Internet of Things. Case study, Department of Computer Science and Engineering (CSE), Khulna University, 9208, Bangladesh
4. Niewolny, D.: How the Internet of Things is revolutionizing healthcare, freescale.com/healthcare. <https://www.nxp.com/docs/en/white-paper/IOTREVHEALCARWP.pdf>
5. Rahane, S.L., Pawase, R.S.: A healthcare monitoring system using wireless sensor network with GSM. *Int. J. Adv. Res. Electr. Electron. Instrum. Eng.* **4**(7) (2015). ISSN 2278-8875
6. Ullah, K., Sha, M.A.: Effective ways to use Internet of Things in the field of medical and smart health care. In: International Conference on Identification, Information, and Knowledge in the Internet of Things. IEEE (2016). 978-1-4673-8753-8/16
7. Malokar, S.N., Mali, S.D.: A IoT based health care monitoring system. *Int. J. Adv. Res. Electr. Electron. Instrum. Eng.* **6**(6) (2017). ISSN 2278-8875
8. Ukil, A., Bandyopadhyay, S., Pal, A.: IoT healthcare analytics: the importance of anomaly detection. In: IEEE 30th International Conference on Advanced Information Networking and Applications (2016). ISSN 1550-445X
9. Howitt, I., Gutierrez, J.A.: IEEE 802.15.4 low rate –wireless personal area network coexistence issues. In: IEEE Conference of Wireless Communications and Networking, New Orleans, vol. 3, pp. 1481–1486 (2003)
10. Lin, B.S., Lin, B.S., Chou, N.K., Chong F.C.: A real-time wireless physiological monitoring system. In: IEEE Conference of Transactions on Information Technology in Biomedicine, vol. 10, pp. 647–656 (2006)
11. Raspberry Pi Forums: Implementation of bi-directional blue-fi gateway in IoT environment. <https://www.raspberrypi.org/forums/>
12. GopiKrishna, P., Srinivasa Ravi, K., Hareesh, P., Ajay Kumar, D., Sudhakar, H.: <https://www.sciencepubco.com/index.php/ijet/article/view/10338/3708>
13. <http://asiandatasience.com/wpcontent/uploads/2017/12/eBook-Internet-of-Things-IoT-2018-Market-Statistics-Use-Cases-and-Trends.pdf>



# Impact of Mobility and Density on Performance of MANET

Vaishali V. Sarbhukan<sup>1</sup>(✉) and Ragha Lata<sup>2</sup>

<sup>1</sup> Department of Information Technology, Terna Engineering College,  
Navi Mumbai, Maharashtra, India  
vaishali5780@gmail.com

<sup>2</sup> Department of Computer Engineering, FRCRIT,  
Vashi, Navi Mumbai, Maharashtra, India  
lata.ragha@gmail.com

**Abstract.** In Mobile ad hoc Networks (MANETs), discovering the stable, reliable and secure routes is a difficult analysis downside because of the open medium and dynamic topology. Most of the recent ways didn't solve the entire downside of data loss in MANETs as they targeted on distinguishing the malicious nodes and forestall them from electronic communication method solely. There are many different reasons corresponding to mobility and congestion of mobile nodes due to which the data could loss in MANETS. Thus planned theme ETSR is meant by considering these parameters so as to provide a more stable, reliable and secure routes.

**Keywords:** Mobile Ad hoc Network (MANET) · Mobility · Density · Secure routing path · Trust

## 1 Introduction

As of late, mobile ad hoc networks (MANETs) turned into a very much enjoyed examination subject on account of their self-design and self-upkeep capacities. Remote hubs will set up a dynamic system while not the need of a set foundation. The IETF set up the mobile ad hoc network systems unit in 1997, with the point of institutionalizing steering conventions for MANETs. Another IETF unit, alluded to as ad hoc systems engine vehicle setup, had as its principle point considering the issues inside the tending to demonstrate for specially appointed systems. MANETs utilize IEEE 802.11 outline components as portrayed in [1]. The essential Service Set (ESS) characterizes relate degree plan amid which all stations will impart between themselves utilizing IEEE 802.11 remote LAN innovation.

Due to mobility and quantifiability properties, Mobile ad hoc Network (MANET) is one among the foremost vital and distinctive applications. With ongoing advances in remote advances and mobile devices, mobile ad hoc networks (MANETs) wound up basic as a key correspondence innovation in military arrangement of activity conditions respect the organization of correspondence systems used to facilitate military preparing among the troopers, vehicles, and operational war rooms [2]. MANETS are used in a military setting to affirm the opportune stream of information and order in fight that



winds up in the achievement. MANETs give save administrations following catastrophic events appreciate seismic tremors or surges. Another significant use of MANETs is on-the-fly agreeable processing outside partner work environment climate. MANETs is used in correspondence dispatch frameworks for taxis in an exceedingly city. At long last, they'll even be used in individual systems administration. Sadly, the open medium, dispersed nature and dynamic topology [3–5] of MANET fabricate it defenseless against fluctuated sorts of steering assaults. Thusly, security is fundamental hindrance in plan of activity MANETs [6].

There are mainly two methodologies which will offer security in MANETs: prevention-based and detection based methodologies [7, 8]. Prevention-based methodologies are contemplated extensively in MANETs [9–11]. One issue of those prevention-based methodologies is that a brought together key administration framework is required, which can not be reasonable in appropriated systems acknowledge MANETs. In the event that the foundation is annihilated, at that point the full system could likewise be incapacitated. So detection based methodologies are most all around preferred. Existing detection based approaches take into account solely identification of malicious nodes however not take into account factors like mobility, density and energy state so these strategies cannot guarantee stable, reliable and secure path. By considering on top of mentioned factors, enhanced projected theme is intended known as ETSR, Enhanced Trust based Secure Routing. It has positive impact on performance of MANET for various eventualities like mobility and density of nodes beside secured sure values.

Rest of paper is sorted out as takes after. Section 2 provides related work. Section 3 depicts the projected system style, ETSR theme. In Sect. 4, the results and discussions with reference to mobility and density are conferred. Finally, Sect. 5 provides the conclusion.

## 2 Related Work

There are reputation based plans, cryptography based plans and trust based plans acclimated offer security in MANET. In [12] Shakshuki et al. gave EAACK (Enhanced Adaptive Acknowledgment) subject that is interruption location framework that is uncommonly intended for MANETs. EAACK has positive exhibitions against Watchdog, TWOACK, and AACK inside the instances of recipient impact, confined transmission control, and false offense report. Here Security is provided by DSA however because of crypto logical operations overhead is additional. Additionally it doesn't contemplate eventualities like variable speed, load on intermediate nodes. In [13] Buchegger et al. planned a strong reputation system for wrongdoing recognition in mobile ad-hoc networks. Amid this approach, every hub keeps up a reputation rating and a trust rating about every other person that they think about. Each hub utilizes it's rating sporadically order distinctive hubs, reliable with two criteria: (1) typical/acting mischievously (2) dependable/deceitful. Likewise Reputation-based plans experience the ill effects of false allegations wherever some fair hubs are distinguished mistakenly known as malevolent. This can be because of the hubs that drop parcels rapidly, e.g., as a result of blockage, is likewise inaccurately known as vindictive by its neighbors.

In [14] BDSTTM (Bayesian Dempster Shafer Theory based Trust Model), DST technique that is a component of unsure reasoning is employed to look at every node in network and task is performed while not secure trustworthy party (TP). This can be one in every of major issue with [14]. Another challenge of this technique is that it improves throughput and packet data rate (PDR) however average finish to finish delay and overhead is just too high. Reason behind this can be that formula utilized by authors during this paper. During this formula every node in network cross verify every and each neighbors, this method takes lot of time and clearly overhead and delay can increase. In brief BDSTTM [14] focuses solely on analysis of realistic and correct trust worth however doesn't contemplate energy and secure routing path. Additionally procedures including second hand perception in many methodologies is only acclimated evaluate the responsiveness of hubs, that don't appear to be inside the shift of the onlooker hub. Hence, erroneous trust esteems is additionally determined. Also, most techniques of trust investigation from direct perception [14] don't separate data bundles and management bundles. Be that as it may, in MANETs, management bundles regularly are more essential than data bundles. In [15] Mohamed M. E. A. et al. thought of energy in conjunction with trust worth to get stable, reliable and secure route. Here payment system is integrated with trust system to ascertain stable, reliable and secure routing path. Security is provided by SHA (Secure Hash Algorithm) formula. However downside was that point taken by this formula is additional for routing communication. Different issue that to ascertain stable route they contemplate solely trust and energy however doesn't contemplate mobility and load on any explicit intermediate nodes. In [16] Hisham et al. presented a trust based generally threshold cryptography key administration for Mobile ad hoc Network. Threshold cryptography has checked to be an effective topic for key administration and dispersion. Amid this framework, threshold cryptography supports security association institution between mobile nodes during a web of trust. It permits the supply and furthermore the goal hubs to with progress finish an authentication chain revelation despite the measure of reliable hubs inside the area of the asking for hubs is unfathomably low. Anyway expanding quality, diminishes the bundle conveyance size connection as a consequences of expanding routing disappointments. In short many solutions conferred supported reputation techniques, cryptography techniques, trust based mostly strategies, and hybrid solutions to guard MANET's communications, but most of the recent strategies centered on characteristic the malicious nodes and forestall them from electronic communication method solely. Such strategies didn't solve the whole downside of data loss in MANETs.

### 3 Proposed System

Figure 1 shows framework of planned system ETSR. It has three main sections information transmission phase exploitation onion routing, trust analysis and update section and stable route institution. Reliable trust-based and energy-aware routing protocol, ETSR establishes stable, reliable and secure routing path in MANET communication.

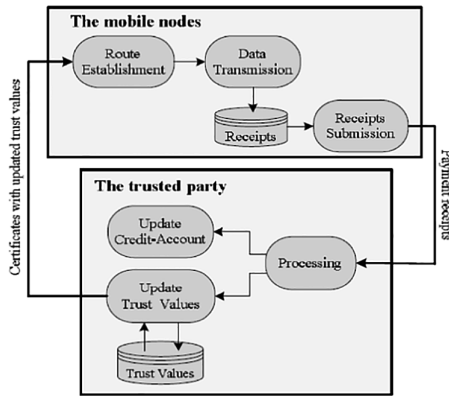
### 3.1 Data Transmission Section Exploitation Onion Routing

There square measure three main steps during which onion routing [17] is performed as anonymous registration request, anonymous registration reply, and anonymous information transmission. At first supply mobile node (SMN) broadcast RREQ packet during this format as given below.

$$SMN \rightarrow *: [RREQ, Rseq, D_{msg}, SD_{msg}, Onion(SMN)]Gs \tag{1}$$

In case of decipherment failure intermediate node (I) send RREQ packet during this format as shown.

$$SMN \rightarrow *: [RREQ, Rseq, D\_msg, SD\_msg, Onion(I)]Gs \tag{2}$$



**Fig. 1.** Framework of proposed system

Then RREQ packet reaches destination mobile node (DMU). DMU validates it equally to the intermediate nodes. Since DMU will decode the part of  $D_{msg}$ , it understands that it is the destination of the RREQ. Once DMU receives the RREQ from its neighbour, it'll assemble associate RREP packet in format given below.

$$DMU \rightarrow *: (RREP, Prt, \langle Skn, Onion(J) \rangle KJDMU) \tag{3}$$

And forward to its neighbor. Once intermediate node receives this, it can't decipher and send next RREP to next intermediate in format as shown below.

$$J \rightarrow *: (RREP, Prt, \langle Skn, Onion(I) \rangle KIJ) \tag{4}$$

When supply node receives this RREP it will decode and also the route discovery method ends with success. SMN is prepared to transmit a knowledge on the route.

Then anonymous information transmission is administered using ETSR that is explained in Sect. 3.3.

### 3.2 Trust Analysis and Update Part

Trust analysis and update module acquire evidences from first hand and second hand observations that is base of AI.

**Pseudocode 1:** Direct trust Calculation

- 1: if hub A, that is spectator, finds that its one-jump neighbor, Node B that is a trustee, gets a parcel **then**
- 2: the measure of parcels got will build one
- 3: if hub A finds that hub B advances the parcel with progress **then**
- 4: the measure of parcels sent will build one
- 5: **else**
- 6: if TTL of the parcel winds up zero or flood of supports in hub B or the condition of remote relationship of hub B is perilous **then**
- 7: the measure of parcels got diminishes one
- 8: **end if**
- 9: **end if**
- 10: **end if**
- 11: Calculate the trust worth  $T^S$  and update the previous one.  $T^S$  is calculated by Bayesian inference using

$$T^S = E_n[\theta] \text{ and } E_n(\theta) = \frac{\alpha_n}{\alpha_n + \beta_n} \quad (5)$$

**Pseudocode 2:** Indirect Trust Calculation

- 1: if hub A, which is an eyewitness, has in excess of one-jump neighbors amongst it and the trustee, hub B **then**
- 2: Calculates the trust value  $T^N$  using following equation
 
$$T_{AB}^N = m_{j1}(H) \oplus m_{j2}(H) \dots \oplus m_{jn}(H) \quad (6)$$
- 3: **else**
- 4: set  $T^N$  to 0
- 5: set  $\lambda$  to 1
- 6: **end if**

Combining  $T^S$  and  $T^N$  more realistic and accurate trust value is calculated as

$$T = \lambda T^S + (1 - \lambda) T^N \quad (7)$$

Here  $\lambda$  is punishment factor which is used to get less biased and realistic trust value.  $\lambda$  is greater than or equal to 1.

### 3.3 Stable Route Institution

ETSR establishes the stable, reliable and secure Route that may satisfy the supply node's trust, energy, and route-length necessities considering mobility and density. ETSR routing protocols have three processes: (i) Route Request Packet (RREQ) delivery; (ii) Route selection; and (iii) Route Reply Packet (RREP) delivery. Here onion routing is employed for secure path it takes less time for cryptographic mechanism as onion routing is more scalable than SHA, DSA, RSA and MD5 mechanisms. Hubs with low trust esteems are prohibited in course.

## 4 Results and Discussions

The planned theme is simulated on ns-2 platform with the ETSR protocol. Within the simulations, the effectiveness of the theme is evaluated in an insecure setting. The performance of the planned theme ETSR is compared with BDSTTM while not security mechanisms for parameters like throughput, PDR, delay, overhead and packet loss. Nodes area unit indiscriminately deployed in outlined space of 1000 m × 1000 m. User Datagram Protocol (UDP) is employed as transport specialist. 802.11 MAC type is employed. Planned theme is evaluated in two totally different situations as scenario 1: mobility of nodes and scenario 2: Density of nodes. For scenario 1, assume variety of nodes as 100 for varied speeds from 10 to 35 m/s. For scenario 2, speed is fastened as 10 m/s for varied density from 100 to 200 nodes. Simulation time is 100 s. Figures 2, 3, 4, 5 and 6 show simulation results for scenario 1. From Figs. 2 and 3, it is observed that as mobility of node increases throughput and PDR decreases as collision is more as speed increases. As collision increases probability of getting packet loss is more. It results in more delay. Figures 4, 5 and 6 depict that ETSR has best performance than BDSTTM in terms of delay, overhead and Packet loss. Figures 7, 8, 9, 10 and 11 are simulation results for Scenario 2 which depict that ETAR has better performance than BDSTTM in terms of all performance measures.

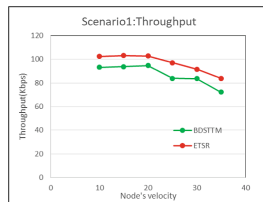


Fig. 2. Simulation results for scenario 1- throughput

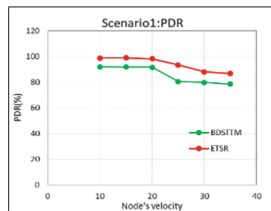
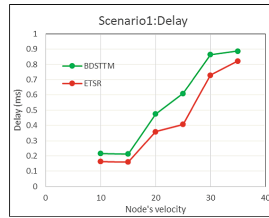
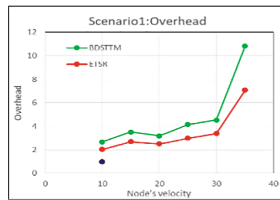


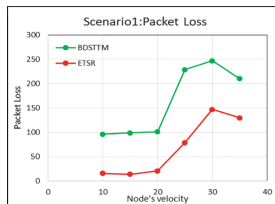
Fig. 3. Simulation results for scenario 1- PDR



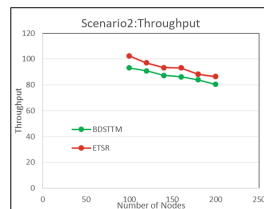
**Fig. 4.** Simulation results for scenario 1- delay



**Fig. 5.** Simulation results for scenario 1- overhead



**Fig. 6.** Simulation results for scenario 1- packet loss



**Fig. 7.** Simulation results for scenario 2- throughput

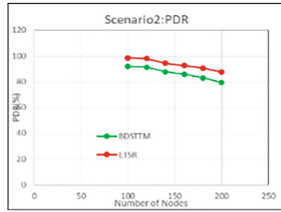


Fig. 8. Simulation results for scenario 2- PDR

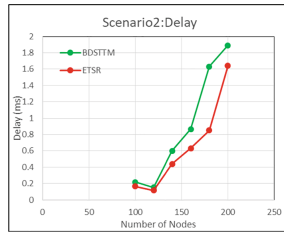


Fig. 9. Simulation results for scenario 2- delay

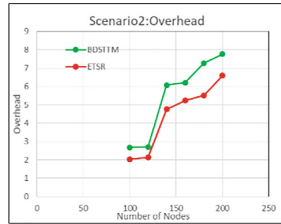


Fig. 10. Simulation results for scenario 2- overhead

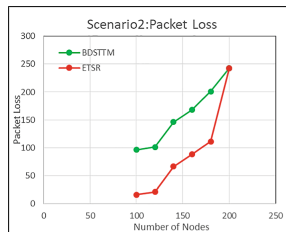


Fig. 11. Simulation results for scenario 2- packet loss

## 5 Conclusions

In this paper ETSR theme is projected with desegregation of secure knowledge transmission mistreatment onion routing cryptologic technique and BDSTTM to ascertain stable, reliable and secure routing path. As onion routing is more scalable it saves cryptologic computations time. Hubs with low trust esteems are prohibited in BDSTTM. BDSTTM uses unsure reasoning ideas like Bayesian approach and DST to mix belief functions. During this system we tend to designed trust model by considering mobility, density that is congestion of nodes parameters together with realistic and correct trust worth and energy. This plays important role to ascertain additional stable, reliable routes together with the information security. Projected system solves complete drawback of data loss in MANET. The experimental results shows that ETSR is better than BDSTTM in terms of throughput, PDR (Packet Delivery Ratio), delay, overhead and packet loss for various situations like mobility and density. So ETSR based mostly unified trust management theme plays important role in MANET security.

## References

1. IEEE Std 802.11-2007. IEEE standard for information technology- Telecommunication and information exchange between systems- Local and metropolitan area network-Specific requirement, Part 11 Wireless LAN medium access control and physical layer specifications, June 2007
2. Loo, J., Mauri, J.L., Ortiz, J.H. (eds.): *Mobile Ad Hoc Networks: Current Status and Future Trends*. CRC, Boca Raton (2011)
3. Guan, Q., Yu, F.R., Jiang, S., Leung, V.: Joint topology control and authentication design in mobile ad hoc networks with cooperative communications. *IEEE Trans. Veh. Tech.* **61**(6), 2674–2685 (2012)
4. Yu, F.R., Tang, H., Bu, S., Zheng, D.: Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks. *EURASIP J. Wirel. Commun. Netw.* **2013**, 188–190 (2013)
5. Wang, Y., Yu, F.R., Tang, H., Huang, M.: A mean field game theoretic approach for security enhancements in mobile ad hoc networks. *IEEE Trans. Wirel. Commun.* **13**(3), 1616–1627 (2014)
6. Chapin, J., Chan V.W.: The next 10 years of DoD wireless networking research. In: *Proceedings IEEE MILCOM*, pp. 2155–2245, November 2011
7. Bu, S., Yu, F.R., Liu, P., Manson, P., Tang, H.: Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. *IEEE Trans. Veh. Technol.* **60**(3), 1025–1036 (2011)
8. Bu, S., Yu, F.R., Liu, X.P., Tang, H.: Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks. *IEEE Trans. Wireless Commun.* **10**(9), 3064–3073 (2011)
9. Zhang, Y., Liu, W., Lou, W., Fang, Y.: Securing mobile ad hoc networks with certificateless public keys. *IEEE Trans. Dependable Secure Comput.* **3**(4), 386–399 (2006)
10. Fang, Y., Zhu, X., Zhang, Y.: Securing resource-constrained wireless ad hoc networks. *IEEE Wireless Commun.* **16**(2), 24–30 (2009)



11. Yu, F.R., Tang, H., Mason, P., Wang, F.: A hierarchical identity based key management scheme in tactical mobile ad hoc networks. *IEEE Trans. Netw. Serv. Manag.* **7**(4), 258–267 (2010)
12. Shakshuki, E.M., Kang, N., Sheltami, T.R.: EAACK—a secure intrusion-detection system for MANETS. In: *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, March 2013
13. Buchegger, S., Boudec, J.-Y.L.: A robust reputation system for P2P and mobile ad-hoc networks. In: *2nd Proceedings Workshop Economics of Peer-to-Peer Systems*, pp. 1–6, November 2004
14. Wei, Z., Tang, H., Yu, F.R., Wang, M., Mason, P.C.: Security enhancements for mobile Ad Hoc networks with trust management using uncertain reasoning. *IEEE Trans. Veh. Technol.* **63**(9), 4647–4658 (2014)
15. Mahmoud, M.M., Lin, X., Shen, X.S.: Secure and reliable routing protocols for heterogeneous multihop wireless networks. *IEEE Trans. Parallel Distrib. Syst.* **26**(4), 1140–1153 (2013)
16. Dahshan, H., Irvine, J.: A trust based threshold cryptography key management for mobile ad hoc networks. In: *IEEE*, pp. 1–5 (2009)
17. Liu, W., Yu, M.: AASR: authenticated anonymous secure routing for MANETs in adversarial environments. *IEEE Trans. Veh. Technol.* **63**(9), 4585–4593 (2014)



# Next Generation Web for Alumni Web Portal

Marmik Patel, Devangi Rami<sup>(✉)</sup>, and Mukesh Soni

Department of Computer, Smt. S. R. Patel Engineering College, Unjha, India  
marmikpatelmel3398@gmail.com, devangi28398@gmail.com,  
soni.mukesh15@gmail.com

**Abstract.** At some point, the understudies have insufficient information to proceed further in their career, so getting right exhortation from experienced individual is vital which will be accomplished by establishing an online alumni interface. With this the alumni can communicate to the students regarding job opportunities and the students can share their department activities to the alumni. The proposed system has the dynamic architecture and less static content, which can empower the full duplex association between all graduated students and understudies. This paper portrays how the system will function and collaborate the graduated class with the present understudies.

**Keywords:** Login · Chat · Database · Smart connect · Post · Placement · Alumni · Dynamic architecture

## 1 Introduction

Now a days alumni are main part of any institution and Alumni web portal provide a common platform to connect the alumni with their institute. Alumni website is created for the students that have graduated from the Institution. It allows former students to take advantage of the benefits and services that Institution offers after graduation [1]. In current scenario, the database of Alumni is maintained by college which is static. Due to this reason, the real time information of alumni is not present on any central platform. In this way, there is a need of an application which can keep subtleties of all the college graduates continuously. Alumni information will be stored in the database of server which will be accessible through web portal [5]. The goal of Alumni web application is to permit old and new undergraduates of the college to connect with one another. This enables understudies to think about one another and their present exercises. This entrance features the element of correspondence, which will empower the present understudies to interface with the graduated class of the school for getting different updates on current industry patterns, Internship opportunity, supported ventures and different referral opening in the corporate world [6]. This portal will serve the reason for incorporating every one of the partners of Institute, for example, Alumni, College understudies, Faculties to profit the direction and information sharing on different areas.

## 2 Literature Survey

### 2.1 IIT Bombay Alumni Association

Landing page of this portal is simple and sober. The principle page has numerous route joins. Highlights of the news, projects, events, jobs, alumni story are present in landing page and its detail portrayal is accessible specifically page. Landing page likewise demonstrate the block of fundraising projects and details of projects. It also displays the amount they have raised. At the home page highlight of almost all the features like, Events, News, Alumni stories, Alumni needs, Jobs, are displayed into the card structure. The Facebook and twitter feed are also displayed on the main page. This portal has a one nice feature in which student can write some problem with their pictures and post it to the wall and after that the graduated class who has some plan to take care of this issue can speak with that student and help that student to take care of the issue. User can search the alumni across the world and explore them in the map. Initiatives page provide awards and scholarship. Post page provide post stories. Also post new letter and alumni needs. Community page provide life membership and chapters. About us page has IIT Bombay Heritage Foundation and IIT Bombay Alumni Association. On the login page any user can login with '@iitbombay.org' ID, this is the better way of authenticate the user who are login to the website [7].

### 2.2 IIT Roorkee Alumni Association

On the landing page of this entrance a decent photograph exhibition of some mesh graduated class of IIT Roorkee is shown. Same as all the alumni portals this portal also have a events and news highlights on the fundamental page. We can explore the alumni on world map. Event page display upcoming events as well as past events. User can also create an event and register himself to some upcoming event. Memory page can contain alumni images and event wise group pictures and image related to college events. News can be uploaded in this site by staff and students. At the main page a list of features is displayed as a tab when the user clicks on the tab an information is display in the box besides the tab list. User can update their information directly from the home page. Highlight of news and events are displayed on the home page in a box. IIT Roorkee alumni association is handle by a team. Details of this team member is displayed at the end of main page [8].

### 2.3 PDPU Alumni Website

This portal has all the functionalities in their homepage like Schedule for present and upcoming occasions and an annual plan of university. Unlike all the alumni portal this portal provides some common features such as post, blog and events. It gives a remarkable element that include two topics one is student life and second is campus life. This website has a simple interface. It's a single page website whatever the content you search is available on the single main page. This portal contains more detail of college and their alumni. Alumni Recruiters arrange alumni lecture and mentorship.

In Job page student can decide campus interview on college. An Event page organize convocation and achievement about PDPU. An About us page can arrange annual plan and manage alumni team [9].

## 2.4 IIT Kanpur Alumni Association

On the primary page of this portal a photo of old alumni of IIT Kanpur is displayed. Same as all the alumni portals this portal also have features of events, news, letter, Academics, Alumni Search, Activities. highlights on the primary page is provide how we reached IIT Kanpur? Event page display upcoming events as well as past events. A separate alumni search page is available there in the portal to search each alumnus. In this portal Activity page has provided short courses, online courses, workshop and conferences. People section on the main page provide details about faculty, staff, research engineers. Research section maintain department facilities, central facilities and project. On the header section there is a link with a label 'Forum' that contain various form like leave form, scholarship form etc. Academics field contains details about undergraduate student, postgraduate student and courses. The gateway additionally has the subtleties of Awards and Honors, distribution and exhibition. IIT Kanpur has addresses subtleties with explicit day and time, Gallery with numerous pictures; contacts which demonstrate whom all are associated with this portal, lady graduated class tradition as independent for the lady just on the Home page. Also, Notice with featured shape is appeared better perception. Additionally gives the Donor Initiative Chance [10].

## 2.5 IIMB Alumni Website

At the main page recent updates, media, directory, jobs and gallery are displayed in highlighted form for better visualization. User can add post and event directly from the home page with one click. IIMB has blog, books and articles, birthday reminder, trending topics, jobs and gallery with many images. It gives the chance of donation, when alumni/student feels that they can help the establishment as far as gift, they can donate through payment gateway. Apart from all this we have observed the unique feature that IIMB provide unique alumni card to all the alumni. IIMB alumni portal has more efficient user identification and authentication [11].

## 2.6 Gathering Alumni Information from Web Social Network

This system proposes novel innovation to advise workers of undergrad tasks to gather data about semi-normally graduate class individuals on the web. For the most part, utilizing two alumni class pages as an arrangement of testing pages, the proposed innovation is twice as differing as the general procedures intended for different graduated class related social relationship information. This structure contains three modules and two repositories. The principal module called searcher, seek applicant pages to having a place with graduated class from an undergrad program from an interpersonal organization on the web. The second module, called Filter, that perform sifting, among the applicant pages recovered by the main module. The third module, called Extraction,

performs separating, from the pages sifted continuously module. The principal vault is called Pages Repository, stores the pages from the underlying arrangement of tests. The second vault is called Final Database, identifies with a database where the data on each previous understudy is secured [12].

## 2.7 Limitations of Community Web Portals: A Classmates' Case Study

In this paper average web-based interfaces supporting correspondence, information sharing and exercises of previous colleagues are examined and the confinements of existing network web-based interfaces are recognized. Existing web portals are experiencing an absence of adaptability, missing functionalities, information input overhead and scanty intelligence. Empowering the Semantic Web will make the network Semantic Web entries increasingly powerful and progressively receptive to the clients' real needs. Semantic work area has a high potential to conquer the constraints of the present network online interfaces [13].

## 3 Limitations

### 3.1 Drawbacks of Online Alumni Interface

- Alumni website does not provide necessary dynamic content.
- This system cannot maintain regularly.
- There is no chatroom for specific topic.
- No chat feature between student and alumni.
- Student record can't be easily navigating through the database.
- Existing system doesn't contain direct chat feature.
- It likewise comes up short on the moment answer for the issue which are identified with training and vocation.
- Existing alumni portals doesn't provide auto registration technique.

### 3.2 Comparison Between Existing Online Alumni System

Services	Existing online alumni portals				
	IIT Bombay	IIT Roorkee	PDPU	IIT Kanpur	Proposed system
Student query post	YES	NO	NO	NO	YES
Direct chat	NO	NO	NO	NO	YES
Alumni search	YES	YES	YES	YES	YES
Event	YES	YES	YES	YES	YES
Giving back	YES	YES	NO	YES	YES
Job post	YES	YES	YES	YES	YES
Article	YES	NO	NO	NO	YES
News latter	YES	YES	NO	YES	YES
Performance & speed	HIGH	HIGH	MEDIUM	HIGH	HIGH
Directory	YES	YES	YES	YES	YES

## 4 Proposed System Structure

The proposed system will be web based applications so it can be accessed by alumni and students with the help of admin. It enables quick and easy communications. Every user will be in charge of updating their very own data. Alumni will be able to organize meetings and find out about job opportunities by using this system (Fig. 1).

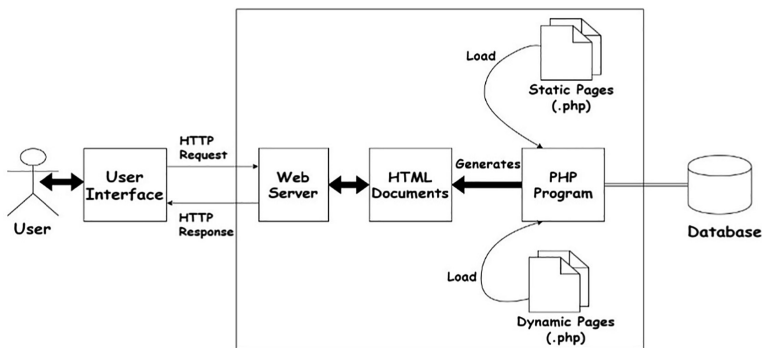


Fig. 1. System architecture.

Proposed system contains following modules:

### 4.1 Registration Module

There are three type of user who can resister themselves into the alumni portal, (1) Alumni (2) Student (3) Faculty. The administrator is in charge of keeping up data of understudies. Understudy/Faculty and graduated class can enroll themselves onto the entry after the endorsement from the admin, they can login into their record and can send mails, post questions, refresh their profiles and even scan for other understudy subtleties. To prevent fake registration, every registration request must undergoes through an authentication process. Once the user fill up the registration details and create an account he/she can login with their credentials but can't have full access to the features of portal until the admin verify and approve registration request.

### 4.2 Event Module

This module keeps up the data about different occasions that are directed by college. Warning updates are additionally part of the event module. The administrator can include, erase, alter and see occasion subtleties. Event supervisor can include or evacuate the data about workshops, temporary jobs, master addresses and so on. All the user can view the event details posted by the event manager and can create an event with specific title, date and description. Completed event are automatically deleted from the event page.

### 4.3 Query Post Module

The post module enables the users to post to what's at the forefront of their thoughts. Sharing and trading of perspectives and thoughts will be done here. Enquiries and questions on employments, entry level positions can be very much elucidated. The data can be posted division shrewd or might be presented on every one of the institute according to the prerequisite or the desire of the user. On the off chance that somebody has a response for the inquiry or a few perspectives in regards to the continuous subject it tends to be finished with the assistance of answer.

### 4.4 User Search Module

At whatever point user looks for the graduated class/understudies in the search bar, the database is questioned so as to recover the exact outcomes. We use PHP, MySQL and Angular Js for realtime searching data from database. User can apply a filter and sort information by city, name, branch, Enrollment number and so on [16].

### 4.5 Article Module

Faculties can post the articles about different innovations, advancement of an item or administration, mindfulness about social issues, data sharing about any subject or absolutely energy for composing. Each user can answer with remark on specific article. All other users can read the article and can comment on it. It is like a blog, through which one can spread the knowledge and awareness on specific topic [17].

### 4.6 Chat Module

The users can chat with each other for their benefit. The user can communicate privately to another user or alumni with the use of chat module and they can also start a conversation in chat room of specific topic. The user can see the enrolled individuals on the portal and as needs be talk with them. We use PHP, MySQL and Angular js with socket.io library for realtime communication. Every online user can see online and offline users list and start a conversation with particular user by clicking on the user name displayed in the online members list [20].

### 4.7 Placement Module

This module would also provide placed students details, company details and various reports which would be helpful for current students as well as alumni which managed by Placement cell or faculty. This module consists of two sub type, (1) On campus placement (2) Off-campus placement. In "*On campus placement*" the job details like, company name, post name, salary, experience, etc. are displayed and user can apply for it by uploading their resume and clicking on apply button. Once user apply for job his resume will be sent to the admin and he/she is eligible for campus interview.

On the other side, In “*Off campus placement*” job details like, company name, post name, salary, experience, etc. are displayed. Once user click to apply button it will be redirect to the google form, after submitting this form user can go to the company on specific date given by company and take an interview.

## 5 Methodology

### 5.1 Auto Registration

In majority of websites people have to enrol themselves by topping off the require subtleties that show up onto the enlistment page. So, this alumni portal will be providing the automatic registration of the students. When the student has carried the enlistment into the college, he/she needs to present their own and instructive subtleties to the college. From this data essential subtleties of that student will be in a split second transferred onto the Alumni portal (Fig. 2).

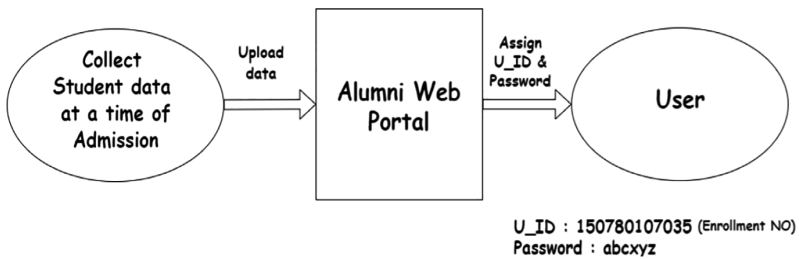


Fig. 2. Auto registration of the users

### 5.2 Personal Messaging

This portal will provide chat rooms with specific topic for different departments such as Electrical Department, IT Department, Mechanical Department, Computer Department etc. and furthermore give ongoing talk between any two users.

### 5.3 Auto and Manual Promotion

Auto advancement of existing understudies into graduated class. For example Understudy conceded in 2015 will move toward becoming graduated class in June 2019.



**Pseudo code for auto promotion**

*student\_course = year of graduation – year of entry*  
*if (student\_course = 4 years and month = June)*  
*then*  
*convert the status of user from student to alumni*  
*else*  
*keep the user in current role.*

**Pseudo code for handling the conversion of the failure student**

*if (user has drop year or detained)*  
*then*  
*send confirmation e-mail to verify the status of user*  
*if (user selects “YES”)*  
*then*  
*keep the user in current role*  
*else*  
*convert the role of current student to an alumnus.*

In case of failure of auto promotion user can change their role manually. User has to select specific role from the profile page and send the request to admin to change the role. Upon receiving the request admin verify the details of that particular student and change the role of that student.

## 6 Objective and Scope of the System

### 6.1 Objective

The aim and objective of alumni web portal are as below:

1. To establish and encourage healthy academic, social and cultural atmosphere among the Alumni and existing students.
2. To bring together all talents of the Alumni to help, all round development of the students and to support them in their academic and professional aims, objectives and activities.
3. Provide a communication way for exchange of ideas on academic, cultural and social issues of the day.
4. To bring together all the old students, existing student and the faculty of institution to share their experiences with each other.
5. To promote the campus placements through the old students working in reputed industries.
6. To get the valuable advices of the Alumni in the overall development of the college.

## 6.2 Project Scope

The scope of the project is to provide the one click access to the student's profile, job portal, and newsletter, Events, alumni activities, achievements, galleries and more. This helps alumni will re-engage themselves with the institution. The application enables understudies to enlist and after that look through the information dependent on various criteria. Understudies and graduated class can see the activity subtleties and apply for employment according to their fields, expertise and interest. The ideal inquiry of the current understudies will be addressed quicker. This keeps the understudies refreshed with the present updates and requests of the modern market. The understudies neither posting nor visiting can likewise quietly be refreshed with the ongoing in the college just as the market. Alumni portal would provide dynamic feature such as user status, chat rooms, personal chatting, Job posting etc. It also provide auto registration, auto and manual promotion.

## 6.3 Future Enhancement

- System can be updated in such a way that it can work on all browser.
- The portal can be extended for a larger user base beyond the Indian users.
- To simplify the work, it is necessary to build an android app.
- Add some social site features like timeline, friend requests etc.
- Provide a login to companies to benefit the administrations of this stage. By doing this the students will get more job opportunity.
- To include certain long range interpersonal communication highlights such as of LinkedIn.

## 7 Conclusion

This paper discuss about Alumni portal UI for the gathering of old students in and Institution. This web application is produced with natural UI components, which encourage simple to get to, comprehend and select different alternatives. This web application is created to permit the graduated class individuals in the organization to have associated and impart effectively. The alumni web portal will help the organization as well alumni association in keeping track of alumni interactions with the institution. It also allows the students to communicate directly with each alumnus, following their specific interests. This portal has been developed for increase the interaction and sharing of ideas among the students and alumni.

**Acknowledgements.** We would like to take this opportunity to thank our mentor Prof. Mukesh Soni for giving us all the help and guidance we needed. He also provided expertise that greatly assisted the research. We are really grateful to them for their kind support.

## References

1. Subashini, S., Sowndarya, A.: Alumni interaction system. *Int. J. Comput. Sci. Trends Technol. (IJCST)* **5**(2) (2017)
2. Breckling, J. (ed.): *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*. Lecture Notes in Statistics, vol. 61. Springer, Berlin (1989)
3. Gannod, G.C., Bachman, K.M., Troy, D.A.: Increasing alumni engagement through the capstone experience. In: 40th ASEE/IEEE Frontiers in Education Conference (2010)
4. Wegmuller, M., von der Weid, J.P., Oberson, P., Gisin, N.: High resolution fiber distributed measurements with coherent OFDR. In: *Proceedings of ECOC 2000*, paper 11.3.4, p. 109 (2000)
5. Jayavant, M., Kawle, S., Khergamkar, P., Gurale, S., Somani, R.: Alumni tracking system. *IOSR J. Eng. (IOSRJEN)* **8**, 80–86 (2018)
6. Arote, J., Chintamani, Y.B., Sonawane, S.A., Kadam, A.R., Pujari, V.D.: Online alumni portal. *Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET)* **4**(III) (2016)
7. IIT Bombay Alumni Website. <https://www.iitbombay.org/>
8. IIT Roorkee Alumni Website. <http://iitraa.in/>
9. PDPU Alumni Website. <https://alumni.pdpu.ac.in/>
10. IIT Kanpur Alumni Website. <https://www.iitk.ac.in/>
11. IIMB Alumni Website. <https://iimbaa.org/>
12. Gonçalves, G.R., Ferreira, A.A., de Assis, G.T.: Gathering alumni information from a web social network. In: 9th Latin American Web Congress (2014)
13. Mercado, C.A., Genove, G.P.C.: Towards Overcoming Limitations of Community Web Portals: a Classmates' Example DERI – Digital Enterprise Research Institute, University of Innsbruck, Austria, and National University of Ireland at Galway, Ireland Anna V. Zhdanova
14. Aruna, P., Sharmila Begum, M., Maghesh Kumar, D.: Alumni smart connect through Android application. Special Issue Published in *International Journal of Trend in Research and Development (IJTRD)*
15. Kengar, V., Jadhav, S., Limkar, N., Ghade, M., Kawtikwar, V.: College communicator. *IJSRD – Int. J. Sci. Res. Dev.* **3**(01) (2015). ISSN (online) 2321-0613
16. Methods and systems for obtaining and presenting alumni data. <https://patents.google.com/patent/US20140101143A1/en>
17. System to attach automatically comment on the information. <https://patents.google.com/patent/JP2008520024A/en>
18. Career and employment services system and apparatus. <https://patents.google.com/patent/US20110231329A1/en>
19. Method and system for employment placement. <https://patents.google.com/patent/US7505919B2/en>
20. Message chat system, message chat information processor, message chat method, and program. <https://patents.google.com/patent/JP2003114858A/en>
21. Ellison, N.B., et al.: Social network sites: definition, history, and scholarship. *J. Comput. Mediated Commun.* **13**(1), 210–230 (2007)
22. Pawar, V., Date, S., Iyer, S., Narvekar, C., Shell, M.: Security mechanism in alumni portal. Department of Information Technology, Xavier Institute of Engineering, Mahim (W), Mumbai (2002)
23. Staab, S., Angele, J., Decker, S., Erdmann, M., Hotho, A., Maedche, A., Schnurr, H.-P., Studer, R., Sure, Y.: Semantic community web portals. *Comput. Netw.* **33**(2000), 473–491 (2000)

24. Gonge, S.S., Joshi, P.S., Kuche, P.R., Chopade, R.M.: Education technology used in education for making student outcomes of engineering graduates. In: International Conference on Advances in Computing, Communications and Informatics (ICACCI) (2017)
25. Brenner, P.R., Schroeder, M., Madey, G.: Student engineers reaching out: case studies in service learning and a survey of technical need. In: Proceedings of the 37th Frontiers in Education Conference. IEEE (2007)



# VLSI Implementation of Image Encryption Using DNA Cryptography

P. Vinotha and Deepa Jose<sup>(✉)</sup>

Electronics and Communication Engineering, KCG College of Technology,  
Karapakkam, Chennai 600097, Tamil Nadu, India  
pvinotha04@gmail.com, deepa.ece@kcgcollege.com

**Abstract.** Image security is emerging as a major problem with the exponential growth of data stored and transformed through the network around the world. Many cryptographic techniques are used for securing the data like images, audio and text files. A new technique of DNA cryptography provides high security based on DNA nucleotides bases A-Adenine, C-Cytosine, G-Guanine and T-Thymine. These alphabets can be easily assigned to binary values (A-00, C-01, G-10, T-11). In this proposed model Polymerase Chain Reaction encoding technique is used in which the image to be encoded is flanked between primer keys. The DNA codons are encoded by the base of four provides keys of 256 combinations for high security, and it reduces the size of cipher text. Primer keys are generated by pseudo random sequence generator. Deciphering the image is possible with encryption key and primer sequence key. The HDL synthesis report for hardware design is implemented for encryption using verilog code on a device Virtex VII.

**Keywords:** MATLAB · Verilog · DNA cryptography ·  
Polymerase chain reaction encoding technique

## 1 Introduction

In the digital world, security of information is existed from ancient times when the data is transferred through the network. Images, text files and audio files to be transformed are in the form of unintelligible text for security. Cryptography is a technique intended to ensure the security of information. Data with perceptual meaning is called plain text. Transformation of plain text in unpredictable form is called encryption. Encrypted text is called cipher text. A cipher text is applied on data with secret key. It includes encryption, cipher text, decryption, and key generation process to ensure secure communication. Many cryptography techniques are used for security. Some examples are AES, RSA and IDEA these are traditional cryptosystems. The new technology of DNA cryptography provides high security using the biological structure of DNA. It is a natural carrier of information in the form of binary by assigning (A-00, C-01, G-10 and T-11). Many DNA secret writing algorithms are available to encode the data in the form of DNA code [11].

In the existing model of DNA secret writing technique, image is encrypted in the form of DNA sequence. Encryption key is generated by the sender using DNA codon with base three. A cipher text formed by substitution of key combination of 64 based

on DNA codons combination [4]. These 64 key combinations are easily guessed by the attackers. In this proposed model DNA sequence and encryption keys using DNA codon with base four provides keys of 256 combinations. The successful guess of key by the attackers is more and size of the cipher text to be transformed is reduced.

## 2 DNA Encoding

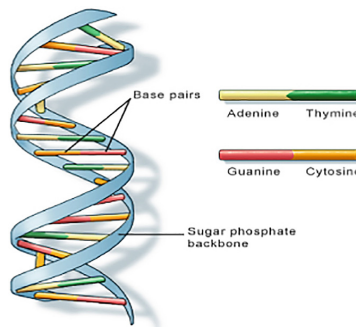
Image is converted into binary values based on the pixel value of an image. Binary code is converted into DNA code by assigning DNA bases in the form of alphabets (A, T, C and G). The DNA sequence is constructed for the entire image of maximum of pixel values 0–255.

**Table 1.** DNA encoding

BINARY CODE	DNA CODE
00	A
01	C
10	G
11	T

### 2.1 DNA Structure

Deoxyribonucleic Acid (DNA) structure consist of four basic nucleic acids A-Adenine, C-Cytosine, G-Guanine, T-Thymine. Single strand DNA formed by sequence of bases and Double strand DNA formed by the process of hybridization [1]. Hybridization is the process of forming complementary of single strand DNA and pairing each other as (A-T) and (C-G) based on the input binary data. Hydrogen bonds last only between complementary pairs: A-T and C-G. DNA strands twist around each other forming a helix is shown in Fig. 1.



**Fig. 1.** DNA structure

### 2.2 DNA as a Storage Medium

Our DNA molecule is very suitable for data storage purposes because it is:

- Very small and dense: 4 g of DNA is capable to store all the data in the world.
- Can last for long years in a good condition particularly when kept cool and dry.
- We can retrieve DNA by using Polymerase Chain Amplification method in which DNA contains information is encoded between F' primer and R' primer sequence.

### 3 Proposed Method

In this proposed method, encryption is the process of converting the data sequence in to the form of DNA strand is encrypted by substituting the alphabets, symbols and special characters which is inaccessible by the attackers. DNA strand is grouped into base four by using encryption key. According to the DNA secret writing technique of Polymerase Chain Reaction based encoding technique encoded data is flanked between unique primer sequences. The encrypted DNA format is shown in Fig. 2.

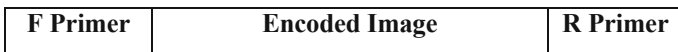


Fig. 2. Encrypted DNA format

The natural structure of DNA is presented in the form of PCR Encoding technique. The required information to be decoded is flanked between the F' Primer and R' Primer sequence. The Primer sequence is otherwise called as genetic marker where the sequence is marked using different colors in natural structure. Here, the Primer key generated using PRBS considered as a OTP which is shared between the sender and receiver.

#### 3.1 Encryption Process

The encryption process using DNA based Polymerase Chain Reaction encoding technique is summarized in Fig. 3.

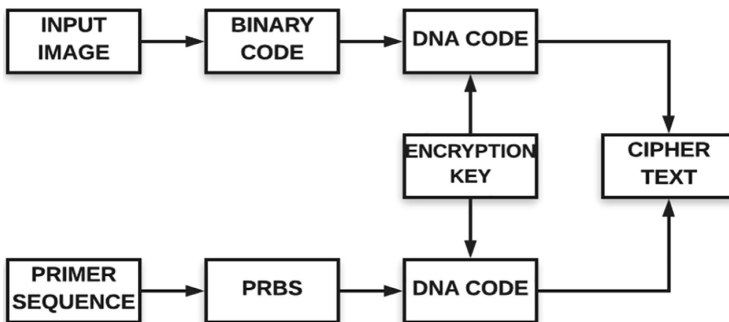


Fig. 3. Block diagram of encrypting a image using PCR encoding technique

Encryption steps as follows

- Providing the input data: Image
- Image is converted into binary code using MATLAB
- Each pixel values of an image is converted into 8 bit binary code.
- Hamming code: Error correction code that is used to detect and correct bit error that can occurs during the data is moved or stored. Transmission station must add extra data to the data to be transmitted.
- DNA Code: Two bit specifying the method A-‘00’, T-‘01’, C-‘10’, G-‘11’ of 8 bit form.

10 00 11 01 (141) → GATC.

- DNA code is converted into cipher text by considering the nucleotides of base four which provides the key combination of four bases.
- The final cipher text is an array composed of the integer values, alphabets, special characters and symbols in the DNA data format shown in Fig. 1.
- Primer key generated by PRBS in the form of DNA sequence is converted into cipher text and encoded message is flanked between these primer keys.
- Cipher text is converted into Encrypted image using MATLAB.

The Encryption key and primer sequence is shared between sender and receiver in the form of microdots or any other communication process.

### 3.2 Key Generation (OTP) Using PRBS

Primer keys are generated by key generation technique of OTP (One Time Pad) with the help of Pseudo Random Sequence Generator (PRBS). The primer sequence is given as the input to the LFSR (Linear Feedback Shift Register) in PRBS. The main function of PRBS is linear feedback shift register. It consists of group of flip flops in series with feedback loop. The primer sequence is given as a seed to LFSR which randomly generates the binary sequence used as key for primer. Binary sequence is converted into DNA code based on Table 1. Primer key is used exactly only once for one image (Fig. 4).

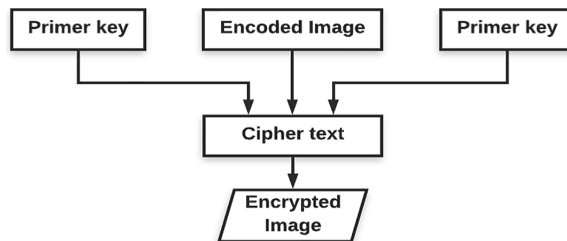


Fig. 4. Cipher texts format



### 3.3 Encryption Key

Encryption is the process of encrypting the message to be sent in the form of unpredictable text is called as cipher text. Here in this method cipher text is formed by substituting alphabets, symbols and special characters on DNA codon base of length 4. The possible combination of DNA codon is 256 to increase the size of key. These 256 combinations of keys and their corresponding DNA sequence is act as encryption key given in “Table 2” between a sender and receiver.

**Table 2.** Encryption key

A = AAAA	K = AATG	U = GGTA
o = TTTT	y = TCAA	p = ACTT
# = GGGG	r = CTAG	@ = GATT
u = ATCC	H = CTAG	'=TCAA
e = AACA	z = ATGC	? = GTAA
t = TTAC	T = CCGA	% = GGAC
<= AGCC	s = GTAC	Y = CCTA

In this method, the time for encryption and complexity is reduced. The size of the key is comparatively large and cipher text to be transformed is reduced. The deciphering of original image is impossible with the knowledge of primer sequence. This method is more secure and prevent an adversary from decipher it.

## 4 Security Analysis

### 4.1 Key Used in DNA Based AES Encryption

The key length used in DNA based AES encryption is of 64 DNA codons of base three [7]. The possible combination of keys is  $4^{64}$ . Probability of successful guess by the attacker is given in (1)

$$P(\text{SG of Key}) = \frac{1}{4^{64}}$$

The total probability of an attacker making successful guess is calculated by (2)

$$P(\text{SG of key}) = \frac{1}{1.63 * 10^8 * 16! * 4 * 4^{64}}$$

### 4.2 Key Used in DNA Based PCR Encoding Technique

In the proposed model the key length used in DNA based PCR encoding technique is of 256 DNA bases. It produces the possible combination of keys is  $4^{256}$ . Probability of successful guess by the attacker is given in (3)

$$P(\text{SG of Key}) = \frac{1}{4^{256}}$$

The total probability of an attacker making successful guess is calculated by (4)

$$P(\text{SG of key}) = \frac{1}{1.63 * 10^8 * 16! * 4 * 4^{256}}$$

The length of nucleotides sequence of four increases the key domain up to 256. There are 4,29,49,67,296 possible combination of DNA sequence. The chance of deciphering the image is possible with both primer key and encryption key.

## 5 Experimental Results

### 5.1 Simulation Output

Using Xilinx– version 14.7, Simulation output for test bench code is shown in Fig. 5. Cipher text is generated using PCR Encoding technique.

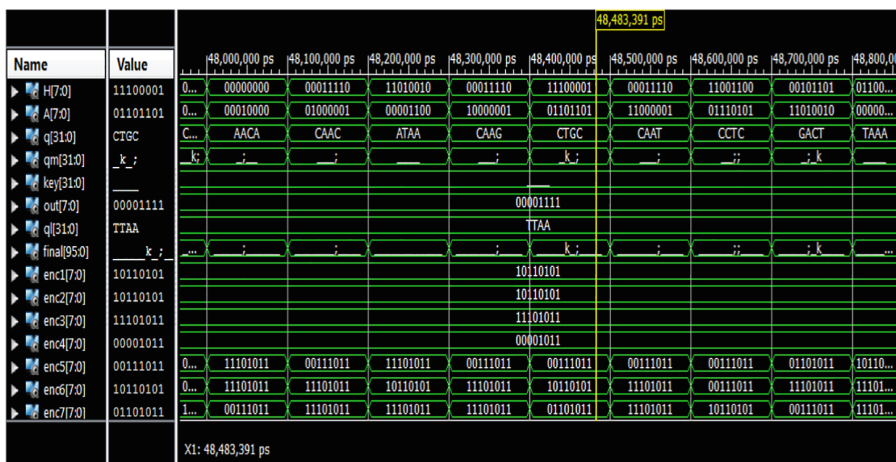


Fig. 5. Simulation output of encryption

- [7:0] D: Input binary values of each pixel value
- [7:0] H: Output of Hamming code from binary code
- [31:0]q: Output of DNA code of hamming using Table 1.
- [31:0]qm: Output of Cipher text of hamming code by using Table 2.
- [7:0]enc: Output of encrypted value is assigned
- [95:0]final: Output of cipher text to be encrypted using PCR encoding technique

## 5.2 Encryption Output

Using MATLAB – version R2015a, Encrypted image of input image is shown in Fig. 6(b) from the cipher text generated using Verilog code.

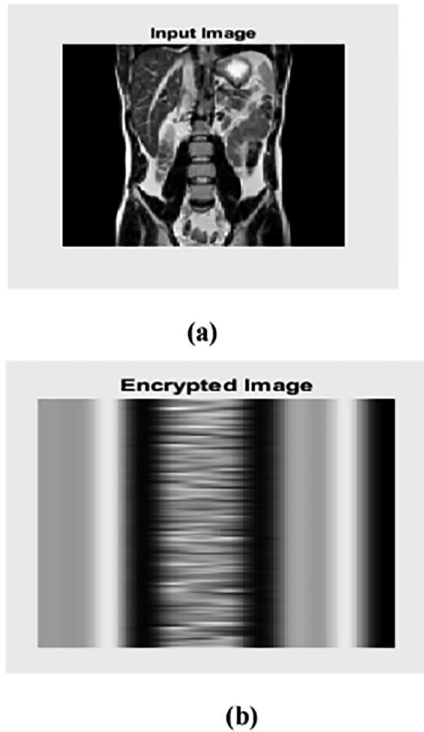


Fig. 6. (a) Input image [10] (b) Encryption image

## 5.3 HDL Synthesis Report on Virtex VII

- From the synthesis report generated the hardware utilization on a device Virtex VII is listed in Table 3.
- Advanced HDL synthesis report shows that the hardware utilization is less with limited number of flip flops and registers used.

## 5.4 Timing Summary

Speed Grade: –3

Minimum period: 0.650 ns

Maximum Frequency: 1537.279 MHz

Minimum input arrival time before clock: 0.899 ns

Maximum output required time after clock: 0.543 ns

Maximum combinational path delay: 1.378 ns

**Table 3.** Macro statistics

Adders/Subtractors	1
8-bit adder	1
Registers	8
Flip-Flops	8
Multiplexers	43
1-bit 2-to-1 multiplexer	43
xors	6
1-bit xor2	4
1-bit xor3	1
1-bit xor7	1

## 5.5 Synthesis Report

See Table 4.

**Table 4.** Device utilization summary

Selected family	7vx330tffg1157-3
Slice Registers	24 out of 408000 (0%)
Slice LUTs	55 out of 204000 (0%)
Bonded IOBs	226 out of 600 (37%)
BUFG/BUFG CTRL/BUFHCEs	Out of 200 (0%)

## 6 Conclusion

The proposed method of Polymerase chain reaction encoding technique increases the key domain and reduces the size of encryption key. The main contribution of proposed method is for hardware realization of encryption and decryption of image. DNA cryptography provides a confidential data transfer. DNA based encryption method is a recent technique added into cryptographic field. In DNA based PCR encoding technique the decipher the encoded image is impossible without primer key. This achieves high security of the system along with DNA based PCR encryption where the data to be transferred is flanked between primer keys. The result of HDL synthesis report implemented by Verilog code using Xilinx provides the hardware realization of DNA cryptography, and the security analysis resistance of PCR technique reduces the possibilities of cryptanalysis and breaking the cipher.

## References

1. Noorbasha, F., Suresh, K.: FPGA implementation of RGB image encryption and decryption using DNA cryptography. *Int. J. Eng. Technol.* **7**(2.8), 397–403 (2018)

2. Leong, M.P., Naziri, S.Z.M., Perng, S.Y.: Image encryption design using FPGA. In: 2013 International Conference on Electrical, Electronics and System Engineering (2013)
3. Sukumaran, S.C., Mohammed, M.: DNA cryptography for secure data storage in cloud. *Int. J. Netw. Secur.* **20**(3), 447–454 (2018)
4. Wang, Z., Zhao, X., Wang, H., Cui, G.: Information Hiding Based on DNA Steganography. National Science Foundation of China (2013)
5. Naveen Jarold, K., Karthigaikumar, P., Sivamangai, N.M., Sandhya, R., Asok, S.B.: Hardware implementation of DNA based cryptography. In: IEEE Conference on Information and Communication Technologies (ICT 2013) (2013)
6. Sajisha, K.S., Mathew, S.: An encryption based on DNA cryptography and steganography. In: 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA) (2017)
7. Jain, S., Bhatnagar, V.: A novel DNA sequence dictionary method for securing data in DNA using spiral approach and framework of DNA cryptography. In: IEEE International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), 01–02 August 2014 (2014)
8. Panda, D., Molla, K.A., Baig, M.J., Swain, A., Behera, D., Dash, M.: DNA as a Digital Information Storage Device. Springer, Germany (2018)
9. Mousa, H.M.: DNA-genetic encryption technique. *Int. J. Comput. Netw. Inf. Secur.* **7**, 1–9 (2016)
10. De Silva, P.Y., Ganegoda, G.U.: New trends of digital data storage in DNA. *Biomed. Res. Int.* **2016**, 14 (2016). Article ID 8072463
11. Monic Borda, M., Tornea, O.: DNA secret writing techniques. In: 2010 8th International Conference on Communications (2010)
12. Vidhya, B., Vidhyapriya, R.: Image compression and reconstruction by exemplar based inpainting using wavelet transform on textural regions. *Cluster Comput.* (2018). <https://doi.org/10.1007/s10586-018-1777-z>
13. Renganayaki, G., Korah, R., Salivahanan, S.: Design and implementation of a reversible logic circuit and its power analysis using conventional CMOS and adiabatic logic. *J. Comput. Theor. Nanosci.* **15**(1), 317–323 (2018)



# Comparative Analysis of Privacy Preserving Approaches for Collaborative Data Processing

Urvashi Solanki and Bintu Kadhiwala<sup>(✉)</sup>

Computer Engineering Department,  
Sarvajanik College of Engineering and Technology, Surat, India  
urvashi3122@gmail.com, bintu.kadhiwala@scet.ac.in

**Abstract.** Data collection by public and private organizations is increasing for extracting hidden knowledge from it that may be used for assisting decision making process. Moreover, availability of high speed internet and sophisticated data mining tools make sharing of this collected data across various organizations possible. As a consequence, these organizations may share and combine their datasets to retrieve the improved result from the combined data using collaborative data processing. Sharing of such data as it is between collaborative organizations may compromise individual's privacy as the collected data may contain sensitive information about individuals in its original form. To address this challenge, two main categories of privacy preserving approaches viz. the non-cryptography based approach and the cryptography based approach can be utilized. This paper aims to discuss an insight of these approaches and to highlight the parametric comparison.

**Keywords:** Collaborative data processing · Privacy preserving · Cryptographic · Non-cryptographic

## 1 Introduction

With the development of network, data collection and storage technology, the data collection by public and private organizations is increasing every day [1]. This collected data is used by executives for extracting hidden knowledge from it and this extracted knowledge is then used for better assessment of business processes [2]. Hence, data mining and knowledge finding techniques in databases are becoming essential.

In addition, it is also possible that two or more organizations may execute a data mining algorithm on the union of their databases with an aim to obtain an improved result from the combined data and also to reduce overall processing cost of the collaborated data. Consider the scenario of multiple supermarkets competitors as an example in which each competitor has a large set of its customers' data records of their buying behaviours. They want to perform data mining on their combined data set for mutual benefit. They do not want to reveal their customers' information to each other, since these companies are competitors in the market. However, they know the results

attained from this collaboration could bring them an improvement over other competitors. This scenario is known as Collaborative Data Processing. In a summary, we can say that collaborative data processing allows parties to extract useful patterns from the union of databases. However, serious concerns with respect to individual privacy may grow in such collaboration scenario [3]. Therefore, a new era of research recommends the reconsideration of existing data processing (mining) algorithms from the privacy preservation perspective [4].

The privacy preserving techniques for collaborative data processing can be classified into non-cryptographic approaches (data distortion based approaches) and cryptographic approaches [5]. The non-cryptographic approaches aim at distorting the original private data in such way that the statistical properties of the original data is preserved [6]. The cryptographic approaches utilize certain encryption schemes and cryptographic primitives on the original private data and generate a modified version of the data [6, 7]. In both the approaches, the resulting data do not divulge any individually identifiable information [8]. The non-cryptographic approaches deal with techniques like data anonymization [9–14], data perturbation [15–18], data randomization [18–20] etc. The cryptographic approaches for privacy preservation can be classified into secure multiparty computation [21–24], secret sharing [7, 25–27], homomorphic encryption [4, 28, 29] etc.

In this paper, we aim to discuss these existing privacy preservation techniques that can be used for collaborative data processing. In addition, we also highlight the parametric evaluation of these techniques.

The rest of the paper is organized as follows. Section 2 reviews different existing privacy preserving techniques that can be used for collaborative data processing. The parametric evaluation of these techniques is presented in Sect. 3. Finally, Sect. 4 puts the concluding remarks.

## 2 State-of-the-Art

This section gives an in depth description of various privacy preserving techniques used for collaborative data processing based on different approaches. As discussed, we can classify these privacy preserving techniques into non-cryptographic approaches and cryptographic approaches [5].

### 2.1 Cryptographic Approaches

In cryptographic approaches, data privacy of individuals is gained with the help of encryption schemes and cryptographic primitives [30].

#### 2.1.1 Secure Multi-party Computation

In [24], the authors introduce the Secure Multi-party Computation (SMC). This approach assumes a number of collaborative parties with their private data. These parties want to compute a certain function jointly over their inputs [21, 22]. This approach ensures that, at the end of the computation, each party knows nothing except its own input and the computed results.

As discussed in [21], one way to view secure multiparty computation is, with a trusted third party, where each collaborative party gives their input to the trusted third party. Then the trusted party performs the computation on the collected data and sends the computed results to the collaborative parties. Another way to view secure multiparty computation is, without having a trusted party. In this scenario, communication between the collaborative parties is required. This communication must ensure the privacy of each party's data that is it must not reveal one party's data to others. This is possible by allowing non-determinism in the exact data values sent in the intermediate communication between collaborative parties. However, this approach is computationally infeasible if the number of collaborative parties are more.

### 2.1.2 Shamir Secret Sharing

The authors of [26, 27] introduce the concept of secret sharing in which several collaborative parties are involved with secret values. The main idea of this scheme is that one party has a secret and this secret is distributed among other parties in such a way that none of the parties can retrieve the whole secret on their own alone. Information from at least  $k$  parties out of all the collaborative parties is required to reconstruct the secret, where  $k$  is a predecided threshold. As a consequence, any effort by less than  $k$  parties to reconstruct the secret is not succeeded and hence, they can learn nothing about the secret. However, due to semi-honest conduct of the parties, problems may arise in this scheme even if the protocol involves additive homomorphic operation. To evade this, verifying secret sharing inserts an extra information to each secret share but it results into communication overheads to the protocol.

### 2.1.3 Homomorphic Encryption

The homomorphic encryption concept was initially proposed in [29] that uses encryption and decryption methods to preserve privacy. It can be defined as a form of encryption that allows specific computations to be carried out on the cipher text and generates an encrypted result. This encrypted result when decrypted matches with the result of operations performed on the plaintexts [31]. This approach enables users to compute certain functions such as secure sum, secure scalar products etc. efficiently. The former homomorphic encryption techniques are not suitable for practical implementation as their decryption is based on exhaustive search. The recent homomorphic encryption scheme withstands the drawback of these traditional homomorphic schemes. However, the limitation of this approach is that users can perform only limited operations using this approach.

## 2.2 Non-cryptographic Approaches

In non-cryptographic approaches, some transformation is applied on the data for privacy preservation. Examples of such transformations may include suppression of specific values or noise addition to the data and so on. Various techniques such as data anonymization [9–14], data perturbation [15–18], data randomization [18–20] etc. using this approach are as follows.



### 2.2.1 Data Anonymization

The data set consists of four types of attributes such as explicit identifier, quasi identifier (QID), sensitive attributes, non-sensitive attributes as discussed in [9, 32]. Data anonymization [12, 33] technique attempts to hide the identity and/or the sensitive data of record owners.

To preserve privacy, the explicit identifiers are removed from the data set. However, in this case, privacy of an individual may still be compromised by linking quasi identifiers with publicly available data [34]. To prevent such record linkage through QID, Samarati and Sweeney [35, 36] proposed the concept of  $k$ -anonymity that says if one record in the table has some QID value, at least  $k-1$  other records also have the same QID value [37]. The  $k$ -anonymity can be achieved by using generalization and suppression operations. Generalization operation involves replacing a QID value with a less specific but semantically consistent value. Suppression operation involves not releasing a value at all. As seen,  $k$ -anonymity prevent record linkage attack but it may fail to protect against attribute disclosure attacks - homogeneity attack and background knowledge attack [14].

To address above discussed limitations of  $k$ -anonymity, the authors of [14] introduced  $l$ -diversity as a stronger notion of privacy. According to [14], an equivalence group is  $l$ -diverse if it contains at least  $l$  “well-represented” values for the sensitive attribute  $S$ . A table is  $l$ -diverse if every equivalence group is  $l$ -diverse. The limitation of  $l$ -diversity is that it cannot protect against attribute disclosure attacks - similarity attack and skewness attack [9, 37, 38].

### 2.2.2 Data Perturbation

The data perturbation based privacy preservation techniques modify the private data values by inserting(adding) noise such as additive noise, multiplicative noise, logarithmic multiplicative noise, Laplace noise [17, 18]. This noise is calculated from a probability distribution of the original private data values [8, 39, 40]. The perturbed data does not reveal private information while preserves the utility of the data for statistical summaries and thus it is “safe” to use for data mining. The limitation of data perturbation approach is that if the values of noise are not properly selected, then the perturbation technique results into the perturbed data values that are closer to the original data values. Hence, the partial disclosure of the original data may be possible. Therefore, it is a challenging task to generate perturbed data such that the resulting data remains statistically close to the original data and also preserves privacy of individuals [17]. Furthermore, as this method reconstructs distributions and not the original data values, it is required to develop the algorithms that mine the data on the generated distribution.

### 2.2.3 Randomization

In this approach, the behavior of individual records can be masked by adding the noise to the data. The noise is added in such a way that individual records cannot be incepted. The original data can be regenerated back by subtracting the noise from the masked data. Additionally, this approach also supports noise multiplication instead of noise addition using the multiplicative strategy. Data records are multiplied with random vectors and then the data is published in this strategy. As this approach adds or multiplies noise in the original data independently, the trusted server is not required to perform transformation on the data. However, this approach is vulnerable to known input-output attack and known sample attack [19].

### 3 Parametric Evaluation

The parametric evaluation of the discussed privacy preserving approaches is summarized in Table 1. These approaches are compared using various parameters such as approach type, operations incorporated for privacy preservation, strategy used, Trusted Third Party required or not, applicable on numeric data and categorical data or not etc. These parameters are described as follows:

- **Approach type:** This parameter specifies that the privacy preserving approach is cryptographic or non-cryptographic.
- **Operations incorporated:** This parameter specifies the operations employed by the approach for preserving privacy.
- **Strategy used:** This parameter identifies strategy/methodology used for privacy preservation.
- **Trusted Third Party (TTP) required:** The trusted third party is utilized or not by the approach is specified by this parameter.
- **Applicable on numeric data:** This parameter specifies whether the technique for privacy preservation is applicable on numeric data or not.
- **Applicable on categorical data:** This parameter indicates whether the technique for privacy preservation is applicable on categorical data or not.

**Table 1.** Parametric evaluation of privacy preserving approaches for collaborative data processing

Sr. No.	Privacy preserving approach	Approach type	Operations incorporated	Strategy used	Requirement of Trusted Third Party (TTP)	Applicable on numeric data	Applicable on categorical data
1.	Secure Multi-party Computation [21–23]	Cryptographic	Oblivious transfer	Bitwise encryption	Yes	Yes	No
2.	Shamir secret sharing [7, 25–27]	Cryptographic	–	Secret key	No	Yes	No
3.	Homomorphic encryption [4, 28, 29]	Cryptographic	Algebraic operations on cipher text	Encryption	Yes	Yes	No
4.	Data anonymization [9–14, 37, 41]	Non-cryptographic	Data generalization, Data suppression	Generalization, Data suppression	Yes	Yes	Yes
5.	Data perturbation [15–18]	Non-cryptographic	Data reconstruction, Data swapping	Value distortion	Yes	Yes	No
6.	Randomization [18–20]	Non-cryptographic	Data distribution, Data reconstruction	Additive noise, Multiplicative noise	No	Yes	No

## 4 Conclusion

As discussed, the existing privacy preserving approaches for collaborative data processing can be categorized into non-cryptographic approaches and cryptographic approaches. Most of the approaches apply a transformation on data for privacy preservation that reduces the effectiveness of the underlying data. Therefore, the important concern is to retain maximum data utility without compromising the privacy of individuals. Better approaches can be developed by mingling the strength(s) of the existing approaches, in order to maximize data utility and data privacy both, for preserving privacy in collaborative data processing scenario.

## References

1. Chen, B.C., Kifer, D., Lefevre, K., Machanavajjhala, A.: Privacy-preserving data publishing. *Found. Trends Databases* **2**(1–2), 1–167 (2009)
2. Ciriani, V., Di Vimercati, S.D.C., Foresti, S., Samarati, P.: *k*-anonymous data mining: a survey. In: Aggarwal, C.C., Yu, P.S. (eds.) *Privacy-Preserving Data Mining: Models and Algorithms*, pp. 105–136. Springer, Boston (2008)
3. The Economist, The end of privacy, p. 15 (1999). <https://www.economist.com/printedition/1999-05-01>
4. Zhan, Z.: *Privacy-Preserving Collaborative Data Mining*. Ph.D thesis, University of Ottawa, Canada (2006)
5. Abbas, A., Khan, S.: A review on the state-of-the-art privacy-preserving approaches in e-health clouds. *J. Biomed. Health Inf. IEEE* **18**(4), 1431–1441 (2014)
6. Hundepool, A., Domingo-Ferrer, J., Franconi, L., Giessing, S., Lenz, R., Longhurst, J., Nordholt, E.S., Seri, G., Wolf, P.: *Handbook on Statistical Disclosure Control*, ESSnet on Statistical Disclosure Control, version 1.0 (2006)
7. Pedersen, T.B., Saygin, Y. and Savas, E.: *Secret Sharing vs. Encryption-Based Techniques for Privacy Preserving Data Mining* (2007)
8. Das, K.: *Privacy preserving distributed data mining based on multi-objective optimization and algorithmic game theory*. Ph.D thesis, University of Maryland, Baltimore County (2009)
9. Fung, B., Wang, K., Chen, R., Yu, P.: Privacy-preserving data publishing: a survey of recent developments. *ACM Comput. Surv. ACM* **42**(4), 1–53 (2010). Article 14
10. Aldeen, Y.A.A.S., Salleh, M., Razzaque, M.A.: A comprehensive review on privacy preserving data mining. *SpringerPlus* **4**(1), 694 (2015)
11. Wang, J., Luo, Y., Zhao, Y., Le, J.: A survey on privacy preserving data mining. In: *First International Workshop on Database Technology and Applications*, pp. 111–114. IEEE (2009)
12. Dalenius, T.: Finding a needle in a haystack - or identifying anonymous census record. *J. Official Stat.* **2**(3), 329–336 (1986)
13. Samarati, P.: Protecting respondents' identities in microdata release. *IEEE Trans. Knowl. Data Eng.* **13**(6), 1010–1027 (2001)
14. Machanavajjhala, A., Gehrke, J., Kifer, D., Venkatasubramaniam, M.: *l*-diversity: privacy beyond *k*-anonymity. In: *Proceedings of the 22nd International Conference on Data Engineering (ICDE 2006)*, p. 24 (2006)

15. Aggarwal, C.C., Yu, P.S.: On static and dynamic methods for condensation-based privacy-preserving data mining. In: *ACM Transactions on Database Systems (TODS)*, vol. 33, no. 1 (2008)
16. Chen, K., Liu, L.: Privacy preserving data classification with rotation perturbation. In: *Fifth IEEE International Conference on Data Mining (ICDM 2005)* (2005)
17. Mivule, K.: Utilizing noise addition for data privacy, an overview. In: *International Conference on Information and Knowledge Engineering, Las Vegas, USA*, pp. 65–71 (2012)
18. Agrawal, R., Srikant, R.: Privacy-preserving data mining. In: *Proceedings of the 19th ACM SIGMOD Conference on Management of Data*, vol. 29, no. 2, pp. 439–450. ACM (2000)
19. Aggarwal, C.C., Philip, S.Y.: A survey of randomization methods for privacy-preserving data mining. In: Aggarwal, C.C., Yu, P.S. (eds.) *privacy-preserving data mining. Advances in Database Systems*, vol. 34, pp. 137–156. Springer, Boston (2008)
20. Huang, Z., Du, W., Chen, B.: Deriving private information from randomized data. In: *Proceedings of the ACM SIGMOD International Conference on Management of Data*, pp. 37–48 (2005)
21. Xu, L., Jiang, C., Wang, J., Yuan, J., Ren, Y.: Information security in big data: privacy and data mining. *IEEE Access* **2**, 1149–1176 (2014)
22. Yao, A.C.C.: How to generate and exchange secrets. In: *27th Annual Symposium on Foundations of Computer Science*, pp. 162–167. IEEE (1986)
23. Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X., Zhu, M.Y.: Tools for privacy preserving distributed data mining. *ACM SIGKDD Explor. Newsl.* **4**(2), 28–34 (2002)
24. Lindell, Y., Pinkas, B.: Secure multiparty computation for privacy-preserving data mining. *J. Priv. Confidentiality* **1**(1), 59–98 (2009)
25. Ge, X., Yan, L., Zhu, J., Shi, W.: Privacy-preserving distributed association rule mining based on the secret sharing technique. In: *2nd International Conference on Software Engineering and Data Mining (SEDM)*, pp. 345–350. IEEE (2010)
26. Shamir, A.: How to share a secret. *Commun. ACM* **22**(11), 612–613 (1979)
27. Blakley, G.R.: Safeguarding cryptographic keys. In: *Proceedings of the National Computer Conference*, vol. 48, pp. 313–317 (1979)
28. Zhan, J., Blosser, G., Yang, C., Singh, L.: Privacy-preserving collaborative social networks. In: *International Conference on Intelligence and Security Informatics*, pp. 114–125. Springer, Heidelberg (2008)
29. Rivest, R.L., Adleman, L., Dertouzos, M.L.: On data banks and privacy homomorphisms. *Found. Secure Comput.* **4**(11), 169–180 (1978)
30. Yang, Z., Zhong, S., Wright, R.N.: Privacy preserving classification of customer data without loss of accuracy. In: *Proceedings of the 5th SIAM International Conference on Data Mining*, pp. 92–102 (2005)
31. Yi, X., Paulet, R., Bertino, E.: *Homomorphic Encryption and Applications*, vol. 3 (2014)
32. Burnett, L., Barlow-Stewart, K., Proos, A.L., Aizenberg, H.: The “GeneTrustee”: a universal identification system that ensures privacy and confidentiality for human genetic databases. *J. Law Med.* **10**(4), 506–513 (2003)
33. Cox, L.H.: Suppression methodology and statistical disclosure control. *J. Am. Stat. Assoc.* **75**(370), 377–385 (1980)
34. Sweeney, L.: Achieving k-anonymity privacy protection using generalization and suppression. *Int. J. Uncertainty Fuzziness Knowl. Based Syst.* **10**(5), 571–588 (2002)
35. Samarati, P., Sweeney, L.: Generalizing data to provide anonymity when disclosing information (Abstract). In: *Proceedings of the Seventeenth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS 98)*, vol. 98, p. 188 (1998)

36. Samarati, P., Sweeney, L.: Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and specialization, Technical report SRI-CSL-98-04, SRI Intl., pp. 101–132 (1998)
37. Domingo-Ferrer, J., Torra, V.: A critique of k-anonymity and some of its enhancements. In: Third International Conference on Availability, Reliability and Security, pp. 990–993. IEEE (2008)
38. Li, N., Li, T., Venkatasubramanian, S.: t-closeness: privacy beyond k-anonymity and l-diversity. In: 23rd International Conference on Data Engineering (ICDE 2007), pp. 106–115. IEEE (2007)
39. Yin, Y., Kaku, I., Tang, J., Zhu, J.: Privacy-preserving data mining. *Data Mining Concepts, Methods and Applications in Management and Engineering Design*, pp. 101–119. Springer, London (2011)
40. Aggarwal, C.C., Yu, P.S.: A condensation approach to privacy preserving data mining. In: *Proceedings of the International Conference on Extending Database Technology (EDBT)*, pp. 183–199 Springer, Heidelberg (2004)
41. Li, D., He, X., Cao, L., Chen, H.: Permutation anonymization. *J. Intell. Inf. Syst.* **47**(3), 427–445 (2015)



# Damage Detection and Evaluation in Wireless Sensor Network for Structural Health Monitoring

S. Surya<sup>(✉)</sup> and R. Ravi

Anna University Recognized Research Centre, Department of Computer Science and Engineering, Francis Xavier Engineering College, Vannarpettai, Tirunelveli 627003, Tamilnadu, India  
suryaselwin@gmail.com

**Abstract.** Structural Health Monitoring (SHM) helps to estimate the health of the structures to detect the damage. A continuous monitoring is provided through wireless sensor Network (WSN). As an enabling technology, WSN along with SHM helps to achieve a low cost estimate. The damage detection is achieved through 2 phases (i) Training phase (ii) Operational phase. The training phase collects the data for the formation of data points. The Data point now forms the boundary region to detect the damaged areas. The operational phase contains three sub processes. They are data collection, transmission and damage evaluation. The clusters are formed and cluster head passes the details to detect the damage. The simulation shows the efficiency of these processes.

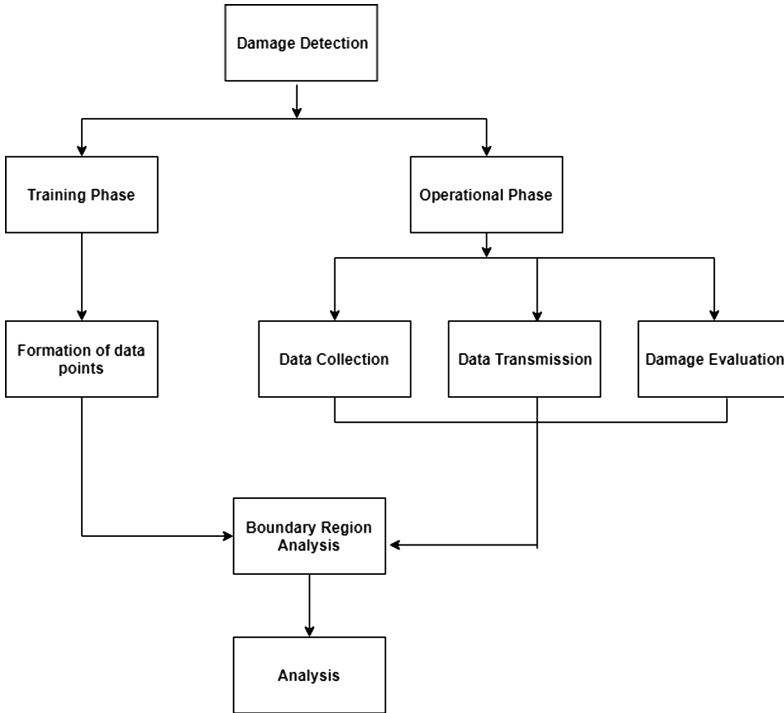
**Keywords:** Structural Health Monitoring · Wireless Sensor Network · Damage detection

## 1 Introduction

Structural Health Monitoring (SHM) provides the mechanism to determine the health of the structures. The structures are buildings, roads bridges and so on. The continuous monitoring of these structures is provided through Wireless Sensor Networks (WSN). SHM provides an added technology with WSN to achieve low cost and maintenance.

To detect the damage in the structure, the most commonly used parameter is vibration [1–6]. The vibrations are based on the operational as well as environmental factors [7–9]. The statistical variables are chosen to assess the status of the structures [10]. In [11], a WSN with SHM method is proposed, there the vibrations are extracted through pattern - matching technique. The sensor nodes are used to detect the damage efficiently. In [12], the cluster formation is proposed such that each cluster has a cluster head that are joined through a single base station. In [13], a damage sensitivity feature is proposed to detect the damage. In [14], the damage estimates are done through impulse response filter. In [15], the regression analysis is proposed to analyse the damage in environment and operational variations.

## 2 Proposed System



### 2.1 Damage Detection Algorithm

For the detection of damage, the random variables are chosen. Here the random variables are structural vibrations obtained from the environmental factors. First, the structural vibrations are measured at the particular location. Each mote is located at the particular location. Each mote has its own random variable to provide the details. These variables are situated in each cluster.

The Damage Detection algorithm is executed through 2 phases. One is the training phase and other is the operational phase. In the first phase, the vibrational data are collected under each duster through each mote. All the statistical feature values are collected and sent to the base station. The base station correlates the values between the clusters.

In the training phase, the data points are formed. The data point contains the values of the statistical variables. The values are calculated in the base station as the combination of two motes in each cluster. The data point provides the linear predictor as a healthy structure with boundary lines above and below the predictor. The above boundary line contains the negative value.

The next phase is the operational phase. There are 3 phases they are

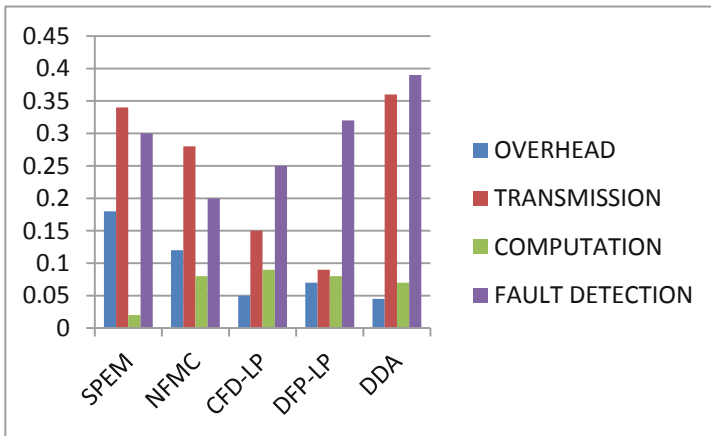
- Collection of data.
- Transmission
- Evaluation of Damage.

In the collection of data, each mote collects the statistical values of variables through vibration. The data are collected until N statistical values are obtained. After the N values are reached, the next process begins. In the transmission process, the collected N statistical values are transmitted to the base station. In the final damage evaluation process, the cluster head combines the statistical values; also two motes in a cluster are combined. Now, the data points are determined. The data points are now checked for boundary regions.

$$B_n = \begin{cases} 1, & \text{Data points fall outside} \\ 0, & \text{Data points fall inside.} \end{cases}$$

After the boundary lines are plotted, the slope is formed. From the slope, the areas under damage can be easily identified.

### 3 Performance Analysis



From the above graph, it is seen that the values are computed for overhead, transmission, computation and fault detection. The comparison is made between the algorithms such as SPEM, NFMC, CFD-LP, DFP-LP and DDA. The variations are shown between the algorithms. The identification of the faults are better than the other algorithms.



## 4 Conclusion

Structural Health Monitoring (SHM) helps to estimate the health of the structures to detect the damage. The continuous monitoring is provided through wireless sensor Network (WSN). As an enabling technology, WSN along with SHM helps to achieve a low cost estimate. The damage detection is achieved through 2 phases (i) Training phase (ii) Operational phase. The training phase collects the data for the formation of data points. The Data point now forms the boundary region to detect the damaged areas. The operational phase contains three sub processes. They are data collection, transmission and damage evaluation. The clusters are formed and cluster head passes the details to detect the damage is proposed.

## References

1. Whelan, M.J., Gangone, M.V., Janoyan, K.D., Jha, R.: Real-time wireless vibration monitoring for operational modal analysis of an integral abutment highway bridge. *Eng. Struct.* **31**(10), 2224–2235 (2009)
2. Ceriotti, M., et al.: Monitoring heritage buildings with wireless sensor networks: the Torre Aquila deployment. In: *Proceedings of International Conference on Information Processing in Sensor Networks*, pp. 277–288, April 2009
3. Kim, S., et al.: Health monitoring of civil infrastructures using wireless sensor networks. In: *Proceedings 6th International Symposium on Information Processing in Sensor Networks*, pp. 254–263, April 2007
4. Bocca, M., Eriksson, L.M., Mahmood, A., Jäntti, R., Kullaa, J.: A synchronized wireless sensor network for experimental modal analysis in structural health monitoring. *Comput. Aided Civil Infrastruct. Eng.* **26**(7), 483–499 (2011)
5. Hackmann, G., Sun, F., Castaneda, N., Lu, C., Dyke, S.: A holistic approach to decentralized structural damage localization using wireless sensor networks. *Comput. Commun.* **36**(1), 29–41 (2012)
6. Bocca, M., Toivola, J., Eriksson, L.M., Hollmén, J., Koivo, H.: Structural health monitoring in wireless sensor networks by the embedded Goertzel algorithm. In: *Proceedings of IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS)*, pp. 206–214, April 2011
7. Chesné, S., Deraemaeker, A.: Damage localization using transmissibility functions: a critical review. *Mech. Syst. Signal Process.* **38**(2), 569–584 (2013)
8. Scianna, A., Jiang, Z., Christenson, R., DeWolf, J.: Implementation of a probabilistic structural health monitoring method on a highway bridge. *Adv. Civil Eng.* **2012** (2012). Article no. 307515
9. Follen, C.W., Sanayei, M., Brenner, B.R., Vogel, R.M.: Statistical bridge signatures. *J. Bridge Eng.* **19**(7) (2014). Article no. 04014022
10. Contreras, W., Ziavras, S.: Efficient infrastructure damage detection and localization using wireless sensor networks with cluster generation for monitoring damage progression. In: *Ubiquitous Computing Electronics and Mobile Communication Conference (UEMCON) 2017 IEEE 8th Annual*, pp. 173–178 (2017)
11. Contreras, W., Ziavras, S.: Wireless sensor network-based pattern matching technique for the circumvention of environmental and stimuli-related variability in structural health monitoring. *IET Wireless Sensor Syst.* **6**(1), 26–33 (2016)

12. de Jager, D., Reeve, J.S.: Efficient information valuation and costing for distributed wireless sensor networks. *IET Wireless Sensor Syst.* **2**(3), 191–200 (2012)
13. Jin, S.-S., Jung, H.-J.: Vibration-based structural health monitoring using adaptive statistical method under varying environmental condition. In: *Proceedings of SPIE*, San Diego, CA, USA, vol. 9064, March 2014
14. Gorinevsky, D., Gordon, G.: Spatio-temporal filter for structural health monitoring. In: *Proceedings of American Control Conference*, Minneapolis, MN, USA, p. 6, June 2006
15. Serker, N.H.M.K., Wu, Z., Li, S.: A non-physics-based approach for vibration-based structural health monitoring under changing environmental conditions. *Struct. Health Monitor.* **9**(2), 145–158 (2010)



# Improvement of Web Performance Using Optimized Prediction Algorithm and Dynamic Webpage Content Updation in Proxy Cache

K. Shyamala and S. Kalavani<sup>(✉)</sup>

Department of Computer Science, Dr. Ambedkar Government Arts College  
(Autonomous), Affiliated to University of Madras, Chennai, India  
Shyamalakannan2000@gmail.com, kalai5391@gmail.com

**Abstract.** Identifying web user activity and interest of the users helps to improve the web access performance. Web usage mining applications like website enhancement, web personalization, prediction and prefetching etc. are used to improve the web performance. Increasing web usage in internet leads to network traffic, user latency, and server burden. Proxy server acts as an intermediate between the web user and web server to reduce the server burden. Updating dynamic content in a proxy cache is the major drawback in proxy server. In recent days various new add-on algorithms are given to server to reduce user latency but then it has become additional overload of the server. In this paper, the work is organised with three portions; the first portion focused in optimized way of running Monte Carlo prediction algorithm to reduce the server load. Second portion works on dynamic content to get update in the proxy cache to improve the performance of the website and finally the third portion deals with the prefetching engine in proxy server which maintains two caches to reduce server load and also to reduce user latency. The successful implementation shows the optimized way of reducing server load for add-on programs.

**Keywords:** Proxy server · HTTP request header · Prediction · Prefetching · Dynamic page

## 1 Introduction

Improving web performance has become an important key factor in recent research works. Website quality has been measured based on how often web user visits the website. Also how long they stay on the website. The combination of web client browser and the web server function are also referred to as client-server system. The web users, who send a request to the web server is called the client and the system which provide a response to the client machine is called web server. Server has multiple responsibilities like collecting requests from multiple clients and all input request should be send to the multiple web resources to get appropriate responses for the clients. The server may communicate with the different types of clients.

### 1.1 How Web Server Can Identify and Classify Web Clients?

The web server receives HTTP requests from the entire client via the internet and makes each request entry in the log file. The web server log file can be analyzed whenever required, and the details can be extracted about the accessing behavior of the web users [1]. The server can identify the different types of a client like browser client, non-browser client and indirect client through HTTP Request Header.

Identifying web user from the log file is a hectic task. Unique users should be identified and distinguished from the web server log file [2–5]. Because the single user can access from many computers or the single computer can be accessed by many web users. Moreover, identification of the web user can be hidden from the proxy server, because many computers on the internet contain the same IP address.

In general, there are several ways to identify clients from the log file which includes HTTP request headers, IP address, cookie based, browser fingerprint, and user registration [1, 6].

### 1.2 User Identification Based on HTTP Request Headers

The web server can identify their client or extract information about their client directly from the HTTP request Headers. HTTP request headers include from, user agent, Referrer, Authorization client IP and cookies.

From: It includes the email address of user only if they provide, but it will be available very rarely in the header for the security purpose.

User-Agent: It has the information about the client browser version. Here customizing content is important, moreover it will not be much useful to identify web user.

Referrer: It includes the source of the user from where they access. It will be helpful to understand user behavior.

Authorization: it holds the username and password on the client.

Client IP: As the name implies, the client can be identified by the server based on the Internet Protocol (IP) address of the client.

Cookie: Server generated ID can be identified by the cookie.

These are the information's available in HTTP request Header to identify their client and to personalize the content of a webpage.

### 1.3 User Identification Based on IP Address

In server user can be identified based on their IP address. Because IP address is unique, moreover proxy generated IP address can be used for security purpose.

Reasons to use IP as user identification:

- Many Internet Service Providers (ISP) make use of NTA firewall to enhance more security.
- Often ISP provides a dynamic IP address.
- Proxy servers can hide the original IP address of the client. Some proxy servers use client IP or X-Forward to prevent the client original IP address.

**1.4 User Identification Based on Cookie**

A cookie is a piece of information sent from the web server to a client browser. The piece of information stored in the client browser. The browser maintains the information in a document. When a user requests a page to the server, each and every time the message is sent back to the server. Personalization of webpages and identification of the user can be mainly done through the cookie. Two types of cookies are there which includes session and persistent cookies. Session cookies are deleted whenever the client leaves from the browser. Persistent cookies are saved on the disk for a long period of time. For example modern web browsers like chrome and firefox can keep the background process working even when the system is shutdown.

**1.5 User Identification Based on User Registration**

It can identify authenticate web user with their user name and password. Their user name and password will be stored in the website database. Each and every time when the user login, it will identify the user.

**2 Direct and Indirect Web Clients**

Web clients were classified as a direct client and indirect client. Direct web client access web pages directly from their web browser through original IP address with the entire proficiency of their web browser. The indirect client can access web pages through the proxy server, which communicates with the new IP address generated by the proxy server and they are called interception client or indirect client.

A proxy server acts as an intermediate between the web client and the web server [7, 8]. When the web client sends a request, then the request will be forwarded to the proxy server which acts as interception to the client to forward the request [9]. The proxy server will search for the client requested page in its own cache. The page will respond to the client when it is found in the cache otherwise on behalf of the web user, proxy server requests a web page to the web server with its own IP address. Once the proxy server requested page is received from the web server, it will keep the copy of the page to its cache and will forward that responded page to the web client.

When the web user accesses the web page via a proxy server, it is hard to find the original IP of the web client. The purpose of accessing a web page via a proxy server is to avoid security issues while accessing via the internet. The proxy server can be used to control the usage of internet in organizations. Most of the organization restricts to

visit some website for their employees, and also parents want to control accessing of some website for their children. Another advantage of using a proxy server is to reduce bandwidth usage and also increase the accessing speed by providing the requested pages from the proxy cache.

There are two types of the proxy server; forward proxy and reserve proxy server. Forward proxy server, directly forward the request to the webserver. Forward proxy server increases the security but sometimes it is used to download illegal things. A reverse proxy server acts on behalf of a client and it will handle to give request to the destination server. Reverse proxy server is mainly used for load balancing between the servers. Whenever the website disallows direct connection from the client for the security purpose, it can be allowed through an indirect connection in reverse proxy. Other than the forward and reverse proxy servers, there are few proxy servers exists which includes transparent proxies, anonymous proxies, highly anonymous proxies, DNS proxies, socks 4 & 5 proxies etc.

### 3 Related Work

In research work, literature survey plays an important role. It contains the previous and current development of the particular topic. Its main intention is to develop effective methods and techniques.

Identifying web user from the log file is a difficult task in web usage mining. Sharma and Rana [10] have presented three various methods to identify web users. They have discussed various methods to identify web user preferences to personalize the website. Based on the user preference, the website will give an interesting page to the user. A first user identification method based on IP address, second identification is done based on cookies and finally it is done based on user registration.

Ivancsy and Juhasz [11] have proposed three methods to identify web user. First two methods are already existing methods which includes data cleaning and user identification. Another method is based on the complex cookie to identify a web server. They have used statistical analysis developed by Web Activity Tracking (WAT). Web Activity Tracking helpful in identifying and categories the web user based on analyzing the web server log file.

Datta et al. [12] have presented a dynamic proxy caching technique which combines the benefits of both proxy-based caching and back end caching. They have provided an improvement in the reduction of bandwidth. Dynamic caching is important to improve the performance of web server. Yuan, Hua, and Zhang [13] have proposed an approach to use dynamic content catching at the proxy server. They have implemented this approach with a simple modification.

Intelligent prefetching is used to mitigate the user latency and to download document easily at the user end. Hussain and McLeod [14] have used an agent to monitor and predict the user future request. Then the predicted pages were prefetched at the proxy server. Caches were separately used which helped in a small number of users exploiting the network. They have split the caches based on hierarchy. Personal cache is used to store the regular browsing activities of a single user.

## 4 Objectives of the Proposed Work

- The main objective is to improve web performance by categorizing the various responsibilities of the web server and proxy server
- To reduce the web server load
- To reduce the accessing of static content from Proxy-Cache
- To optimize the cache accessing in Proxy Server

The research work is a step forward in improving web performance by categorizing the responsibility between server and proxy server. The server handles multiple clients who were accessing through a proxy server that is an indirect client. This work is purely related to the communication between the web server and the web client who is accessing via a proxy server.

Increasing in the usage of internet leads user-perceived latency, though many users access the internet through high-speed Digital Subscriber Line (DSL). We can improve web performance by reducing the web user latency time and server burden. It will be helpful for web users and internet service providers to increase browsing speed.

## 5 Proposed Architecture for Improving Web Performance

In the proposed architecture, we have categorized the responsibilities of both web server and proxy server which will be helpful in improving the web performance. Figure 1 shows the complete architecture. From the proposed architecture (Fig. 1) it has been shown the three major portions, the first portion defines the different clients who may access the server directly and some clients may access the server page via a proxy server. When the client access the server directly then the predicted pages hint will be sent directly to the client such that the prefetching will be done in the client browser cache. When the request of the client is directed through a proxy server then the predicted page hint will be sent to the proxy server then prefetching will be done in proxy's cache 2. The second portion of the architecture shows the proxy server, which used to act as an intermediate between some clients and the server. Here the proxy server has the responsibilities to direct the client and also used as prefetching engine [14, 18–20]. The proxy server can have two caches, cache 1 is used to store the client requested page and cache 2 used to store the prefetched pages. So that when the clients request the page it can be searched in cache 1 and later in cache 2. If the page is found then it will be send to the client. The third portion completely defines the responsibilities of the web server. The part of the prediction portion is already implemented in our previous work [15, 16]. The major responsibilities of the server are categorized as follows:

- Identify the client through HTTP Request Header
- Optimized running of prediction algorithm to reduce the load
- Make predicted pages as a prefetching link (Hints) to the client
- Send the hints of the recently updated web page link to the proxy to reduce user latency

In our previous work [15, 16] we have implemented the prediction algorithm called Rank based prediction using the Monte Carlo algorithm to reduce the user latency. The core concept is to predict the user future access page through Monte Carlo Ranking based algorithm and send the prefetching hints to the client to reduce their latency time. The complexity arises when the Monte Carlo prediction algorithm [16] which will be running for each and every request even for the same page this increase the server load. So, it is decided to reduce the repeated running of prediction algorithm in the server (i.e.) when the page1 is requested by the client1 then he/she can get the prefetching link as hints because of accessing prediction algorithm from the server. When the same page has been requested in a short period of time, again the server has to run the same

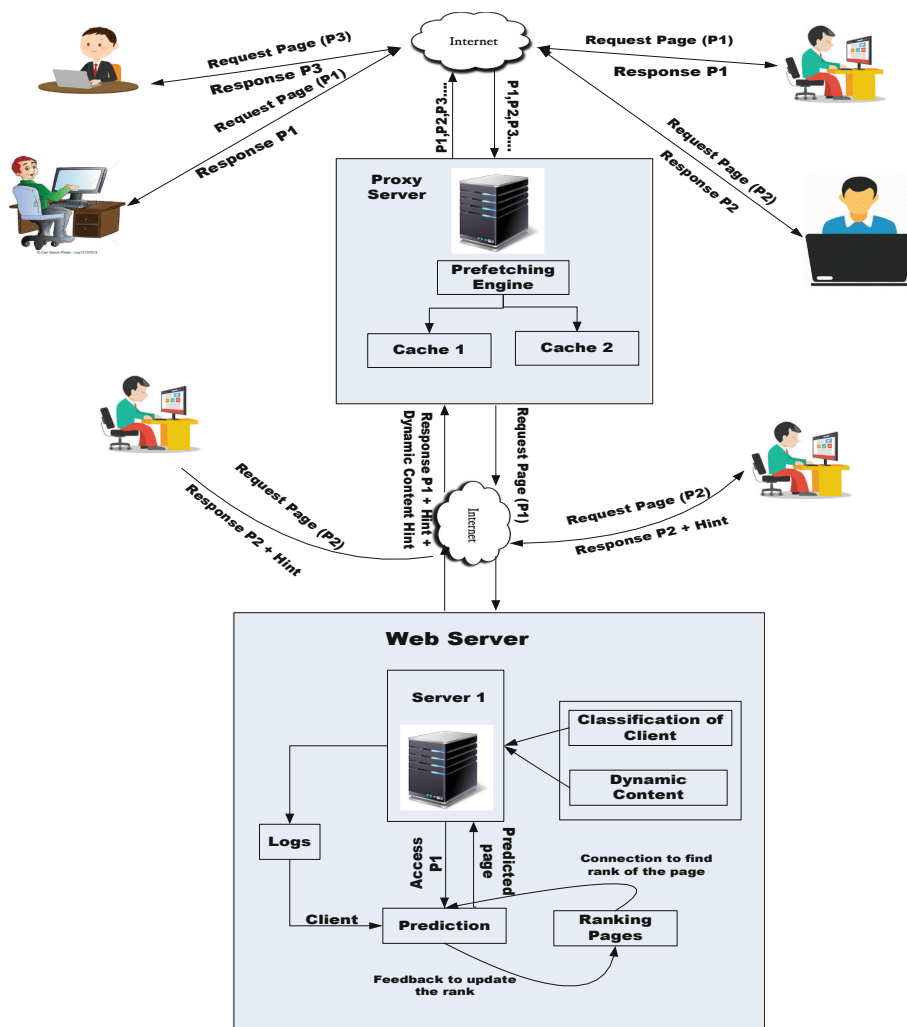


Fig. 1. Architecture to improve the web performance



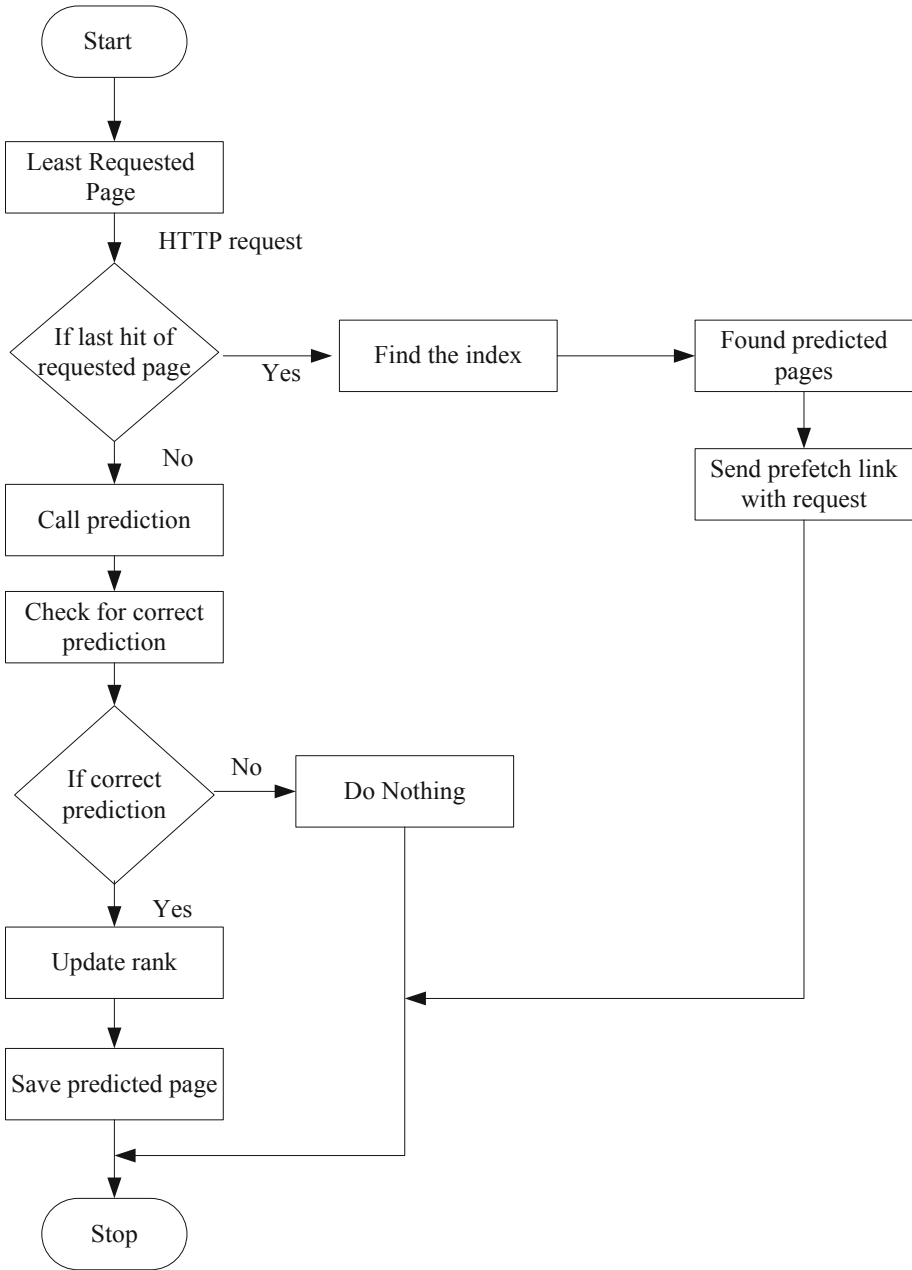


Fig. 2. Work flow for optimized running of prediction algorithm

prediction algorithm for the same page. This creates unnecessary frequent access to prediction algorithm for the same page and this leads to an increasing server load. This problem has been solved by creating a temporary array list to hold the predicted page of currently requested page in a short time period. The prediction may change according to the user behaviour so the array list value can be used with in short term period then the array will be flushed to hold newly predicted pages. This was shown in Algorithm 2 (Optimized Running of Prediction Algorithm). Figure 2 shows the flow of prediction and optimized running of the prediction algorithm in the server.

In recent days, the websites are purely dynamic, often the content of the web page is updating. The content of recently accessed web pages in the proxy server was not getting updated when it is updated in the web server. This leads to static content access for the web clients who were accessing via proxy. This research work highlights an immediate updation of a web page in the proxy server for the web pages which hit recently and updated recently in web server. Here also the work is optimized when updating the dynamic content from the web server to the proxy. The page will get updated in the proxy server if and only if the page should hit recently and updated recently in the web server. Such that server make the page as a hint and send a prefetching hint to the proxy server. This web page content updating technique is also applicable for e-commerce website but less applicable to the web content that changes based on the behavior, preferences and interest of the user.

In this work, the prefetching engine is used in the proxy server which collects the prefetching pages and saves into the separate cache. Here the proxy cache has been divided into two parts. The first part of cache (Cache1) holds default response pages and the second part of cache (Cache2) holds the prefetching pages. Such that when the request is received by the proxy server, it will search the page on Cache1 and Cache2. If the page is found, it will send a response to the web client otherwise the request will be forwarded to the web server.

## 6 Implementation

This section elucidates the algorithm for classification of clients, optimized running of prediction algorithm and dynamic webpage content updation in proxy cache algorithm.

### 6.1 Classification of Clients

The web server can identify the client through the HTTP request Header which includes all the details about the web user as mentioned before. The client can be identified and classified based on their IP address. User access via proxy server can be identified by the HTTP request Header which contains X-Forward-for. Whenever the client access through the proxy server, then the value for X-Forward-for will be set. For example: In JSP can identify the proxy client using the script `<%=request.getHeader("X-Forwarded-For") %>`. In .NET can identify the proxy client using the script `Var IP = (Http.content.current.request.server variables ["HTTP- X-Forwarded-For"]! = null)`. Algorithm 1 shows the implementation in JAVA.

---

**Algorithm 1:** Classification of Client

**Input:** Web Server Log file

**Output:** Identify Interception Client

---

**Begin**

```

For each request from client do
  If ((request.getHeader("X-Forwarded-For")!=null) then
    IP←request.getHeader("Proxy-Client-IP")
    PClient← Add IP to PClient list
  Endif
Endfor

```

**End**

---

Algorithm 1 elucidates the general technique which is used for classification of the client. For example if one of the parameters in the HTTP Request Header contains X-Forwarded-For value is not null then the server can identify it as a client which access through a proxy server. Either the client can access the webpage via a proxy server or else can access directly from the web server. In Algorithm 1 where 'request' represents the object of HttpServletRequest. The variable IP is used to extract the proxy client IP. The collected Proxies IP's were collected in the ArrayList called PClient. Algorithm 1 is a common procedure used by the servers to identify Direct and Indirect client. This part of work shows the typical arrangements in the server to identify different clients.

## 6.2 Optimized Running of the Prediction Algorithm

Algorithm 2 elucidates the minimized running of a prediction algorithm to reduce server load. Each and every time the prediction algorithm will not run for the same request either it is a direct client or proxy client.

---

**Algorithm 2:** Optimized running of the prediction algorithm

**Input:** Web log file

**Output:** Minimized running of the prediction algorithm

---

**Begin**

```

Predict← ArrayList for predicted page
For each request do
  LH ← from HTTP header request (date)
  If (LH is recently accessed) then
    PL ← Predict.indexOf [RP] // <Link rel = "prefetch" href = PL>
  Else
    RP← from Http header
    Call prediction algorithm (from paper [16])
    Call ranking algorithm (from paper [17])
    If rank of a page increased then
      I← find the index of requested page (pages.IndexOf(RP))
      Predict [I] ← predicted page
    Endif
  Endif
Endfor

```

**End**

---

Whenever the user requests a page to the server, it will be identified whether it is recently accessed or recently hit by any other user. If the requested page is a new request, then the server will run the prediction algorithm [15] and include the predicted page hint with the response. When the prediction is accurate, then the rank of the page is updated via feedback connection and the page is stored in the predicted ArrayList. If the same page is requested by some other user with in the short time period, then the server will not go for the prediction algorithm again instead it can directly give hint by using ArrayList. In Algorithm 2 the variables are expanded as follows:

LH  $\leftarrow$  Last Hit,  
 RP  $\leftarrow$  Requested Page  
 PL  $\leftarrow$  Prefetching Link  
 I  $\leftarrow$  Index of a Requested page from prediction algorithm [16]

### 6.3 Dynamic Webpage Content Updation in the Proxy Cache

Algorithm 3 elucidates the webpage content updation in the proxy cache. When the webpage is updated in the web server that updated version will not be available in the proxy cache. It will be a major drawback for the proxy client because many proxy clients access the old version of the webpage from the proxy cache. To overcome this drawback, the updated webpage link will be sent to the proxy server as a prefetching hint and Algorithm 3 shows the steps to be processed.

---

**Algorithm 3:** Dynamic webpage content updation in the proxy cache

**Input:** Dynamic updated webpages

**Output:** Updated webpages in proxy-caches

---

**Begin**

**For** (every updated webpage in web server) **do**

**For** (Recent entries from the web log) **do**

Recently-hit  $\leftarrow$  identify recent access of the page from request header

**If** (Recent-hit is true) && (HTTP Request header contains X-Forwarded-For) **!= then**

Identify the Proxy server IP

Make the updated page as prefetch link for the specific IP ( by using request header)

// <Link = "prefetch" href = "dpage.html">

**Endif**

**Endfor**

**Endfor**

**End**

---

The algorithm checks each and every updated webpage in the web server. Once the page is updated, it will check the recently accessed time of that updated page if it is accessed very recently. Then it will find whether the HTTP Request form proxy-client or direct client using X-Forwarded-For. If it is not null, then identify the proxy server IP and send the updated page as a hint. Then the prefetching link will be sent to proxy cache and it will download the page when the server is idle. For example consider an ecommerce website, it contains thousands of pages will get updated each and every day. Within a Fraction of a second, many pages get evicted from the proxy cache.

For this purpose the constraint has given that whether the page is very recently accessed by any proxy client or not. If the page is least recently accessed then the technique will not be applied because the proxy cache itself gets replaced with the new pages.

## 7 Results and Discussions

The successful implementation shows the reduced running time of server add-on algorithms, here the add-on algorithm is a prediction and prefetching which was implemented in our previous work [15]. The work shows the optimized way of running our add-on program which reduces the server load by avoiding the unnecessary running of the prediction algorithm.

The web server log file has collected from NASA Kennedy space center [17] for the experiment. Figure 3 shows the sample log file and the data which is considered for sample analysis is given in Table 1. For this experiment have considered two hours of user access from the dataset on 28-07-1995 from the time: 11:33 to the time: 28-07-1995 13:32. The same page was accessed by the different client within the given time period. This shows that running of prediction at each time increases the server load as high.

Table 1 consists of different page request which is taken from the web log file with the accessing time limit of half an hour, one hour and two hours. With the two hours of access, there may be a chance of requesting the same page from different clients may be a direct client or indirect client. For each type of client, the server has to run the prediction algorithm for the same page. Here the Algorithm 2 plays a major role to minimize the running of the same algorithm twice, thrice or etc. Table 1 shows that when time increases the number of time accessing the prediction algorithm for the same page also get increases. This paves the way to set some minimal time where the prediction of the page may not change. The approximate time taken to run prediction for a single page from the constructed graph [15] is 3 to 5 s. Such that Table 2 shows the extreme load for the server to run prediction for the same page within two hours. The number of seconds gets vary depends upon the depth of the graph. Here for example we considered that if prediction of page1 may not change for the two hours then it is unnecessary load for the server to access the prediction algorithm repeatedly. To reduce this unnecessary access we can set time boundary to access the prediction algorithm for each page.

From the analysis it has been found that within an hour or minimum number of hours, the prediction for the same page never gets change. So that the predicted page of the requested page can be saved in temporary memory for some period of time. The predicted pages can be used for future access of the user. When the time limits exceed, then refresh the graph and again the server runs the prediction algorithm. This part of work reduces the server load at least some cost. Figure 4 shows the time difference and also reduced the working load of the server. In Fig. 4 it shows the reduced load of server when the prediction algorithm access is optimized (i.e.) accessing single time of prediction algorithm for the same page with the considered time boundary as two hours. Another set of plotting shows the unnecessary access of prediction algorithm for same page which increases the server load.

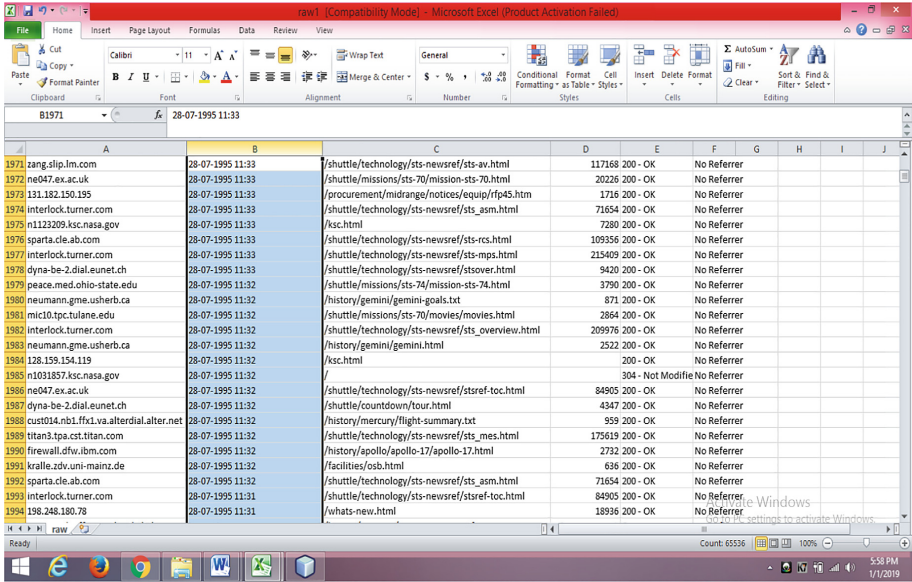


Fig. 3. Sample log entries

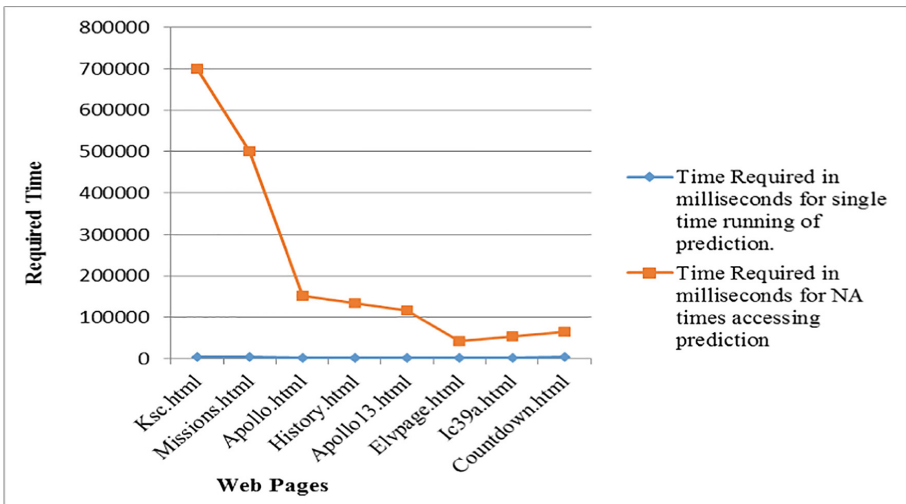
Table 1. List of pages accessed within two hours

Web log : NASA Kennedy space centre  
 Accessed Time: From : 28-07-1995 11:33  
 To : 28-07-1995 13:32  
 No. of Records : 1978

S. no	Pages	Number of times accessed a page with considered minimal time bound		
		Half an hour	One hour	Two hours
1.	Ksc.html	24	49	175
2.	Missions.html	17	46	100
3.	Apollo.html	14	28	51
4.	History.html	7	18	45
5.	Apollo13.html	6	10	39
6.	Elvpage.html	4	11	21
7.	Ic39a.html	3	8	18
8.	Countdown.html	9	14	16

**Table 2.** Time taken for unnecessarily accessing prediction algorithm

S. no	Pages	No. of access (NA)	Time Required in milliseconds for single time running of prediction	Time Required in milliseconds for NA times accessing prediction
1	Ksc.html	175	4000	700000
2	Missions.html	100	5000	500000
3	Apollo.html	51	3000	153000
4	History.html	45	3000	135000
5	Apollo13.html	39	3000	117000
6	Elvpage.html	21	2000	42000
7	Ic39a.html	18	3000	54000
8	Countdown.html	16	4000	64000



**Fig. 4.** Graph showing that output of optimized prediction algorithm – Reduced server load

## 8 Conclusion

The main aim of this paper was to improve web performance in the way of reducing server load by optimized time of running servers add-on algorithms like a prediction. The successful implementation of our rank based Monte Carlo add-on prediction algorithm [15] is now enhanced with the minimal running to reduce user latency. This work also shows the successful implementation of dynamic content updation in proxy-cache through the prefetching engine. On the whole, the works depict that by including add-on programs in the server it can reduce the server load. Prediction can be used only at the time of need, and then this work shows the kind of optimization.

## References

1. <https://www.ionos.com/digitalguide/online-marketing/web-analytics/log-analysis-user-statistics-from-the-server-log/>
2. Chen, M.S., Park, J.S., Yu, P.S.: Data mining for path traversal patterns in a web environment. In: Sixteenth International Conference on Distributed Computing Systems, pp. 385–392 (1996)
3. Punin, J., Krishnamoorthy, M., Zaki, M.: Web usage mining: languages and algorithms. Studies in Classification, Data Analysis, and Knowledge Organization. Springer, Heidelberg (2001)
4. Batista, P., Silva, M.J.: Mining web access logs of an on-line newspaper (2002)
5. Zaiane, O.R., Xin, M., Han, J.: Discovering web access patterns and trends by applying OLAP and data mining technology on web logs. In: ADL 1998: Proceedings of the Advances in Digital Libraries Conference, Washington, DC, USA, pp. 1–19. IEEE Computer Society (1998)
6. <https://softwareengineering.stackexchange.com/questions/191840/how-web-servers-identify-a-client>
7. Grace, L.K., Maheswari, V., Nagamalai, D.: Analysis of web logs and web user in web mining (2011). arXiv preprint: [arXiv:1101.5668](https://arxiv.org/abs/1101.5668)
8. [https://en.wikipedia.org/wiki/Proxy\\_server](https://en.wikipedia.org/wiki/Proxy_server)
9. Davison, B.D., Wu, B.: Implementing a web proxy evaluation architecture. In: Proceedings of the 30th International Conference for the Resource Management and Performance Evaluation of Enterprise Computing Systems (CMG) (2004)
10. Sharma, S., Rana, V.: Web user identification: a review of approaches and issues. Int. J. Comput. Eng. Technol. (IJCET) **8**(4), 12–18 (2017)
11. Ivancsy, R., Juhasz, S.: Analysis of web user identification methods. World Acad. Sci. Eng. Technol. **2**(3), 212–219 (2007)
12. Datta, A., et al.: A proxy-based approach for dynamic content acceleration on the WWW. In: Proceedings of the Fourth IEEE International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS 2002). IEEE (2002)
13. Yuan, C., Hua, Z., Zhang, Z.: Proxy+: simple proxy augmentation for dynamic content processing. In: Web Content Caching and Distribution, pp. 91–108. Springer, Dordrecht (2004)
14. Hussain, S., McLeod, R.D.: Intelligent prefetching at a proxy server. In: 2000 Canadian Conference on Electrical and Computer Engineering, vol. 1. IEEE (2000)
15. Shyamala, K., Kalaivani, S.: Application of Monte Carlo search for performance improvement of webpage prediction. Int. J. Eng. Technol. (UAE) **7**(3–4), 133–137 (2018)
16. Shyamala, K., Kalaivani, S.: Enhanced webpage prediction using rank based feedback process. Lecture Notes in Computational Science and Engineering. Springer (accepted)
17. <http://ita.ee.lbl.gov/html/contrib/NASA-HTTP.html>
18. Horng, Y.-W., Lin, W.-J., Mei, H.: Hybrid prefetching for WWW proxy servers. In: Proceedings of the 1998 International Conference on Parallel and Distributed Systems. IEEE (1998)
19. Yeh, T., Pan, Y.: Improving the performance of the web proxy server through group prefetching. In: Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication. ACM (2012)
20. Gracia, C.D., et al.: Prefetching in information superhighway-a retrospective study





# An Approach for Generating SQL Query Using Natural Language Processing

Priyanka More<sup>1(✉)</sup>, Bharti Kudale<sup>2(✉)</sup>, Pranali Deshmukh<sup>1(✉)</sup>,  
Indira N. Biswas<sup>1(✉)</sup>, Neha J. More<sup>1(✉)</sup>, and Francisco S. Gomes<sup>1(✉)</sup>

<sup>1</sup> Information Technology, Genba Sopanrao Moze CoE, Balewadi, Pune, India  
morepriyankad@gmail.com, desh mukhpranali3@gmail.com,  
Indira.biswas27@gmail.com, nehamore2911@gmail.com,  
fransgomes26@gmail.com

<sup>2</sup> Computer Engineering, Genba Sopanrao Moze CoE, Balewadi, Pune, India  
gaikwadbharati3@gmail.com

**Abstract.** Today's databases of corporations are so huge, that they can only be approached by experienced programmers. Accessing data from a database usually needs notable skills such as knowledge of SQL; however, the most of us who interact with databases every day don't have that background. Hence it's an increase demand for non-technical user to be able to redeem data from databases without having to list SQL queries. And this problem is solved by using approach of Natural Language Processing. This research work presents an approach for querying system for natural language processing. Hence it will dramatically simplify the process of handling with large data and making data available for everyone.

**Keywords:** Natural Language Processing · Tokenization · Tagging · Relational database · Semantic analysis · SQL query

## 1 Introduction

The users who know databases can easily access the data but in case of a nontechnical user, it becomes difficult. So an interface system between natural language processing and databases will help non-technical users to work with databases by using natural language (i.e., English). This interface will open the platform for users to access the data in databases by answering the queries in English Natural Language Query. The main benefit of this system that it works independently of database language and it will also learn and improve its knowledge bases through past references.

In this paper, we introduce Global English Language Interface to Database. This interface will grant the users to interact with the database without database language knowledge. The user will access the data with the help of typing queries in the English Language rather than SQL (Structured Query Language). This will ease the extraction of data from the database for users without the need to have skills in SQL. The system uses NLP techniques to translate English language Query to SQL query.

## 2 Literature Survey

The first effort of natural language interfaces to databases came into account as early as the sixties. An example of the system is LUNAR, developed to answer naturally written questions about the analysis based on geological features of lunar rocks returned by Apollo mission [1].

- (a) Another system is LADDER which could be used with huge databases, it basically uses semantic grammar, which needed elaboration of a particular grammar for a single database [1].
- (b) Another system is “Linked Open Data Query on Natural Language”. This system they proposed a method for constructing DAG and triples, they use Web to connect data in URLs and resource framework and is open to all Web users. This system converts Natural language query into SPARQL [2].
- (c) “Philips Question Answering Machine”. This system gives the explicit variance of semantic parsing and syntactic parsing of users input (i.e., Natural language query). It defined a semantic analysis of three stages:

Formal Language

World Model Language

Database Language.

Using these three stages, desired output is obtained [3].

- (d) “Algorithm for solving natural language query execution problems on relational databases.” This system develops a model to extend the proposition and MAPPER was developed and used on student databases, where an interface was used on relational databases [4].
- (e) “DBIQS and Mining Databases using NLP.”  
This system portrays veritable automatic, fast and authentic way to query databases. In a first stage the system creates S-Map which contains lexicons and their relationships. The second stage comprises of MR generator (Meaningful representation) that takes the set of token and their relationship information to create MR Map. In the last stage DBIQS produces SQL query and present the information extracted after firing it in the form of tables, pie charts, and graphs [5].

## 3 System Architecture

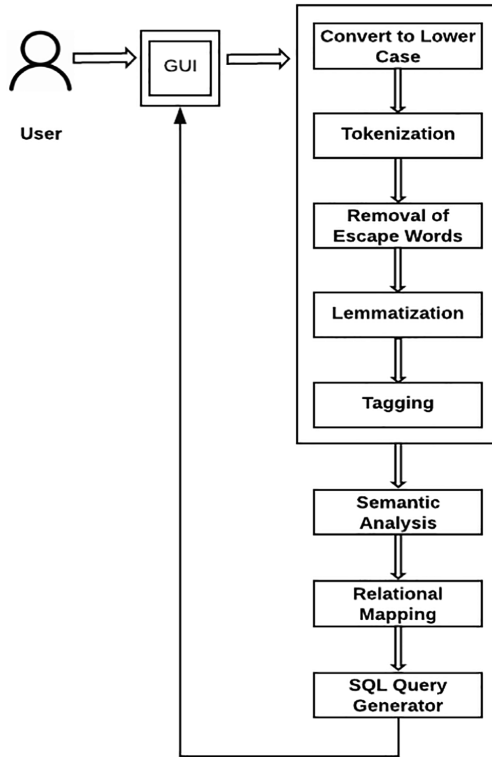
Below figure gives the simple architecture of the system. It consists of conversion of the lower case, tokenization, removal of escape words, lemmatization, Tagging of part of speech, semantic analysis, relational mapping and finally SQL query is generated. The input to the system is natural language query (Fig. 1).

### 1. Natural Language Input

An input to the proposed system is the English query which is given by users.

### 2. Convert to Lower Case

English query is then converted into lowercase



**Fig. 1.** A figure shows System Architecture of

3. Tokenization

Each sentence is further divided into tokens, for each token distinct token id is provided.

4. Removal of escape words

Text may contain stop words like ‘the’, ‘is’, ‘are’. Stop words can be filtered from the text to proceed. In this stages, this stop words are removed.

5. Lemmatization

In this stage, all token is converted into its roots form. For example “Am, are, is” into “be”

“Cars, car’s” into “car”. These root forms are basically known as lemmas.

6. Tagging

The lemmas are further tagged according to their part of a speech form. For example, the tag will determine the noun in the lemmas and help to find tables and attributes in the database.

7. Semantic Analysis

It starts by reading all of the words in content to capture the real meaning of any text. It determines the text elements and assigns them to their logical and grammatical role. For example, “destination” and “last stop” technically mean the same thing.

#### 8. Relational Mapping

The attribute values are related to their attribute through the relation operators like equal to, is greater than, is less than, etc. For example, Greater than is mapped into “>”, Equal to is mapped into “=”, etc. In this, the comparing attribute has to be written first, and the logical operator is then attached to it after the value which is to be compared is attached.

#### 9. SQL query generator

This is the final stage where actual query is generated and fired on the database management system to get the desired output on GUI.

## 4 Open NLP Libraries

### (a) Natural Language Toolkit

This toolkit is used for tasks like tokenization, lemmatization, parsing, POS tagging, etc. This library has tools for almost all NLP tasks.

### (b) Stanford CoreNLP

Natural language processing depends on the client server architecture and it will be more reliable and accurate analysis.

### (c) Spacy

This library provides most of the standard functionality and provides the fast accessing system. Spacy provokes the better interface scheme between deep learning and frameworks.

## 5 Conclusion

In the proposed system user can enter the query in natural language, then the system will translate it into the SQL query and will get the result from the database. The developed system gives the correct result for simple queries.

## References

1. Woods, W., Kaplan, R., Webber, B.: The Lunar science natural language information system (1972)
2. Liu, J., Li, W., Lu, L., Zhou, J., Han, X., Shi, J.: Linked open data query based on natural language. *Chin. J. Electron.* **26**, 230–235 (2017)
3. Seha, R.J.H.: Philips question answering system PHILIQAI (1977)
4. Enikuomihin, A.O., Okwufulueze, D.O.: An algorithm for solving natural language query execution problems on relational databases. *Int. J. Adv. Comput. Sci. Appl.* **3**, 169–175 (2012)
5. Agrawal, R., Chakkarwar, A., Choudhary, P., Jogalekar, U.A., Kulkarni, D.H.: DBIQS – an intelligent system for querying and mining databases using NLP (2014)
6. More, P., Phalnikar, R.: Generating UML diagrams from natural language specifications. *IJAIS* **1**(8), 19–23 (2012)

7. Yorozu, Y., Hirano, M., Oka, K., Tagawa, Y.: Electron spectroscopy studies on magneto-optical media and plastic substrate interface. *IEEE Transl. J. Magn. Jpn.* **2**, 740–741 (1987). Digests 9th Annual Conf. Magnetism Japan, p. 301, 1982
8. Androutsopoulos, I., Richie, G.D., Thanisch, P.: Natural language interface to databases – an introduction. *J. Nat. Lang. Eng.* **1**(1), 29–81 (1995)
9. Küçükünç, O., Gudukbay, U., Ulusoy, O.: A natural language-based interface for querying a video database. *IEEE Multimed.* **14**, 83–89 (2007)
10. Mahmud, T., Azharul Hasan, K.M., Ahmed, M., Chak, T.H.C.: A rule-based approach for NLP based query processing. *IEEE* (2015)
11. Fulford, K., Olmsted, A.: Mobile natural language database interface for accessing relational data. *IEEE* (2017)
12. Gupta, P., Goswami, A.: IQS-Intelligent Querying System using natural language processing. *IEEE* (2017)
13. Chandhana Surabhi, M.: Natural language processing future. *IEEE* (2013)
14. Nicole, R.: Database System Concepts, 4th edn.



# Sentiment Analysis and Deep Learning Based Chatbot for User Feedback

Nivethan<sup>(✉)</sup> and Sriram Sankar

Department of Information Technology, Madras Institute of Technology,  
Anna University, Chennai, India  
niveniranj@gmail.com, srisankar98@gmail.com

**Abstract.** Recently, the conversational agents like Chatbots are widely employed for achieving a better Human-Computer Interaction (HCI). In this paper, a retrieval based chatbot is designed using Natural Language Processing (NLP) techniques and a Multilayer Perceptron (MLP) neural network. The purpose of the chatbot is to extract user's feedback based on the services provided to them. User feedback is a very essential component for the betterment of the service. Chatbot serves as a better interface for obtaining an appropriate user feedback. Furthermore, sentiment analysis is done on the feedback as a result a suitable response is delivered to the user. A Long Short Term Neural Network (LSTM) is used to classify the sentiment of the feedback.

**Keywords:** Chatbot · Sentiment analysis · User feedback · Deep learning

## 1 Introduction

Evolution is inseparable in the rise of the nation especially in the field of technology. Similar to living organisms, technology evolves too. For a long time, the Human-Computer Interaction (HCI) has been not like a human-to-human communication. We used mouse, keyboard to interact with a computer. Recent advances like speech recognition, gesture recognition, etc. has made HCI to evolve. Chatbots are Artificial Intelligence (AI) agents and are one among such trend. Chatbots or chatting robots provide a human-to-human conversation experience. This is a better way of interaction especially for obtaining user feedback. The first chatbots like. Nowadays it is possible to build a chatbot using various online AI platforms. But this work does not make use of any online AI platforms. The chatbot is built only to retrieve user feedback and not in engaging them for a long time or serve as a personal assistant.

Chatbots are built in two ways: generation type chatbots and retrieval type chatbots. The retrieval type chatbots are simple and have predefined inputs in the knowledge base. The generative type chatbots generate their own sentences from learned examples. Retrieval type chatbots are comparatively easier to build than generative types because they have to just a proper response for the current conversation. Wang et al. [8] created retrieval based chatbot that considers only the last message from the user and not previous queries. Speak-to-me is also based on a single-turn conversation as it is sufficient for the purpose of the chatbot.

There are billions of human beings around the world speaking different languages and we are not able to understand what a person is trying to convey without knowing or understanding the language. Similarly a chatbot or a conversational agent needs knowledge of the human language to understand it and process it. Thus in choosing the appropriate response the chatbot model must be trained on different queries it might get. This is the key to input-response matching.

Sentiment detection plays an important role in business these days. An organization provides services to its customers. Customers after utilization provide their feedback which can either a satisfied response or dissatisfied one. Either way the company has to collect user feedback in order to improve its future services. Due to huge amount of data in customer reviews, it is impossible for a person to read all the reviews and improve the service. With deep learning and machine learning blooming to automate things, it is easy now to collect user feedback and to analyse it for user satisfaction.

In our work, we have employed the chatbot to collect user feedback and another model at the background analyses the review and provides an appropriate response to the user. The model used to analyse the reviews gives better insight into the service provided.

## 2 Related Work

### 2.1 Chatbots

Chatbots or conversational agents were implemented by different researchers for different kinds of tasks and purposes. Most chatbots were capable of communicating well with the users in a more human-like way. The chatbot, Chappie [2] by Bibek Behra was born as a business requirement to automate the personal assistant or concierge. It uses natural language processing (nlp) to analyse chats and extracts intent of the user with a score similar to the likes of WIT. Then it uses this information and AIML(Artificial Intelligence Mark-up Language) to make a conversation with the user. Later chatbots have been built using AI methods.

Much of the earlier chatbots were retrieval-based chatbots. Those retrieval-based chatbots were also a single turn conversation chatbots. Wang et al. [8], Wang et al. [9] and Wu et al. [10] created single-turn conversation and retrieval-based chatbots. Recently multi-turn conversation chatbots were also paid attention. Lowe et al. [6], Yan et al. [11] and Zhou et al. [12] built multi-turn conversation chatbots which considers previous queries and responses to retrieve the next appropriate response from the knowledge base.

In our work, we employed a retrieval-based chatbot for the purpose of feedback gathering. A retrieval-based chatbot suffices the purpose. The chatbot has a classification model at its core to classify the queries. The queries are classified and a suitable response is chosen. An artificial neural network serves as the classification model.

## 2.2 Sentiment Detection

Sentiment Detection has become one of the widely researched areas and it has been already explored a lot. Most of the works in sentiment analysis are focused on Twitter dataset. The tweets are widely analysed for sentiment detection and the tweets are retrieved using hashtags such as positive, negative. The analysis is made on the assumption that tweets with hashtags reflect the appropriate sentiment. Sentiment analysis methods are of three types: Lexicon-based methods, machine learning-based methods and hybrid methods. Lexicon-based methods require predefined sentiment lexicon to determine the polarity of any document. Khan et al. [5] work on sentiment analysis is lexicon-based.

Bravo et al. [3] proposed a machine learning approach for sentiment analysis which is a supervised method combining strength, emotions and polarities of the tweets. Basari et al. [1] proposed a hybrid method which used support vector machine (SVM) and particle swarm optimisation (PSO) to categorize a movie. Pandey et al. [7] used tweets to perform sentiment analysis using a hybrid approach. They make use of modified approach which is based on both K-means clustering and Cuckoo search.

In this work, we use a supervised learning approach. A LSTM model is used to analyse the review and classify it as either a positive review or a negative one.

## 3 Proposed Work

### 3.1 Preprocessing

The dataset for the chatbot was grouped into categories based on the queries. Each category served as the class to be classified by the chatbot model. The queries for each class is taken. All the queries were tokenized using Natural Language ToolKit (NLTK). NLTK is an essential tool for NLP. The tokens were stored in a list and duplicate words were removed and it served as the bag of words. The length of the bag of words is the input size of the chatbot model. The number of categories of queries is the output size of the model. The words in the bag of words are stemmed using Lancaster stemmer. It is a very aggressive stemming algorithm and faster one. It will reduce the working set of words hugely.

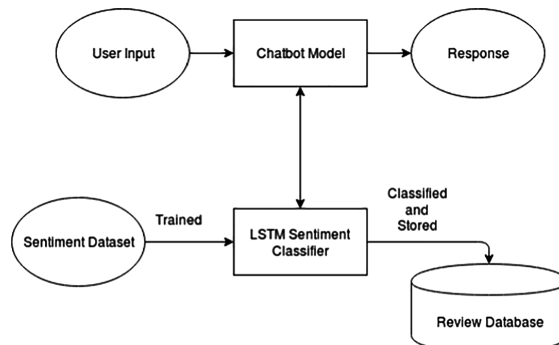


Fig. 1. Overview of the proposed work.



Stemming is a method in which a set of words are trimmed to its root words. It is very useful while processing raw text.

### 3.2 Chatbot

The chatbot model is a classifier which classifies the input from user. A multilayer perceptron (MLP) network is used to classify the input. The network has two hidden layers with 8 hidden nodes in both layers. A single node in output layer classifies the input from the user. The bag of words are converted into one hot vectors before providing as input to the model. When a particular word is present in the input text, the corresponding position in one-hot vector is marked as “1” and the corresponding neuron nodes get activated. The network learns to classify the input using the presence and absence of words in input vector. An overview of the work is shown in Fig. 1. A screenshot of the working chatbot is shown in Fig. 2. The architecture of the chatbot model is shown in Fig. 3.

```
Bot : Hello!!!!
User: Hey
Bot : Hi there, please provide your valuable feedback?
User: It was good
Bot : I'm happy that you are happy, Thank you. :)
User: Thank you
Bot : Don't mention it
User: What is your name?
Bot : My boss named me SentiBot and you?
User: I'm Jack
Bot : Your name is sweet
User: Can you tell me a joke?
Bot : Oops!! Never heard of it
User: Bye
Bot : Bye! Come back again soon.
..
```

Fig. 2. Chatbot speaking with a user.

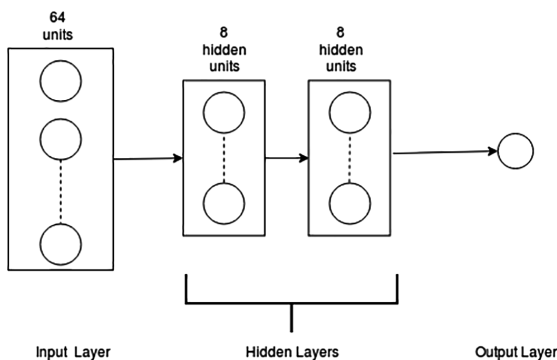


Fig. 3. Architecture of the MultiLayer Perceptron used as the chatbot model.

### 3.3 Sentiment Detection

A LSTM network is used to classify the feedback of the user. The LSTM network had 100 hidden units. The first layer in the network is an embedding layer and the LSTM layer follows it. The output layer classifies the reviews. Summary of the LSTM model is shown in Table 1.

**Table 1.** Summary of LSTM model to classify feedback.

Layer	Output size
Embedding layer	(None, 500, 32)
LSTM layer	(None, 500)
Dense layer	(None, 1)

## 4 Implementation

The dataset for sentiment analysis is obtained from Kaggle's Amazon reviews dataset [4] for sentiment analysis. The other tools that were used for the work are Keras for the deep learning models and NLTK for NLP. The work is done in Python 2 as it very suitable for deep learning researches. The chatbot model was run for 1000 epochs with a batch size of 8 and gradient descent algorithm was used as an optimizer. The sentiment analysis model was run for 100 epochs and Adam optimizer was used and the batch size was 64.

## 5 Experimental Results

The purpose of the chatbot was able to obtain user feedback and the proposed model fulfilled the purpose. The chatbot model after training 1000 epochs was able to achieve an accuracy of 97.35% and Fig. 4 shows the image of the training phase of chatbot. The sentiment analysis model was able to achieve a train accuracy of 99.99% in 100 epochs and test accuracy of 92.19%. Figure 5 shows the training phase of sentiment analysis model.

```

Training Step: 4965 | total loss: 0.11204 | time: 0.009s
| Adam | epoch: 993 | loss: 0.11204 - acc: 0.9853 -- iter: 34/34
--
Training Step: 4970 | total loss: 0.08599 | time: 0.013s
| Adam | epoch: 994 | loss: 0.08599 - acc: 0.9913 -- iter: 34/34
--
Training Step: 4975 | total loss: 0.06886 | time: 0.013s
| Adam | epoch: 995 | loss: 0.06886 - acc: 0.9949 -- iter: 34/34
--
Training Step: 4980 | total loss: 0.05790 | time: 0.010s
| Adam | epoch: 996 | loss: 0.05790 - acc: 0.9970 -- iter: 34/34
--
Training Step: 4985 | total loss: 0.05226 | time: 0.009s
| Adam | epoch: 997 | loss: 0.05226 - acc: 0.9982 -- iter: 34/34
--
Training Step: 4990 | total loss: 0.33770 | time: 0.010s
| Adam | epoch: 998 | loss: 0.33770 - acc: 0.9239 -- iter: 34/34
--
Training Step: 4995 | total loss: 0.21680 | time: 0.008s
| Adam | epoch: 999 | loss: 0.21680 - acc: 0.9551 -- iter: 34/34
--
Training Step: 5000 | total loss: 0.14776 | time: 0.010s
| Adam | epoch: 1000 | loss: 0.14776 - acc: 0.9735 -- iter: 34/34
--

```

Fig. 4. Training the chatbot model

```

24936/24936 [=====] - 253s 10ms/step - loss: 0.0705 - acc: 0.9769 - val_loss: 0.3250 - val_acc: 0.9062
Epoch 31/100
24936/24936 [=====] - 253s 10ms/step - loss: 0.0263 - acc: 0.9928 - val_loss: 0.4676 - val_acc: 0.9219
Epoch 32/100
24936/24936 [=====] - 253s 10ms/step - loss: 0.0164 - acc: 0.9962 - val_loss: 0.4085 - val_acc: 0.9219
Epoch 33/100
24936/24936 [=====] - 252s 10ms/step - loss: 0.0207 - acc: 0.9943 - val_loss: 0.4465 - val_acc: 0.9062
Epoch 34/100
24936/24936 [=====] - 252s 10ms/step - loss: 0.0158 - acc: 0.9963 - val_loss: 0.3943 - val_acc: 0.8594
Epoch 35/100
24936/24936 [=====] - 251s 10ms/step - loss: 0.0350 - acc: 0.9893 - val_loss: 0.4213 - val_acc: 0.9219
Epoch 36/100
24936/24936 [=====] - 251s 10ms/step - loss: 0.0255 - acc: 0.9933 - val_loss: 0.5422 - val_acc: 0.8966
Epoch 37/100
24936/24936 [=====] - 252s 10ms/step - loss: 0.0172 - acc: 0.9947 - val_loss: 0.4311 - val_acc: 0.9375
Epoch 38/100
24936/24936 [=====] - 253s 10ms/step - loss: 0.0216 - acc: 0.9944 - val_loss: 0.4929 - val_acc: 0.9219
Epoch 39/100
10304/24936 [=====>.....] - ETA: 2:28 - loss: 0.0091 - acc: 0.9975

```

Fig. 5. Training the Sentiment Model for classification

## 6 Conclusion

Thus a chatbot for obtaining user feedback, classifying the feedback and providing an appropriate response was built. The chatbot was simple and served the purpose it was built for. It was faster to train and retrieve response accounting to its simple architecture. This could be employed in real time to obtain feedback from users.

## 7 Future Work

Future work includes producing a generative model which can identify the sentiment of the user from the user input and. Also, in future better sentiment classification model is intended to be built. Another important part of the future work is to build a speech recognizing chatbot which recognizes the user sentiment via the user’s vocal input.

## References

1. Basari, A.S.H., Hussin, B., Ananta, I.G.P., Zeniarja, J.: Opinion mining of movie review using hybrid method of support vector machine and particle swarm optimisation. *Procedia Eng.* **53**, 453–462 (2013)
2. Behera, B.: bibek@magictiger.com
3. Bravo-Marquez, F., Mendoza, M., Poblete, B.: Combining strengths, emotions and polarities for boosting twitter sentiment analysis. In: *Proceedings of the Second International Workshop on Issues of Sentiment Discovery and Opinion Mining*, p. 2 (2013)
4. Kaggle Amazon Reviews for Sentiment Analysis. <https://www.kaggle.com/bittlingmayer/amazonreviews>
5. Khan, A.Z., Atique, M., Thakare, V.: Combining lexicon-based and learning based methods for twitter sentiment analysis. *Int. J. Electron. Commun. Soft Comput. Sci. Eng. (IJECSCE)*, 89 (2015)
6. Lowe, R., Pow, N., Serban, I., Pineau, J.: The ubuntu dialogue corpus: a large dataset for research in unstructured multi-turn dialogue systems (2015). [arXiv:1506.08909](https://arxiv.org/abs/1506.08909)
7. Pandey, A.C., Rajpoot, D.S., Muskesh, S.: Twitter sentiment analysis using hybrid cuckoo search method (2017). <http://dx.doi.org/10.1016/j.ipm.2017.02.004>
8. Wang, H., Lu, Z., Li, H., Chen, E.: A dataset for research on short-text conversations. In: *EMNLP*, pp. 935–945 (2013)
9. Wang, S., Jiang, J.: Learning natural language inference with LSTM (2015). [arXiv:1512.08849](https://arxiv.org/abs/1512.08849)
10. Wu, Y., Wu, W., Li, Z., Zhou, M.: Topic augmented neural network for short text conversation. *CoRR abs/1605.00090* (2016)
11. Yan, R., Song, Y., Wu, H.: Learning to respond with deep neural networks for retrieval-based human-computer conversation system. In: *SIGIR 2016, Pisa, Italy*, pp. 55–64, 17–21 July 2016. <https://doi.org/10.1145/2911451.2911542>
12. Zhou, X., Dong, D., Wu, H., Zhao, S., Yan, R., Yu, D., Liu, X., Tian, H.: Multiview response selection for human-computer conversation. In: *EMNLP 2016* (2016)



# Semantic Concept Detection for Multilabel Unbalanced Dataset Using Global Features

Nita Patil and Sudhir Sawarkar<sup>(✉)</sup>

Datta Meghe College of Engineering, Airoli, Navi Mumbai, India  
nsp.cm.dmce@gmail.com, Sudhir\_sawarkar@gmail.com

**Abstract.** Digital evolution in capturing video, advances in compression technology and internet leads to availability of large videos on the web. There is growing need for efficiently retrieving relevant videos. Semantic Concept detection assigns multiple labels to segmented shots or entire video which facilitates many applications like multimedia indexing and retrieval. This paper presents the semantic concept detector architecture for unbalanced dataset which assigns multiple labels with probability to input video. The proposed architecture uses visual features extracted on global scale. The unbalanced dataset problem is handled by partitioning dataset into segments further evaluating classifiers on these dataset. Feature fusion and decision fusion is evaluated using machine learning algorithm for all segments. Performance of the concept detection architecture for above fusion methods are reported with Mean Average Precision. The proposed method for multilabel concept detection is evaluated on TRECVID 2007 dataset and performance is better than existing early and late fusion.

**Keywords:** Semantic Concept Detection · Feature Extraction · Early fusion · Late fusion · SVM · Unbalanced dataset

## 1 Introduction

In the era of digital evolution of multimedia information capturing devices and fast network, large amount of multimedia data is available in repositories on the web. To deal with large repositories of multimedia data automatic analysis of these data especially video is needed. Conventional system performs analysis of content of video to perform annotation and indexing of the video required for various applications like browsing and searching. But due the lack of correspondance between low level features and high level semantics of video data, annotations are inaccurate and incomplete. Semantic Concept Detection system helps to bridge this semantic gap by performing mapping of low level features to high-level video semantics to enhance the semantic indexing. Extensive research in this field has improved the efficiency of semantic concept detection systems but it is still a challenging problem due to the large variations in low level features of semantic concepts and inter concept similarities. Low level features color, texture, shape extracted from key-frame or object has to selected painstakingly for effective representation. SVM classifier has become default choice in concept detection systems. In scenario where database in unbalanced performance of classifier degrades as it tends to overfit for majority classes during training.

In the unbalanced dataset problem relevant examples are less as compared to irrelevant examples. This leads to inaccurate classifier model creation during training phase. Many researchers used methods to deal with unbalanced dataset problem mostly based on over sampling positive examples and down sampling negative samples which may lead to over fitting of the classifier.

In this paper, we propose a framework for Semantic video concept detection to deal with above mentioned issues. The proposed framework consists of five major components: segmentation of training dataset, feature extraction, modeling, and classification and fusion modules. Our model is implemented using global low-level features only, so as to keep low computational complexity.

### 1.1 Semantic Concept Detection

The goal of the semantic concept detection system is to recognize the presence or absence of the semantic concept observed in keyframe of video based on the visual properties of keyframe or image. Human Visual System can recognize and interpret the object or concept present from the visual appearance but automatic semantic techniques detects based on the low level features extracted from the video. This is called semantic gap. Semantic concept detection system works towards bridging this semantic gap. The general block diagram of semantic concept detection system is shown in Fig. 1. It includes following broad steps.

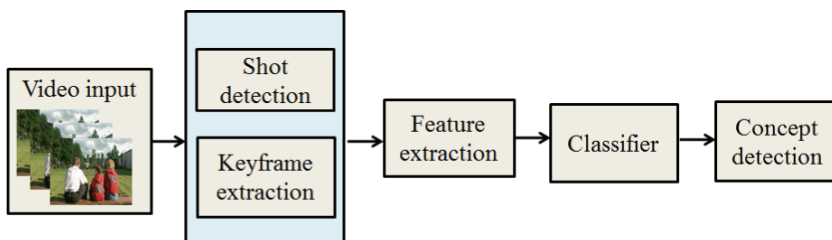


Fig. 1. Block diagram of Semantic Concept Detection system

**Shot Boundary Detection:** It is preprocessing step where video is segmented into shots. Shots exhibits strong correlation between the frames of the video and are important step towards precise concept detection. Shot boundary detection is based on the identification of visual dissimilarity due to the transitions. The shot boundary detection methods usually extract visual features from each frame and the similarities are measured to detect shot boundaries between frames that are dissimilar.

**Key-Frame Extraction:** In concept detection system, shots are represented by summary keyframe which is representative frame for shot. There are great similarities among the frames from the same shot; therefore certain frames that best reflect the shot contents are chosen as key-frames.

**Feature Extraction from Shots or Keyframe:** Low level features are extracted from shots or key-frames. These features include static features in key frames, object features, motion features, etc.

**Annotations or Ground Truth Utilization:** Extracted keyframes from above steps are either manually labeled by user or expert, or ground truth if available with dataset is used for training and validation of trained model.

**Concept Detection:** This step finds the co-relation between low level feature extracted and high level concept assigned to training shots or key-frames by using machine learning approaches detecting concepts available in key-frame with probability of label.

Section 2 covers related work. Section 3 focuses on the methodology and concept selection for segments as well as the generation of concept training data. Section 4 presents the results of the experimental evaluation of the concept detector system. Finally, Sect. 5 concludes this paper by discussing the key aspects of the presented concept detection system.

## 2 Related Work

In this section we discuss work related to low levels feature extraction, classifiers and unbalanced dataset problem.

### 2.1 Feature Extraction

Feature detection and feature selection is fundamental and important step in concept detection task. Li et al. [1] presented review on recent features used for visual feature detection.

Le et al. [2] evaluated the performance of global features and local features for the semantic concept detection task on Trecvid dataset from 2005 to 2009. They demonstrated the performance of the individual global features like color moments, color histogram, edge orientation histogram, and local binary patterns on grid of varying size, various color spaces including HSV, RGB, Luv, and YCrCb and variation in bin sizes. The local feature used is SIFT with BOW. They also considered late fusion of all features by averaging probability scores of SVM classifier. They concluded that global features are compact and effective in feature representation as compared to the computational complexity of local features.

Global level features are compact and easy to extract as compared with local features. Local features require more time and storage if obtained around all keypoints.

**Multi-Feature Learning and multimodality fusion methods:** Multimodal feature representation uses extracting features from different modalities like visual, audio, text and speech stream. The fusion methods are divided into the following three categories: rule-based methods, classification based methods, and estimation-based methods. Muhling [3] investigated a bag of auditory words approach that models MFCC features in an auditory vocabulary combined with visual features via multiple kernel learning.

## 2.2 Fusion Levels

Atrey [4] presented a survey of strategies for multimodal fusion considering fusion methodology and the level of fusion. Multimodality fusion can be performed at three levels: feature level or early fusion, decision level or late fusion and hybrid fusion.

**Early Fusion:** In early fusion strategy feature combination creates large size feature vector by concatenating features from different modality. Modalities considered for fusion are visual audio, text, motion features and metadata attached to video. Snoek et al. [5] described early fusion and late fusion methods implemented on TRECVID dataset. Early fusion has high computational complexity and degrades performance as dimension size increases especially when the features are independent or heterogeneous. The main advantage of early fusion is that it requires only one classifier.

**Late Fusion:** In late fusion strategy features from multiple modalities are extracted and fed to classifiers and decision or scores obtained from classifiers are combined. Fusion of score is simple and easy as output of classifier has same representation. It also gives flexibility in choosing appropriate classifier for specific modality like HMM for audio and SVM for keyframe of video.

Liu et al. [6] used variety of low level global features and SVM in late fusion strategy to combine scores from multiple modality. Liu [7] proposed selective weighted late fusion giving weight to each classifier depending on the MiAP of each concept. They fused features from multiple modalities like textual and visual features and proposed Histogram of Textual Concepts to capture the relatedness of the semantic concepts obtained from tags of images to create dictionary. Cao [8] fused low level features and high level semantic features for multimedia event detection. van Hout [9] evaluated two parametric approaches to late fusion: a normalization scheme for arithmetic mean fusion and a fusion scheme based on logistic regression. These schemes are compared to rule-based fusion schemes.

**Hybrid Fusion:** Several researchers have also tried with hybrid fusion strategy, which is a combination of both early and late fusion methods. A hybrid fusion can get the advantages of both the methods. Lan [10] performed feature extraction from modalities like visual, audio and text and trained classifier for all three streams as single feature and two feature combination in early fusion way and later fused the output of above nine classifiers in late fusion way using two different two rule-based fusion methods called double fusion. Diou [11] used early fusion and concept fusion to evaluate effectiveness of cross-domain concept fusion by experimenting with two datasets. Strat [12] used three approaches for late fusion of classifiers, first grouped classifiers of similar origin, in a hierarchical manner and in second and third approaches grouped classifiers according to their output scores, either iteratively in an agglomerative fashion. Lv [13] proposed pre-filtering process which filtered majority of the negative samples far away from classification boundary and retained informative samples close to the classification boundary based on Adaboost and SVM classifier.



### 3 Materials and Methods

This section describes techniques used for proposed feature fusion on partitioned dataset.

#### 3.1 Shot Detection Methods

For shot boundary detection approach used by Janwe et al. [14] is followed and hierarchical clustering algorithm is used for keyframe extraction.

#### 3.2 Unbalanced Dataset Issue

In unbalanced dataset the number of samples belonging to one concept class is significantly more than those belonging to other class. The predictive classifier model developed using such imbalanced dataset can be biased and inaccurate. Over-Sampling can be used to increase the number of instances in the minority class by randomly replicating them in order to increase the number of samples of the minority class in the sample. Here we have partitioned dataset into three segments based on frequency of the samples in dataset. Concepts having low frequency are kept in segment one, moderate frequency between 0.1 to 0.5 in segment two and more than 0.5 are in segment three.

#### 3.3 Feature Extraction

Effective feature representation and selection of appropriate feature is important. In this paper color and texture features are used as low level features as shown in Table 1.

**Color Feature:** Color acts as a discriminative feature for understanding image or key-frame content. Color feature is independent of image size and orientation. For example blue color is prominent in beach or sky concept whereas brown color is dominating in desert or sunset concepts. There are primarily two methods available based on considering distribution of color and color histogram.

*Color Moments (CM):* Color moments are invariant to scaling and rotation. The color distribution in an image can be interpreted as a probability distribution. The moments of this distribution can then be used as features to identify that image based on color. In this work two lower order moments Mean and Standard Deviation for each channel in HSV space have been used since most of the color distribution information is contained in the low-order moments. This results in a six dimensional feature vector. Equations 1 and 2 are the formulae to calculate mean and standard deviation.

$$E_i = \frac{1}{N} \sum_{i=0}^N I_{ij} \quad (1)$$

$$\sigma_i = \sqrt{\left(\frac{1}{N} \left(\sum_{j=1}^N (I_{ij} - E_i)^2\right)\right)} \quad (2)$$

**HSV Histogram (HSV):** Hue and Saturation define the chromaticity. Hue is a color element and represents a dominant color. Saturation expresses the degree to which white light dilutes a pure color. The HSV model is motivated by the human visual system as it better describes a color image than the RGB model. HSV histogram is distribution of colors of the keyframe in HSV color space. HSV color space is quantized into 40 bins then histogram is generated.

**Texture Features:** Texture is an important visual feature used in domain-specific applications. It can give us information about the content of an image efficiently. It is a repeated pattern of information or arrangement of the structure with regular intervals. It quantifies the properties such as smoothness, coarseness and regularity in an image. The texture feature used in our system is:

**Wavelet Transform (WT):** The wavelet transform is one of the current popular feature extraction methods used in texture classification. The wavelet transform is able to de-correlate the data and provides orientation sensitive information which is vital in texture analysis. It uses wavelet decomposition to significantly reduce the computational complexity and enhance the classification rate.

Table 1 summarizes the feature set used in our experiments.

**Table 1.** Features used in experiment

Feature	Feature description	Dimension
Color Moments (CM) (normalized)	Low order moments (mean and standard deviation)	6
HSV Color Histogram (HSV) (normalized)	Each of h, s and v channel is quantized to $8 \times 2 \times 2$ bins respectively	32
Wavelet Transform (WT) (normalized)	Mean square energy and standard deviation	40

**Feature Fusion:** Feature extraction and feature selection is important in concept detection. There are two types of general approaches observed in feature extraction. In first approach, features are extracted from a single modality like visual stream only, called as unimodal features extraction. In second approach, features are extracted from multiple modalities like audio and text, called as multimodal fusion. After feature extraction and selection supervised machine algorithms are used to classify semantic concepts. In single modality most of the existing approaches use visual stream as important information is stored in this modality dominating other streams.

**Early Fusion Dealing with Unbalanced Dataset Problem:** In the proposed approach the annotated key-frame dataset is partitioned into three segments to improve performance. Three low level features described in the previous section are extracted from all the three segments. Features are normalized using statistical methods. Each feature vector is normalized using min-max normalization. For  $M$  feature vector  $\{Y_1, Y_2, Y_M\}$ , the minimum and maximum value of each feature vector are obtained where  $y_i$  is  $N$  dimensional feature vector comprising of total key-frames in dataset.

The features are normalized using equation

$$Y' = \frac{Y - \text{Min}Y_i}{(\text{Max}Y_i - \text{Min}Y_i)} \tag{3}$$

where  $Y'$  is the normalized vector and  $\text{Max}Y_i$ ,  $\text{Min}Y_i$  are the maximum and minimum value of feature vector  $Y_i$ . Figure 2 shows diagram for Early Fusion approach.

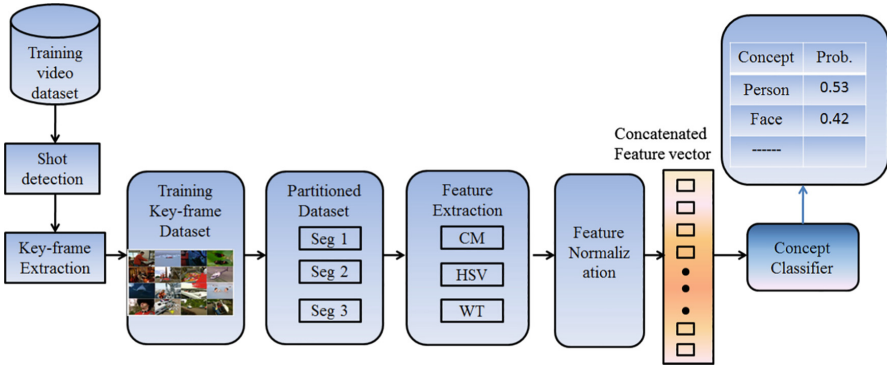


Fig. 2. Early fusion of features on partitioned segments of Dataset.

**Late Fusion:** Three low level features are extracted from first segment. Separate classifiers are trained for these three individual features and classifier models are created for given features. Similar procedure is adopted for other segments and created models are saved for further testing of keyframes. Figure 3 shows classifier model creation for late fusion approach.

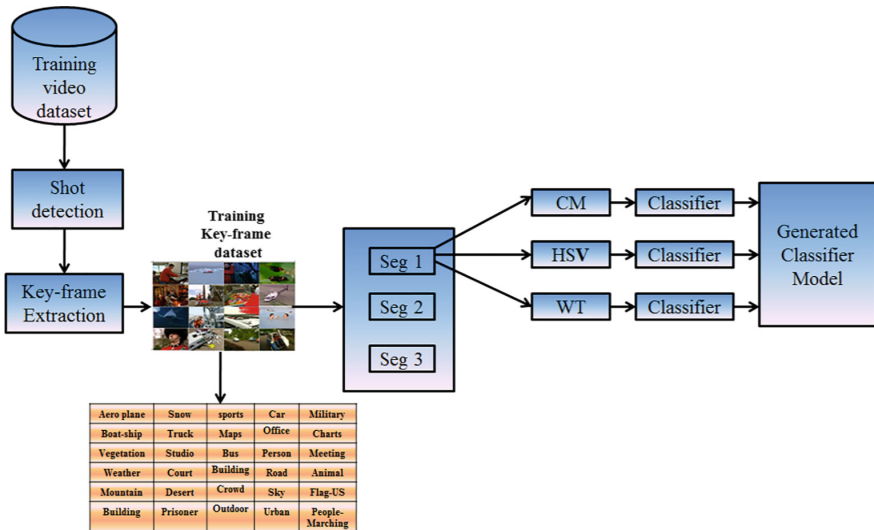


Fig. 3. Late fusion Model trained on Partitioned Dataset.

### 3.4 Classifier Design

Support Vector Machine (SVM): SVM is basically a classifier that performs classification tasks by constructing hyperplanes in a multidimensional space that separates cases of different class labels. The output of a SVM can be a classification map that contains class labels for keyframe (or object), or a probability map that contains probability estimates for keyframe or each object to belong to the assigned concept class. Here multi-label annotation task is transformed into binary classification problem. In this experiment, LIBSVM-3.20 [9] package with Matlab implementation is used and a binary classifier is trained for each concept class. Test key-frame is passed through combined model which predicts the score belonging to each concept class.

### 3.5 Dataset Description

TRECVID’s 2007 Video dataset and ground-truth dataset is used to conduct experiments. The National Institute of Standards and Technology (NIST) is responsible for the annual Text Retrieval Conference (TREC) Video Retrieval Evaluation (TRECVID). Every year, it provides a test collection of video datasets along with a task list. It focuses its efforts to promote progress in video analysis and retrieval. It also provides ground-truth for researchers. Figure 4 shows sample keyframes of concepts used in this experiment (Tables 2 and 3).



Fig. 4. Sample key-frames of various concepts in TRECVID dataset

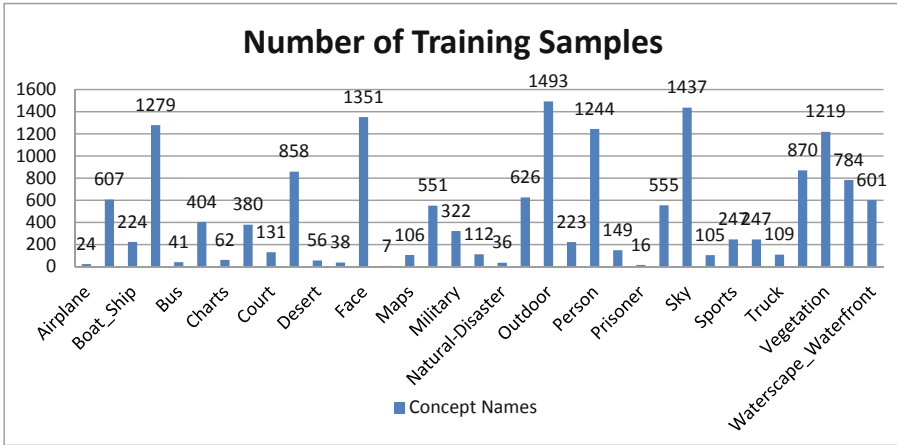
**Table 2.** Details of Partitions used from TRECVID development Dataset

Dataset	Dataset name	Partitions	No. of videos	No. of keyframes
TRECVID development dataset	Partition I	Validation dataset	80	4213
		Training dataset		16542
	Partition II	Test dataset	30	12615

**Table 3.** Details of the Number of key-Frames of segments of TRECVID development dataset

Segment no.	No. of training key-frames	No. of testing key-frames
Segment 1	871	311
Segment 2	3955	1176
Segment 3	11716	10528
Total	16542	12015

Table 4 shows names of concept belonging to three segments and number of annotated keyframes available for training for each concept (Fig. 5).



**Fig. 5.** Number of positive keyframe in TRECVID dataset

**Table 4.** Concepts in three segments with number of key-Frames in each concept.

Segment 1 (871)			
No. of Key-	Concept Name	Sr. No.	
24	Aiplane	1	
41	Bus	2	
62	Charts	3	
131	Court	4	
56	Desert	5	
38	Explosion_Fire	6	
7	Flag-US	7	
106	Maps	8	
112	Mountain	9	
36	Natural-Disaster	10	
16	Prisoner	11	
105	Snow	12	
109	Truck	13	
28	Weather	14	

Segment 2 (3955)			
No. of Key-	Concept Name	Sr. No.	
607	Animal	1	
224	Boat_ship	2	
404	Car	3	
380	Computer-TV-screen	4	
551	Meeting	5	
322	Military	6	
223	People-Marching	7	
149	Police_security	8	
247	Sports	9	
247	Studio	10	
601	Waterscape Waterfront	11	

Segment 3 (11716)			
No. of Key-	Concept Name	Sr. No.	
1279	Building	1	
858	Crowd	2	
1351	Face	3	
626	Office	4	
1493	Outdoor	5	
1244	Person	6	
555	Road	7	
1437	Sky	8	
870	Urban	9	
1219	Vegetation	10	
784	Walking_Running	11	

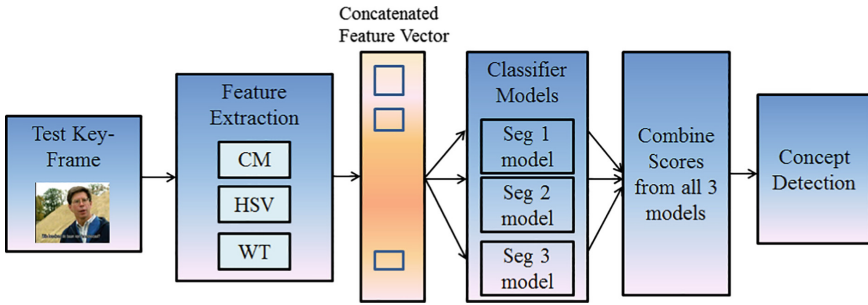


Fig. 6. Concept Detection by EF approach on Test Dataset.

### 3.6 Evaluation Measures

Mean Average Precision (MAP) is used as the performance evaluation of the proposed concept detection method by measuring top d ranked concepts sorted in descending order. Here we have considered top 5, top 10 and top N ranked concepts. In top N, N is considered to the maximum number of annotations of keyframe in training dataset.

## 4 Experimental Results

In Early Fusion approach, all features extracted from segment are combined to form concatenated feature vector. Early fused trained models predict scores for each concept. Only three SVM classifiers are required for three segments. Output scores are ranked and MAP is calculated for all concepts.

Whereas in Late Fusion approach, a single SVM classifier is trained for individual feature of a segments thus requires total 9 classifiers. This requires more time as compared to EF method.

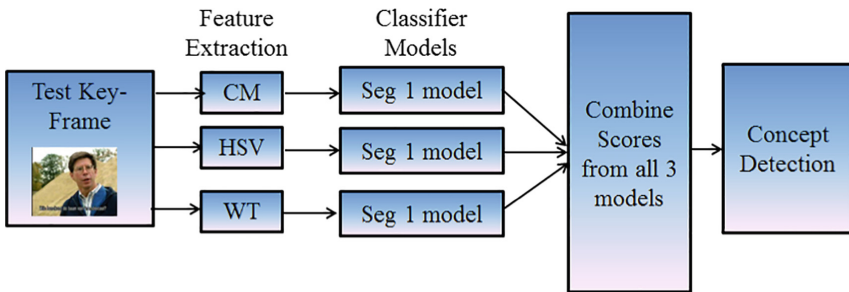


Fig. 7. Concept Detection by LF approach on Test Dataset.

Table 5. Map for Early and Late Fusion

Method	Map 5	Map 10	Map n
Early Fusion	0.422	0.53	0.37
Late Fusion	0.26	0.52	0.32

**Table 6.** Detected concepts Using EF and LF approaches.

Key-Frame No	Key-Frame Name	Test Key-Frame	Concepts in Ground-Truth Dataset	Correctly Detected Concepts	
				EF	LF
12214	Shot_102_144_RKF		Crowd, Military, Outdoor, Person, Police_Security, Sky, Snow, Waterscape_Waterfront	Military, Outdoor, Person, Sky, Snow, Waterscape_Waterfront	Person, Outdoor, Sky, snow, Waterscape_Waterfront
No. Of concepts			8	6	5
12209	Shot_638_RKF		Building, Bus, Car, Outdoor, Road, Sky, Vegetation	Building, Bus, Car, Outdoor, Sky, Vegetation'	Car, Outdoor, Sky
No. Of concepts			7	6	3
11915	Shot_5621_RKF		Face, Outdoor, Person	Face, Outdoor	Face, Outdoor
No. Of concepts			3	2	2
207	Shot26_113_RKF		Boat_Ship, Face, Outdoor, Sky, Snow, Waterscape_Waterfront	Outdoor, Sky, Snow, Waterscape_Waterfront	Face, Outdoor, Sky, Snow, Waterscape_Waterfront
No. Of concepts			6	4	5
1066	Shot4_255_RKF		Building, Face, Meeting, Office, Person, Studio	Building, Face, Meeting	Building, Face, Outdoor, Person,
No. Of concepts			6	3	4
764	Shot63_25_RKF		Building, Car, Outdoor, Sky, Urban	Building, Car, Outdoor, Sky	Building, Car, Outdoor
No. Of concepts			5	4	3
12108	Shot86_114_NRKF_1		Face, Outdoor, Person, Vegetation	Face, Outdoor, Person	Face, Outdoor, Vegetation
No. Of concepts			4	3	3



The output scores by each feature classifier of a segment are combined by average fusion approach. Figures 6 and 7 shows Concept Detection by EF and LF approaches.

Table 5 presents MAP for EF and LF methods. Maximum annotation to single key-frame are 11 so in this experiment top 10 ranked concepts are considered as MAP 10. Map for Early fusion for selected feature is slightly more than EF. For few concepts Early fusion approach work better than LF while for few others Lf strategy proved to be effective.

Table 6 presents the experimental results for some of the test samples, showing the comparison of correctly detected concepts and their count by EF and LF methods.

For a test sample key-frame named Shot\_102\_144\_RKF, ground-truth annotations has 8 labels. EF detected 6 and LF detected 5 labels whereas in Shot4\_255\_RKF keyframe LF detected 4 as compared to 3 of LF. LF approach is better for concepts like Face.

## 5 Conclusion

Video concept detection systems detects one or multiple concepts present in the shots or keyframe of video and automatically assign labels to unseen video which provides facilities to automatically indexing of multimedia data. Visual concept bridges the semantic gap between low level data representation and high level interpretation of the same by human visual system. Selection of compact and effective low level feature and feature fusion strategies are important. Also because of imbalanced dataset samples, accurate classifier models cannot be created resulting into less accuracy.

In this paper, imbalanced dataset issue is solved by partitioning dataset into three segments. Performance of the individual features, fused features and score fusion in Late fusion approach are evaluated on multilabel TRECVID 2007 dataset. Mean Average Precision evaluation measure for multilabel dataset is used for comparison. Early Fusion approach for globally selected features performed better then Late fusion strategy. Partitioned dataset improved performance measure.

## References

1. Li, Y., Wang, S., Tian, Q., Ding, X.: A survey of recent advances in visual feature detection. *Neurocomputing* **149**(PB), 736–751 (2014)
2. Le, D., Satoh, S.: A comprehensive study of features representations for semantic concept detection. In: *IEEE Fifth International Conference on Semantic Computing* (2011)
3. Muhling, M., Ewerth, R., Zhou, J., Freisleben, B.: Multimodal video concept detection via bag of auditory words and multiple kernel learnin. *LNCS, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7131, pp. 40–50 (2012)
4. Atrey, P.K., Hossain, M.A., El Saddik, A., Kankanhalli, M.S.: Multimodal fusion for multimedia analysis: a survey. *Multimed. Syst.* **16**(6), 345–379 (2010)
5. Snoek, C.G.M., Worring, M., Smeulders, A.W.M.: Early versus late fusion in semantic video analysis. In: *Proceedings of the 13th Annual ACM International Conference on Multimedia*, p. 399, January 2005

6. Zha, Z., Liu, Y., Mei, T., Hua, X.: Video concept detection using support vector machines - TRECVID 2007 evaluations (2007)
7. Liu, N., et al.: Multimodal recognition of visual concepts using histograms of textual concepts and selective weighted late fusion scheme. *Comput. Vis. Image Underst.* **117**(5), 493–512 (2013)
8. Cao, L., et al.: Multimedia Event Detection (MED) System, no. 4 (2011)
9. Van Hout, J., et al.: Late fusion and calibration for multimedia event detection using few examples. International, Menlo Park, USA University of Amsterdam, The Netherlands University of Southern California, Los Angeles, USA, pp. 4631–4635 (2014)
10. Lan, Z., Bao, L., Yu, S., Liu, W., Hauptmann, A.G.: Double fusion for multimedia event detection, pp. 173–185 (2012)
11. Diou, C., Stephanopoulos, G., Panagiotopoulos, P., Papachristou, C., Dimitriou, N., Delopoulos, A.: Large-scale concept detection in multimedia data using small training sets and cross-domain concept fusion. *IEEE Trans. Circ. Syst. Video Technol.* **20**(12), 1808–1821 (2010)
12. Strat, S.T., Benoit, A., Qu, G., Lambert, P.: Hierarchical late fusion for concept detection in videos. In: Fusiello, A., Murino, V., Cucchiara, R. (eds.) *Computer Vision – ECCV* (2012)
13. Lv, G., Zheng, C.: A novel framework for concept detection on large scale video database and feature pool. *Artif. Intell. Rev.* **40**(4), 391–403 (2013)
14. Janwe, N.J., Bhojar, K.K.: Video shot boundary detection based on JND color histogram. In: 2013 IEEE Second International Conference on Image Information Process (ICIIP), pp. 476–480, December 2013



# A Survey on the Impact of DDoS Attacks in Cloud Computing: Prevention, Detection and Mitigation Techniques

Karthik Srinivasan<sup>1</sup>, Azath Mubarakali<sup>2(✉)</sup>,  
Abdulrahman Saad Alqahtani<sup>3</sup>, and A. Dinesh Kumar<sup>4</sup>

<sup>1</sup> Saudi Electronic University, Riyadh, Saudi Arabia

<sup>2</sup> King Khalid University, Abha, Saudi Arabia  
mailmeazath@gmail.com

<sup>3</sup> Vice Dean of College of Computer Science and Information System,  
Najran University, Najran, Kingdom of Saudi Arabia

<sup>4</sup> Department of Computer Science and Engineering, Koneru Lakshmaiah  
Education Foundation, Vaddeswaram, Andhra Pradesh, India

**Abstract.** In recent years, cloud services are emerging popular among the public and business ventures. Most of companies are trusting on cloud computing technology for production tasks. Distributed Denial of Service (DDoS) attack is a major general and critical type of attack on the cloud that proved extremely damaging the services. In current years, several efforts have been taken to identify the numerous types of DDoS attacks. This paper explains the various types of DDoS attack and its consequence in cloud computing. Also, this paper provides the various impacts of DDoS attack on cloud environment. The main goal of this paper is to discuss about prevention, detection and mitigation approaches of DDoS attacks on cloud environment with strengths, challenges and limitations of each approach. So that researchers can get completely novel intuitive understanding into how to alleviate DDoS attacks in the field of cloud computing.

**Keywords:** Distributed Denial of Service (DDoS) · Mitigation · Defense · Prevention · Identification · Cloud computing

## 1 Introduction

Nowadays the usage of online trading and e-commerce is increasing rapidly. Most of the people depend on Internet for their day-by-day operations. This Internet-based computing, known as cloud computing became more popular and almost all business organizations adopt this technology for their operations.

Cloud computing became a more convenient and effective mode of accessing services, resources and applications over the Internet. The cloud environment has moved to the attention of business and associations take away from the deployment and everyday maintenance of IT amenities through offering a self-service, on-demand, and pay-as-you-go pricing industry model. The cloud computing has sustained to improve the popularity of current period. It provides the freedom to utilize resources/services for

each requirement and pay for what is utilized. The cloud computing minimizes software and hardware demand from the client's side.

Most of the companies deploy hybrid cloud includes public and private cloud features to allow them to measure computing necessities beyond their infrastructure capacity while still uses their private cloud to decrease the cost. A hybrid cloud environment can also provide new opportunities to effectively utilize all the resources in distributed environment.

National Institute of Standards and Technology (NIST) society describes a cloud computing exploitation method comprise private, public, hybrid, and society models [1]. Public cloud lets permit the accessibility of frameworks and services easily. The Private cloud permits the accessibility of frameworks and services within the association, and it is functioned only within a specific association. The Hybrid cloud is the integration of public and private cloud. Non-critical actions are achieved by public cloud while critical actions are achieved by the private cloud.

The three major cloud computing offerings are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS is a software sharing model in which applications are hosted by a seller or service provider and create accessible to clients over the Internet. PaaS offers the required platform for computing and IaaS provides access to computing resources in a virtualized infrastructure "the cloud" on the Internet. These services are hosted in the cloud and accessed by the clients via the Internet.

In recent years, cloud computing is gradually in development as numerous associations which accepted the cloud technology, but in the similar view, numerous protection problems are elevated. Every association selects secure environments when they shift its information to remote locations. Majority of the questions are particularly associated with information and business reason defense [2]. Various security correlated attacks are well-addressed for the conventional non-cloud IT environments.

Distributed Denial of Service (DDoS) attacks [3] make cloud services unavailable to legitimate users by producing heavy traffic from multiple devices called bots. As many organizations migrate their operations online, DDoS attacks lead to cause significant financial losses [4]. There is an extensive effect on DDoS, and it generates hugest threat [5]. Over 20% of associations on the world met no less than one informed DDoS attack occurrence on their infrastructure [6]. Authors in [6] express strong anticipation regarding the DDoS attacker's target move towards cloud environment and services. Table 1 list some of the popular DDoS attacks happened over the years and how it advanced [5–7].

The rest of the paper is categorized as follows. Section 2 illustrates about major DDoS attacks in cloud environment and presents its working principles. Section 3 describes direct and indirect impacts of DDoS attacks and its effects. Section 4 describes various DDoS defense mechanism, which comprises various prevention, detection and mitigation techniques. Section 5 discusses open issues and future works. Lastly, Sect. 6 describes the conclusion of the paper.

**Table 1.** List of some popular DDoS attacks in past years

Year	Details
1998	The initial version of DDoS tools was developed. However, DDoS tools were not frequently utilized but still Smurf amplification attacks, and point-to-point DoS attacks were continued
1999	By using a trinoo network, a single system was flooded which made the network unusable for more than two days at the University of Minnesota. Also, one of the massive attacks was detected using Shaft
2000	A 15-year-old Michael Calce a.k.a. “Mafiaboy,” launched a project called “Project Rivolta”, which made to took down number 1 search engine website at that time and next affected website called “Yahoo”. This event made an alarm for everyone to show that how easily one kid can shut down major websites to the world
2001	The attack was gradually increased and moved from Mbps to Gbps. Efnets is an organization, which was affected by the 3 Gbps DDoS attack
2002	Due to the congestion created by attackers, several name servers were unreachable in few days. While servers give a response to all the queries, many valid queries were unable to attain some root name servers
2003	Shutdown the service of SCO gathering’s site by utilizing Mydoom. A few a huge numbers of PC’s were contaminated to convey the information to the target server
2004	Online payment processing firms such as Authorize-IT and 2Checkout were targeted by attackers. Later it was identified that attackers threatened and extorted to shut down their sites
2005	A gambling site, “jaxx.de” was under DDoS attack and attackers demanded 40K Euros to stop this attack
2006	The blog of Michelle Malkin was under DDoS attacks. The attack continuously occurred in one week
2007	Russian government sites affected by severe DDoS attacks during the riots time. Access to IP address, Many of them denied accessing IP addresses outside Estonia for several days
2008	A popular European news organization’s website was attacked. The server is under the control of attacker for an hour or 90 min which marking the longest period the site under offline
2009	Many organizations affected such as Asian country’s largest daily newspaper, the country’s president, a bank and many websites of the country’s North America came under DDoS attack. Nearly, 1.6 million computers act as a botnet to perform this attack
2010	Operation Payback: Websites of Master was under DDoS attack. Many services such as Master card, PayPal and Visa were stopped to providing service to WikiLeaks
2011	The anonymous DDoS attack on North Korea. One of the popular DDoS tool “LOIC” used by Anonymous and other online attackers to overload websites with requests and frequently disrupt the target server
2012	Numerous attacks on US banks imply to utilize the DDoS tool
2013	Spamhaus attack, the DDoS attack essentially over-burdens the victim’s servers by flooding them with information. It can interfere with the victim’s business, or knock its site offline
2014	One of the most volumetric DDoS attacks was recorded, with more than 100 measures over 100 GB/sec reported

*(continued)*

**Table 1.** (continued)

Year	Details
2015	One of the biggest combined attacks regarding Proton mail was made by the attackers. The attack continued few days and reached 80 Gbps of traffic
2016	1 Tbps attack is targeting the French Web host OVH. After few days, the botnet source code of IoT goes to the public which is called “marquee” attack of the year

## 2 DDoS Attacks in Cloud Environment

The DDoS attack is the main issue to the availability of resource in the cloud. There are some studies and researches about DDoS attacks in the cloud [8–10]. In [8] presents a comprehensive survey on the nature, prevention, identification and mitigation mechanisms of DDoS attacks. Furthermore, the community to help towards designing effective defense mechanisms that provide a guideline to make a procedure to protect resources from attacks [8]. DDoS attacks develop in an alternate of flavors. Comprehensively, DDoS attacks are characterized based on the sort amount of traffic utilized for the attack and the abused vulnerability of the target.

### 2.1 Volume Based Attacks

Attacks utilize a huge quantity of traffic which saturating the total bandwidth of the target. Volumetric attacks are simple and easy to produce by utilizing simple amplification methodologies.

#### 2.1.1 ICMP Floods

Internet Control Message Protocol (ICMP) is one of the connectionless protocols, which is majorly utilized for network analytics, errors and IP operations. An ICMP Flood by transferring an abnormally huge amount of ICMP packets of any kind such as “ping” packets which can overcome a destination server. It tries to procedure each incoming ICMP request and this action can influence the outcome in a denial-of-service condition for the destination server. The DDoS form of a Ping (ICMP) flood can be divided into two replicating steps:

1. A large number of ICMP echo request packets send by the attacker to the destination server utilizing many devices.
2. The destination server replies an ICMP echo response packet to every requesting device’s IP address as a response.

#### 2.1.2 DNS Amplification

In the case, DNS amplification attack and the attacker initiates DNS requests with a spoofed IP address. The attacker relies on reflection; responses are not sent back to the attacker but are instead sent “back” to the victim server. Because the DNS response is larger than the DNS request (usually), it amplifies the amount of data being passed to the victim. An attacker can use a small number of systems with little bandwidth to create a sizable attack.

The primary way of preventing this attack is to block spoofed source packets. It can also be prevented by blocking specific DNS servers, blocking open recursive reply servers, rate limiting, and updating one's DNS server(s) often.

## 2.2 Application Layer Attacks

Application layer attack consist of legitimate and scrupulous demands, the intention of these attacks is to crash the web server. In the attack can abuse a fault of the 7 Layer protocol stack.

Application attacks illustrate a relationship with the destination and after that exhaust the server assets through monopolizing procedures and operations.

### 2.2.1 DNS Flood

DDoS attacks have become increasingly popular due to their readily available exploit plans and their ease for execution. However, these attacks can be the most dangerous because they can, in a relatively short amount of time, compromise even the largest Internet servers.

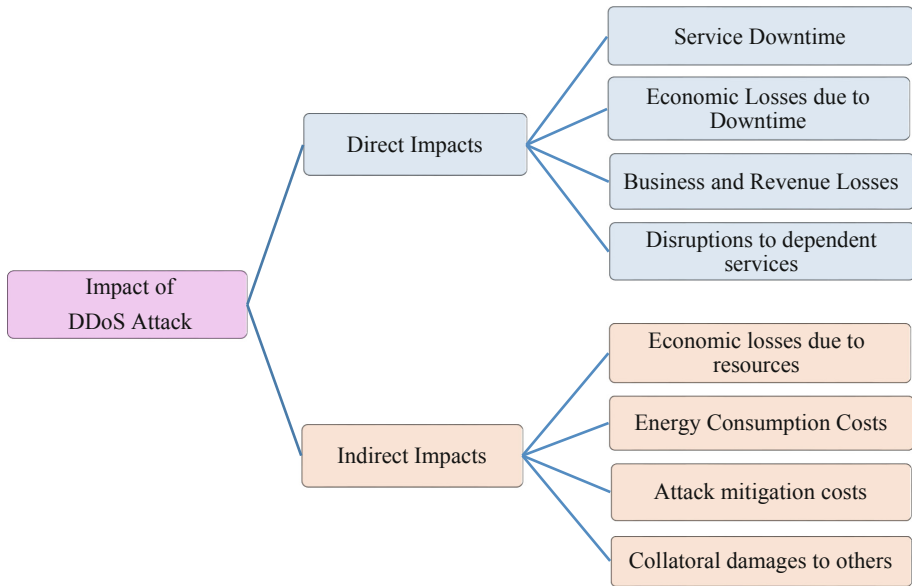
## 3 Impact of DDoS Attack

The impact of DDoS attacks acquires greater and harder to overlook each year. The DDoS attacks computed and learned via a variety of security resolutions for suppliers in the market [11–14]. Most part of the DDoS attacks are botnet-driven and anywhere a botnet checker organizes a significant quantity of robotized malware-driven bots to transmit the attack [62]. Typically, DDoS attackers compromise huge number of devices and make an attack against a server which leads to huge loss in business. Figure 1 shows that the impacts of DDoS attack in cloud environment.

A few DDoS attacks there are both direct and indirect expenses to the casualty. Direct expenses, when all is said in done, are less demanding to quantify and can be quickly connected with the attack. Indirect expenses, then again, are harder to identify and their effects are frequently not felt for weeks, months or some cases years following the real attack itself.

Loss of profit is normally the most straightforward metric to gather, especially if your essential business is an electronic trade. Online vendors, streaming media services, web-based gaming, business to business centers, online commercial centers, Internet-based publicists and web trade organizations are among those that experience direct profit loss with any disturbance of service. These organizations regularly compute profit in clicks or impressions every moment or average profit every moment or exchange. Profit is lost for the duration of any attack that takes them disconnected or can be extremely lessened during periods when their online frameworks are performing outside of their ordinary working level.

Loss of profitability is another effect. Numerous organizations and associations utilize their system, online assets and openly accessible services to help their essential business. Any interruption to the accessibility of these important assets brings about lost profitability.



**Fig. 1.** Impacts of DDoS attacks in cloud environment

The effects of a DDoS attack including interruption of service and burglary of client data can cause loss of trust in client side. The clients can choose to move their business to a competitor or utilize web-based social networking to vent their anger and dissatisfaction. Unmistakably none of these results is desirable, and tragically it might require some investment to understand the full degree of any client losses.

A few organizations offer service level agreements to their clients that assurance a specific level of service accessibility. DDoS attacks can keep these organizations from meeting these commitments and frequently result in finance punishments. Additionally, numerous organizations and retailers are forced to discount purchases or credit back services to retain clients or enhance loyalty and fulfillment after suffering the impacts of DDoS attacks [66].

A lot of businesses have strict regulations concerning the handling of sensitive information and the revealing of any cyber security attacks and breaks. In these examples, detailed crime scene investigation and cause investigation must be performed. The actions can take a stretched-out time of opportunity to finish, and their expenses can be considerable. Likewise, legal expenses can be acquired with a specific end goal to protect against parties looking for pay for the disturbance of service.

A few victims of DDoS attacks wind up going through extra cash with advertising firms with an end goal to reestablish the generosity and confidence of the general public or their clients after an outage. These organizations will frequently enable the victims to make clear informing about the incident and what is being done to prevent attacks of this kind in the future. They can also help with press declarations, publication date-books, contributed articles, talking engagements or even broadcast meetings and publicizing.



A few organizations spend a significant bit of their operating budget to make and sustain their brand picture through promoting, PR, post office-based mail campaigns and different activities. Acquiring the trust and confidence of clients and constituents regularly takes years of time, effort and cash. The present DDoS attacks can harm your image and ruin your reputation in a shockingly short measure of time.

The impacts of a DDoS attack containing disturbance of service and robbery of client data can cause loss of trust in your client base. These clients can choose to move their business to a competitor or utilize online networking to vent their anger and dissatisfaction. Unmistakably none of these results is desirable, and unfortunately, it might require some time to understand the full extent of any client losses.

Robbery of crucial information is a troubling pattern in recent DDoS attacks is for risk performing artists to utilize the DDoS attack as a smokescreen or diversion to hide different malicious action. The DDoS attack itself is just denoted by an end. The real objective of the attack is to take critical information. In this style of attack, the risk performer guides a DDoS attack to a specific bit of the system while launching specially crafted attacks at different targets. The objective is to compromise these different targets and either take critical information during the DDoS attack or introduce a backdoor that will allow future access to the system and its assets. These attacks can be successful because IT staffs are focused around moderating the DDoS attack itself while different malicious activity goes unnoticed.

## 4 DDoS Defense Mechanism

This section concentrates on the detailed solution based on the categorization of DDoS attacks in the cloud. The contributions of this part were assembled utilizing systematic search procedure. The works correlated to DDoS defense mechanism in the cloud have been broadly computed and organized as a categorization. The categorization comprises of three main parts which are prevention, discovery and moderation of DDoS attacks.

In the prevention stage, thoughtful security piece of equipment is set up together in different areas to achieve secured services and keep information against DDoS attack. In the discovery stage, incorporates investigation of the running frameworks are estimated, to decide the source of malicious attempts or malicious traffic to the base of DDoS attack [15, 16]. In moderation, the stage is called final stage, which concludes the defense life-cycle by evaluating the effect of the attack and picking the right response [17] at the correct time [18]. While in the moderation stage, a response framework selects the proper countermeasures to effectively deal with a DDoS attack or slow down the malicious customers [19].

The existing defense strategies which are against the DDoS attacks have achieved insufficient progress since they can't address the considerable difficulty of accomplishing simultaneously effective detection, effective reaction, sufficient rate of false alarms, and the real-time exchange of all packets [20–22].

Failure to prevent and poor discovery leads to huge money related losses and made negative impact on the business worldwide [23, 24]. The works associated with DDoS defense mechanism in the cloud have been broadly measured and organized as a

classification as shown in Fig. 2. The given Classification consists of three major parts which are prevention, detection and mitigation of DDoS attacks.

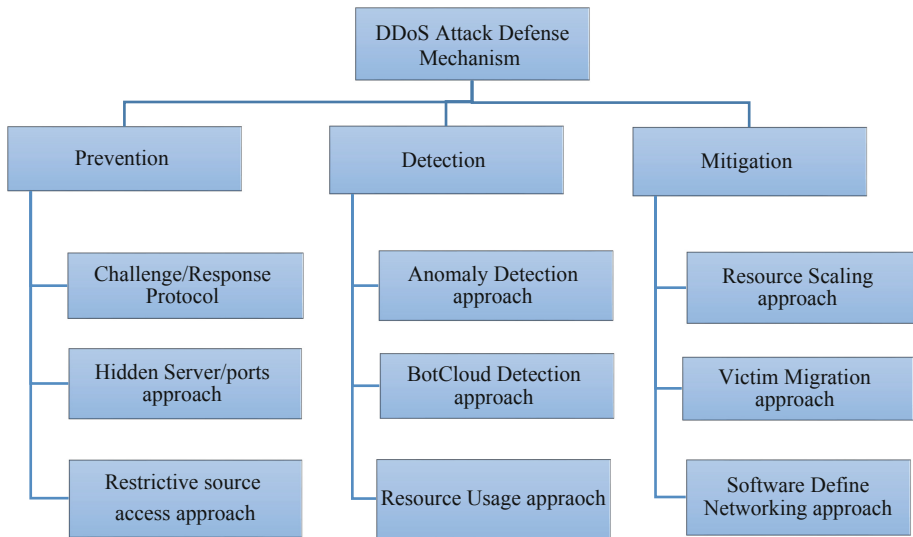


Fig. 2. Classification of DDoS Defense mechanism

### 4.1 Attack Prevention

The mechanism of DDoS prevention in the cloud is considered as a pro-active strategy, where the presumed attacker’s requests are checked, separated or dropped before these requests start to influence the server. This type of prevention strategy doesn’t contain any “presence of attack” state in that capacity, which is ordinarily accessible to the attack discovery and moderation strategies. Thus, the prevention strategies are connected to all clients whether they are legitimate or illegitimate.

For a rapid view of each arrangement of these methodologies, their qualities, difficulties, and weaknesses are recorded in Table 2.

Table 2. Strength, Challenge and Limitations of DDoS attack Prevention approaches

Approaches	Strengths	Challenges	Weaknesses	Contributions
Challenge/Response protocol	Effectively differentiate human and bots using various types of puzzles	Excessive amount of graphics generation and need more storage to process	Dictionary and parsing assaults, OCR, Image segmentation and puzzle accumulation attacks	[25–32]

(continued)

**Table 2.** (continued)

Approaches	Strengths	Challenges	Weaknesses	Contributions
Hidden Servers/Ports technique	Service is provided to genuine clients even though there is no direct link is created with the actual server at the primary time	More server ports needed and also load balancing between them is required	Extra Security layer with redirections is needed	[30, 33–35]
Restrictive source Access approach	Effective admission control and prioritized blocking/dropping responses with different classes	Mainly concerns on Quality of Service (QoS) and more maintaining required for some connections	Difficult to scale in case of huge DDoS spoofing by more number of bot source	[25, 33, 36, 37]

#### 4.1.1 Hidden Servers/Ports Approach

The hidden servers or hidden assets containing some features such as ports are an important strategy to eradicate a straight communication channel between the customer and the server. It is achieved by putting a middle hub/proxy to carry out as a transmitting specialist. Main task of transmitting specialist may involve balancing the load among the servers, error resilience of servers, recovery of servers and checking the incoming activity for any vulnerability.

Some variety of strategies broadly utilized the aspects of concealing the assets, for example ephemeral servers, intermediary server [30], and concealed ports [33]. The creators in [30] studied a moving target methodology to shield from DDoS attacks. Integration of numerous hidden intermediary servers should be dynamically assigned and changed to save genuine customers. In the kind of strategy have some practical problems such as scalability and great number of proxy servers and rearranging.

Hidden servers or ports are defensive systems to protect the genuine service to meet the DDoS attack. Like this, demands to the hidden servers or ports are diverted by validation/proxy servers and it is a key server to be experience through a customer. Validation offers a security layer to secure the real service. The hidden server helps to stopping the malicious activity to influence the original server. The extra layer may help another reason for redirection and load balancing among servers.

The disadvantage contains time delay, the price of the mediator servers and calculation overhead of redirection and its administration at the moderate hubs.

#### 4.1.2 Prohibitive Access Approach

The conditional access approach is normally affirmation control strategies, and it applies preventive actions against the serviceability [25, 26]. A few of these approaches have been designed and implemented with the prevention by basically delaying

reactions/access to the more speculated attackers or in some cases even extra customers. In majority of the contributions, this kind of interruption is initiated by organizing the genuine customers or selecting customers with “great” previous performs. There are few more frameworks depend on “Specific access” and “Postponed access”. It is mostly similar, except that the methods to provide access to the customers are unique.

Almost every admission control strategies are implemented utilizing prohibitive access to stopover the DDoS attacks to happen that are given reputation based or delayed access. In this way, these methodologies give a decent manner to optimize the server ability by permitting demands that depends on the accessible assets. The “ability” or “reputation” is computed, and it depends on the previous access prototype or the time taken to tackle the crypto puzzles.

### 4.2 Attack Detection

It is resolved and the attack symptoms are accessible to the server-side in-terms of its services and performance measurements. Some kinds of attack symptoms are initial indications and the attack recently initiated to take shape or might be an infrastructure [45]. The attack diminished the performance of the server. The techniques might observe to be comparable “attack prevention” sometimes, and a lot of supporting contributions have given.

For a rapid view of each arrangement of the categorized strategies, their strengths, difficulties, and weaknesses are recorded in Table 3.

**Table 3.** Strength, Challenge and Limitations of DDoS attack Detection approaches

Approaches	Strengths	Challenges	Weaknesses	Contributions
Anomaly Detection approach	Mostly the detection is based on machine learning and its feature extraction	Identification of feature, IP spoofing, testing and minimizing the false alarms	Scalability problems and requirement of more training, identical matching, mixing and statistical analysis of data traffic features	[39–44, 46]
BotCloud Detection approach	Finding the bot attack resources within the cloud in continuously checking the attributes of virtual machines and the network	Recognizing the behavior and action thresholds for numerous doubtful behaviours	More complex to identify every kind of attack sequence (comprising Zero-day attack). In this case, the identification works at the boundary of attack initiating cloud	[47–51]

(continued)

**Table 3.** (continued)

Approaches	Strengths	Challenges	Weaknesses	Contributions
Usage of Resource Method	Hypervisor stage/OS stage identification strategies to continuously check the abnormal usage	Understanding the maximum usage and check either it is due to the real traffic or due to the attack	Only provides a signal regarding the probability of possible attacks and needs the additional detection mechanisms	[47, 50, 52]

#### 4.2.1 Anomaly Detection Approach

The anomalous traffic patterns are commonly detected from packet traces, web access logs, established links or demand headers. The anomalous pattern can be identified in the log file which consist attack traces and previous historic patterns. The web behavioral activity has been developed by utilizing more number of qualities and measurements are working on those attributes. In most of the time, developers have been utilized the web action of normal web traffic as a benchmark prototype. This kind of common web action is gathered from the duration when the attack isn't performed. This type of feature selection, dataset preparation and testing against these studied principles are the necessary arrangements of operations; those are involved with these recognition techniques.

To illustrate a couple of major strategies associated to DDoS attack anomaly recognition in cloud computing, Idziorek et al. [38] helped to web access logs and argued that original web access prototypes. It followed "Zipf" allocation and based on the web access prototype preparing and identifies the outliers which don't follow the distribution in prototype [32]. The researchers in [33] utilized the baseline profiling of different IP and TCP flags and it includes the framework activity model. The creators recommended the recognition of flooding in the cloud depend on utilizing the preparation of general and unusual movement. It utilized the covariance matrix strategy to distinguish the anomaly. Among alternative methodologies, depicted in [35] examined statistical filtering-based attack identification.

The main quality of attack detection strategies reclines in the machine learning to the history of good activity or the harmful activity. The entry of the patterns, for example, software-defined systems and big data analytics these identification strategies have increased more important in observing and quick attack detection.

A complete overview of identification strategies is proposed for a conventional type of frameworks in [5]. These kinds of methodologies are now becoming very common for cloud focused on attacks. The key difficulties for DDoS attack identification strategies introduce based on the behavioral distinguishing regarding feature extraction and correlating preparing. The investigation criteria of methodologies present in the false alarms (negative and positives) and it create the testing time of the incoming activity. The challenge present in preventing the IP spoofing can overcome some of the detection methodologies.

### 4.2.2 Usage of Resource

In the presence of the DDoS attack, a virtual machine can also provide vital data or an expectation of the upcoming DDoS attack. Cloud infrastructures normally run Infrastructure as a Service cloud utilizing virtualized servers where the hypervisor can consistently note down the resource utilization of every virtual machine on a physical server.

Once these virtual machines begin to achieve the defined resource usage thresholds, the likely possibility of an attack can be suspected. In [51], creators recommended solutions based on an accessible resource with virtual machines and their upcoming prerequisites. Similarly, [53] used performance counters and activity to recognize usage of resource in a virtual machine and derive conceivable moderation of the attack. Asset utilization has an exceptionally large and indirect metric deciding the possibility of an attack. The creators in [52] utilized asset limits as the technique for the DDoS identification and recommended moderation strategies.

Authors in [33] discussed a DDoS aware asset distribution strategy and if the overburdened virtual machines are not flagged for expanded resource utilization. In its place, creators to develop the separated movement and increment the assets in the demands of legitimate flagged demands. The creators in [40] displayed the asset utilization anomalies of virtual machines utilizing virtual machine introspection to identify the possibility of asset surge owing to the DDoS attack.

The DDoS attacks are becoming asset-intensive attacks which give an indirect relationship to the accomplishment of the asset utilization-based profiling and recognition strategies. Another method, for example, auto-scaling methodologies are triggered based on “over-burden” and “under load” conditions of the selected targeted virtual machines. The quality gives a probable connection among the virtual machine asset usage and a DDoS originated asset surge.

The weakness of the methodologies exists in the interpretation of the great asset utilization. Also, it is an unpredictable task to conclude whether the asset surge is owing to the certain activity or due to the attack. The resource surge just gives an alarm signal about the probable resource surges; there is a necessity for other supplementary discovery techniques.

## 4.3 Attack Mitigation

It collected all methodologies and it helps a victim server to keep servicing the requests in the frequency of an attack. The downtime is a fundamental business aspect of sites, and an association may include losing a critical number of potential clients. In this area, we have gathered the methodologies, which would enable the victim server to keep servicing the requests in the presence of an attack.

Mitigation and recovery are the two equal things to hold the server alive and it is under the attack. Some kinds of methodologies are mostly utilized to recover the server. That is once the attack subsides, the server might be taken back to the original circumstance. A considerable lot of the mitigating and recovery techniques are entirely identified with an environment clouds, and their answers are toward mitigating Economic Denial of Sustainability (EDoS) attacks. For a rapid view of each arrangement of the categorized strategies, their qualities, difficulties, and weaknesses are recorded in Table 4.

**Table 4.** Strength, Challenge and Limitations of DDoS attack Mitigation approaches

Approaches	Strengths	Challenges	Weaknesses	Contributions
Resource Scaling approach	Offers a fast release to asset bottlenecks	Appropriate decision making whether and when additional resources are needed	Designing a false alert sometimes might bring to EDoS. Co-hosted virtual machines are also be influenced	[38, 47, 52, 53, 61]
Victim Migration approach	Minimizing losses by migration of the DDoS victim service with some other servers	Migration selection for both candidate and host is difficult	More migration costs and leads to overheads Consequent migrations or trades in cloud	[47, 53, 54]
Software Defined Networking (SDN) approach	Timely and abstract interpretation of the system and monitoring the received activity utilizing software controllers	SDN itself sometimes might be a simple target of the DDoS attacks	Most of the time beneficial only at the ISP level network control and network boundaries	[56–60]

**4.3.1 Resource Scaling**

One of the first and main leading contributions in the area, which traces cloud-particular problems, is by Shui Yu et al. [50]. The creators analyzed the dynamic asset assignment attribute of the cloud helps the victim server to gain extra assets for DDoS moderation. Comparative along these lines, individual cloud clients are shielded from DDoS attacks by dynamic asset distribution. Genuine website data sets are involved with the experimentations demonstrates that their queuing hypothesis which depends on scheme work to mitigate the DDoS attack. The creators in [47] designed three unique scenarios to prevent the DDoS attack in the cloud, which comprises the three scenarios such that internal attacks to inside servers, outside attacks to internal servers and inner attacks to external servers. The creators developed the techniques to identify the attack and become recovered utilizing scaling and migrations in a related cloud infrastructure. The assets are reserved which are kept in [39] to help the server in attack times. Here, the essential question is “How much-reserved assets should be kept?” The cost of idle and additional assets is one of the disadvantages. While, then again, creators in [38] have proposed an asset distribution procedure, which it doesn’t scale the assets on DDoS created asset surges.

**4.3.2 Victim Migration**

The virtual machine migration has improved the way that the whole running virtual machine server is moved starting with one server then onto the next physical server without recognizable downtime. The contributions are utilizing victim relocation mitigating the DDoS attack. The creators [63] designed a similar strategy by keeping some private assets to a server.

Victim migration is essentially utilized to backup assets. Additionally, it provides an approach to diminish the attack impacts and implement the attack moderation. It helps with estimating the services by utilizing relocating to great ability host servers and migrate server can utilize the additional assets to identify and mitigate the attack.

At present, there are some preliminary and progressing research works related to SDN helped DDoS mitigation techniques. The creators in [57] designed an outline of SDN-based solution where ISP-stage checking, and routing of malicious activity is finished by particularly planned secure switches. The victim is required to create a demand to ISP for DDoS mitigation. The ISP is having a general perspective of the incoming activity and implements the movement marking utilizing Open Flow switches. If several suspicious activities distinguished, then it is redirected to the security center boxes where access policies are applied to the movement. The creators have not talked about the effective identification and the mitigation parts on the client side.

Further, a similar kind of idea designed by researchers in [57] comprises a pattern implementation of SDN-based discovery technique. In this method, the fundamental idea is to construct a strict access control policy for the incoming movement. Additionally, it involves strict authentication for every incoming request. Another investigation concentrated on advanced deep packet assessment depends on the methodologies utilizing software defined networking are discussed in [60]. A whole regulation and instructional exercise of software defined networking-based solutions are provided in [65].

The SDN has enormous potential outcomes to help for the attack mitigation. Because of its reconfigurability and speedy systems view and checking, it helps massive and the low-rate DDoS attacks. By utilizing SDN abilities, mitigation solutions are still evolving. It might become so useful because of their vital aspects. However, a few investigations [59] are determined that the SDN environment itself can turn into a victim of DDoS attacks.

The attack moderation techniques portrayed above offered an extensive overview of various attack moderation and required recovery solutions accessible in distributed computing space [55]. The proposed moderation strategies are regularly a loyal layer for the protection for the attack prevention and identification solutions. Much more, the moderation strategies play an essential part for the instance of distributed computing, because of their applicability to asset management during the attack.

In summary, most resistances began with experiments plan and performance, regardless of whether hypothetical or practical apart from protection structures. While replicating good circumstances, the creators could deliberately select the features of interest and utilize a few arrangements of information; they could know and concentrate the reaction of their framework under various workloads. Further, they determined the possibility of accepting their framework. Concerning scenario (real time), the price, overhead, precision (number of false positives or negatives), best practices (how to legitimately set up the framework for best execution), usefulness to distinguish and filter attack messages and ability to recognize new attacks.



## 5 Open Issues for Future Direction

There is few research works mainly focus to give a superior effort to tackle the security issues in cloud domain. In any case, still, there is much of open problems are existent that is required to be resolved by providing a safe cloud framework. The first critical open issue is to plan a wide-ranging and coordinated security solution that may achieve all primary security necessities in the cloud [64].

Each researcher focuses on a particular security issue and tackles the issues in its specific manner. While investigating issues and findings are solution of the issue may outcome numerous security resolutions for an issue. In a certain circumstance, it is not practical to implement numerous security resolutions for a single issue. Arrangement and employment of few security resolutions itself might be dangerous. A typical and more integrated security resolution is more secure and easy to implement in the security devices.

Multi-tenancy is an approach in cloud for effective hardware utilization of powerful servers. Suppose the multi-tenancy is not properly implemented, it leads to underutilization of server hardware in cloud. Suppose DDoS attack affect the multi-tenancy environment and make server resources unavailable to most of the tenants. Effective use multi-tenancy is another challenge of cloud that need attention.

## 6 Conclusion

Finally, this work conclude that the different types of distributed denial of service attacks and its defensive solutions in the cloud computing environment. This survey assist the authors to detect the different DDoS attacks and provides an effective solutions to overcome the network failure and provide the successful transmission. Here, it provides a variety of solutions for the respective distributed denial of service attacks and mostly it concentrated on detection, prevention and mitigation of attacks. By using these types of solutions, can be implemented in cloud environment with different features like resource allocation based on demand services, botcloud and topology maintenance with the help of software defined networks. These survey helps to analyse the merits and demerits of different attacks and its solutions. We hope that this smart way of approach providing the comprehensive set of estimation tool for a various types of Distributed DoS mitigations which may support for assisting future solutions. At last, we have suggested open issues which are still dealing some threat to cloud and the future directions are given.

## References

1. NIST: The NIST Definition of Cloud Computing (2011). <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
2. Kaufman, L.M.: Data security in the world of cloud computing. *IEEE Secur. Priv.* 7(4), 61–64 (2009). <https://doi.org/10.1109/MSP.2009.87>

3. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. *Future Gener. Comput. Syst.* **28**(3), 583–592 (2012). <https://doi.org/10.1016/j.future.2010.12.006>
4. Mirkovic, J., Reiher, P.: A Taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Comput. Commun. Rev.* **34**(2), 39–53 (2004). <https://doi.org/10.1145/997150.997156>
5. Mansfield-Devine, S.: The growth and evolution of DDoS. *Netw. Secur.* **10**, 13–20 (2015)
6. Kaspersky Labs, Global IT Security Risks Survey 2014 - Distributed Denial of Service (DDoS) Attacks (2014). <http://media.kaspersky.com/en/B2B-International-2014-Survey-DDoS-Summary-Report.pdf>
7. Nelson, P.: Cybercriminals Moving into Cloud Big Time, Report Says (2015). <http://www.networkworld.com/article/2900125/malwarecybercrime/criminals/-moving-into-cloud-big-time-says-report.html>
8. Somani, G., et al.: DDoS attacks in cloud computing: issues, taxonomy, and future directions (2015). arXiv preprint: [arXiv:1512.08187](https://arxiv.org/abs/1512.08187)
9. Shameli-Sendi, A., et al.: Taxonomy of distributed denial of service mitigation approaches for cloud computing. *J. Netw. Comput. Appl.* **58**, 165–179 (2015). <https://doi.org/10.1016/j.jnca.2015.09.005>
10. Deshmukh, R.V., Devadkar, K.K.: Understanding DDoS attack & its effect in a cloud environment. *Procedia Comput. Sci.* **49**, 202–210 (2015)
11. Akamai Technologies, Akamai's State of the Internet Q4 2013 Executive Summary **6**(4) (2013). <http://www.akamai.com/dl/akamai/akamai-soti-q413-exec-summary.pdf>
12. Neustar News, DDoS Attacks and Impact Report Finds Unpredictable DDoS Landscape (2014). [http://www.neustar.biz/aboutus/news-room/press-releases/2014/neustar-2014-ddosattacks-and-impact-report-finds-unpredictable-ddos-/landscape#.U33B\\_nbzdsV](http://www.neustar.biz/aboutus/news-room/press-releases/2014/neustar-2014-ddosattacks-and-impact-report-finds-unpredictable-ddos-/landscape#.U33B_nbzdsV)
13. P. Technologies (2014). <http://www.prolexic.com/>
14. Arbor Networks, Understanding the nature of DDoS attacks (2014). <http://www.arbornetworks.com/asert/2012/09/understandingthe-nature-of-ddos-attacks/>
15. Tripwire-New Research Shows Global DDoS Attacks Grew 90% in Q4 2014 (2014). <https://www.tripwire.com/state-of-security/latest-security-news/new-research-shows-global-ddos-attacks-grew-90-in-q4-2014/>
16. Abliz, M.: Internet Denial of Service Attacks and defence Mechanisms, University of Pittsburgh, Department of Computer Science, Technical report. TR-11-178 (2011)
17. Shin, S., Yegneswaran, V., Porras, P., Gu, G.: AVANT-GUARD: scalable and vigilant switch ow management in software-defined networks. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security, pp. 413–424 (2013)
18. Shameli-Sendi, A., Dagenais, M.: ARITO: cyber-attack response system using accurate risk impact tolerance. *Int. J. Inf. Secur.* (2013). <https://doi.org/10.1007/s10207-013-0222-9>
19. Shameli-Sendi, A., Ezzati-Jivan, N., Jabbarifar, M., Dagenais, M.: Intrusion response systems: survey and taxonomy. *Int. J. Comput. Sci. Netw. Secur.* **12**(1), 1–14 (2012)
20. Walfish, M., Vutukuru, M., Balakrishnan, H., Karger, D., Shenker, S.: DDoS defence by offense. *ACM Trans. Comput. Syst. (TOCS)* **28**(1), 1–54 (2010). Article 3
21. Zargar, S.T., Joshi, J., Tipper, D.: A survey of defence mechanisms against Distributed Denial of Service (DDoS) flooding attacks. *IEEE Commun. Surv. Tutor.* **99**, 1–24 (2013)
22. PC World. <http://www.pcworld.com/article/2035407/ddos-attacks-have-increased-in-number-and-size-this-year-report-says.html>
23. Khor, S.H., Nakao, A.: sPoW: on-demand cloud-based EDDoS mitigation mechanism. In: HotDep (Fifth Workshop on Hot Topics in System Dependability) (2009)

24. Kumar, M.N., Sujatha, P., Kalva, V., Nagori, R., Katukojwala, A.K., Kumar, M.: Mitigating Economic Denial of Sustainability (EDoS) in cloud computing using in-cloud scrubber service. In: Proceedings of the 2012 Fourth International Conference on Computational Intelligence and Communication Networks, CICN 2012, Washington, DC, USA, pp. 535–539. IEEE Computer Society (2012). <https://doi.org/10.1109/CICN.2012.149>
25. Al-Haidari, F., Sqalli, M.H., Salah, K.: Enhanced EDoS-Shield for mitigating EDoS attacks originating from spoofed IP addresses. In: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1167–1174. IEEE (2012)
26. Sqalli, M.H., Al-Haidari, F., Salah, K.: EDoS-Shield - a two-steps mitigation technique against EDoS attacks in cloud computing. In: 2011 Fourth IEEE International Conference on Utility and Cloud Computing (UCC), pp. 49–56. IEEE (2011)
27. Alosaimi, W., Al-Begain, K.: A new method to mitigate the impacts of the economical denial of sustainability attacks against the cloud. In: Proceedings of the 14th Annual Post Graduates Symposium on the Convergence of Telecommunication, Networking and Broadcasting (PGNet), pp. 116–121 (2013)
28. Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F., Stavrou, A.: A moving target DDoS defense mechanism. *Comput. Commun.* **46**, 10–21 (2014)
29. Karnwal, T., Sivakumar, T., Aghila, G.: A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In: 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECs), pp. 1–5. IEEE (2012)
30. Anderson, T., Roscoe, T., Wetherall, D.: Preventing internet Denial-of-Service with capabilities. *ACM SIGCOMM Comput. Commun. Rev.* **34**(1), 39–44 (2004)
31. Masood, M., Anwar, Z., Raza, S.A., Hur, M.A.: EDoS Armor: a cost effective economic denial of sustainability attack mitigation framework for E-commerce applications in cloud environments. In: 2013 16th International Multi Topic Conference (INMIC), pp. 37–42 (2013). <https://doi.org/10.1109/INMIC.2013.6731321>
32. Jia, Q., Wang, H., Fleck, D., Li, F., Stavrou, A., Powell, W.: Catch Me if You Can: a cloud-enabled DDoS defense. In: 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 264–275. IEEE (2014)
33. Jeyanthi, N., Mogankumar, P.: A virtual firewall mechanism using army nodes to protect cloud infrastructure from DDoS attacks. *Cybern. Inf. Technol.* **14**(3), 71–85 (2014)
34. Baig, Z.A., Binbeshr, F.: Controlled virtual resource access to mitigate Economic Denial of Sustainability (EDoS) attacks against cloud infrastructures. In: Proceedings of the 2013 International Conference on Cloud Computing and Big Data, CLOUDCOM-ASIA 2013, Washington, DC, USA, pp. 346–353. IEEE Computer Society (2013). <https://doi.org/10.1109/CLOUDCOM-ASIA.2013.51>
35. Saini, B., Somani, G.: Index page based EDoS attacks in infrastructure cloud. In: International Conference on Security in Computer Networks and Distributed Systems, pp. 382–395. Springer, Heidelberg (2014)
36. Idziorek, J., Tannian, M., Jacobson, D.: Detecting fraudulent use of cloud resources. In: Proceedings of the 3rd ACM Workshop on Cloud Computing Security, pp. 61–72. ACM (2011)
37. Ismail, M.N., Aborujilah, A., Musa, S., Shahzad, A.: Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach. In: Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, p. 36. ACM (2013)
38. Feinstein, L., Schnackenberg, D., Balupari, R., Kindred, D.: Statistical approaches to DDoS attack detection and response. In: Proceedings of the DARPA Information Survivability Conference and Exposition, vol. 1, pp. 303–314. IEEE (2003)

39. Shamsolmoali, P., Zareapoor, M.: Statistical-based filtering system against DDoS attacks in cloud computing. In: 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI 2014), pp. 1234–1239. IEEE (2014)
40. Gómez-Lopera, J.F., Martínez-Aroza, J., Robles-Pérez, A.M., Román-Roldán, R.: An analysis of edge detection by using the Jensen-Shannon divergence. *J. Math. Imaging Vis.* **13**(1), 35–56 (2000)
41. Templeton, S.J., Levitt, K.E.: Detecting spoofed packets. In: Proceedings of the DARPA Information Survivability Conference and Exposition, vol. 1, pp. 164–175. IEEE (2003)
42. Chen, Q., Lin, W., Dou, W., Yu, S.: CBF: a packet filtering method for DDoS attack defense in cloud environment. In: IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), pp. 427–434. IEEE (2011)
43. Jeyanthi, N., Iyengar, N.C.S., Kumar, P.M., Kannammal, A.: An enhanced entropy approach to detect and prevent DDoS in Cloud environment. *Int. J. Commun. Netw. Inf. Secur. (IJCNIS)* **5**(2), 110 (2013)
44. Vissers, T., Somasundaram, T.S., Pieters, L., Govindarajan, K., Hellinckx, P.: DDoS defense system for web services in a cloud environment. *Future Gener. Comput. Syst.* **37**, 37–45 (2014)
45. Latanicki, J., Massonet, P., Naqvi, S., Rochwerger, B., Villari, M.: Scalable cloud defenses for detection, analysis and mitigation of DDoS attacks. In: Future Internet Assembly, pp. 127–137 (2010)
46. Li, B., Niu, W., Xu, K., Zhang, C., Zhang, P.: You cant hide: a novel methodology to defend DDoS attack based on but cloud. In: Applications and Techniques in Information Security. Communications in Computer and Information Science, pp. 203–214. Springer, Heidelberg (2015)
47. Graham, M., Adrian, W., Erika, S.-V.: Botnet detection within cloud service provider networks using flow protocols. In: 2015 IEEE 13th International Conference on Industrial Informatics (INDIN), pp. 1614–1619. IEEE (2015)
48. Badis, H., Doyen, G., Khatoun, R.: A collaborative approach for a source-based detection of but clouds. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 906–909. IEEE (2015)
49. Mohammad, R.M., Mauro, C., Ville, L.: EyeCloud: a BotCloud detection system. In: Proceedings of the 5th IEEE International Symposium on Trust and Security in Cloud Computing (IEEE TSCloud 2015), Helsinki, Finland. IEEE (2015)
50. Yu, S., Tian, Y., Guo, S., Wu, D.O.: Can we beat DDoS attacks in clouds? *IEEE Trans. Parallel Distrib. Syst.* **25**(9), 2245–2254 (2014)
51. Yossi, G., Amir, H., Michael, S., Michael, G.: CDN-on-Demand: an affordable DDoS defense via un-trusted clouds. In: Network and Distributed System Security Symposium (NDSS) (2016)
52. Somani, G., Gaur, M.S., Sanghi, D., Conti, M., Buyya, R.: Service resizing for quick DDoS mitigation in cloud computing environment. *Ann. Telecommun.* **72**(5–6), 237–252 (2016)
53. Somani, G., Gaur, M.S., Sanghi, D., Conti, M., Rajarajan, M.: DDoS victim service containment to minimize the internal collateral damages in cloud computing. *Comput. Electr. Eng.* (2016)
54. Sahay, R., Blanc, G., Zhang, Z., Debar, H.: Towards autonomic DDoS mitigation using software defined networking. In: SENT 2015: NDSS Workshop on Security of Emerging Networking Technologies, Internet Society, San Diego, California, US (2015). <https://doi.org/10.14722/sent.2015.23004>
55. Wang, X., Chen, M., Xing, C.: SDSNM: a software-defined security networking mechanism to defend against DDoS attacks. In: 2015 Ninth International Conference on Frontier of Computer Science and Technology (FCST), pp. 115–121. IEEE (2015)

56. Wang, B., Zheng, Y., Lou, W., Hou, Y.T.: DDoS attack protection in the era of cloud computing and software-defined networking. *Comput. Netw.* **81**, 308–319 (2015)
57. Yan, Q., Yu, F.: Distributed denial of service attacks in software-defined networking with cloud computing. *IEEE Commun. Mag.* **53**(4), 52–59 (2015)
58. Tsai, S.-C., Liu, I.-H., Lu, C.-T., Chang, C.-H., Li, J.-S.: Defending cloud computing environment against the challenge of DDoS attacks based on software-defined network. In: *Advances in Intelligent Information Hiding and Multimedia Signal Processing: Proceeding of the Twelfth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Kaohsiung, Taiwan, 21–23 November 2016, vol. 1, pp. 285–292. Springer, Cham (2017)
59. Stillwell, M., Schanzenbach, D., Vivien, F., Casanova, H.: Resource allocation algorithms for virtualized service hosting platforms. *J. Parallel Distrib. Comput.* **70**(9), 962–974 (2010)
60. Somani, G., Gaur, M.S., Sanghi, D., Conti, M., Rajarajan, M., Buyya, R.: Combating DDoS attacks in the cloud: requirements, trends, and future directions. *IEEE Cloud Comput.* **4**, 22–32 (2017)
61. Zhao, S., Chen, K., Zheng, W.: Defend against Denial of Service attack with VMM. In: *Eighth International Conference on Grid and Cooperative Computing*, GCC 2009, pp. 91–96. IEEE (2009)
62. Silva, S.S., Silva, R.M., Pinto, R.C., Salles, R.M.: Botnets: a survey. *Comput. Netw.* **57**(2), 378–403 (2013)
63. Yan, Q., Yu, R., Gong, Q., Li, J.: Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges. *Commun. Surv. Tutor.* **PP**(99), 1 (2015). <https://doi.org/10.1109/COMST.2015.2487361>
64. Singh, A., Chatterjee, K.: Cloud security issues and challenges: a survey. *J. Netw. Comput. Appl.* **79**(1), 88–115 (2017)
65. Online The Truth about DDoS Attacks: Part 1 (2013). <http://www.carbon60.com/the-truthabout-ddos-attacks-part-1/>. Accessed 12 July 2015
66. Kaspersky Lab. [https://www.kaspersky.com/about/press-releases/2015\\_one-in-five-ddos-attacks-last-for-days-or-even-weeks](https://www.kaspersky.com/about/press-releases/2015_one-in-five-ddos-attacks-last-for-days-or-even-weeks)



# A Study of Biology-Based Congestion Control Algorithms for Wireless Sensor Network

S. Panimalar<sup>(✉)</sup> and T. Prem Jacob<sup>(✉)</sup>

Faculty of Computing, Sathyabama Institute of Science and Technology,  
Chennai, India

panimalarjerome@gmail.com, premjac@yahoo.com

**Abstract.** Network Traffic is one of the major issues in wireless Sensor Networks (WSNs). WSN is a self-constructed and organization less wireless networks which is used to observe and check the physical or environmental conditions and to cooperatively pass their data through the network to a sink where the data can be appropriately observed and examined. Number of research works in wireless sensor networks (WSNs) is primarily focused on improving the network performance along with enhancing the quality of service parameters such as the data arrival rate, available bandwidth, congestion, transmission rate, queue length and energy. Various natural computational algorithms have been proposed for overcoming these issues. In this paper we have discussed about some of the bio-based algorithms such as Genetic Algorithms, Simulated Annealing, Ant Colony Optimization, Particle Swarm Optimization, Firefly Algorithm, etc. to control congestion in wireless sensor networks.

**Keywords:** Wireless sensor networks (WSNs) · Congestion control · Quality of service (QoS) · Bio-inspired algorithms

## 1 Introduction

A Wireless Sensor Network WSN is a wireless network that comprises a huge collections of tiny, low powered, inexpensive, self-directed devices called as sensor nodes. Each of these sensor nodes contains a radio, antenna, transceiver and micro controller. Sensor node is used to gather the data, manipulate the data and direct it to a base station. Figure 1 shows the architecture of a wireless sensor network. The group of sensor nodes is deployed in an area called as sensor field. The sensor nodes in field monitor their environment and collect data and pass them to the sink node. The sink node in turn passes the data to the base station through the gateway. WSNs are widely used in many applications like healthcare monitoring, forest fire detection, home application, military applications water quality monitoring etc.

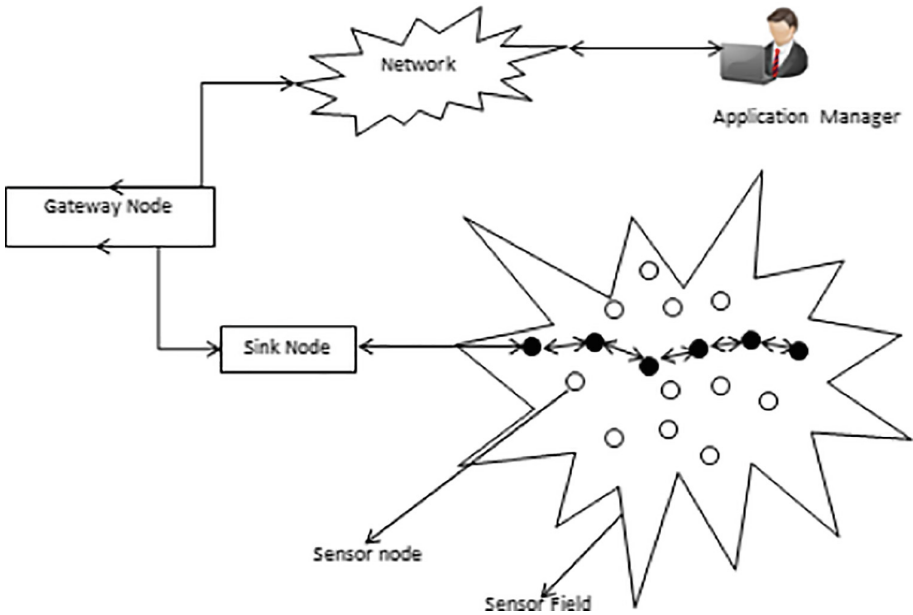


Fig. 1. Architecture of wireless sensor network

The following are the some of the issues in handling WSN

- Energy
- Limited bandwidth
- Node Costs
- Deployment
- Congestion
- Design Constraints
- Security

## 2 Congestion

When numerous nodes in a WSN direct data at the sole base station at the similar period, there are possibilities of jamming in the network [1]. When a sensor node receives data packets at greater amount than its ability to convey, additional data need to be kept in a buffer [8]. Due to inadequate availability of space, buffer becomes full and data packets (new or old) have to be released at a result of congestion [9]. As a result the data cannot be determined properly and hence the network performance gets degraded. Congestion has a direct influence on energy competence and applications QoS [10]. Thus, congestion in WSN need to be handled proficiently. Congestion in WSN can occur in node level or link level [11]. When a packet coming amount is greater than the packet service amount then node level congestion will occur. This type

of congestion leads to packet loss and affects the network lifetime. When many sensor nodes within the same range attempts to transmit data at the same time severe link collision will occur. This type of collision will affect link utilization and overall throughput (Fig 2).

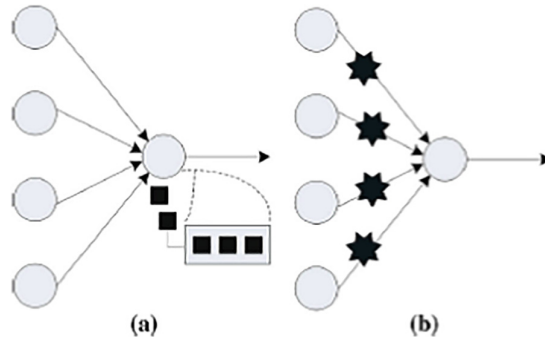


Fig. 2. (a) Node level congestion, (b) Link level congestion

### 3 Nature Inspired Algorithms (NIA)

Nature provides some interesting ways to solve hard problems. Many algorithms were developed by imitating the behavior of nature. These algorithm works on various combinations to solve certain numeric problems and also provide ideas in solving optimization difficulties. The algorithms are carried out in such a way that grouping the similarities that are found with the working of biological systems. These algorithms are used to solve various problems belonging to different domains. They are used in the field of medicines, engineering designs, Manufacturing systems, and Agricultural sciences etc. They are classified in to three types as biology-based algorithms, physics based algorithms and chemistry based algorithms. In this paper we are going to discuss about biology-based algorithms (Fig 3).

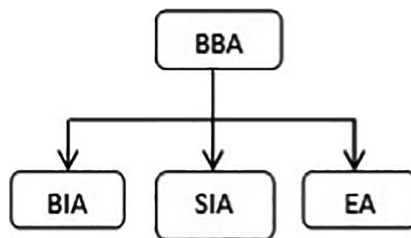


Fig. 3. Classification of nature inspired algorithm.



### 3.1 Biology-Based Algorithms Classifications

The ideas derived from biological activities leads to biology-based algorithms. Biology-based algorithms are categorized as Bio-inspired algorithms (BIA), Swarm intelligence-based algorithms (SIA), Evolutionary algorithms (EA) (Fig 4).

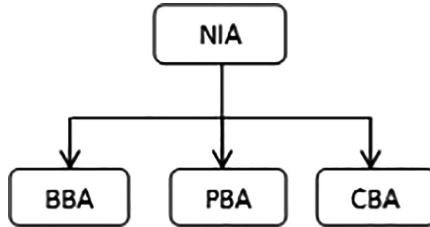


Fig. 4. Classification of biology-based algorithm.

#### 3.1.1 Bio-Inspired Algorithms (BIA)

The BIA is based on the concept of usually perceived portent in specific animal species and association of organism [14]. The few classification of BIA's are Particle Swarm Optimization (PSO), Bird Flocking (BF), Fish School (FS), Biogeography Based Optimization (BBO), Artificial Immune Systems (AIS).

#### 3.1.2 Swarm Intelligence-Based Algorithm (SIA)

The SIA is built on the notion of combined compartments of insects existing in associations such as ants, bees, wasps and termites [14]. The few classification of SIA's is Ant colony Optimization (ACO), Artificial Bee Colony (ABC), Bat Algorithm, Cuckoo Search (CS), Firefly Algorithm (FA) and Bacterial Foraging Optimization Algorithm (BFOA).

#### 3.1.3 Evolutionary Algorithm (EA)

This is one of the heuristic based algorithm based on Darwin's theory of evolution. The basic steps followed in EA algorithm are initialization, selection, variation operator, and termination. The few classification of EA's is Evolutionary programming (EP), Evolution Strategies (ES), Genetic Algorithms (GA), Genetic Programming (GP), Differential Evolution (DE) and Cultural Algorithm (CA) [14].

## 4 Biology-Based Algorithm Approaches Used in WSN

This section presents some of the biology-based approaches that can be used in wireless sensor networks.

#### **4.1 Genetic Algorithm**

Genetic Algorithm was proposed by Holland in the year 1970. GA are inspired by mimicking the natural selection process and by Charles Darwin's survival of fittest. In GA the better populations are selected as parents. The collection of the population is built on the fitness standards corresponding to the problem domain. After the selection operation crossover and mutation operation are applied. Thus the process iterated repeatedly by applying these three operators until the ending benchmark is encountered.

#### **4.2 Particle Swarm Optimization**

This algorithm was established by Eberhart and Kennedy in the year 1995. This algorithm is stimulated by the civic foraging by the number of small number animals a well-known as flocking process of birds and the schooling practice of fish [13]. Thus the algorithm is based on the concept of social interaction to solve the problem that is the experience of an individual will be shared with others in a working group. The algorithm is initialized with a set of possible solutions (Particles). At each step the solutions are evaluated based on the fitness function.

#### **4.3 Bat Algorithm**

Bat algorithm is one of the meta heuristic system established by Xin-she yang in the year 2010. The algorithm is built on the echolocation manners of bats. Bats to sense its target and to evade hurdles they produces a precise loud sound and wait for the resonance from the neighboring objects. Using the strength of the echo signal bats can able to identify the prey and its obstacles.

#### **4.4 Ant Colony Optimization Algorithm**

This algorithm was established by Marco Dorigo in the year 1992. It is one of the population based meta heuristic algorithm used to explain search based problem with optimal solution. This algorithm was based on the nature of an ant in searching for its food. This algorithm is stimulated by the seeking comportment of ants, exactly the pheromone communication among ants concerning a noble lane among the colony and a food source in an surroundings. This is called as stigmergy [13]. Ants arbitrarily walk around their surroundings in search of their food. Once the ant found its food it will release the chemical substances called pheromone in the environment. Other ants also follow the same path to the food and also releases. Pheromone will evaporate in the surroundings hence the older lanes are less likely to be followed. This phenomenon is used to identify shortest and best path between source and destination.

#### 4.5 The Bees Algorithm

This algorithm was established by Pham in the year 2005. The Algorithm is based on the comportment of honey bees i.e. in what way they gather honey from flowers as a food source around their beehive. Bees converse with all other at the hive via a waggle dance that notifies other bees in the hive as to the path, remoteness, and quality rating of food sources [13].

#### 4.6 The Bacterial Foraging Optimization Algorithm

This algorithm was established by Passino. It is inspired by the group seeking manners of bacteria. Bacteria observe the path to food built on the ramps of chemicals in their surroundings. Similarly, bacteria release fascinating and deterring chemicals into the surroundings and can observe every other in a related manner. Bacteria can travel everywhere using locomotion mechanisms either messily or in a directed manner. Bacterial cells are preserved like representatives in surroundings, using their observation of food and other cells as motivation to move and stochastic reducing and spinning like effort to re-locate. Depending on the cell-cell interactions, cells may flock a food source and/or may violently prevent or ignore all other [13].

#### 4.7 Cuckoo Search Algorithm

In the year 2009 Yang and Deb proposed a new optimization algorithm called Cuckoo Search algorithm. The algorithm is based on how cuckoos lay their eggs in the host nests.. The cuckoo egg positioning and manners is the first simple inspiration for the growth of innovative optimization algorithm. This optimization algorithm increases the competence, correctness, and union rate [15].

### 5 Literature Survey

**Karishna Singh (2018).** In this paper a fusion multi-objective optimization algorithm was suggested for congestion optimization algorithm PSO GSA is used for rate maximization and regularly coming rate of records from every child node to the parent node. The energy of the wireless sensor Network node is considered in Fitness function evaluation. The precedence centred-communication is used as the optimization method which adjusts the coming amount on the basis of priority. To avoid the rate of the data is adjusted to optimum value to avoid congestion [1].

**Vaibhav Eknath Narawade (2017).** In this paper proposed an algorithm to evade and control the congestion based adaptive cuckoo search. This algorithm formulated a Fitness function using epsilon constraint value. The algorithm is used to define the best share rate and it is also used to produce the answer in which phase scope is adjusted to offer the improved transmission amount to avoid congestion. The performance of the algorithm was evaluated using the parameter like delay, packet loss & queue size [2].

**Mukhdeep Singh Manshahia (2017).** In this paper water wave optimization algorithm was proposed to avoid congestion control in WSN. In objective function based on the factors like network throughput, residual energy and packet loss rate was objective function and as optimal solution is obtained. The results of the algorithm showed that the Queue extent of every node drops by increasing the amount of hops. This showed that the traffic is shared among all the nodes rather than a specific one and this congestion was avoided [3].

**J. Lalitha (2016).** In this paper firefly algorithm was implemented in transport layer of wireless sensor network to control congestion. In this route is decided by using reactive route technique. Once a node is ready to transmit the data it will generate a route request message and it was passed within the network. The route is decided based on the early arrival of route request message either through single or multiple hops. By the process of bioluminescence the firefly insect produces short flashes of light. The role of the flashing light is to attract the prey, to attract the partner and it is used as a warning to predator. The algorithm was implemented by taking attractiveness feature of the firefly. Data will be moved in a path of nodes with high residual energy. The result showed that the queue extent of each node drops by increasing the number of hops. The results showed that the method was preeminent as matched to Congestion Detection and avoidance (CODA) and Particle Swarm improvement (PSO) on network life and turnout of the network [4].

**Mayank Dave (2015).** In this paper an enhanced bat algorithm was used to control bottleneck in wireless sensor network. The algorithm was built on the idea of echolocation of bats. Bats uses sonar resonances for hurdle detection and avoidance. Those resonances are converted in to frequency and the time interval between the production and reproduction was used for navigation. This idea of bats was used to develop the bat algorithm. The results showed that by increasing the amount of hops in the path of packet transmission the queue length gets decreased. The packets are transmitted through different through different path instead of collecting on a single node. Thus congestion in the network was reduced. The algorithm showed improvements in network lifetime and throughput when associated to Congestion Detection and Avoidance and Particle Swarm Optimization algorithm [5].

**Anu Verma (2014).** In this paper genetic algorithm (GA) was used to control congestion control. The algorithm finds a best path from source to destination for various situations of mobility of source or sink node. The optimal path was determined by using the concept of connection value and localization region. The algorithm was applied every time before packet transmission to find an optimal path and reduces the congestion. The result shows that the algorithm was efficient even if the network complexity was increased [6].

**Pavlos Antoniou (2013).** In this paper congestion was controlled using the bird flocking behaviour. Using this behaviour they designed a scalable, robust and self-adaptive congestion control protocol for wireless sensor network. In this method data packets are grouped as a flocks and move towards the sink node. The way in which

flocks of packet should flow is done by repulsive and attractive forces among the packets as well as the field of view and the artificial magnetic pole that is the sink node. The result showed that the performance poverty in terms of delay, packet loss, packet delivery ratio and energy. The algorithm was also proved to be robust and scalable [7].

## 6 Results and Analysis

The performances of proposed work are analyzed on three network parameters, (1) Delay, (2) Error rate, (3) Life time. End-to-end delay is well-defined as the period occupied by a data packet to move from a source to the destination and vice versa. The error rate can be defined as the amount at which the error occurs during the transmission of the packets. Network lifetime is the amount of time that a Wireless Sensor Network node would be fully operative. Simulation carried out in MATLAB 2010. The simulation parameters are shown in Table 1.

**Table 1.** Simulation parameters

Number of nodes	100
Network length	1000 m
Network Width	1000 m
Parameters	End to End delay, Error rate, Network lifetime.
Algorithms	Genetic algorithm, Particle swarm optimization algorithm, BFO, GA-PSO
No. of iterations	100

### 6.1 Comparison of GA, PSO and Hybrid of GA-PSO Algorithms

By using GA, PSO and Hybrid (GA-PSO) algorithm the results were obtained for delay, error rate and lifetime and it is shown in Table 2. The comparison of delay, error rate and lifetime is shown in Figs. 5, 6 and 7.

**Table 2.** Calculated Delay, Error rate, Life time

Parameters	GA	PSO	Hybrid (GA-PSO)
Delay	11.09	13.65	0.122
Error-rate	13.5	32.55	11.00
Lifetime	122.00	3.94	140.00

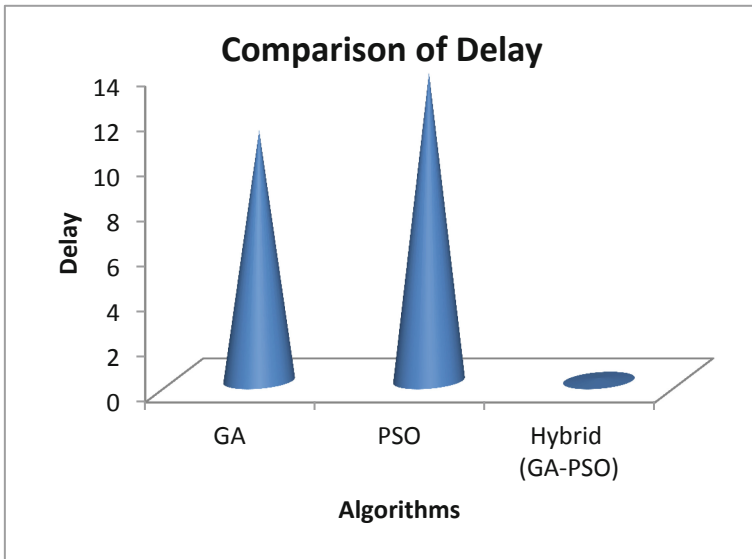


Fig. 5. Comparison of delay

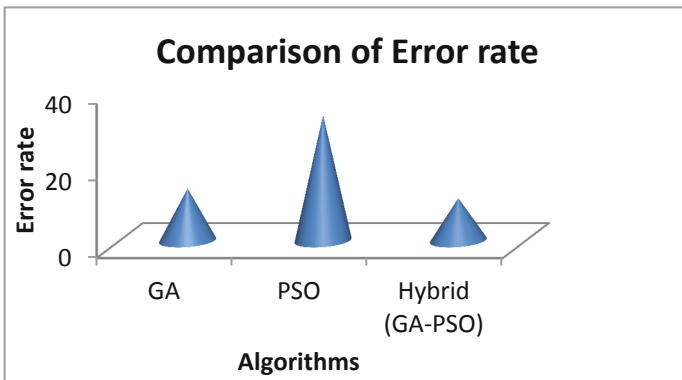


Fig. 6. Comparison of error rate

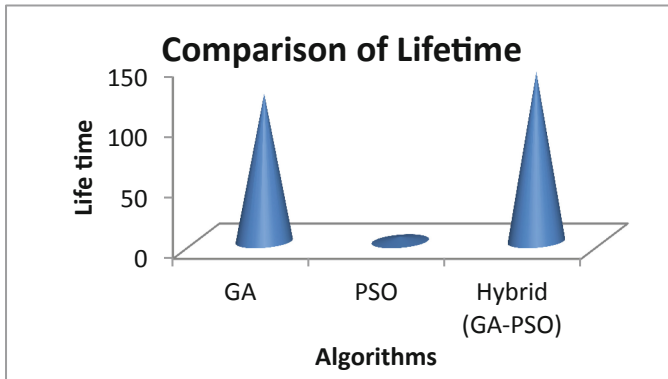


Fig. 7. Comparison of lifetime

## 7 Conclusion

The objective of using optimization algorithm is to increase the effective consumption of the restricted resources of WSNs like energy, bandwidth, computational power etc. This evaluation shows that the field of Biology-based computing is huge and growing. This paper provides an overview of Biology-based Algorithms such as GA, PSO, ACO, CS etc. and a comparative study of the GA, PSO and GA-PSO optimization algorithms. The given algorithms report numerous problems associated with optimization in WSNs such as QoS, energy efficiency and security. There is important possibility for further work in these areas. The results show that the hybrid algorithms perform better than the other algorithms. Future scope lies in implementation of other forms of hybrid algorithms in congestion control.

## References

1. Singh, K., Singh, K., Son, L.H., Aziz, A.: Congestion control in wireless sensor networks by hybrid multi-objective optimization algorithm. *Comput. Netw.* **138**, 90–101 (2018)
2. Narawade, V.E., Kolekar, U.D.: Congestion avoidance and control in wireless sensor networks using epsilon constraint based adaptive cuckoo search. *Int. Educ. Res. J. IERJ* **3**(5), 715–720 (2017)
3. Manshahia, M.S.: Water wave optimization algorithm based congestion control and quality of service improvement in wireless sensor networks. *Trans. Netw. Commun.* **5**(4), 31–39 (2017)
4. Lalitha, J., Kalaiselvi, C.: Energy efficient & congestion control in wireless sensor network using firefly algorithm. *Int. J. Emerg. Technol. Comput. Sci. Electron. IJETCSE* **23**(5) (2016)
5. Manshahia, M.S., Dave, M., Singh, S.B.: Bio inspired congestion control mechanism for wireless sensor networks. In: *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 141–146 (2015)

6. Verma, A., Mittal, N.: Congestion Controlled WSN using genetic algorithm with different source and sink mobility scenarios. *Int. J. Comput. Appl.* **101**(13), 0975–8887 (2014)
7. Antoniou, P., Pitsillides, A., Blackwell, T., Engelbrecht, A., Michael, L.: Congestion control in wireless sensor networks based on bird flocking behavior. *Comput. Netw.* **57**(5), 1167–1191 (2013)
8. Taherkhani, N., Pierre, S.: Prioritizing and scheduling messages for congestion control in vehicular ad hoc networks. *Comput. Netw. Int. J. Comput. Telecommun. Network.* **108**, 15–28 (2016)
9. Mahmood, M.A., Seah, W.K., Welch, I.: Reliability in wireless sensor networks: a survey and challenges ahead. *Comput. Netw.* **79**, 166–187 (2015)
10. Motdhare, S.: Congestion control in wireless sensor networks: mobile sink approach. *Int. J. Sci. Res. IJSR* **4**(1), 2561–2565 (2015)
11. Rezaee, A.A., Yaghmaee, M.H., Rahmani, A.M.: Optimized congestion management protocol for healthcare wireless sensor networks. *Wirel. Pers. Commun. Int. J.* **75**(1), 11–34 (2014)
12. Brownlee, J.: *Evolutionary Algorithms in Clever. Nature-Inspired Programming Recipes Algorithms*, 1st edn. LuLu, Morrisville (2011). ISBN: 978-1-4467-8506-5. <http://www.cleveralgorithms.com>
13. Brownlee, J.: *Swarm Algorithms in Clever Algorithms. Nature-Inspired Programming Recipes*, 1st edn. LuLu, Morrisville (2011). ISBN: 978-1-4467-8506-5. <http://www.cleveralgorithms.com>
14. Siddique, N., Adeli, H.: Nature inspired computing: an overview and some future directions. *Cogn. Comput.* **7**(6), 706–714 (2015)
15. Venkata Vijaya, G.P., Ravi Kiran, V.: Cuckoo search optimization and its applications: a review. *Int. J. Adv. Res. Comput. Commun. Eng.* **5**(11) (2016)





# A Comparison of GFDM and OFDM at Same and Different Spectral Efficiency Condition

Chhavi Sharma<sup>1</sup>(✉), S. K. Tomar<sup>2</sup>, and Arvind Kumar<sup>1</sup>

<sup>1</sup> National Institute of Engineering and Technology, Kurukshetra, India  
yash\_naina@yahoo.co.in

<sup>2</sup> Institute of Engineering and Technology, M.J.P.R. University, Bareilly, India

**Abstract.** Generalized frequency division multiplexing (GFDM) is an upcoming modulation method for fifth generation (5G) wireless communication systems with many advantages over conventional orthogonal frequency division multiplexing (OFDM). In this work, GFDM with clipping and filtering technique is proposed and its performance in terms of peak to average power ratio (PAPR) is presented. The proposed GFDM system along with Rapp's solid state high power amplifier (SSPA) is simulated to evaluate its PAPR and BER performance. The performance of the present system is compared with the OFDM system for equal and unequal spectral efficiency conditions. The simulation results show that at equal spectral efficiency condition (ESE), the PAPR of clipped and filtered GFDM signal is reduced by 1.6 dB as compared to clipped and filtered OFDM signal with almost similar BER performance. In addition to that, the complexity of GFDM system is less than that of OFDM for equal spectral efficiency condition.

**Keywords:** GFDM · OFDM · PAPR · Clipping and filtering · BER · SSPA

## 1 Introduction

In recent years, high speed and broad coverage area are the basic requirements for future wireless communication systems. Though fifth generation (5G) standard promises the high data rate, higher efficiency and lower latency but implementation of machine to machine (MTM) communication and internet of things (IoT) based 5G systems is still a bigger challenge as these systems require more flexibility, relaxation of synchronization and low out of band radiation [1].

Orthogonal frequency division multiplexing (OFDM) is a popular modulation method for high data rate wireless networks as it effectively mitigates inter-symbol interference (ISI) caused by delay spread of wireless channels but high peak to average power ratio(PAPR) is one of the major drawbacks of OFDM system. The high PAPR OFDM signal introduces additional interference into the system in the form of in-band and out of band radiation after passing through the high power amplifier(HPA). OFDM signal is also very sensitive to time and frequency offsets and to avoid it, strict synchronization between users is required [2]. Therefore OFDM might not be a suitable candidate in 5G scenario. Filter bank multicarrier (FBMC) and generalized frequency division multiplexing (GFDM) are new modulation schemes which are proposed recently and suitable for 5G wireless systems [3].

In GFDM, the data transmission is in time-frequency block manner which reduces the requirement of large subcarriers, so PAPR in GFDM system is less compared to OFDM system for equal spectral efficiency condition. Pulse shaping property of GFDM controls out of band radiation. Though it introduces self induced interference which can be compensated by interference cancellation techniques at the receiver side [4]. Cyclic prefix is added to the entire block in this system which makes GFDM more spectrally efficient compared to OFDM system [5–7].

The above properties of GFDM system make it an attractive choice for 5G communication systems. However, the problem of PAPR becomes larger in GFDM if subcarriers become comparable to OFDM subcarriers and it becomes severe in the presence of high power amplifier [7]. Therefore it is worth to analyse the comparative study of PAPR performance for OFDM and GFDM system for equal and unequal spectral efficiency conditions. The performance of OFDM, GFDM and WCP-COQAM systems is discussed under these two conditions in [8] but it has focused only about the out of band radiation parameter of the systems. To the best of author's knowledge none of the work has shown the comparative PAPR performance of both OFDM and GFDM systems for equal and unequal spectral efficiency conditions. In this work authors have presented the comparison of PAPR performance of GFDM system with OFDM system at two different spectral efficiency conditions.

Many PAPR reduction techniques are discussed in literature for OFDM system such as coding, partial transmit sequence, clipping and filtering, Tone reservation, Tone injection, companding, precoding etc. [2]. Among all these techniques, clipping is simple in operation and easy to implement but it increases in band and out of band radiation in the signal hence filtering can be applied after clipping [10]. In the proposed work, clipping with filtering is applied with GFDM system in an iterative manner. The performance of the proposed GFDM system is compared with clipped and filtered OFDM system at equal and unequal spectral efficiency condition for different performance metrics such as PAPR, BER and complexity.

The rest of paper is organized as follows: Sect. 2 describes the basic transmitter and receiver model of GFDM. Section 3 presents the proposed scheme with high power amplifier model. Simulation results are presented in Sects. 4 and 5 concludes the paper.

## 2 Basic GFDM Transmitter and Receiver Model

The baseband GFDM transmitter and receiver systems are depicted in Figs. 1 and 2 respectively.

### 2.1 Baseband GFDM Transmitter Model

For GFDM transmission, initially data bits are mapped using 16-QAM modulation then these symbols are passed through serial to parallel converter block for converting them to a block of  $KM \times 1$  parallel data symbols  $D$ . The  $KM$  data symbols are represented as  $M$  time slots and frequency samples. After S/P conversion, GFDM modulation is performed on to each  $KM \times 1$  parallel data block.

GFDM transmission is based on three operations as shown in Fig. 1, which are up sampling, pulse shaping and carrier up conversion. All three operations can be described mathematically as in [9]

$$x[n] = \sum_{k=0}^{K-1} \sum_{m=0}^{M-1} d_{k,m} g_{k,m}[n], \quad n = 0, 1, \dots, NM - 1 \tag{1}$$

where,  $d_{k,m}$  is complex data symbol transmitted on the  $k^{th}$  subcarrier and  $m^{th}$  time slot and  $g_{k,m}[n]$  is time and frequency transformation of the circular pulse shaping filter of length  $NM$  which is defined as

$$g_{k,m}[n] = g[(n - mK) \bmod N] w^{k,n} \tag{2}$$

where,  $w^{k,n} = e^{-j2\pi kn/N}$  and  $N$  is the no. of samples per time slot.

The GFDM transmitted signal in (1) can also be expressed as  $MN \times MN$  modulation matrix as:

$$x = Rd \tag{3}$$

where  $d$  is the data vector and matrix  $R$  includes all the GFDM signal processing steps represented as

$$[R]_{nm} = g[(n - mN) \bmod MN] e^{j2\pi mn/N} \tag{4}$$

To avoid the aliasing, signal is then up sampled and up conversion of the subcarriers can be done through the IFFT.

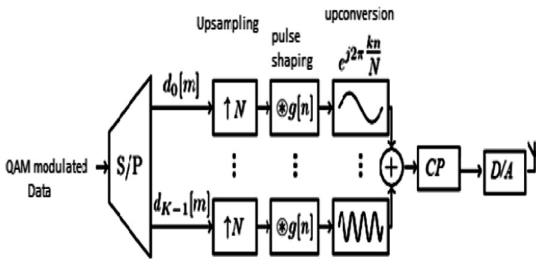


Fig. 1. GFDM transmitter

### 2.2 GFDM Receiver

GFDM receiver process is depicted in Fig. 2. The received GFDM signal is initially converted back from analog to digital and then cyclic prefix is removed. Further three operations are applied on the signals which are down conversion, inverse pulse shaping and down sampling to get back the original signal. Now data stream is converted back from parallel to serial data stream and processes for symbol detection. In the proposed work zero forcing (ZF) detection method is applied [5].

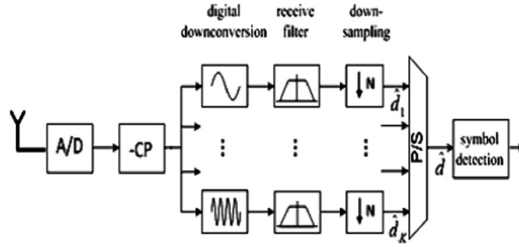


Fig. 2. GFDM receiver

After removal of cyclic prefix the received signal can be written as

$$r[n] = a[n] * x[n] + w[n] \tag{5}$$

where  $a[n]$  is the channel impulse response,  $w[n]$  is the complex AWGN noise with variance  $N_0$ . In the GFDM system the channel distortion is removed by using frequency domain equalizer (FDE) [4]. In this paper zero forcing (ZF) receiver for detection is considered. The signal before channel equalization can be represented as

$$\vec{y} = IDFT(\vec{H} \cdot \vec{X}) + \vec{w} \tag{6}$$

After channel equalization received signal is represented as

$$\vec{y}_{eq} = \vec{x} + IDFT\left(\frac{\vec{W}}{\vec{H}}\right) \tag{7}$$

where,  $\vec{X}$ ,  $\vec{H}$  and  $\vec{W}$  represents signal, channel impulse response and noise in frequency domain respectively. In order to estimate the transmitted data vector from equalized signal  $\vec{y}_{eq}$ , zero forcing detector is applied, as it completely removes intercarrier interference (ICI) from subcarriers. The estimated data vector  $\hat{d}$  after applying zero forcing detector will be

$$\hat{d} = G \cdot \vec{y}_{eq} \tag{8}$$

where  $G = (H^H \cdot H)^{-1} H^H$  and  $\vec{y}_{eq} = HX + W$  and after putting the values of  $G$  and  $\vec{y}_{eq}$  in Eq. (8) we get

$$\hat{d} = X + GW \tag{9}$$

from (9) data signal can be recovered and then finally passed through a slicer to get estimated input

$$\hat{X} = slice(\hat{d}) \tag{10}$$

### 3 Proposed Scheme

The baseband GFDM signal when passed through HPA, nonlinear distortions occur in the form of out of band emission (OOB) due to nonlinear behavior of HPA and these distortions become severe with high PAPR signal. To avoid these distortions, clipping and filtering technique is applied to the baseband GFDM signal before passing through the power amplifier.

The detailed process of proposed GFDM signal transmission is depicted in Fig. 3. The QAM mapped data is converted from serial to parallel and then passed through GFDM modulator. Further, GFDM modulated signal is clipped and filtered and converted back from parallel to serial and finally cyclic prefix is added to the whole data block of the signal. Now after digital to analog conversion, the GFDM signal is passed through high power amplifier.

For more details, Sect. 3.1 gives the idea of clipping and filtering technique and Sect. 3.2 describes high power amplifier model adopted in the proposed method

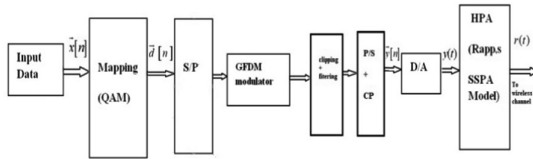


Fig. 3. Clipped and filtered GFDM with high power amplifier

#### 3.1 Clipping and Filtering

In the proposed work, clipping and filtering method is applied iteratively for peak to average power ratio (PAPR) reduction of GFDM signal. Clipping is very simple technique for PAPR reduction which is deliberately performed to limit the peaks in the signal to be transmitted in the nonlinear channel. The clipped signal can be written as in [10]:

$$f(x[n]) = \begin{cases} x[n] & \text{if } |x[n]| \leq V_{\max} \\ V_{\max} e^{j\psi(x[n])} & \text{if } |x[n]| \geq V_{\max} \end{cases} \tag{11}$$

where  $x[n]$  is the original signal and  $\psi(x[n])$  is phase of the signal. The clipping ratio is defined by

$$CR = 10 \log_{10}(\xi) \text{ in dB} \quad (12)$$

$$\text{If } \xi = \frac{V_{\max}^2}{P_0}$$

The operation of clipping causes nonlinear degradation in the signal also BER performance of the clipped signal is badly degraded due to out of band emissions. In the proposed work, filtering technique is applied after clipping to reduce the out of band emission [11].

### 3.2 High Power Amplifier Model

The most commonly used baseband power amplifier models are Saleh model for travelling wave tube amplifier (TWTA), Ghorbani model for field-effect transistor (FET) amplifier, Rapp's model for envelope characteristic of solid state power amplifier (SSPA). The output signal of nonlinear HPA is expressed as in [12]

$$f(t) = r(t)e^{j\varphi(t)} \quad (13)$$

where  $R[\cdot]$  and  $\varphi[\cdot]$  is AM/AM and AM/PM characteristics of high power amplifier. In the proposed work the performance of GFDM system is evaluated in presence of Rapp's SSPA Model. For SSPA, the AM/AM and AM/PM conversion characteristics are expressed as

$$R_{out} = \frac{R_{in}}{\left[1 + (R_{in}/R_0)^{2p}\right]^{1/2p}} \quad (14)$$

$$\varphi[R_{in}] = 0 \quad (15)$$

where  $R_{in}$  and  $R_{out}$  are input and output amplitudes of high power amplifier respectively.  $R_0$  is the saturated amplitude parameter which can found to be  $R_0 = R_{sat}/\sqrt{2}$  and  $p$  is the smoothness parameter which controls the transition from linear region to saturation. The range of parameter  $p$  may be between 2 to 3. In the proposed work parameter  $p$  is set to two.

## 4 Results

The performance of the proposed method is evaluated for OFDM and GFDM system with 16-QAM modulation. Table 1 shows the simulation parameters for the proposed method. All the simulation results are obtained in the presence of Rapp's SSPA model of HPA with smoothness parameter  $p = 2$ .

**Table 1.** Simulation parameters

Parameters	OFDM	GFDM
No. of Frequency slots K (subcarriers)	128 (for unequal SE) 512 (for equal SE)	128
No. of time slots M	1	4
Modulation technique	16QAM	16QAM
Oversampling factor L	4	4
Root raised cosine filter Roll off factor	0.3	0.3
HPA model	SSPA	SSPA
Clipping ratio CR	1.2	1.2

#### 4.1 PAPR Performance

In this section, PAPR performance of GFDM and OFDM system is compared for equal and unequal spectral efficiency conditions with clipping and filtering technique.

##### 4.1.1 Unequal Spectral Efficiency Condition

It is discussed previously that GFDM transmits data symbols in frequency and time grid which consists of K subcarriers and M time slots but OFDM consists of single time slot and in this case spectral efficiency of GFDM will be higher than OFDM for same no. of subcarriers. This is called the unequal spectral efficiency condition and in this case no. of subcarriers for OFDM and GFDM are kept 128. After applying clipping and filtering technique on both systems, signals are passed through the high power amplifier and then the PAPR performance of both systems is compared.

PAPR performance curves for GFDM and OFDM with clipping and filtering for unequal spectral efficiency condition are depicted in Fig. 4. Simulation results show that for the same number of subcarriers the PAPR of clipped and filtered OFDM signal is reduced by 0.8 dB than that of clipped and filtered GFDM signal at threshold level  $10^{-1}$  at the cost of lesser spectral efficiency.

##### 4.1.2 Equal Spectral Efficiency Condition

Now in the second case, the PAPR performance of both systems for equal spectral efficiency condition is evaluated. Increasing the number of subcarriers is one method to increase the spectral efficiency of OFDM system comparable to GFDM system spectral efficiency. Here the number of subcarriers in OFDM system are increased from 128 to 512 and rest of the simulation parameters remains same as above. The simulated results of PAPR performance of OFDM and GFDM modulation techniques with clipping and filtering are shown in Fig. 5. From the results it can be concluded that PAPR of clipped and filtered GFDM signal is reduced by 1.4 dB than clipped and filtered OFDM signal, which clearly show the performance improvement of GFDM over OFDM at same spectral efficiency condition.

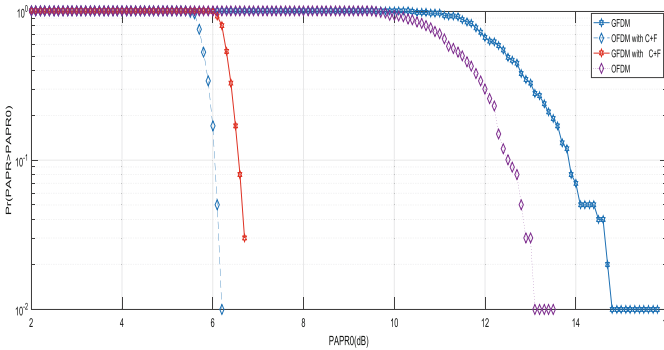


Fig. 4. PAPR performance comparison of OFDM and GFDM with clipping and filtering at unequal spectral efficiency condition

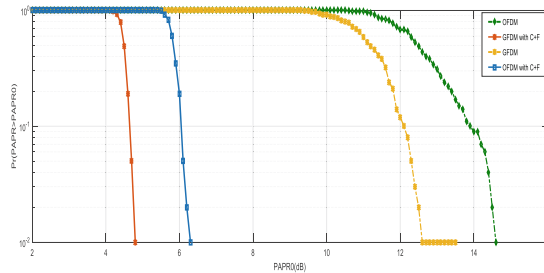


Fig. 5. PAPR performance comparison of OFDM and GFDM with clipping and filtering at equal spectral efficiency

### 4.2 Complexity

This section gives the complete idea of complexity comparison of OFDM and GFDM modulation techniques at the same and different spectral efficiency conditions. In this simulation work also the no. of subcarriers of OFDM are set to 512 and 128 for same and unequal spectral efficiency conditions respectively and for GFDM system, subcarriers  $K$  are set to 128 with  $M = 4$  time slots.  $J = 5$  iterations are taken for successive interference cancellation in GFDM.

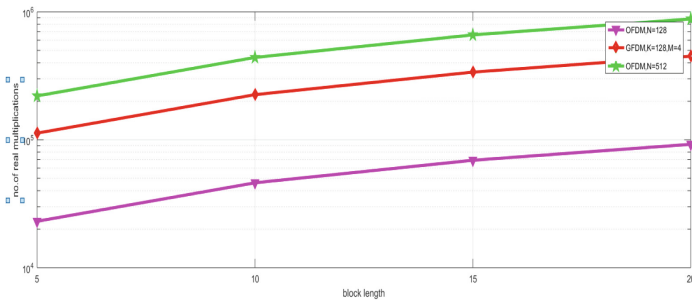
In general, computational complexity is considered as the no. of real multiplications of FFT/IFFT operations per symbol at the transmitter and receiver side. Here we have not considered the operations involved in windowing and channel estimation. Table 2 shows the complexity of OFDM and GFDM systems in terms of real multiplications at transmitter and receiver side. The simulations are performed for  $b$  no. of multicarrier symbols in OFDM signal and for GFDM the transmitted symbols are  $b'_{GFDM} = \frac{b}{M}$ .



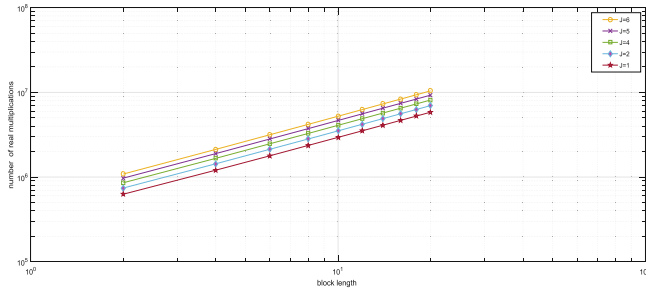
**Table 2.** Computational complexity comparison of OFDM and GFDM system under unequal and equal Spectral efficiency condition

Type	Complexity	Complexity for unequal spectral efficiency condition, N = 128 for OFDM	Complexity for equal spectral efficiency condition (ESE), N = 512 for OFDM
OFDM Tx	$b[2N \log_2 N + 4N]$	$b \times 2304$	$b \times 11264$
OFDM Rx.	$b[2N \log_2 N + 4N]$	$b \times 2304$	$b \times 11264$
GFDM Tx.	$b'_{GFDM} [K(M \log_2 M + 2M \times 2) + MK \log_2 MK]$	$b \times 1920$	$b \times 1920$
GFDM Rx.	$b'_{GFDM} \left[ \begin{matrix} MK \log_2 MK + K(M \log_2 M + 4M \times 2) + \\ 2MK \log_2 MK + 4MK + J(2KM \log_2 M + 2MK) \end{matrix} \right]$	$b \times 9088$	$b \times 9088$

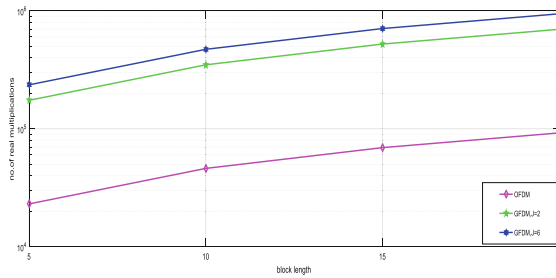
The simulation result of computational complexity of GFDM and OFDM is compared in Fig. 6 for same and unequal spectral efficiency conditions. The results in Fig. 6 clearly show that the computational complexity of conventional GFDM is less than the conventional OFDM for equal spectral efficiency (ESE) condition. It can also be concluded from the same result that OFDM system outperforms over GFDM for unequal spectral efficiency (USE) condition at the cost of reduced spectral efficiency. To reduce the effect of intercarrier interference introduced in the GFDM system, successive interference cancellation technique is used which increases the complexity of the system with every iteration. Figure 7 shows that the system complexity is increasing with large no. of iterations. System complexity of clipped and filtered GFDM is also compared in Fig. 8 for  $J = 2$  and  $J = 6$ .



**Fig. 6.** Complexity comparison of OFDM with GFDM at same and different spectral efficiency condition



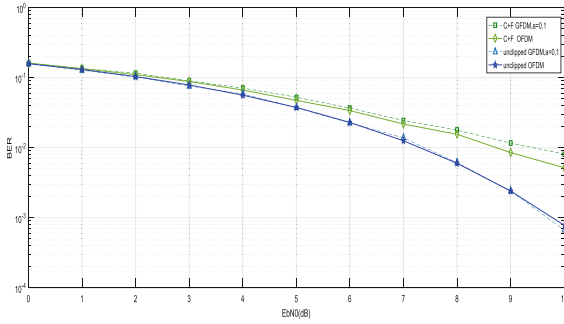
**Fig. 7.** Computational complexity of GFDM system at different no. of successive interference cancellation iterations



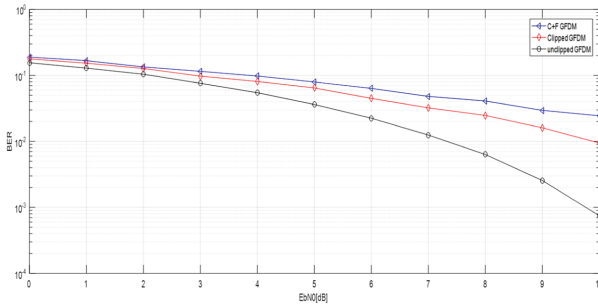
**Fig. 8.** Complexity comparison of clipped and filtered OFDM and GFDM for unequal spectral efficiency condition

**4.3 BER Performance**

The comparative BER performance results for conventional GFDM (without clipping and filtering) and clipped and filtered GFDM are depicted in Fig. 9 for same spectral efficiency condition. It is shown that the BER performance of clipped and filtered GFDM is almost equal to clipped and filtered OFDM signal for J = 5 iterations. BER performance curves of conventional GFDM, clipped GFDM (without filtering) and clipped & filtered (C + F) GFDM signal are compared in Fig. 10, which show a small degradation in BER performance for clipped GFDM as well as in clipped and filtered GFDM signal.



**Fig. 9.** BER performance comparison of conventional OFDM and conventional GFDM with clipped and filtered OFDM and GFDM for roll off factor  $\alpha = 0.3$  and clipping ratio  $CR = 1.2$



**Fig. 10.** BER performance of conventional GFDM, Clipped GFDM & Clipped and filtered (C + F) GFDM signal

### 5 Conclusion

In this work, a comparison of OFDM and GFDM is presented for three different performance metrics which are PAPR, BER and complexity. The comparison is mainly performed for equal and different spectral efficiency conditions and it is concluded that GFDM signal performance is superior than OFDM signal at equal spectral condition for PAPR and complexity as two performance metrics. Though the BER performance of clipped and filtered (C + F) GFDM is slightly degraded as compared to conventional GFDM but the C + F GFDM gives similar BER performance as C + F OFDM. In this work, clipping and filtering technique is applied with GFDM which reduces peak to average power ratio of GFDM signal and also improves the efficiency of the system. The work presented here verifies that GFDM can be a good choice for future wireless communication systems.

## References

1. Banelli, P., Buzzi, S., Colavolpe, G., Modenini, A., Rusek, F., Ugolini, A.: Modulation formats and waveforms for 5G networks: who will be the heir of OFDM?: An overview of alternative modulation schemes for improved spectral efficiency. *IEEE Sign. Proc. Mag.* **31** (6), 80–93 (2014). <https://doi.org/10.1109/msp.2014.2337391>
2. Tao, J., Yiyan, W.: An overview of PAPR reduction techniques in OFDM signals. *IEEE Trans. Broadcast.* **54**(2), 257–268 (2008). <https://doi.org/10.1109/tbc.2008.915770>
3. Michailow, N., Matthe, M., Gaspar, I., Caldevilla, A., Mendes, L., Festag, A., Fettweis, G.: Generalized frequency division multiplexing for 5th generation cellular networks. *IEEE Trans. Commun.* **62**(9), 3045–3061 (2014). <https://doi.org/10.1109/tcomm.2014.2345566>
4. Fettweis, G., Krondorf, M., Bittner, S.: GFDM-generalized frequency division multiplexing. In: *Proceedings of IEEE Vehicular Technology Conference*, pp. 1–4 (2009). <https://doi.org/10.1109/vetecs.2009.5073571>
5. Wunder, G., Jung, P., Asparick, M.K., Wild, T., Schaich, F., Chen, Y., Brink, S., Gaspar, I., Michailow, N., Festag, A., Mendes, L., Assiau, N., Ktenas, D., Dryjanski, M., Pietrzyk, S., Eged, B., Vago, P., Wiedmann, F.: 5GNOW: non-orthogonal, synchronous waveforms for future mobile applications. *IEEE Commun. Mag.* **52**(2), 97–105 (2014). <https://doi.org/10.1109/mcom.2014.6736749>
6. Gaspar, I., Matthé, M., Michailow, N., Mendes, L., Zhang, D., Fettweis, G.: Frequency-shift offset-QAM for GFDM. *IEEE Commun. Lett.* **19**(8), 1454–1457 (2015). <https://doi.org/10.1109/lcomm.2015.2445334>
7. Michailow, N., Fettweis, G.: Low peak-to-average power ratio for next generation cellular systems with generalized frequency division multiplexing. In: *International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS)*, pp. 651–655 (2013)
8. Ücuncu, A.B.: *Out-of-Band Radiation and CFO Immunity of Potential 5G Multicarrier Modulation Schemes*. Graduate School of Natural and Applied Sciences, Middle East Technical University (2015)
9. Juliano, F., Henry, R., Arturo, G., Ahmad, N., Maximilian, M., Dan, Z., Lucian, M., Gerhard, F.: GFDM frame design For 5G application scenarios. *J. Commun. Inf. Syst.* **32**(1), 54–60 (2017). <https://doi.org/10.14209/jcis.2017.6>
10. Wang, L.Q., Tellambura, C.: A Simplified clipping and filtering technique for PAR reduction in OFDM Systems. *IEEE Sign. Process. Lett.* **12**(6), 453–456 (2005). <https://doi.org/10.1109/lsp.2005.847886>
11. Gurung, A.K., Al-Qahtani, F.S., Sadik, A.Z., Hussain, Z.M.: One-Iteration-Clipping-Filtering (OICF) scheme for PAPR reduction of OFDM signals. In: *Proceedings of the International Conference of Advanced Technology Communication*, pp. 207–210 (2008)
12. Zhidkov, S.V.: Performance analysis of multicarrier systems in the presence of smooth nonlinearity. *EURASIP J. Wirel. Commun. Network.* **2004**(2), 335–343 (2004). <https://doi.org/10.1155/s1687147204406124>



# Modified Multinomial Naïve Bayes Algorithm for Heart Disease Prediction

T. Marikani<sup>1</sup> and K. Shyamala<sup>2</sup>

<sup>1</sup> Department of Computer Science, Sree Muthukumaraswamy College,  
Chennai, Tamil Nadu, India  
tmkani330@gmail.com

<sup>2</sup> Department of Computer Science,  
Dr. Ambedkar Govt. Arts College (Autonomous), Chennai, Tamil Nadu, India  
shyamalakannan2000@gmail.com

**Abstract.** There are number of challenging research areas available in the field of medical technologies. Among them cardio-vascular disease prediction plays a vital role. By applying data mining techniques, valuable knowledge can be extracted from the health care system. In this proposed work heart disease can be detected by using a classifier algorithm. The world health organization has projected 17.7 million people died from CVDs in 2015, representing 31% of all global deaths. According to this survey, it is anticipated that nearly 7.4 million people will die due to coronary heart disease and 6.7 million were due to stroke. The proposed algorithm was Modified Multinomial Naïve Bayes algorithms (MMNB). This algorithm helps us to predict the heart disease more accurately compared to other supervised algorithm. The proposed algorithm provides 74.8% of accuracy which is better than the Naïve Bayes Algorithm.

**Keywords:** Data Mining · Classification algorithm · Naïve Bayes · Python · Multinomial Naïve Bayes

## 1 Introduction

Basically cardio-vascular diseases embrace the disorders of the blood vessels and the heart. The common form of heart disease is narrowing of blood vessels. According to recent survey, by the year of 2030 hardly 23.6 million of people would die by cardio-vascular problem due to the modern trend like improper diet, unhealthy food habit, huge pollution etc., are allowed to continue. The healthcare industry collects large amounts of heart disease data which unfortunately are not “mined” to discover hidden information for effective decision making [1].

According to the Herbert A. Simon (Nobel Prize winner in Artificial Intelligence in 1978), “The performance of the learning process is improved by experience”. In order to instruct the machine for appropriate decision making and to demonstrate excellent result and performance machine learning methodology is used [11].

Cardiovascular Disease (CVD) residue at the crest in the hierarchy of life threatening disease in the modern time. CVD deals with the heart and associated vascular conditions of the people. Blockage of the coronary arteries is one of the most familiar

causes of heart disease. The composed database contains together of numerical and categorical data. In order to filter the irrelevant data, data preprocessing technique like cleaning and filtering process are applied to the collected database [3].

### 1.1 Myocardial Infarction

The word myocardial infarction (MI) means damaged heart muscle. It is generally identified as heart attack. Infarction occurs when the part of the heart muscle get damaged. It occurs when the blood gush stops to a part of the heart causing injury to the heart muscle. It provides discomforts in jaw, neck, shoulder, arm and back of the patient. Due to the damage, it causes cardiac arrest for the patient by blocking the pathway of blood flow creates heart failure and irregular heartbeat.

## 2 Literature Review

In paper [1], the author explained study of PCA has been done which finds the minimum number of attributes required to enhance the precision of various supervised machine learning algorithms. Since data mining has various algorithms the author analyses the classification algorithm, decision tree and so on. The intention of the research is to study the classification algorithms to predict heart disease.

Rajkumar et al. [7] worked on supervised learning algorithm by detecting the heart disease among the patients. In order to classify the data the author used Tanagra tool and to assess the data 10 fold cross validation is used, finally the result are compared. The whole dataset is split into two sections, i.e., 80% data is used for training and 20% for testing. Among the various classification algorithms, the lower error ratio is produced by Naïve Bayes and the time taken to do the work is very least.

Florence et al. [8] proposed a structure which uses the classification algorithm like neural network and Decision tree (ID3) for the prediction of heart disease. The dataset for the research work is obtained from UCI machine learning repository. Supervised algorithms like Decision tree, CART, ID3 and C4.5 are used. The data which is collected from UCI is used to test the system. Results are generated by Neural Network and Decision Tree. The Rapid Miner Studio is used to predict the output.

Purusothaman et al. [9] have surveyed and compared different classification techniques for heart disease prediction. The authors used various classification techniques like ANN, Decision tree and Naïve Bayes. The classification algorithms like Decision tree, artificial neural network and Naïve Bayes provide 76%, 85% and 69% respectively. Since, the author used hybrid model, it produce the accuracy of 96%. Finally, it was concluded that hybrid model is dependable and predict the heart disease among patients with good accuracy.

In paper [11], the author defined that with the help of Naive Bayesian classification algorithm and Laplace smoothing technique the decision support system is developed. The proposed decision support system is supposed to let alone needless diagnosis test conducted in a patient and the delay in beginning appropriate treatment by quickly diagnosing heart disease in a patient. Presently the users use 13 attributes which prediction is more accurate since it has 86% accuracy.

### 3 Classification Algorithm

Fundamentally there are two types of methods available in data mining. They are classification and clustering. The Health care institutions usually follow the classification algorithm to predict the accurate result. Classification divides data samples into test data and training data and also fixes the target classes. For each and every data point the target class was fixed by classification algorithm. The training dataset helps to train the classifier whereas the correctness of the classifier is found by the test dataset [12].

Naïve Bayes classification is one of the simplest types of classification. Multinomial bayes type of classification used for the proposed work. Basically the datasets under the classification algorithm is divided in two. One third of the dataset is used as a test data and the remaining dataset is used as training data. The association between the values of the predictors and the target class are described in the training process of the classification algorithm. The predicted values are compared with the target values in a set of data in the classification models.

### 4 Naïve Bayes Algorithm

Naïve Bayes algorithm is one among the supervised learning technique based on Bayes' Theorem. It facility through a hypothesis of independence among predictors. The Bayes theorem follows on the conditional probability for the further classification of research work. The Bayesian Classification represents by statistical technique for classification of the dataset. In order to predict the label of a text, the Naïve Bayes algorithm uses the probability theory and Bayes theorem. In order to classify the text documents in an accurate manner, the naïve bayes classifier is used.

#### 4.1 Conditional Probability

$P(A|B)$  stands for “the conditional probability of A given B” else “the probability of A under the condition B”, i.e. the probability of some event A took place under the assumption of the event B.

The conditional probability is defined by;

$$P(A|B) = (P(A) * P(B|A))/(P(B))$$

### 5 Multinomial Naïve Bayes Algorithm

The initial supervised learning method which pioneered is multinomial Naive Bayes (NB) model, a probabilistic learning method. It equipment the Naive Bayes algorithm for multinomially distributed data. This classifier is suitable for classification with discrete feature. This algorithm is used when the data is distributed multinomially, i.e., multiple occurrences matter more. The distribution is parameterized by vectors

$\theta_y = (\theta_{y1}, \dots, \theta_{yn})$  for each class  $y$ , where  $n$  is the number of feature and  $\theta_{yi}$  is the probability  $P(x_i|y)$  of feature  $i$  appearing in a model belonging to class  $y$ .

The parameters  $\theta_y$  is estimated by a smoothed version of maximum likelihood, i.e. relative frequency counting:

$$\hat{\theta}_{yi} = \frac{N_{yi} + \alpha}{N_y + \alpha n}$$

where  $N_{yi} = \sum_{x \in T} x_i$  is the number of times feature  $i$  appears in a sample of class  $y$  in the training set  $T$ , and  $N_y = \sum_{i=1}^{|T|} N_{yi}$  is the total count of all features for class  $y$ .

The smoothing priors  $\alpha \geq 0$  accounts for features not present in the learning samples and prevents zero probabilities in further computations. Setting  $\alpha = 1$  is called Laplace smoothing, while  $\alpha < 1$  is called Lidstone smoothing. The probability of a document  $d$  being in class  $c$  is computed as:

$$P(c|d) \propto P(c) \prod_{1 \leq k \leq n_d} P(t_k|c)$$

- where  $P(t_k | c)$  is the conditional probability of term ' $t_k$ ' occurring in a document of class ' $c$ '.
- We interpret  $P(t_k | c)$  as a measure of how much evidence ' $t_k$ ' contributes that ' $c$ ' is the correct class.
- $P(c)$  is the prior probability of a text stirring in class ' $c$ '.
- $(t_1, t_2, \dots, t_{nd})$  are the tokens in ' $d$ ' that are part of the vocabulary we use for classification and ' $nd$ ' is the number of such tokens in ' $d$ '.

The following proposed algorithm is Modified Multinomial Naïve Bayes Algorithm. This algorithm helps us to foretell the heart disease among patients. The proposed algorithm provide accurate result compare to other classification algorithms.

In the proposed algorithm, the process begin by declaring the dataset as  $V$ , total number of terms as  $T$ ,  $C$  as class and count documents as  $N$ . In step 3 to 5, it generates the total length of data and set the membership as,  $c$  is the element of  $C$  and repeats the process. In the step 6 to 9, it count the documents in class and calculate the prior of  $c$  and concatenate the text of all documents in the class until the element found in the set.



---

Algorithm: Modified Multinomial Naïve Bayes

Input: MMNB (Dataset, count\_docs, class, Total number of terms)

Output: Accuracy percentage with training algorithm

---

```

1 Begin
2.   Total Dataset=V, Count Docs (D) = N, C=class, T=total number of
terms
3.   generate len(data)
4.   for each c ∈ C
5.     repeat
6.       Count the Docs in class (D,C)
7.       prior [c] ← Nc \ N
8.       concatenate text of all Docs in class
9.       until element found in the set
10.    for each t ∈ V
11.      repeat
12.        do Tct ← count token of terms (Textc, t)
13.        until the total terms counted
14.    for each t ∈ V
15.      repeat
16.        do condprob[t][c] ← [len(data)/2 -1]
17.        until conditional probability obtained
18.    Return V, prior, condprob
19. End

```

In step 10 to 13, it check whether ‘t’ is the set of V (total dataset) then repeat the same process until the total terms counted. In the step 14 to 19, check for each ‘t’ is the set of total dataset ‘V’, i.e., it check the condition for all the rows (place the probability) and calculate the conditional probability by dividing the total data by 2 minus 1 until the conditional probability obtained. Finally, it return the value of V, c and conditional probability.

## 6 K-Nearest Neighbor Algorithm

KNN is the simplest classification algorithm among the various supervised learning algorithms. The data points in the database are separated into several classes to predict the classification of a new sample point. KNN algorithm captures the information of all training data and classifies the new data based on a similarity.

The following is the output which is obtained by applying the SPSS statistics to the Cleveland database. The experimental analysis of KNN algorithm as shown in the following Table 1. This table explains the training and holdout data percentage clearly.

**Table 1.** Provide the case processing summary for K-Nearest Neighbor Algorithm

		N	Percent
Sample	Training	217	71.6%
	Holdout	86	28.4%
Valid		303	100.0%
Excluded		0	–
Total		303	–

## 7 Result and Discussion

In the proposed work the experimental measures is calculated by using the performance factors such as error rates and classification accuracy. The accuracy measure and the performance factors by class for the Naïve Bayes classifier is given in the following Table 2.

The following is correctness results provided by Modified Multinomial Naïve Bayes Algorithm for the given dataset:

**Table 2.** Performance factors for MMNB algorithm

Instances	Total number of instances	Percentage
Correctly classified	253	74.87%
Incorrectly classified	50	25.13%

Following Table 3 provide the comparison analysis of proposed work with existing algorithm.

**Table 3.** Comparison analysis of MMNB algorithm with existing algorithms

Classification algorithm	Accuracy %
Modified Multinomial Naïve Bayes	74.87%
K-Nearest Neighbour	71.6%
Naïve Bayes	70%

## 8 Conclusion and Future Work

Prediction of heart disease with least number of attribute is a challenging task in Data Mining [7]. In order to predict the heart disease among the patients 14 attributes are used from UCI machine learning repository of heart disease. Different models are worn to envisage the incidence of heart disease. The proposed work was Modified Multinomial Naïve Bayes algorithm which uses the probability theorem to get the accurate result.

In recent studies, with the introduction of machine learning and medical sciences, one can actually help in preventing any such a kind of disease. For making a good decision, machine learning helps in extracting relevant data from huge database which are available in hospital. By using supervised learning algorithm, various kinds of techniques have been applied in the prediction of heart diseases. In future, unsupervised learning algorithm can be implemented to the medical dataset and can get better accuracy.

## References

1. Dhomse Kanchan, B., Mahale Kishor, M.: Study of machine learning algorithms for special disease prediction using principal of component analysis. In: Proceedings of IEEE Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC) (2016)
2. Gudadhe, M., Wankhade, K., Dongre, S.: Decision support system for heart disease based on support vector machine and artificial neural network. In: Proceedings of International Conference on Computer and Communication Technology (ICCT), pp. 741–745 (2010)
3. Singh, P., Singh, S., Pandi-Jain, G.S.: Effective heart disease prediction system using data mining techniques. *Int. J. Nano Med.* **13**, 121–124 (2018)
4. Sayad, A.T., Halkarnikar, P.P.: Diagnosis of heart disease using neural network approach. In: International Journal of Advance Science of Engineering Technology, vol. 2, pp. 88–92 (2014). ISSN 2321-9009
5. Bangi, S., Gadakh, P., Gaikwad, P., Rajpure, P.: Survey paper on prediction of heart disease using data mining technique. *Int. J. Recent Trends Eng. Res. (IJRTER)* **02**(03), 21–24 (2016)
6. World Health Organisation (WHO) Report on Cardiovascular Disease (CVDs), Fact Sheet (2016)
7. Rajkumar, A., Sophia Reena, G.: Diagnosis of heart disease using data mining algorithms. *Glob. J. Comput. Sci. Technol.* **10**(10), 38–43 (2010)
8. Florence, S., Bhuvanewari Amma, N.G., Annapoorani, G., Malathi, K.: Predicting the risk of heart attacks using neural network and decision tree. *Int. J. Innovative Res. Comput. Commun. Eng.* **2**(11), 7025–7028 (2014). ISSN (Online) 2320-9801
9. Purusothaman, G., Krishnakumari, P.: A survey of data mining techniques on risk prediction: heart disease. *Indian J. Sci. Technol.* **8**(12), 1–5 (2015)
10. Cherian, V., Bindu, M.S.: Heart disease prediction using Naïve Bayes algorithm and Laplace smoothing technique. *Int. J. Comput. Sci. Trends Technol. (IJCST)* **5**(2), 68–73 (2017)
11. Santhanam, T., Ephzibah, E.P.: Heart disease classification using PCA and feed forward neural networks. In: Proceedings of First International Conference, Mining Intelligence and Knowledge Exploration (MIKE), Part of Lecture Note in Artificial Intelligence (LNAI), vol. 8284, pp. 90–99 (2013)
12. Tomar, D., Agarwal, S.: A survey on data mining approaches for healthcare. *Int. J. Bio-Sci. Bio-Technol.* **5**, 241–266 (2013)



# Discovering Web Users' Web Access Pattern Based on Psychology

E. Manohar<sup>1</sup>(✉) and E. Anandha Banu<sup>2</sup>

<sup>1</sup> Computer Science and Engineering, Francis Xavier Engineering College,  
Tirunelveli, India

manohar2k@ymail.com

<sup>2</sup> Electrical and Electronics Engineering, Panimalar Engineering College,  
Chennai, India

banu3k@yahoo.co.in

**Abstract.** The web access behaviour of the web users is influenced by customers' state of mind. The influence of the customers' psychology in web access behaviour is analysed in this paper. Positive emotion along with positive mood induces better attitude in the web users' behaviour whereas negative emotion along with negative mood induces a negative attitude among web users. The state of human mind changes along with the temporal property based on the emotion and mood. The statistical study on the historical data is used to discover the influence of mental state which affects the web users' behaviour. Various machine learning algorithms along with statistics and psychology are studied to discover the knowledge about the web users' access behaviour.

**Keywords:** Psychology · E-commerce · Web navigation · Knowledge discovery

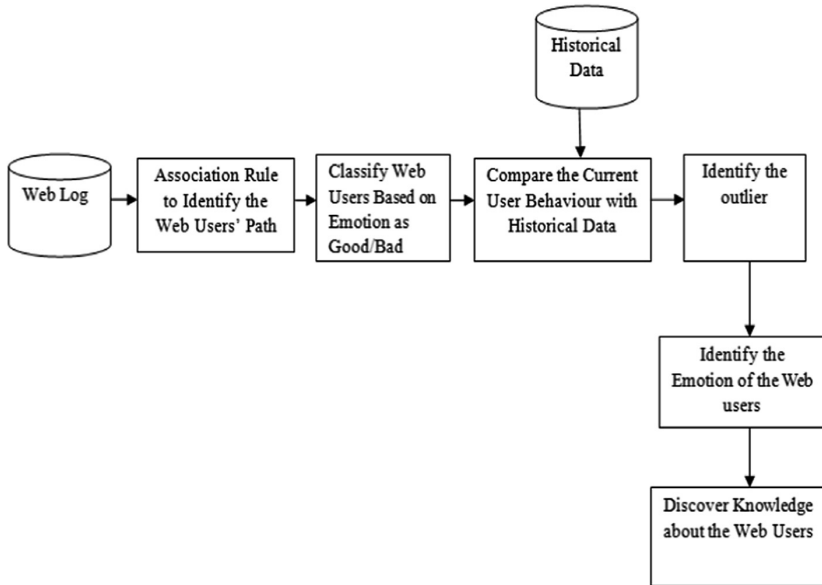
## 1 Introduction

The usage of the web has increased tremendously. The web designers always try to deliver the website more effectively in order to have more number of customers. The customers' state of mind is a major factor that influences the web users' behaviour. The psychology of the customers' web access behaviour changes based on their mood and emotion with respect to temporal property. Emotions are short-lived feelings, whereas mood is permanent feeling. Emotion can be categorized as happiness, sadness, contempt, anger, fear, surprise and disgust. Mood can be categorized as occasional mood and non-occasional mood. Mood occurs because of personal emotion or of the society. The web users' behaviour analysis is very important in various web applications such as web search and e-commerce [1]. The users' personal involvement inventory scale is introduced to measure the product involvement [2]. The inventory scale consists of seven point items. The web page advertisement formats have different effects on the advertisement attitude [3]. The user psychology is generally based on mood and emotions. The mood is a global feeling [4]. The positive emotion appeals to perform better even in low involvement situations [5]. The web page avoidance might encompass intentional refraining from the future action of the web page [6]. Therefore,

whether the viewers read the web page or not may not affect the effectiveness of the web page. Emotional web page may moderate the mood effect on web page effectiveness [7]. The most common categorization dimensions are information with respect to emotion which is investigated in most of the previous researches [8]. The web user clicking stream is used to track the content of the visited pages where mood is not considered for the system [9]. The catching and prefetching of click stream is important, since the time criterion is crucial [10]. Clustering techniques are used to group the similarity of the web users' session [11]. Genfen et al. [12] discuss the usage difference in email based on the gender. Yao et al. [13] introduced a hybrid recommendation system by combining context based features and web services. A neighborhood based collaborative filtering approach to predict the unknown value is proposed by Wu et al. [14]. The web user click is identified based on the hidden semi Markov model which is used to identify the path of the web users [15]. The Markov model is used to identify the anomaly in web users' browsing behaviour [16]. Lee et al. [17] introduce an automatic user need identification system to identify the web users' need. Identifying the web user click to discover the path of web user can be implemented based on dependency graph [18]. The understanding of the web traffic is essential in discovering knowledge about the web users [19]. Kang et al. [20] introduced a web service recommendation system based on usage history which incorporates both user interest and quality of service preference. The web services with best quality of service values on certain quality of service criterion exploiting user potential quality of service preferences may be mined from the web users' usage history [21]. Most of the quality of service was based on collaborative filtering technique [22].

## 2 Proposed Methodology

The study examines the psychological factor which influences the web users' web access behaviour. Internet provides hybrid information where web users can navigate the information according to their needs. To identify the user psychology, a statistical study by using machine learning technique is used to discover the web users' behaviour. The web log file is going to be considered as the input and the discovered knowledge about the user is the final output of this system. The path of each web user's session is completed by using the association rule. The web users are classified based on their emotions. In the human psychology, when the person is not in a good emotion, he is either too fast or too slow in his behavior. Based on the rule, the web users' web log file is going to be analyzed. Then the current user session behaviour is compared with the existing user session behaviour by using outlier analysis. By identifying the outlier, the mood of the user can be identified. If there is more number of outlier, then we can arrive at a conclusion that the mood of the web user is not normal. Then by analysing the outlier, it may be concluded that if the data are too much distance, then the user may be in occasional mood and if the data are not that much distance, then we may conclude that the user may be in non-occasional mood. The mood may prevail because of the social festival or of the personal festival.



**Fig. 1.** Architecture of psychology based knowledge discovery system

The Fig. 1 shows the architecture of the proposed system. Here, the statistical analysis along with the machine learning technique is applied to discover knowledge about the web users.

### 2.1 Identify the Web Users' Path

The web users' path analysis is very important in identifying the web users' behaviour. It is easy for anyone to identify the human emotion by visibly monitoring any person. But it is little difficult to identify their emotions without any visual image. Human facial index is the important and widely used method to identify the human behaviour. Here the path of the web users is to be used for identifying their behaviour. The length of the path and the time spent over each web page is to be identified; so that the current emotion of the web user can be discovered. For that, support and confidence is to be calculated. Support indicates how frequently the web users access the website and confidence indicates the number of times the users access the path.

### 2.2 Classify the Users Based on Emotion

After analyzing the path of web users and time spent by the user over a web page, classify the web users by using decision tree classification. Based on the analysis, we can categorize the emotion of a user into three categories: 1. Positive emotions, 2. Bad

emotions, 3. Normal Emotion. If the user is in positive emotion, then the user shows a good attitude in the usage behaviour. If the user is in negative emotion, then he will show a bad attitude which will affect the web usage behaviour.

### **2.3 Outlier Analysis on Web Users' Behaviour**

The web users' current behaviour is compared with that of their existing behaviour. The existing behaviour of the web users will be there in a database. The knowledge about the web users will be there in the historical database. The behaviour of the web users which is already stored in the historical database is clustered with current web users' data. Then outlier of the cluster is identified and it shows the deviation in web user's web access. If the distance between data which falls outside the cluster area is short, then it shows that the web user is in occasional mood. If the distance between data which falls outside the cluster area is long, then it shows that the web user is in non occasional mood. If the web user is in positive mood, then their web access behaviour attitude will be automatically good. If the user is in negative mood, then it automatically affects the web users' web access behaviour.

### **2.4 Discovery of Knowledge**

Based on the various psychological analysis, the knowledge about every user and his behaviour based on his emotion and mood can be identified. By analyzing the person under various psychological states, the web designer can present the website in a better way. This analysis is very much essential for any website, especially e-commerce site and to promote the advertisement in any website. If the web designer presents the website to the web users according to the psychological factor of the web users, then it will boost the popularity of the website among new web users and also it is very effective in retaining the existing web users.

## **3 Result and Analysis**

The effectiveness of the system is analyzed by comparing two methods. They are indirect method and direct method. The knowledge discovered by using statistical data and machine learning techniques is the indirect method. To ensure that the indirect method is correct, the direct method is to be compared with indirect method. In direct method, a direct survey is to be conducted to discover the knowledge about the web users. To ensure the effectiveness of this method, the recall, precision and accuracy is to be calculated. To measure the accuracy, 20 participants are analyzed for a week. The 20 participants' browsing behaviour is measured using the proposed technique and compared with the survey conducted among the participants to ensure the accuracy of the system.

**Table 1.** Emotion based on indirect method

ID of the users'	Number of sessions	Session of positive emotion in percentage	Session of negative emotion in percentage	Session of normal emotion in percentage
ID1	15	33	20	47
ID2	8	50	24	55
ID3	13	54	26	26
ID4	17	59	23	21
ID5	6	67	23	13
ID6	12	67	21	13
ID7	10	40	23	40
ID8	8	50	24	30
ID9	7	29	23	51
ID10	13	38	23	42
ID11	12	50	22	30
ID12	15	33	27	47
ID13	17	24	21	56
ID14	10	20	26	60
ID15	12	33	23	47
ID16	9	33	24	47
ID17	7	57	25	51
ID18	6	33	23	47
ID19	13	31	24	49
ID20	11	45	23	35

The Table 1 shows the measurement of web users behaviour based on the study conducted through the proposed system. The calculated value is expressed in terms of percentage. The web users' emotion is represented as positive emotion, negative emotion and normal emotion.

**Table 2.** Emotion based on direct method

ID of the users	Session of positive emotion in percentage	Session of negative emotion in percentage	Session of normal emotion in percentage
ID1	30	21	50
ID2	16	24	60
ID3	50	25	24
ID4	55	23	22
ID5	63	22	14
ID6	64	23	15
ID7	36	23	41

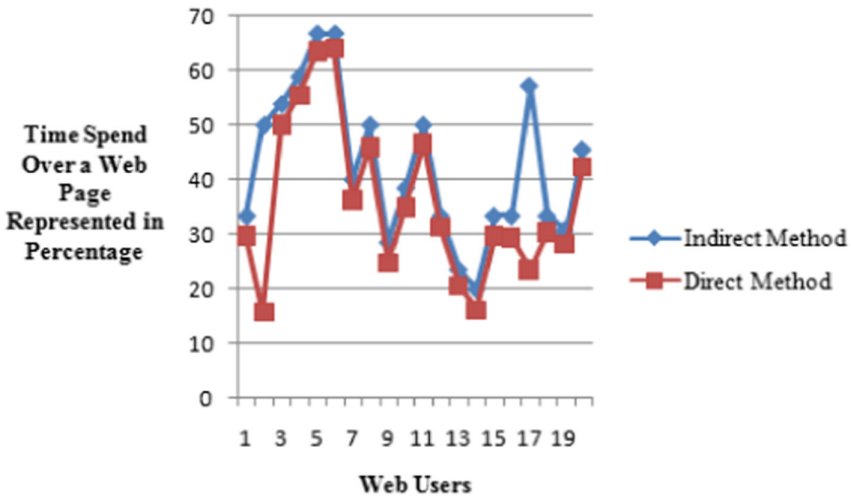
(continued)



**Table 2.** (continued)

ID of the users	Session of positive emotion in percentage	Session of negative emotion in percentage	Session of normal emotion in percentage
ID8	46	24	30
ID9	25	22	52
ID10	35	22	42
ID11	47	22	32
ID12	31	26	42
ID13	21	21	58
ID14	16	24	58
ID15	30	23	47
ID16	29	24	47
ID17	24	24	51
ID18	30	23	47
ID19	28	24	48
ID20	42	22	35

The measurement of web users’ web access based on the survey conducted among the web users is shown in Table 2. In the direct method, the web users express their web access details by mentioning the number of times they access the website with positive emotion, negative emotion and normal emotion.



**Fig. 2.** Session of positive emotion

The Fig. 2 analyses the web users' web access behavior based on positive emotions using direct method and indirect method. The graph shows that the measurement through direct method and indirect method represent similar results.

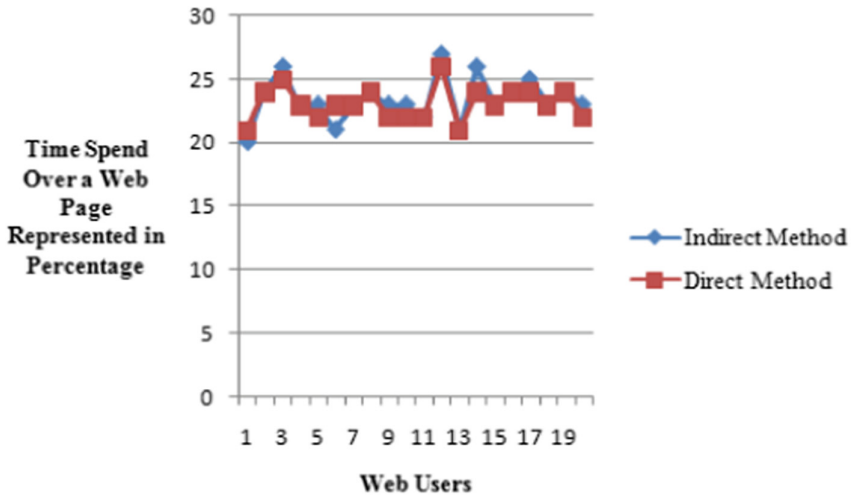


Fig. 3. Session of negative emotion

The session of negative emotion of the various web users calculated through direct method and indirect method is shown in the Fig. 3. It represents the access behaviour of web users during their negative mood. The result shows that the knowledge discovered through our proposed method is similar to direct method which represents that the proposed method is accurate in discovering knowledge.

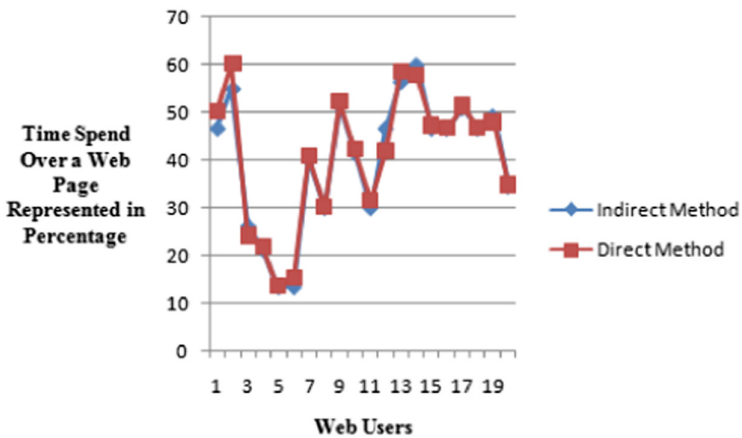


Fig. 4. Session of normal emotion

The web users' web access based on the session when the user is in normal emotion is shown in Fig. 4. The graph shows the measurement made through both direct method and indirect method. The graph represents the web access prediction during their normal emotion. It also suggests that the proposed method is accurate in predicting the knowledge.

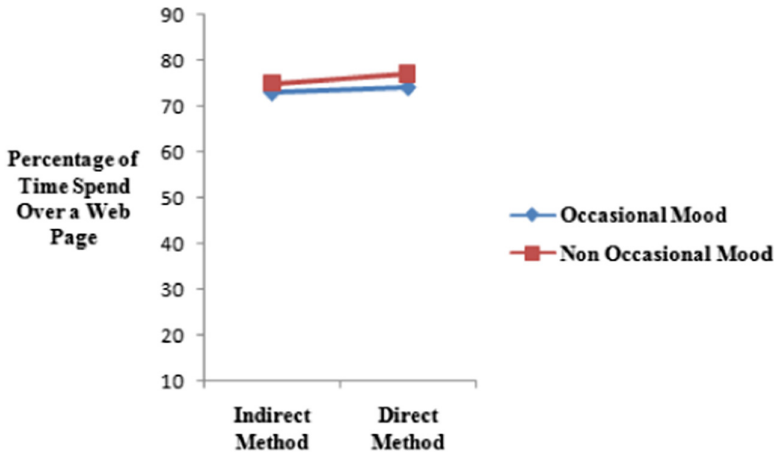


Fig. 5. Analysis of web usage based on mood

The web users' browsing behaviour based on the mood of the web users is shown in the Fig. 5. The web users' browsing behaviour is classified as occasional mood and non occasional mood. The analysis made through direct method and indirect method is shown in the Fig. 5. The result shows the interest of web users analysed through direct method is accurate.

## 4 Conclusion

Discovery of knowledge about the web users' web access behaviour is the challenging and essential thing in the current technological development, growth in the number of websites and the rapid increase in the web users' rate. The knowledge discovery is very essential in e-commerce, web advertisement and web personalization. Although there are various techniques available in discovering knowledge about web users' web access behavior, all the techniques fail to give importance to the psychological factor which is the driving factor of the web users' web access behaviour. In this system, the psychological factor of the web users is identified and the influence of the psychological factor over their web access behavior is also discovered. The recall, precision and accuracy shows the effectiveness of the knowledge discovered through this system.

## References

1. Choi, D.H., Ahn, B.S.: Eliciting customer preferences for products from navigation behaviour on the web: a multicriteria decision approach with implicit feed back. *IEEE Trans. Syst. Man Cybern.* **39**(4), 880–889 (2009)
2. Mittal, B.: A comparative analysis of four scales of consumer involvement. *Psychol. Mark.* **12**(7), 663–682 (1995)
3. Burns, K.S., Lutz, R.J.: The function of format: consumer response to six online advertisement format. *J. Advertising* **35**(1), 55–63 (2006)
4. Richard, P.B., Mahesh, G., Prashanth, U.N.: The role of emotions in marketing. *Acad. Mark. Sci.* **27**(2), 184–206 (1999)
5. Dens, N., Pelsmacker, P.D.: Consumer response to different advertising appeals for new products: the moderating influence of branding strategy and product category involvement. *Brand Manag.* **18**(1), 50–65 (2010)
6. Cho, C.H., Cheon, H.J.: Why do people avoid advertising on the internet? *J. Advertising* **33**(4), 89–97 (2004)
7. Geuens, M., De Pelsmacker, P., Fasseur, T.: Emotional advertising: revisiting the role of product category. In: *AMA Winter Educators Conference Proceedings*, vol. 18, pp. 322–324 (2007)
8. Lee, J.G., Thorson, E.: Cognitive and emotional processes in individuals and commercial web sites. *J. Bus. Psychol.* **24**(1), 105–115 (2009)
9. Deane, J., Paathak, P.: Ontological analysis of web surf history to maximize the click-through probability of web advertisements. *Decis. Support Syst.* **47**(4), 364–373 (2009)
10. Xu, J., Liu, J., Jia, X.: Catching and perfecting for web content distribution. *Comput. Sci. Eng.* **6**(4), 54–59 (2004)
11. Bianco, A., Mardente, G., Mellia, M., Munafo, M., Muscariello, L.: Web user session characterization via clustering techniques. In: *GLOBECOM 2005* (2005)
12. Gefen, D., Straub, D.W.: Gender and gender variation in weblogs. *J. Sociolinguistics* **10**(4), 439–459 (2006)
13. Yao, L., Sheng, Q.Z., Segev, A., Yu, J.: Recommending web services via combining collaborative filtering with content based features, pp. 42–49. *IEEE Computer Society* (2013)
14. Wu, J., Cheng, L., Feng, Y., Zheng, Z., Zhou, M.C., Wu, Z.: Predicting quality of services for selection by neighborhood based collaborative filtering. *IEEE Trans. Syst.* **43**(2), 428–439 (2013)
15. Xu, C., Du, C., Zhao, G.F., Yu, S.: A novel model for user clicks identification based on hidden semi-Markov. *J. Netw. Comput. Appl.* **36**, 791–798 (2012)
16. Xie, Y., Yu, S.Z.: A large scale hidden semi Markov model for anomaly detection on user browsing behaviour. *ACM Trans. Networking* **17**(1), 54–65 (2009)
17. Zhang, Y., Chen, W., Wang, D., Yang, Q.: User click modeling for understanding and predicting search behaviour. In: *ACM International Conference on Knowledge Discovery and Data Mining*, pp. 1388–1396 (2011)
18. Liu, J., Fang, C., Ansari, N.: Identifying user clicks based on dependency graph. In: *IEEE Wireless and Optical Communication Conference*, pp. 1–5 (2014)
19. Lhm, S., Pai, V.S.: Towards understanding modern web traffic. In: *ACIM SIGCOMM Conference on Internet Measurement*, pp. 295–312 (2011)
20. Kang, G., Liu, J., Tang, M., Liu, X., Cao, B., Xu, Y.: AWSR: active web service recommendation based on usage history, pp. 186–193. *IEEE Computer Society* (2012)

21. Gong, M., Xu, Z., Xu, L., Li, Y., Chen, L.: Recommendation web service based on user relationship and preferences, pp. 380–386. IEEE Computer Society (2013)
22. Jiang, Y., Liu, J., Tang, M., Liu, X.: An effective web service recommendation based on personalized collaborative filtering, pp. 211–218. IEEE Computer Society (2011)



# Non-invasive Haemoglobin Measurement Using Photoplethysmographic Technique

S. Selva Nidhyananthan, R. Dharshana Shahini<sup>(✉)</sup>, and S. Hari Priya

Mepco Schlenk Engineering College, Sivakasi, India  
nidhyan@mepcoeng.ac.in, shahini.r98@gmail.com,  
haripriyal9897@gmail.com

**Abstract.** The important component for complete blood count is haemoglobin. The normal Hemoglobin (Hb) concentration in blood is about 12–15 gm/dl for females, 13.5–17.5 gm/dl for males and 11 to 16 g/dl for children. The invasive methods are used to measure the Haemoglobin concentration by ejecting the blood from the patient and subsequently analyzed. The disadvantages of the invasive methods are it causes delay between the blood collection and its analysis causes pain while ejecting the blood and the temperature should be maintained for the blood samples during transportation. The non-invasive method overcomes these disadvantages by pain free analysis of the blood, real time analysis. Proposed technique has 96.56% accuracy compared to clinical measurements.

**Keywords:** Haemoglobin · Near infrared · Non-invasive

## 1 Introduction

The red blood corpuscles contain the Hemoglobin (Hb) which is used for the transportation of oxygen from the lungs to the body tissues and the carbon dioxide from body tissues to the lungs. Hb is important for oxygen transportation. It is composed of globin which is a protein compound and heme which is an iron compound. The value of the haemoglobin differs from person to person according to the condition of the person. The value of the haemoglobin may be higher or lower than the normal range which may result in different types of diseases like anemia and polycythemia. Anemia is caused when the haemoglobin concentration is lower than the normal range and polycythemia is caused when the haemoglobin concentration is higher than the normal range. Anemia is the disease which is caused due to the kidney, liver related diseases and iron deficiency.

In the invasive methods, the blood is drawn by pricking the finger. The collected blood sample is sent to the laboratories for analysis. During the transportation the temperature of the blood sample should be maintained [11]. In the laboratories the blood sample is analyzed. This method takes more time. The non-invasive method is done by passing the near infrared light of 940 nm wavelength [10]. The light transmitted through the finger is detected using a photo detector [6]. The obtained signal is amplified and then analyzed to find the haemoglobin concentration.

*Jens Kraith, Ulrich Timm, HartmutEwald, Elfed Lewis* on 2011 have proposed a method in which the absorption coefficient of blood which differs at different wave-length is used to calculate the optical absorbability characteristics of blood [3]. The measured signals and the ratio between the peak to peak pulse amplitudes are used for a calculation of these parameters. *A. Mohamed Abbas, S. Ashok, S. Prabhu Kumar and P. Balavenkateswarlu* on 2016 used Sigview software to record the signal and then processed it using MatLab [1]. Then the signal was converted into image. The regression analysis was taken for the obtained values. Variance and mean values are compared and the output was plotted to determine the haemoglobin content. *Tatiparti Padma, Pinjala Jahnavi* on 2018 recorded the signal using Sigview software and regression analysis is done [5].

## 2 Proposed Method

### 2.1 Hardware Implementation

The hardware components used are 940 nm infrared photodetector [9], opamp and C2000. The 940 nm infrared LED is used as a transmitter [2]. The light is passed through the finger. The photo detector is used to convert the light into electrical signal [7]. The output voltage depends on the infrared signal it receives [4]. The non-inverting operational amplifier is used to amplify the signal for further analysis [8]. The Figs. 1 and 2 show the block diagram and transmitter circuit.

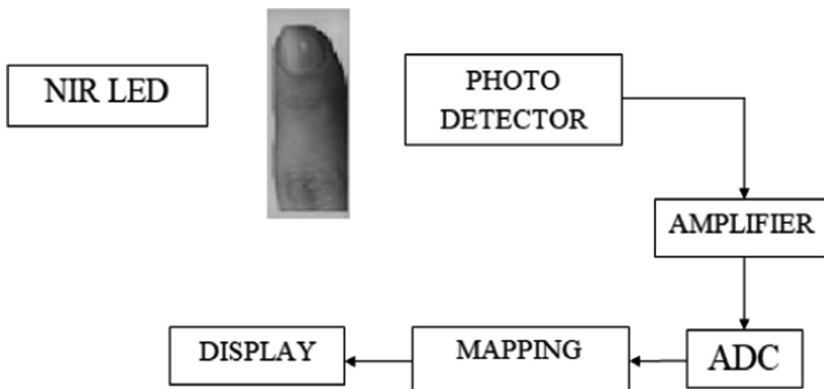
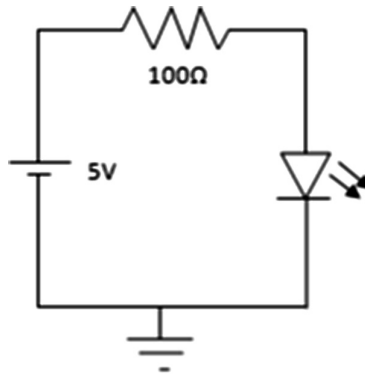


Fig. 1. Block diagram



**Fig. 2.** IRLED transmitter circuit

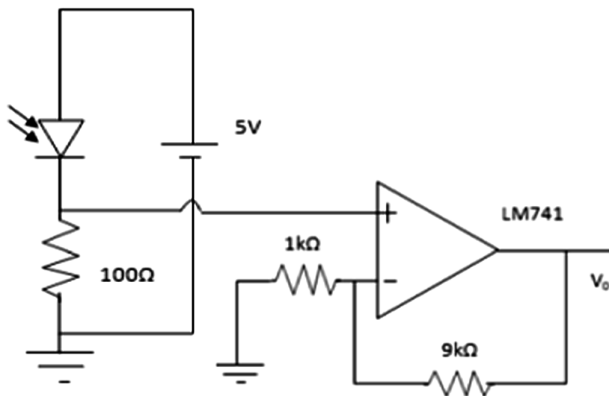
The non-inverting operational amplifier of gain 10 is designed by the Eqs. (1) and (2). The amplified signal is then converted into digital value by analog to digital conversion.

$$A_v = V_o/V_i \tag{1}$$

$$A_v = 1 + (R_f/R_1) \tag{2}$$

where  $A_v$  is the gain of the non-inverting amplifier which is 10.  $R_f$  is the feedback resistance which is chosen as 9 kΩ and  $R_1$  is chosen as 1 kΩ.

The Fig. 3 below is the amplifier circuit for the photo detector output.



**Fig. 3.** Non-inverting amplifier circuit for photodetected output

The C2000 is used to calculate the haemoglobin value using the digitally converted value. Finally, the calculated value is displayed using Liquid Crystal Display (LCD).



## 2.2 Software Development

**C2000 Launchpad.** The software tool used for this non-invasive method is C2000. The analog to digital conversion is done using C2000. C2000 has a 12-bit single-ended input or 16-bit differential inputs, single analog to digital converter with dual sample and hold or multiple analog to digital converters with single sample-and-hold. This allows for sequential or simultaneous sampling operation. The conversion speed is from 1MSPS to greater than 12MSPS.

The C2000 launchpad is shown in the Fig. 4.

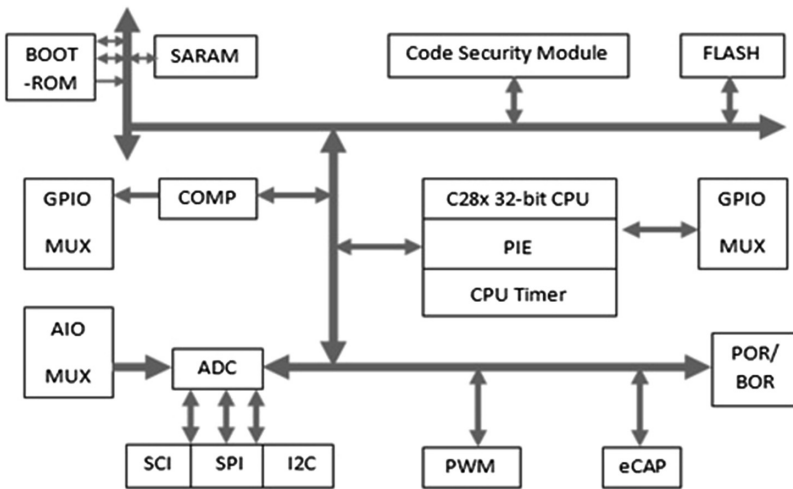


Fig. 4. The functional block diagram of C2000 Launchpad

**Regression Analysis.** The actual haemoglobin counts for different persons were found using the invasive methods. The amplified voltage values are recorded for the same persons [12]. The regression analysis is used to find the regression equation by plotting a graph between the values obtained by the invasive method and the amplified voltage values.

The obtained equation is given in (3),

$$y = -0.8331x + 19.94 \tag{3}$$

where  $y$  is the hemoglobin count in milligram per deciliter (mg/dl) and  $x$  is the output voltage in volt (V).

The percentage error between the invasive and non-invasive method was calculated as in (4),

$$\text{Percentage Error} = \frac{(\text{Hemoglobin}_{\text{invasive}} - \text{Hemoglobin}_{\text{non-invasive}}) * 100\%}{\text{Hemoglobin}_{\text{non-invasive}}} \quad (4)$$

### 3 Results

The index finger is placed in between the 940 nm near infrared and the photo detector. The photo detector converts the light into electrical signal. The signal is amplified by an amplifier with gain of 10 in order to strengthen the signal.

The amplified signal is then converted into digital value by using the C2000 launchpad and the calculations are done to find the haemoglobin value. Finally, the result is displayed in LCD.

The percentage of the error between the values obtained from the traditional invasive method and the non-invasive method is about ±3.44%.

The Table 1 shows the relationship between the haemoglobin values for both the invasive and non-invasive methods for different persons and the percentage error.

**Table 1.** Relationship between the haemoglobin values obtained by the invasive and non-invasive methods

Name	Photo detector voltage (V)	Mapped value (mg/dl)	Lab value (mg/dl)	Error (%)
Person1	10.9	10.85	11.3	4
Person2	11.5	10.35	10	3
Person3	9.2	12.27	12.9	5
Person4	9.6	11.94	12.5	4.7
Person5	9.6	11.94	12	0.5
<b>Average error</b>				3.44%
<b>Average accuracy</b>				96.56%

### 4 Conclusion

The non-invasive method reduces the delay between the collection and analysis of blood and thus provides real time analysis. This method also avoids the infection caused due to the pricking of blood in the traditional method since, it is non-invasive. It does not require any experts help to eject the blood. The proposed Non-Invasive Haemoglobin Measurement Using Photoplethysmographic Technique has achieved 96.56% accuracy which is sufficient for commercial non-invasive Haemoglobin measuring device development.

## References

1. Mohamed Abbas, A., Ashok, S., Prabhu Kumar, S., Balavenkateswarlu, P.: Haemoglobin detection in blood by signal to image scanning using Photo-Plethysmo-Graphic-Technique (PPG). *Indian J. Sci. Technol.* **9**(1) (2016). <https://doi.org/10.17485/ijst/2016/v9i1/85764>
2. Sharma, P., Kumar, A., Kumar, G., Sanjana, Km.: Estimation of haemoglobin using optical sensor based system. *Int. J. Adv. Res. Electr. Electron. Instrum. Eng.* **7**(4) (2018)
3. Kraitl, J., Timm, U., Ewald, H., Lewis, E.: Non-invasive sensor for an in vivo hemoglobin measurement. In: *SENSORS 2011*. IEEE (2011)
4. Bobade, C.D., Patil, M.S.: Non-invasive monitoring of glucose level in blood using near-infrared spectroscopy. *Int. J. Recent Trends Eng. Res. (IJRTER)* **02**(06) (2016)
5. Padma, T., Jahnavi, P.: Non-invasive haemoglobin estimation through embedded technology on mobile application. *Int. J. Appl. Eng. Res.* **13**(10) (2018). ISSN 0973-4562
6. Buda, R.A., Mohd. Addi, M.: A portable non-invasive blood glucose monitoring device. In: *IEEE Conference on Biomedical Engineering and Sciences*, 8–10 December 2014, Miri (2014)
7. Timm, U., Lewis, E., McGrath, D., Kraitl, J., Ewald, H.: LED based sensor system for non-invasive measurement of the haemoglobin concentration in human blood. In: *ICBME 2008, Proceedings 23*, pp. 825–828 (2009)
8. Pavithra, A.G., Menesha Karan, D., Ajith Kumar, D., Anu Shalin, P.S.: Non invasive technique to measure glucose and haemoglobin level in blood using NIR-occlusion spectroscopy. *Int. J. Sci. Res. Manag. (IJSRM)* **2**(4), 756–759 (2013)
9. Kumar, R., Ranganathan, H.: Non invasive sensor technology for total haemoglobin measurement in blood. *J. Ind. Intell. Inf.* **1**(4) (2013)
10. Narkhede, P., Dhalwar, S., Karthikeyan, B.: NIR based non-invasive blood glucose measurement. *Indian J. Sci. Technol.* **9**(41) (2016). <https://doi.org/10.17485/ijst/2016/v9i41/98996>
11. Haxha, S., Jhoja, J.: Optical based noninvasive glucose monitoring sensor prototype. *IEEE Photonics J.* **8**(6), 1–11 (2016)
12. Ali, H., Bensaali, F., Jaber, F.: Novel approach to non-invasive blood glucose monitoring based on transmittance and refraction of visible laser light. *IEEE Access* (2017)



# A Novel Method to Safeguard Patients Details in IoT Healthcare Sector Using Encryption Techniques

R. Venkat Tejas<sup>(✉)</sup> and N. Rakesh

Department of Computer Science and Engineering, Amrita School of Engineering, Bengaluru, Amrita Vishwa Vidyapeetham, Bengaluru, India  
venkattejas96@gmail.com, n\_rakesh@blr.amrita.edu

**Abstract.** Internet has become a part of our daily life. Most of the communications or the transfer of the data across the globe is happening over the internet. With Internet of Things [IoT], the devices can transmit data with each other over the internet. As the internet play a crucial role, the security of the data also becomes important. Confidentiality is important in the healthcare sector where encryption plays an important role. There are many effective encryption algorithms available, but through this work we are proposing a novel method that aims at adding the randomness to the encryption algorithm. The random number generation technique used in this paper is Web Scraping, here the data is scraped from the web page where the data gets constantly updated which adds to the randomness. The random number generation module is added to the existing encryption algorithm and the encryption algorithm is tested on different file sizes to test the level of encryption.

**Keywords:** IOT · Random number generation · Encryption · Web Scraping · Security

## 1 Introduction

Internet provides an interconnected environment which enables the devices to communicate universally using standard protocols and helps in connecting various random and heterogeneous networks like business, academics, governments etc. Internet can be seen everywhere around us and it has come into the hands of each and every person. The issues with security in Internet of Things bring a serious threat to the applications using it. The attackers can use unusual techniques in various layers of the IoT. As the IoT technology develops there is always a serious pressure of cyberattacks becoming more physical threats. One of the main concerns in the designing of the IoT network is Data security. This paper focuses on improving the security by adding random number generation module to the encryption algorithm.

## 2 Related Works

Jha and Shahi et al. [1] propose a mechanism to ensure encryption for an end to end scenario and for communications in embedded systems. The proposed system uses a system which is a matrix and consists of numbers as an access key. The matrix which is

used is equivalent to both including the sender and the receiver. Every instance at which a connection is made a unique key is picked up from the matrix. Each time the device is connected to the network a password is given. The individual password which is generated is converted into its corresponding or equivalent ASCII value. There is already an predefined series which is set which defines that the first ASCII value present in the series. Similarly the consecutive ASCII values are multiplied with its consecutive values defined. The results generated which are numbers were additionally given more security or encryption by utilizing the key which is generated using the matrix where the cipher text is given as  $\text{key} + 5x$ . The 'x' was the value obtained from the previous step. Device will be reset if the value in the matrix has reached maximum. In the decryption process the matrix key similar to the encryption key was used. To access a key similar procedure was used but now the decipher text was obtained using the equation  $x = (\text{C-key})/5$ . The proposed mechanism is a useful way and is also a unique way which can be implemented in real time and can also be tested on embedded systems under real time conditions.

Lakshmi et al. [2] studied a case of applying the Diffie-Hellman algorithm on the embedded device. Diffie-Hellman cryptography algorithm has been implemented on the embedded devices communicating over the Ethernet. The implementation was as follows, Raspberry Pi was configured as server by porting Raspberrian OS onto it and the application was written in C language. As a server it could send and receive messages. The client in this work was an Arduino Uno which was programmed and compiled using an IDE tool. An ethernet connection was first established using static IP. The client was then connected to the server using the port number. They analyzed that Raspberry Pi and Arduino work well when the parameters selected are within the range. Fast modular exponentiation was used to avoid using the direct method of calculation. The method simplifies the complexity and makes it faster. They also concluded that it is possible to decode the hidden key by looking at the information from the power consumption or the electromagnetic analysis. Fast modular exponentiation was used for computing which is otherwise not possible in Arduino or Raspberry Pi. Drawbacks mentioned in this paper is that the communication is done over the pre assigned port which can be easily traced by third parties.

Majumder and Sinha et al. [3] proposed an innovative algorithm which uses the twitter data stream to generate the keys which will be used for communication in IOT securely. The approach was of the idea that on the theory the twitter messages also known as tweets are independently generated by several people on the internet which would be the most random sequence. Periodically a large number of tweets were taken from the twitter streaming API. The whitespaces, punctuations, emoticons and others were eliminated. The remaining characters left in the tweet would be the count. A random count of M was selected and only the first M characters starting from the left were selected. For every S size of bytes the number of keys which are to be generate vary. To verify the randomness they made use of the standard procedures which are provided by the NIST test suite. When a dataset having 10,000 characters was chosen in theory even for big dataset of key words a low proportion or amount of values was found. But the amount of values which would pass the test will always increase when the characters increase in the dataset. For a size of 4 bytes the key used to transmit a session of 350 MB

appeared to be small which is negligible. For a key size using 256 bytes the computation time making the proposed system suitable for random key generation.

Tao et al. [4] proposes a system where it mainly deals with privacy attacks including data breaching, data integrity and data collision. He proposes a healthcare system named SecureData to tackle the above mentioned physical attacks. It includes two techniques FPGA Hardware-based cipher algorithm and secret software share algorithm named KATAN. This algorithm has been used to optimize on the hardware platform whereas the secret cipher sharing technique is used to prevent the patient's privacy. The results in the paper show the effect of the algorithms on the Fpga board and its inefficiency where many algorithms cannot be applied on the board because of the computational complexity.

Philip et al. [5] made a survey on all the available lightweight cryptographic algorithms which can be applied on the embedded devices. Different lightweight algorithms are KATAN, Humming Bird, SIMON, Espresso and many others. Comparison of the algorithms have been presented based on the key size, area, throughput, number of rounds, and the type of network. The results are useful as they give an insight into the algorithms which are application specific and the limitations in its wide range of use.

Kumar et al. [6] and cluster planned a knowledge security model for IOT applications that is light-weight that is a technique using dynamic key. The work focuses on a chaos-based encryption system to supply security in IOT based devices. Key generation process is as follows, at first random information of 128 bit is taken and divided into eight sub keys which are bit sized. The primary eight bytes of the information are initially XORed and then subsequently shuffled which increase the encryption. Then the parities of those shuffled bits are XORed with the at first chosen information of 128 bit. The generated result is used as the input for the next ulterior information block, and also the same procedure was continuing till the last information block is first XORed and then shuffled. Next procedure which is enforced is the shuffling that shuffles the data given as input which is based on the key generated within the initial procedure. During this procedure, two unique arrays are generated. This was done using the logistic map which is intertwined. The results showed that the method is extremely sensitive even for minor changes within the key. The time taken for encryption is also smaller when compared to other models.

Vernekar and Henriques et al. [7] used the combination asymmetric and symmetric cryptography to secure the IOT communication between the devices. They modified the already existing Vigenere cipher which is a polyalphabetic substituting cipher. In their proposed modified vigenere cipher. The plain text P is taken, and a random key K is generated using the timestamp and alphabets. The randomizing value was the deciding factor. If the randomizing value was 0, then the message was encrypted using a particular method and if the randomizing values was 1 it was encrypted in another method using another equation. The randomizing factor was checked and if the value was 0, normal vigenere cipher was used and if the value was 1 the next character would give the randomizing index. The reverse process of the encryption process was used in the decryption process. This method was successful as the randomness was increased using timestamp and alphabets as random key. Future scope was mentioned to further increase the complexity by adding a multiplicative element in the modified Vigenere cipher. Alternatively hashing could also be used.

Rakesh et al. [8] and [9] worked on the performance of the LEACH algorithm and anomaly detection which helps to locate the positions of the sensors which are placed in the area. This will let us know where to collect the sensor data from when a certain area is to be picked to collect the data from.

Reddy et al. [10] proposed a technique where they make use of the probabilistic scheme of encryption rather than deterministic scheme. The paper claim that the probabilistic scheme may make the encryption scheme faster when the algorithm is run on an multi-processor system and when it is run concurrently. Here the random data which is generated is not added to the block directly but it is added to the data which generates the random cipher data.

Sathya et al. [11] proposed a technique where they used Ferro Electric Field Effective Transistors (FeFETs). This FeFET is Hafnium Oxide based. They were basically used because FeFETs are believed to have a volatile memory which makes their system random and makes it difficult to detect any pattern. These FeFETs also have abrupt switching and multilevel switching capacities which brings out another advantage in their proposed method.

Mulaosmanovic et al. [12] proposed a method which makes use of the sensors data as the random number generation module. The data coming from the sensor is very much random which creates the randomness and provides a good probability for the randomness.

### 3 Proposed Work

This work mainly aims at generating a random number to the already existing encryption techniques. The random number generation which we created must go through some tests which give an indication whether the method which is being used in this work is truly random or not. Then this random number generation will be used in the encryption algorithm in generation an encryption message each time the random number changes. This will add the strength to the already existing encryption algorithm by adding randomness to it.

The proposed encryption algorithm and the implementation of the system is divided mainly into 4 parts mentioned as follows:

- Random Number Generation.
- Adding it to the encryption algorithm.
- Implementing the modified algorithm in encrypting files of different sizes.
- Check the encryption time taken for files of different sizes.

#### 3.1 Random Number Generation

To produce randomness, we use Web Scraping technique, where we scrape any random site and take values from it. The randomness comes from the fact that the value which we are taking from the site is constantly updated and will be difficult to track upon for the attackers. Also, it is difficult for the attackers to know what site exactly we are scraping from. This is a lot more helpful because, we can change the web scraping site to any other site and can still extract the same randomness. When this is done only the HTML tags need to be mentioned correctly and then the required information can be scraped out easily.

The online site which we chose to scrape the detail from is the [FlightRadar.com](https://www.flightradar.com) which gives us the details of the number of flights which are in that particular region for that moment. The site is constantly updated with the number of flights in that region So to scrape the data from this site the HTML path needs to be provided correctly to get the number which gets updated. The code to extract this is written using Python language and its libraries. The site is refreshed with a new number every 4 s which is a good frequency to generate a random number. This way we get the required random number. Now the next step is to add this to an encryption algorithm and increase its cryptic strength.

### **3.2 Addition to the Encryption Algorithm**

The creation of the random number is done and now that module is to be added to the existing algorithm. The random number is added in such a way that each time the random number changes the encrypted text also changes, which increases the encryption level. This random number generation is added to an already existing encryption algorithm which is used to test the authenticity of the random number generation. So, in this way we add the randomness to an already existing algorithm.

### **3.3 Implementation on Different File Sizes**

Once the encryption algorithm is implemented, that has to be applied on various files of different sizes. This is to test whether the encryption algorithm works fine even when the file size changes. The time taken would obviously change as the file size increases. The file size in our case varies from 8 Mb to 700 Mb as that is what the maximum this encryption algorithm can handle. Once the file is encrypted even if anyone tries to open it, there would be some random text which no one can understand. This is what the encryption algorithm does. The decryption method is also written, and it should ideally take the same amount of time to decrypt as it takes to encrypt. Once the file is decrypted the file will retain the original contents and can be used normally.

### **3.4 Encryption Time for Different File Sizes**

Depending on different sizes of files the encryption time will change. If the file size increases the encryption time also increases. Normally the encryption time for an existing algorithm is captured for different file sizes. Since our algorithm has web scraping it takes a little more time to encrypt the files as it has to make the HTTP request, scrape and then return the value. Keeping all these factors in check we analyze the time taken to encrypt the file.

## **4 Experimental Results**

To test the randomness generated by the random number generation module randomness tests are done. Kolmogorov-Smirnov Test and Chi-square test were carried out to test the randomness. These test conditions are two of the many test cases which a randomness test has to go through. These two tests come under the functional part of



the testing where the internal functioning of the system is tested to meet the requirements of a better system.

Once the random number generation part is added to the original algorithm the encryption strength of the algorithm is increased which provides more security to the file or the application in which this algorithm is applied. The encryption algorithm is tested on files of different sizes to test whether the algorithm has the capacity to handle it.

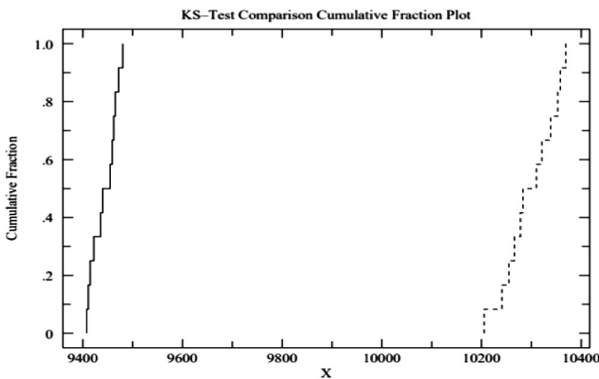
The first test which was conducted is Chi-square test. Chi-square test was conducted using an online Chi-square simulator which tells us whether the numbers generated are significant enough and cannot be predicted when used again. So the factors which are mainly considered when a Chi-square test is calculated are the Chi-Square characteristic, the P value which checks whether the given value is significant or not.

**Table 1.** Test results of Chi-Square test.

Significance level	P value	Significant or not
0.01	0.15556	P > 0.01, Not Significant
0.05	0.04332	P < 0.05, Significant
0.10	0.07789	P < 0.10, Significant

As shown in the Table 1 above, the Random number generation in our method passed the Chi-Square test when the Significance level was 0.05 and 0.10 but it failed when the Significance level was 0.01. This indicates that our method is useful when the significance level is moderate or simple, but may break when the significance level is increased.

The next test which was run to test the randomness is the Kolmogorov-Smirnoff test. The random values were different in some sense but almost followed a similar pattern in producing the random numbers. The encryption still showed strong because even when there is a slight change in the random numbers the encrypted text was pretty strong and could not be easily read through or decrypted (Fig. 1).



**Fig. 1.** Kolmogorov Smirnoff test for first set

For another set of values which were taken for the test. This time the numbers did not show any pattern and it was pretty difficult to track trace out the pattern in this case. The test showed accumulative distribution value of 0.667 and a probability value of 0.005, which is considered to be a good number for not predicting the next set of numbers (Fig. 2).

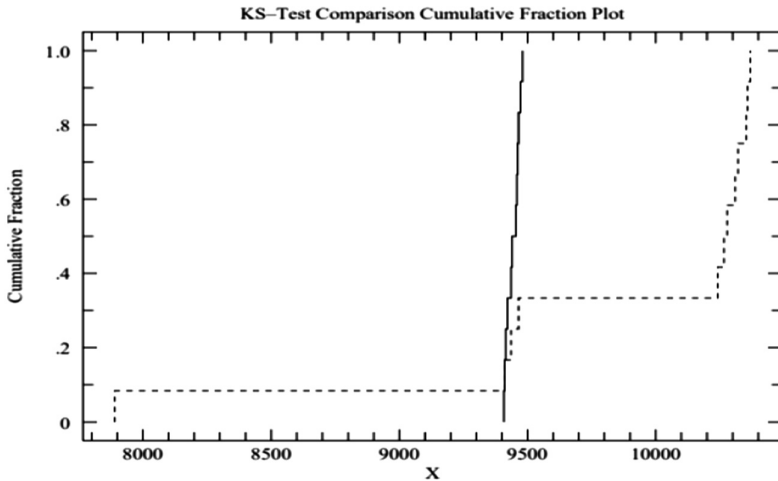


Fig. 2. Kolmogorov Smirnov test for first set

Next the system was tested as a whole integrating both the randomness generation module and the existing encryption algorithm which was used. The system was tested for various test cases where the files were of different sizes.

This is done to test whether the modified encryption algorithm works well for different file sizes. The range of files varies from 8 Mb to 700 Mb.

When the encryption mechanism is performed on the file the file is converted into an encrypted file (Figs. 3 and 4).

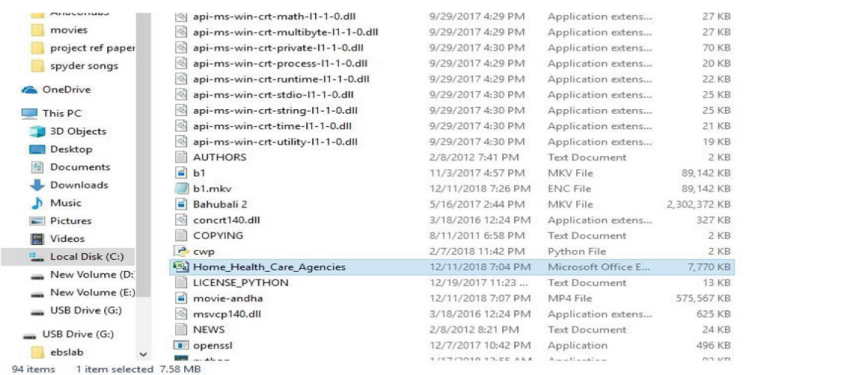


Fig. 3. File Size of 8 Mb before encryption

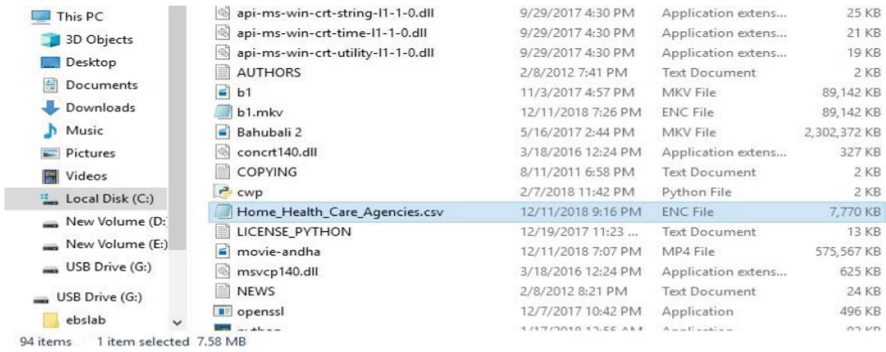


Fig. 4. File Size of 8 Mb after encryption

The file before encryption is a CSV file i.e. an Microsoft Excel File whereas after the encryption the file is converted into an encrypted file with an extension ENC. The time it takes to encrypt the file starts from scraping the web and creating a random number and then encrypting the file (Figs. 5 and 6).

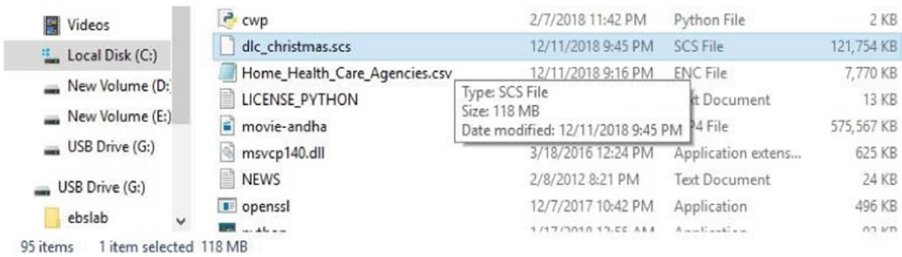


Fig. 5. File size of 100 Mb before encryption

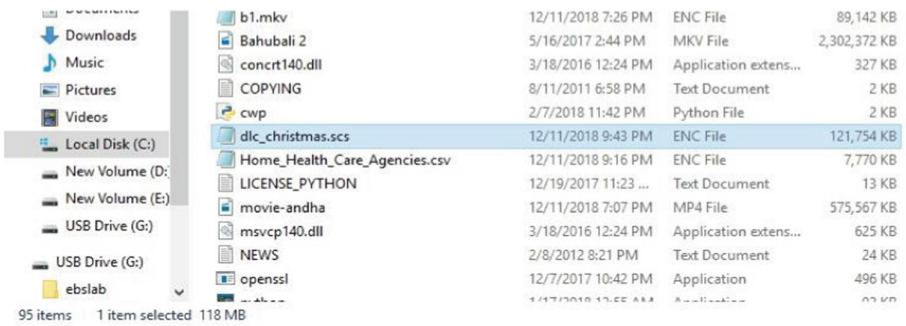
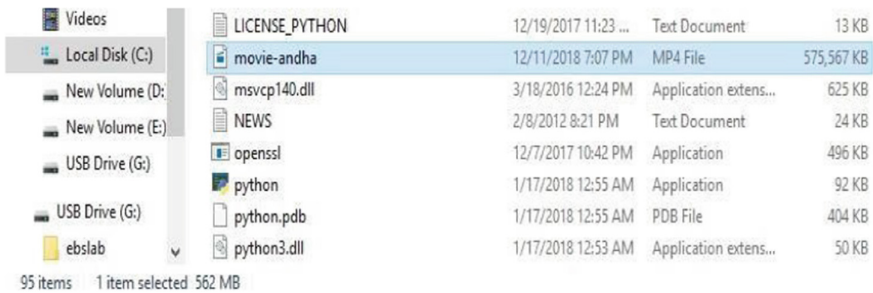
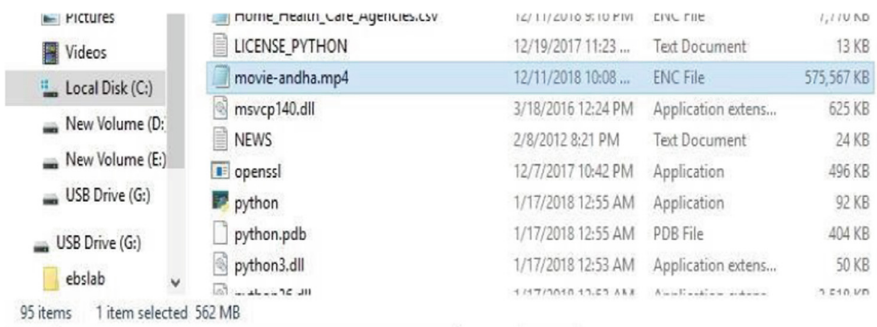


Fig. 6. File size of 100 Mb after encryption.

As shown in the above two figures we can observe that this works well for file size of 100 Mb.



**Fig. 7.** File Size of 600 Mb before encryption



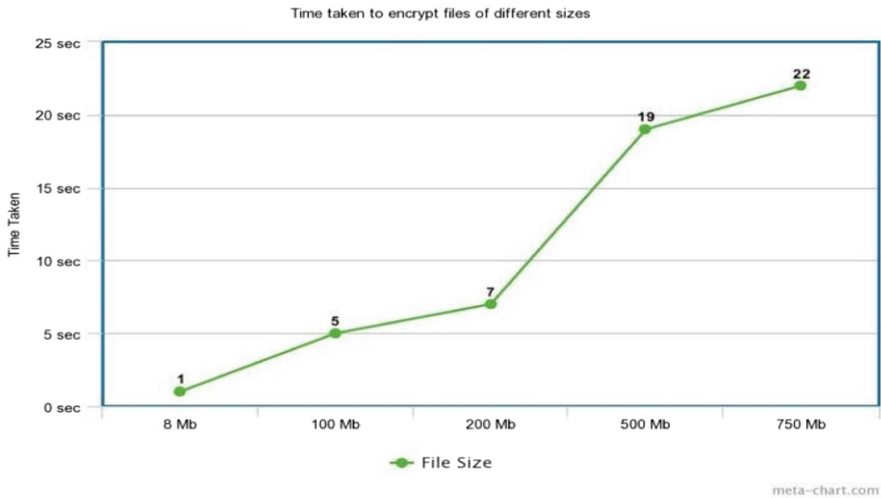
**Fig. 8.** File Size of 600 Mb after encryption

As shown in the above two Figs. 7 and 8, and also mentioned previously the encryption algorithm works well for file size of 600 Mb as the file is converted from an MP4 file to an encrypted file. The file cannot be read as it is an encrypted file.

The results of the file encryption time taken for files of different sizes is shown in the form of plot, it is the result of how much time is the encryption algorithm taking to encrypt a file of particular file size. Generally files of smaller sizes must take lesser time to encrypt but as the encryption algorithm is involved with random number generation the time is slightly increased. This is because the random number must parse through the web and scrape the values and must return the values which takes the extra time as mentioned earlier.

The time taken to parse the web was checked for various number of times and the time taken was approximately the same each time as to the figures mentioned below in the plot. Also the time may vary depending on the speed of the connectivity to the internet. The results shown below were conducted with a good internet connectivity which is available everywhere. The time taken may further decrease if the internet connectivity is better or the time taken may increase if the internet connectivity is very slow.

At the cost of time, the security is not compromised. The level of security is not decreased and to the least it will remain the same as the encryption algorithm earlier had (Fig. 9).



**Fig. 9.** Time taken to encrypt the files

## 5 Conclusion and Future Works

In conclusion the work done in this work was mainly to secure the data from external threats and the precautionary measure which was taken to execute that was to provide encryption for the file which may possess the threat of being hacked or attacked. The main modules which were a part of this work were the generation of the random numbers and using this in an existing algorithm to enhance the security performance of that particular algorithm. The random number generation technique which was used in this work was using web scraping. The web site which was chosen to scrape from updates its data constantly which makes the data more random and makes the encryption more stronger.

This was applied to the encryption algorithm and the time taken by the new algorithm to encrypt was noted for files of different sizes. There is a small change in the time values when compared to the original algorithm because in the new algorithm the code has to scrape through the web and produce the random number. The random number generation has been tested with the randomness tests and it has passed most of the tests which it is supposed to. As future works, the encryption algorithm as a whole must be tested with the attacks such as the brute force attacks, replay attacks and many such and check whether it can sustain them. It also has to be tested when to apply this algorithm when to apply to particular attacks.

## References

1. Jha, D., Shahi, B.: A proposed methodology for end to end encryption for communicating embedded systems. In: International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore (2017)
2. Deshpande, P., Santhanalakshmi, S., Lakshmi, P., Vishwa, A.: Experimental study of Diffie-Hellman key exchange algorithm on embedded devices. In: International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai (2017)
3. Majumder, P., Sinha, K.: A novel key generation algorithm from twitter data stream for secure communication in IoT (2017)
4. Tao, H., Bhuiyan, M.Z.A., Abdalla, A.N., Hassan, M.M., Zain, J.M., Hayajneh, T.: Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet Things J.* **6**, 410–420 (2018)
5. Philip, M.A., Vaithyanathan: A survey on lightweight ciphers for IoT devices. In: International Conference on Technological Advancements in Power and Energy (TAP Energy), Kollam (2017)
6. Kumar, M., Kumar, S., Budhiraja, R., Das, M.K., Singh, S.: Lightweight data security model for IoT applications: a dynamic key approach. In: IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), Chengdu (2016)
7. Henriques, M.S., Vernekar, N.K.: Using symmetric and asymmetric cryptography to secure communication between devices in IoT. In: International Conference on IoT and Application (ICIOT), Nagapattinam (2017)
8. Rakesh, N.: Performance analysis of anomaly detection of different IoT datasets using cloud micro services. In: International Conference on InventiveComputationTechnologies (ICICT), Coimbatore, pp. 1–5 (2016)
9. Ashwini, M., Rakesh, N.: Enhancement and performance analysis of LEACH algorithm in IOT. In: International Conference on Inventive Systems and Control (ICISC), Coimbatore, pp. 1–5 (2017)
10. Reddy, B.D., Kumari, V.V., Raju, K.: A new symmetric probabilistic encryption scheme based on random numbers. In: First International Conference on Networks Soft Computing (ICNSC 2014), Guntur, pp. 267–272 (2014)
11. Sathya, K., Premalatha, J., Rajasekar, V.: Random number generation based on sensor with decimation method. In: IEEE Workshop on Computational Intelligence: Theories, Applications and Future Directions (WCI), Kanpur, pp. 1–5 (2015)
12. Mulaosmanovic, H., Mikolajick, T., Slesazek, S.: Random number generation based on ferroelectric switching. *IEEE Electron Device Lett.* **39**(1), 135–138 (2018)



# An Extensive Survey on Recent Machine Learning Algorithms for Diabetes Mellitus Prediction

R. Thanga Selvi<sup>(✉)</sup> and I. Muthulakshmi<sup>(✉)</sup>

Department of CSE, V V College of Engineering, Tisaiyanvilai, India  
golda.selvi@gmail.com, jeevikrithick@gmail.com

**Abstract.** Presently, the number of people affected by Diabetes Mellitus (DM) is significantly increased because of the presence of high blood sugar level because of the failure of pancreas to generate enough insulin. DM is one of the chronic diseases and is widely spread all over the world. In recent days, there is an exponential growth in the number of researches carried out in this field because of the DM leads to death causing disease like heart stroke, eye blindness, etc. So, the prediction of DM at the earlier stage is highly useful to prevent the increasing mortality rate. Numerous data mining and machine learning (ML) models has been developed to diagnose, and handle DM. Keeping this in mind, in this paper, we try to review the recently developed ML and data mining models to predict DM. The existing DM prediction techniques in different aspects have been reviewed and a detailed comparison is also made at the end of the survey.

**Keywords:** Classification · Data mining · Diabetes · Machine learning

## 1 Introduction

Diabetes Mellitus (DM) is a swarm of metabolic infection arises in a patient having high blood sugar level because of the failure of pancreas to create enough insulin of the cells does not react to the produced insulin. The increased blood sugar level leads to the classic symptoms of often urination, more liquid drinking and more starvation. Generally, DM can be categorized into 3 main types: “Type I DM”, as a result of the failure of pancreas to generate insulin and leads to provide insulin artificially; “Type II DM” as a result of insulin conflict where the cells cannot effectively exploit the produced insulin and leads to insufficient insulin; the third type is “Non Insulin Dependent DM/adult-onset diabetes”. Finally, “gestational diabetes” takes place for pregnant women with no prior diagnose of diabetes and it probably results to type I DM. Gestational DM has the feature of intolerant carbohydrates of different severity levels in case of pregnancy. The pregnant women have the higher chance of having DM specially Type II DM.

Among all the three types of DM, a similar thing will be present. In general, the human body will divide the consumed carbohydrate and sugar into a particular form of sugar called glucose, which stimulates the body cells. However, the cells necessitate

insulin to take glucose as well as for energy. Each type of DM is curable due to the fact that the insulin is developed in the year of 1921 itself. The Types I and II are chronic conditions that are not easier to treat. In case of type I DM, transplantation of pancreas leads to better results in a limited way whereas gastric bypass is efficient in a considerable way. The untreated DM will leads to different difficulties like heart stroke, eye blindness and diabetic retinopathy. Hence, regular treatment of the DM is highly needed in the present scenario like no smoking or alcohol drinking and controlling body weight. Since the cells will not consume insulin from blood, it begins to produce in the blood itself. The increased level of glucose in blood damages the small vessels of blood in several body parts like heart, kidney, eyes or nerves. These complications leads to heart stroke, kidney disease, stroke, nerve damage and color blindness. For the elimination of these issues, the earlier identification of DM is preferable by the use of efficient techniques. Keeping this in mind, various classification algorithms has been developed to diagnose DM utilizing data mining and ML approaches.

Data Mining indicates the process of knowledge extraction from massive quantity of data. It helps to discover massive patterns and investigate the same using statistical and Artificial Intelligence in huge dataset [1, 3]. Data mining approaches predicts the upcoming characteristics or to explore the hidden patterns exist in the nature of the data. Some of them are Artificial Neural Network (ANN), Decision Tree (DT), Classification, Clustering, Association rule mining, etc [2]. [1paper] Classification is an important decision making tool widely used to solve real world problems. Bassam et al (2013) developed a classification technique for DM by the use of ML approaches. In a generic

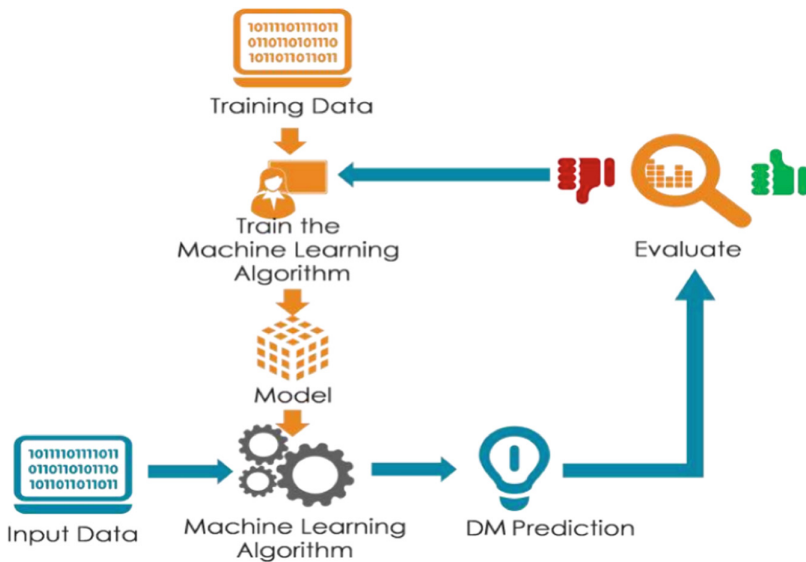


Fig. 1. Process involved in ML based DM prediciton



classification problem, the presence of more number of selected samples does not always leads to increased classification performance. Most of the cases, the classification results will be high interms of speed with the cost of poor classification accuracy. The accuracy will be enhanced when large amount of dataset is used to train the model and less amount of dataset is used to test the data [4].

In this paper, we investigate various recently proposed ML models which classify the data into diabetic and non diabetic data under several aspects. A detailed review of the recently developed ML and data mining models to predict DM takes place (Fig 1).

The existing DM prediction techniques in different aspects have been reviewed and a detailed comparison is also made at the end of the survey.

The upcoming part of the survey is arranged as follows: a review of ML techniques for DM prediction takes place in Sect. 2 and conclusions are drawn in Sect. 3.

## 2 Review of DM Prediction Techniques

A new classifier using ML algorithm is built for diabetes, hypertension and comorbidity data Kuwait [6]. It reports that the rise in proneness in DM patients have the tendency to have hypertension and vice versa. The ML algorithms used here are k-nearest neighbors (k-NN), multifactor dimensionality reduction and support vector machine (SVM). The study uses fivefold cross validation to obtain generalization accuracies and errors. Among the other employed ML classifiers, kNN is found to be effective than the other methods interms of classification performance.

[7] intended to develop a technique which predicts the possibility of DM in patients with effective performance. So, three ML approaches such as DT, SVM and NB are employed in this study to identify DM at the earlier phase. The experimentation takes place on Pima Indians Diabetes Database (PIDD) from UCI repository. The results of these approaches are validated interms of Precision, Accuracy, F-Measure, and Recall. Accuracy is measured over correctly and incorrectly classified instances. The simulations reported that NB is superior with the maximum accuracy of 76.30% which is higher than the compared methods. Additionally, Receiver Operating Characteristic (ROC) curves are also derived to validate this study.

In [8], effective data mining approaches has been used to predict Type 2 DM to achieve improved classification performance and makes it adaptable to any of the applied dataset. Using a sequence of preprocessing methods, the proposed model consists of two levels: improved K-means algorithm and LR. The PDD and the WEKA tool are used for the comparison of performance with other methods. The results concluded that it is better than the existing methods with an increased accuracy of 3.04%. Another two DM dataset is also used for further validation of the proposed model. In addition, this approach can be employed to the real time health management of DM.

DM identification is a significant research area in the field of healthcare [9]. Though many data mining methods are available to analyze the causes of DM, only a less number of clinical risks are taken. Because of this fact, some main characteristics like pre-diabetes health conditions are not measured in the investigation process. Hence, the outcome of these methods might not suitable to properly detect the diabetes patterns and risk factors.

[10] intends to identify serious diseases like heart disease and cancer among the patients of DM. The interlink among the diseases are investigated depending upon the parameters which cause the diseases such as sex, age, period of diabetic condition, living habits and so on. The proposed work operates on two phases: in the first pahse, the attributes are detected and filtered by PSO algorithm. In the latter phase, the ANFIS (Adaptive Neuro Fuzzy Inference System) with Adaptive Group based K-Nearest Neighbor (AGKNN) method is employed for data classification. The obtained values imply better classification performance and signify that the ANFIS with AGKNN along with feature selection by the use of PSO. The results are validated by performance measures and verified that the classification results of the identification of heart diseases and cancer among the patients of DM.

The use of Frequent Pattern Growth algorithm on patient data is hard [11]. Association rule mining is an important research field which can be used to diagnose the disease at the earlier stage. The discretization phase is needed to convert the numerical characteristics and is provided to the Complete Frequent Patten Growth++ to generate rules. Based on this, Modified PSO algorithm with least square SVM (LSSVM) is used with outlier detection scheme. Pima Indians Diabetes Data Set is taken as an input. The computation time, rule count and the identification of outlier percentage are investigated. The simulation results revealed that effective classification with a higher accuracy of 95% is obtained and ensured that it is applicable to detect Type 2 DM at the earlier stage.

In [11], a fuzzy logic based detection technique is proposed which has the capability to detect the DM at the beginning level. To facilitate data, an eastern Jakarta hospital lab in Indonesia is used which provides the required data and conduct interviews with two physicians in the form of questionnaire. The overall model is based on the fact that how a physician decides to indication that someone has the possibility against DM. For validation, a comparison is made with the physician decisions and the outcome reported the accuracy of 87.46% of the 311 relevant data is identical to the doctor decision.

[13] focuses on the identification of DM using a regression-based data mining approach. The Oracle Data Miner (ODM) is used as software mining tool to predict the ways to treat DM. the SVM is employed for the experimentation purposes. The dataset of Non Communicable Diseases (NCD) risk factors in Saudi Arabia are attained from WHO and are employed for investigation. The dataset is studied and investigated to determine the efficiency among various treatment types for diverse age people. The results reported that the drug treatment for patients in the younger age group can be

postponed to eliminate side effects. Contrastingly, patients in the older age group should begin the treatment immediately due to the absence of no substitutes.

A hybridization of Type 2 DM prediction method [14] is introduced by the use of data mining techniques. Here, K-means is employed to reduce data with J48 DT as a classification model. For obtaining the experimental results, PIDD from UCI repository is used. The outcome implies that the presented technique attains improved performance than the earlier works.

[15] presented a DT based approach for the identification of DM. The conventional DT classifier has the issue of crisp boundary. By the use of fuzzy concepts, better decision rules can be formed from the medical data. The main process is the detection of split points are detected by the use of Gini index. A new approach to reduce the computation of Gini indices by the identification of false split points and employed the Gaussian fuzzy function due to the fact that the clinical dataset are not crisp. Since the effectiveness of the DT is based on various factors like node count and tree depth, the pruning of DT plays an important task. The enhanced Gini index-Gaussian fuzzy DT method is presented and is validated on PIDD and the proposed method is better than the DT classifier.

[16] developed an effective model for the DM prediction and also additional risks. The authors have utilized GA, KNN, fuzzy approach to design a precise prediction model. For the experimentation, medical data from 235 people are gathered. The optimal features are created by the proposed approach includes age, heredity, personal habits, and so on related to the existence of other diabetes difficulties assumed to predict diseases. The presented approach is highly effective using the selection of optimal features chosen by varying GA based on the different kinds of kNN.

A medical expert system to diagnose disease is presented. Diabetes ontology is presented by the use of the OWL format with 9 sub-classes [17]. The interval results with the weighted OWA similarity algorithm are expressed for easy interpretation by users. The expert system is presented in the form of web-based application with web service architecture. A total consistency rate of 90.7% is attained against the test data of 65 patients. The experimental values depict that the proposed model assist to identify diabetes at the earlier stage and serves as a guide for patients to observe the disease. It is probable that the proposed model can be effectively employed to medical data for dealing with issue of disease diagnosis effectively. [18] employs Bayes Network for the prediction of Type-2 DM and applied to Pima Indians Diabetes Data Set.

[19] makes use of DT to predict patients with developing diabetes. The dataset used is the PIMA, which gathers patient data with and without diabetes. The proposed work operates on two phases: preprocessing and disease prediction. The preprocessing phase includes attribute selection, missing values and numerical discretization. Next, identification of DM is done by the use of DT (Table 1).

**Table 1.** Comparison of reviewed DM prediction techniques

Reference	Year	Objective	Disease	Algorithm	Data	Compared with	Metrics
[5]	2013	To build a new classifier for diabetes, hypertension and comorbidity data	DM, hypertension and comorbidity	KNN	Medical data from Kuwait	Multifactor dimensionality reduction and SVM	Accuracy
[6]	2018	To predict the possibility of DM in patients		NB	PIDD	DT, SVM	Accuracy, ROC
[7]	2018	To employ data mining approaches for Type II DM	DM	Improved K-means algorithm and LR	PIDD	SVM, LR, DT	Accuracy
[8]	2015	To study the pre-diabetes health conditions	DM	C4.5 rules and partial tree	-	-	Accuracy
[10]	2015	To identify serious diseases in DM patients	Heart disease and cancer	ANFIS- AGKNN	-	-	Accuracy
[11]	2015			MPSO-LSSVM	PIDD	SVM	Computation time, accuracy, rule count
[11]	2015	To detect the DM at the beginning level	DM	Fuzzy logic		Doctor decision	Accuracy
[11]	2013	To identify DM in young and old patients	DM	Oracle Data Miner, SVM	Saudi Arabia	-	Accuracy
[12]	2017	To develop a hybrid method for DM	DM	K-means and DT	PIDD	DT	Accuracy
[13]	2014	To develop a classifier for better diagnosis of DM		Fuzzy logic	PIDD	DT	Accuracy
[14]	2015	To detect type II DM Soft Computing Techniques	Type II DM	GA, KNN, fuzzy approach	Medical data from 235 people	GA, KNN, fuzzy approach	Accuracy
[15]	2016	To develop an ontology based medical expert system	DM	OWA similarity algorithm	Data of 65 patients	-	Accuracy
[17]	2011	To predict patients with developing diabetes	DM	DT	PIMA	-	Accuracy

### 3 Conclusion

In recent days, there is an exponential growth in the number of researches carried out in this field because of the DM leads to death causing disease like heart stroke, eye blindness, etc. So, the prediction of DM at the earlier stage is highly useful to prevent the increasing mortality rate. Numerous data mining and machine learning (ML) models has been developed to diagnose, and handle DM. In this paper, we investigate various recently proposed ML models which classify the data into diabetic and non diabetic data under several aspects. A detailed review of the recently developed ML and data mining models to predict DM takes place. The existing DM prediction techniques in different aspects have been reviewed and a detailed comparison is also made at the end of the survey.

### References

1. Screening for type-2 diabetes: Report of a World Health Organization and International Diabetes Federation meeting. [www.who.int/diabetes/publications/en/screening-mnc03.pdf](http://www.who.int/diabetes/publications/en/screening-mnc03.pdf)
2. Patil, B.M., Joshi, R.C., Toshniwal, D.: Association rule for classification of type-2 diabetic patients. In: Proceedings of the Second International Conference on Machine Learning and Computing, pp 330–334 (2010)
3. Han, J., Kamber, M.: Data Mining: Concepts and Techniques, 2nd edn., vol. 2, no. 6, pp. 251–261, June 2012
4. Papagcoriou, E., Kotsioni, I., Lions, A.: Data mining: a new technique in medical research. *Hormones* **4**(2), 114–118 (2013)
5. Patil, B.M., Joshi, R.C., Toshniwal, D.: Association rule for classification of type-2 diabetic patients. In: Proceedings of the Second International Conference on Machine Learning and Computing, vol.7, no.4, pp.140–166, March 2009
6. Farran, B., Channanath, A.M., Behbehani, K., Thanaraj, T.A.: Predictive models to assess risk of type 2 diabetes, hypertension and comorbidity: machine-learning algorithms and validation using national health data from Kuwait—a cohort study. *BMJ Open* **3**(5), e002457 (2013)
7. Sisodia, D., Sisodia, D.S.: Prediction of diabetes using classification algorithms. *Procedia Comput. Sci.* **132**, 1578–1585 (2018)
8. Wu, H., Yang, S., Huang, Z., He, J., Wang, X.: Type 2 diabetes mellitus prediction model based on data mining. *Inform. Med. Unlocked* **10**, 100–107 (2018)
9. Saxena, K., Sharma, R.: Diabetes mellitus prediction system evaluation using c4. 5 rules and partial tree. In: 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), pp. 1–6. IEEE, September 2015
10. Kalaiselvi, C., Nasira, G.M.: Prediction of heart diseases and cancer in diabetic patients using data mining techniques. *Indian J. Sci. Technol.* **8**(14), 1 (2015)
11. Karthikeyan, T., Vembandasamy, K.: A novel algorithm to diagnosis type II diabetes mellitus based on association rule mining using MPSO-LSSVM with outlier detection method. *Indian J. Sci. Technol.* **8**(S8), 310–320 (2015)
12. Lukmanto, R.B., Irwansyah, E.: The early detection of Diabetes Mellitus (DM) using fuzzy hierarchical model. *Procedia Comput. Sci.* **59**, 312–319 (2015)
13. Aljumah, A.A., Ahamad, M.G., Siddiqui, M.K.: Application of data mining: diabetes health care in young and old patients. *J. King Saud Univ.-Comput. Inf. Sci.* **25**(2), 127–136 (2013)

14. Chen, W., Chen, S., Zhang, H., Wu, T.: A hybrid prediction model for type 2 diabetes using K-means and decision tree. In: 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp. 386–390. IEEE, November 2017
15. Varma, K.V., Rao, A.A., Lakshmi, T.S.M., Rao, P.N.: A computational intelligence approach for a better diagnosis of diabetic patients. *Comput. Electr. Eng.* **40**(5), 1758–1765 (2014)
16. Pavate, A., Ansari, N.: Risk prediction of disease complications in type 2 diabetes patients using soft computing techniques. In: 2015 Fifth International Conference on Advances in Computing and Communications (ICACC), pp. 371–375. IEEE, September 2015
17. Mekruksavanich, S.: Medical expert system based ontology for diabetes disease diagnosis. In: 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp. 383–389. IEEE, August 2016
18. Guo, Y., Bai, G., Hu, Y.: Using bayes network for prediction of type-2 diabetes. In: 2012 International Conference for Internet Technology and Secured Transactions, pp. 471–472. IEEE, December 2012
19. Al Jarullah, A.A.: Decision tree discovery for the diagnosis of type II diabetes. In: 2011 International Conference on Innovations in Information Technology (IIT), pp. 303–307. IEEE, April 2011



# Rawism and Fruits Condition Examination System Victimization Sensors and Image Method

J. Yamuna Bee, S. Balaji<sup>(✉)</sup>, and Mukesk Krishnan

Department of Computer Science and Engineering, Tirunelveli, India  
yamikhan@gmail.com, sbalajiphd@gmail.com

**Abstract.** Recent technological trends have sealed the method for rising and provides advanced services for the stake holders within the agricultural sector. A lucky shift is current from proprietary and tools to IoT-based, open systems which will change simpler collaboration between stakeholders. This approach includes the technological support of application developers to start specialized services which will seamlessly interoperate, therefore making a complicated and customizable operating atmosphere for the tip users. we tend to propose the implementation of AN design that instantiates such AN approach, supported set of domain freelance code application known as “generic enablers” that are developed within the context of the FI-WARE project.

**Keywords:** Plants · Weed · Filtering enhancement · IoT · Wi-Fi · MATLAB · Arduino UNO

## 1 Introduction

To increasing previous technology fruits’ quality and production potency the standard ways, cut back labor intensity. Fruit non-destructive detection is nothing however method of distinguishing fruits’ within and out of doors quality with none injury, mistreatment some police investigation technology to form analysis according some classic rules. Nowadays, the standard, volume estimation of fruit cannot assess on line by. With the advance of image process and net of things technology and laptop package and hardware, it becomes a lot of engaging to spot fruits’ quality by mistreatment machine vision police investigation technology. The foremost existing fruit quality police investigation and grading system have the various disadvantages of low potency, manual review work, and low speed of grading, high value and quality (Fig. 1).

In case we have a tendency to are sorted circular formed fruits according color and grading is completed supported its size. The machine-controlled classification, volume estimation and grading system are designed to mix 3 processes like feature extraction victimization GLCM, sorting consistent with color and grading consistent with its size. software package development is very necessary during this color system victimization classifier and for locating size of a fruit.



**Fig. 1.** Fruits and vegetables

## 2 Related Work

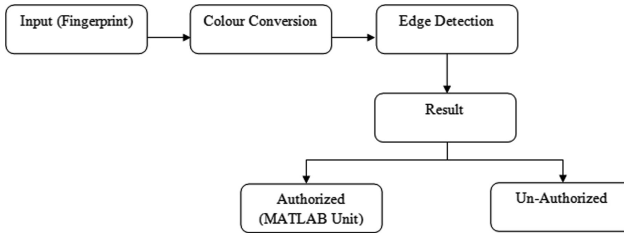
In existing system, the gardening house is controlled with only Simple sensors and 8051 microcontroller. The following sensors are 1. Temperature sensor 2. humidity sensor. The sensors will detect soil moisture content (i.e.) water contents of the soil, conductivity level and drive the water motor. This system collects frames from camera that is placed on conveyer to hide agriculture space. Then image process is finished to induce needed options of fruits like texture options exploitation GLCM, color and size. Defected fruit is detected supported blob detection non-effectively, color detection is finished supported thresholding and size detection is predicated on binary image of fruit.

## 3 System Implementation

### 3.1 Proposed System

In this project, we represent farm house maintenance automatically with the help of Arduino microcontroller and MATLAB for vision. The Arduino UNO microcontroller that helps to water irrigation for the plant. The subsequent sensors are used: 1. Temperature device a 2. wetness device 3. Soil wetness device and 4. LDR The soil moisture sensor which helps to find out soil moisture content to avoid water conductivity (i.e.) water content of the soil reduced and driven the water motor automatically. The temperature and humidity sensor detects temperature of form house and also drive the water motor automatically. Matlab is used to find out the insect damage in the leaf using image processing, feature extraction and texture features. It will detect insect damage on the leaf and turn on the chemical motor for pesticide of particular plant to protect plant. The Matlab also used for to detect the cultivation of vegetable, inspect the fruits whether fruits status cultivated or bad. The microcontroller will update through Ethernet cultivation of vegetable (Fig. 2).





**Fig. 2.** Biometric image

## 4 Methods

### 4.1 Input Image

The RGB (Red, inexperienced and Blue) color model is color model inside that red, inexperienced and blue light-weight are combined on in varied ways in which during which to breed a broad array of colors. This name of the model comes from the beginning of the 3 additive primary colors, red, inexperienced and blue. RGB could be a dependent color model: completely different individual devices observe or produce a given RGB price otherwise, since the colour (such as phosphors or dyes) and their reaction to the individual Red, Green, and Blue levels vary from user to user, or perhaps within the same device over time. Thus Red inexperienced and Blue price doesn't outline the identical color across devices while not some reasonably color management. To make a color with Red, inexperienced and Blue, 3 totally different light-weight beams (one red, one green, and one blue) should be superimposed. Every of the 3 beams is named a product of that color, and every of them will have associate degree higher intensity, from absolutely off to completely on, within the mixture.

### 4.2 Gray Image

In photography and computing technology, a grayscale or greyscale digital image could be a image conversion varieties throughout that the price of each part is also one sample, that is, it carries entirely intensity values data. Pictures of this type, conjointly called black and white, are combined completely of reminder grey, variable from black at all-time low intensity to white at the strongest.

### 4.3 Filtering

In signal processing, a filter is a device or process or technique that reduces unnecessary components or features from a signal. Filtering is a signal, image or frames processing, the defining feature of active or passive filters being the complete suppression or partial of some aspect of the signal. It is a one of the non-linear digital filtering techniques, typically accustomed take away noise and unwanted distortion from a picture or signal. Such noise reduction could also be a typical method step to reinforce the results of edge detection like sobel, canny etc. Median filtering is utilized in digital image method analysis to induce obviate noise in original second image. It

prevents edges whereas removing noise, in addition having wide applications in signal and image method. the foremost set up of the filter is to run through the signal step by step, substitution each entry with the median of neighboring entries.

#### **4.4 Contrast Enhancement**

Contrast sweetening could be a technique or approach in image process of distinction modification exploitation the image's bar chart. Histogram exploit will this by up spreading out the most intensity values to clear blur. Adaptive bar graph deed (AHE) may be a pc image process or machine vision technique accustomed improve distinction in pictures or signals. It differentiates from different bar graph deed with respect that the strategy computes many histograms and uses them to unfold the non-darkness values of the image. Imadjust technique adjusts intensity values.

#### **4.5 Hardware Description**

##### **4.5.1 Power Supply Unit**

Power provide unit could be a relevance a supply of power. A system that gives energy in associate degree kind to an output load is named an influence provide unit or PSU. This term is usually applied largely to electricity provides, less seldom to others and sometimes to mechanical. Basic power provide the input power electrical device has its coil connected to the mains (line) provide. A secondary, coupled in associate degree electro-magnetically manner however it absolutely was electrically isolated from the first is employed to urge associate degree electricity voltage of most well-liked amplitude, and once additional process by the ability provide Unit, to drive the physical science circuit it's to provide. remaining AC pulses. Voltage regulator Integrated Circuits are offered in each mounted and variable output voltages. Rectifier circuit is used to convert the choice Current input is regenerate to electricity.

##### **4.5.2 ArduinoUNO**

An Arduino is truly a microcontroller primarily based kit which may be either used directly by buying from the seller or may be created reception exploitation the elements, attributable to its open supply hardware feature. it's essentially utilized in communications and in dominant or operational several devices. it absolutely was supported by Massimo Banzi and David Cuartielles in 2005. The Arduino Uno is also a microcontroller board supported the ATmega328. it's fourteen digital input/output pins (of that half-dozen is also used as PWM outputs), half-dozen analog inputs, a sixteen megahertz generator, a USB affiliation, AN influence jack, Associate in Nursing ICSP header, and a button.

##### **4.5.3 Temperature Sensor (LM 35)**

Temperature is that the measured method variable in industrial automation basis. LM35 is employed to convert temperature worth to AN electrical worth. Temperature Sensors are the device to browse temperatures and to manage temperature in industrials automation applications.

#### 4.5.4 Humidity Sensor

A humidity detector could be a device that's used to live the humidity of in an environmental space. A humidity detector are often used and enforced in each inside and outdoors atmosphere. they're out there in each analog and digital signals. This wetness detector module converts ratio into voltage and may be utilized in weather watching application or home applications.

#### 4.5.5 Soil Moisture Sensor

The soil wetness detector that helps to seek out soil wetness content to avoid water physical phenomenon (i.e.) water content of the soil reduced.

#### 4.5.6 Relay

The Relay may be used to management a circuit. it's employed in places wherever signal may be used to management plenty of circuits like motors, fan and 230 V Bulb. The applications of channel relays need high power to be driven by electrical motors and then on. Such relays are referred to as contactors. Relays are straightforward switches that are worked. Switch primarily based Relays include AN magnet and conjointly a collection of contacts. The shift mechanism is sustained with the assistance of the magnet. however they disagree consistent with their applications.

#### 4.5.7 Motor

A DC motor is any of a category of electrical and electronic machines that converts DC power into mechanical power. The foremost common varieties relay on the forces made by magnetic fields.

#### 4.5.8 Buzzer

A buzzer is associate degree audio device for alert system. A buzzer takes some arrangement of input and emits a sound in. they will use numerous suggests that to make the sound; everything from metal clappers to mechanical device devices.

### 4.6 Adaptive Histogram Equalization Algorithms

Adaptive bar graph feat (AHE) could be a pc image process technique accustomed improve distinction in pictures. It differs from standard bar graph feat within the respect that the adaptational methodology computes many histograms, every equivalent to a definite section of the image, and uses them to distribute the lightness values of the image. it's thus appropriate for rising the native distinction and enhancing the definitions of edges in every region of a picture. However, AHE contains a tendency to overamplify noise in comparatively undiversified regions of a picture. A variant of adaptational bar graph feat referred to as distinction restricted adaptational bar graph feat (CLAHE) prevents this by limiting the amplification. Histogram feat algorithms are classified into 2 categories: dysfunctional and adaptational. within the dysfunctional algorithms every picture element is changed by applying the identical pattern of computation that uses the bar graph of entire original image. In general sensible quality pictures are degraded during a dysfunctional bar graph feat method. In works with higher result for pictures that has details hidden in dark regions.

In the adaptational algorithms every constituent is changed supported the constituents that are in an exceedingly region close that pixel. This region is named discourse region. The adaptational bar graph equalizations is computationally intense and for this reason was developed some strategies to extend the speed of the first technique. If we've got a picture of  $n \times n$  pixels, with  $k$  intensity levels and therefore the size of discourse region is  $m \times m$ , then the time needed for calculations is  $O(n \text{ two } (m + k))$ . higher results are obtained if we tend to use rather than the bar graph of neighborhood pixels from a moving window solely four nearest grid points. The transformation of every constituent is created by interpolating mappings of the four nearest points. If  $(x, y)$  could be a constituent of intensity  $i$  from the image, then we tend to note with  $m+, -$  the mapping of right higher  $x+, -$ ,  $m+, +$  the mapping of right lower  $x+, +$ ,  $m-, +$  the mapping of left lower  $x-, +$  and  $m-, -$  the mapping of left lower  $x-, -$ , then the interpolated adaptational bar graph leveling is cypher with:

$$m(i) = a [bm-, -(i) + (1 - b)m+, -(i)] + [1 - a] [bm-, +(i) + (1 - b)m+, +(i)]$$

where

$$a = \frac{y - y_-}{y_+ - y_-}, a = \frac{x - x_-}{x_+ - x_-}$$

### 5 Result Analysis

In Fig. 3 Fingerprint module is shown. First of all user should give input of the fingerprint to access the application (Fig. 4).



Fig. 3. Finger print module

In this figure Input is converted into gray image and as well as black and white image. After implementation of edge detection, statistical and texture features are used. After identification process, Authorized person will be accessed in next figure (Figs. 5 and 6).

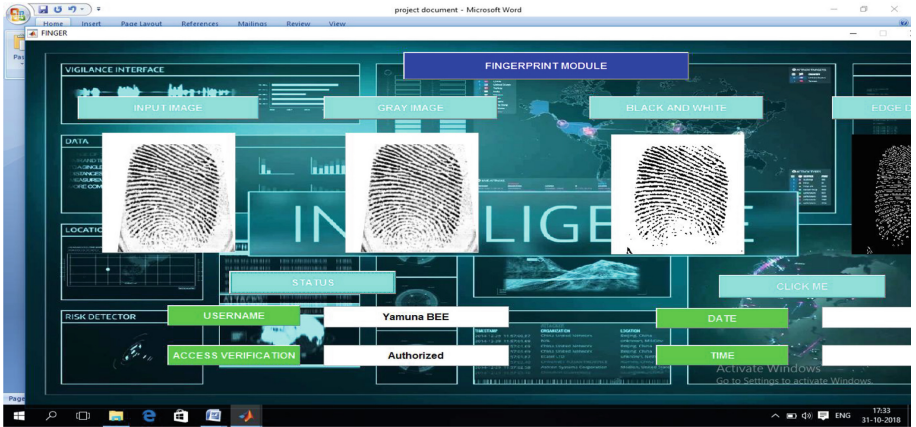


Fig. 4.

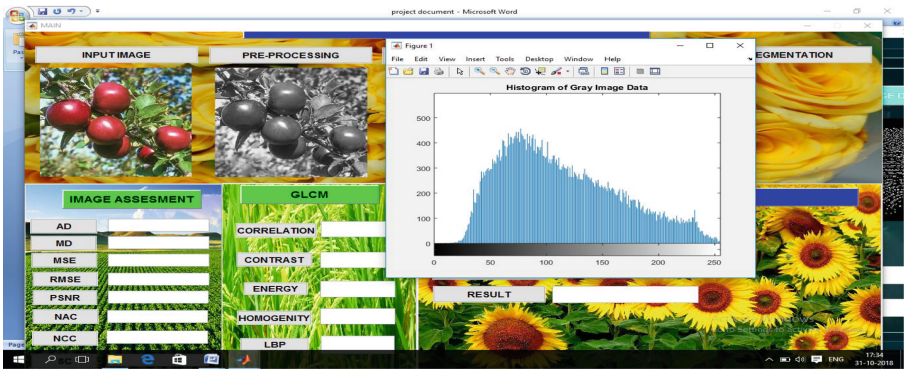


Fig. 5. Pre-processing histogram of gray image data

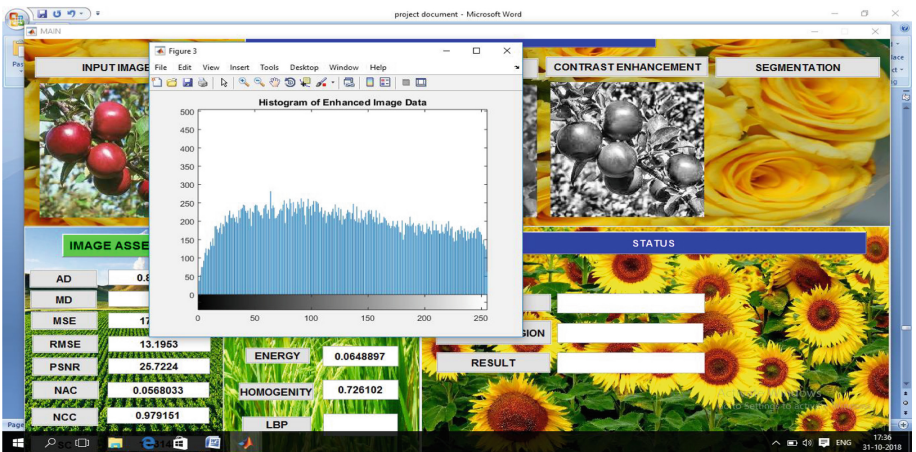


Fig. 6. Contrast enhancement histogram of enhancement of data

In this figure, input is uploaded in application. After gray colour conversion, input is converted into gray image and gives histogram plot.

## 6 Conclusion

The project system might be a mixture of package and hardware, so for associate oversized scale farming production the number of cameras and length of conveyor system is modified system. This paper presents integrated techniques for sorting and grading of assorted food and fruits. sometimes image capture might be a large decision task and challenge as there is a chance of high uncertainty thanks to the external lighting conditions, so we have a tendency to tend to are taking the advantage of gray scale image that are user friendly to the external setting changes to boot as useful for locating size of a food and fruit. Same approach whereas aggregation fruits or vegetables from conveyor system by a main plate there is variation among the burden mensuration of a food and fruit so any vogue is modified so fruits is collected stably. Speed and efficiency of a system is any improved by Arduino UNO for the identical purpose.

## REFERENCES

1. Agriculture in India: Information About Indian Agriculture & Its Importance. <https://www.ibef.org/industry/agriculture-india.aspx>. Accessed 18 June 2017
2. Agriculture in India. [https://en.m.wikipedia.org/wiki/Agriculture\\_in\\_India](https://en.m.wikipedia.org/wiki/Agriculture_in_India). Accessed 18 June 2017
3. Google I/O. <https://events.google.com/io/>. Accessed 18 June 2017
4. Gomes, J.F.S., et al.: Applications of computer vision techniques in the agriculture and food industry: a review. *Eur. Food Res. Technol.* **235**(6), 989–1000 (2012)
5. Zhang, F., et al.: Application of computer vision technology in agricultural field. *Appl. Mech. Mater.* **462**, 72–76 (2014)
6. Vibhute, A., et al.: Applications of image processing in agriculture: a survey. *Int. J. Comput. Appl.* **52**(2), 34–40 (2012)
7. Pérez, D.S., et al.: Image classification for detection of winter grapevine buds in natural conditions using scale-invariant features transform, bag of features and support vector machines. *Comput. Electron. Agric.* **135**, 81–95 (2017)
8. Vyas, A., et al.: Colour feature extraction techniques of fruits: a survey. *Int. J. Comput. Appl.* (0975 – 8887) **83**(15) (2013)
9. Naik, S., et al.: Shape, size and maturity features extraction with fuzzy classifier for non-destructive mango (*Mangifera Indica L.*, cv. Kesar) grading, *TIAR*(978-1-4799-7758-1), 5–11, July 2015
10. Pandey, R., et al.: Image processing and machine learning for automated fruit grading system: a technical review. *Int. J. Comput. Appl.* (0975 – 8887), **81**(16) 2013



# An Approximation to m-Ranking Method in Networks

K. Reji Kumar<sup>1</sup>(✉) and Shibu Manuel<sup>2</sup>

<sup>1</sup> Department of Mathematics, N. S. S. College, Cherthala, India  
rkkmaths@yahoo.co.in

<sup>2</sup> Department of Mathematics, St. Dominic's College, Kanjirapally, India  
manuelshibu@gmail.com

**Abstract.** Identifying important nodes in a network is an important area of research in network science. m-ranking method is a method proposed Reji Kumar et al. [18] for ranking the nodes in a network which avoids the chance of assigning same rank for two nodes with different physical characteristics. This ranking takes into account the degree of all nodes and weights of all edges in a network. As the network becomes bigger and bigger the m-ranking method takes more and more time to complete. To overcome this difficulty in this paper we propose an approximation to this method, which simplifies the calculations without undermining the ranking outcome. We illustrate the procedure in some example networks.

**Keywords:** Social networks · Centrality measures · m-ranking method · Approximation to m-ranking method

## 1 Introduction

Identifying important nodes in a network is an active area of research. A large number of articles are available in this area in the literature of social network analysis [3, 5, 19]. Some nodes play prominent role in spreading process in a network compared to other nodes. Role of such nodes variably affects the spreading process which depends on the context. A node which is connected to a majority of nodes in a network can spread information in a faster pace than those nodes which have less connection to other nodes. In the spreading of rumor or gossip in a network the content of the information and the level of interest shown by the person who transmits etc. can also affect the spreading process [10]. In the context of spreading virus in a computer network or spreading disease in network of individuals, identifying the potential spreaders is crucial to the control of spread [3]. By removal or deactivation of potential spreaders, we can control the spread of infection in the network. In some different contexts we need to boost up the spreading. For example, marketing of a new product, spread of innovative trends and cultural diffusion in a society we treat potential spreaders in an entirely different way [3]. Due to the dynamic nature of social networks, status of nodes changes over time. Some nodes which are important in the beginning may become less important and vice versa. Nodes having high degree are known as popular nodes. Popular nodes can attract the attention of other members and consequently contact of

popular nodes increases further [6]. Ordinary members prefer to establish link with the hubs (popular nodes), because it may help them to increase their popularity.

Degree centrality [9] is the simplest method which is used to rank the nodes. It is one of the oldest methods as well. Closeness centrality and betweenness centrality are two widely used measures which are used to distinguish nodes according to their importance. The k-shell decomposition method [11, 17] partition all nodes of a network into k shells by removing nodes iteratively.

In the Mixed Degree Decomposition [1] both residual degree (number of links connected to the remaining nodes) and exhausted degree (number of links connected to the removed nodes) are considered in the next level of decomposition. Neighborhood coreness [7] is a method which is designed based on the assumption that a spreader node with more connections to nodes located in the core of the network is more powerful. Page-Rank [2], Leader-Rank [8] etc. are some measures, which are very recently developed. All the methods have some limitations as a measure of nodes importance in the network. In 2012, Garas et al. [4] proposed a ranking method for weighted networks. In this method,  $k_i^1$ , the weighted degree of each node is first calculated. On the basis of the weighted degree the nodes are ranked. A common limitation of the above mentioned methods is that they rank some nodes having different network related properties in the same position. So these methods are less reliable.

A more reliable measure was proposed by Reji Kumar et al. in 2017 [18]. In this new ranking method, named m-Ranking of nodes, degrees of all nodes are considered to rank nodes of a network. Total power of each node in a network is calculated giving due consideration to the degree of all nodes and the weights of all edges in the network. Ranks of the nodes are determined using the total power. A node getting highest value is ranked first. Effectiveness of this method has been tested by the authors on a variety of networks [11–14, 16]. A similar procedure has been developed to identify important nodes in directed networks [15]. The formula used for m-ranking is given below.

$$T(i) = \left\{ A \left[ d_i^{(0)} + \frac{1}{B} \sum d_i^{(1)} + \frac{1}{B^2} \sum d_i^{(2)} + \dots \right] + (1 - A) \left[ \sum W_i^{(0)} + \frac{1}{B} \sum W_i^{(1)} + \frac{1}{B^2} \sum W_i^{(2)} + \dots \right] \right\}$$

In the formula  $A = P/q$  (a real number) is a parameter between 0 and 1 and  $B > 1$  is another parameter. It is good practice to choose  $B$  an integer close to the average degree of the nodes of the graph. The first series in the formula contains at most  $D + 1$  terms and second series contains at most  $D$  terms, where  $D$  is the diameter of the graph. Here  $d_i^{(0)}$  is the degree of the node  $i$ ,  $\sum d_i^{(j)}$  is the sum of the degrees of the nodes at a distance  $j$  from  $i$ . Similarly,  $\sum W_i^{(0)}$ , is the sum of the weights of incident edges to  $i$  and  $\sum W_i^{(j)}$  is the sum of weights of edges  $j$  away from the node  $i$ . Since we are considering degree of all nodes and weights of all links, usually total power of nodes will be different. Therefore, there are very little chance for different nodes have equal rank. When  $B$  value is very large this method gives usual degree centrality.



Since the m-ranking method uses the weights of all nodes and edges in the network for the calculation of the total power of each node, this method takes more time for its computation. This may make the method inappropriate when we apply in network having huge size. In practice it is not required to consider all nodes and edges in the calculation. While calculating the total value of a node  $v$ , we can limit the use of nodes and edges which lay within a pre-decided distance say  $k$ . Total values of the nodes are calculated for  $k = 1, 2, 3, \dots$ . This approximation is illustrated with the help of suitable examples in the following section.

## 2 An Approximation to the m-Ranking Formula

We calculate different levels of ranks for the nodes using specific number of terms in the formula. Let  $R^1$  be rank obtained by considering only one term in the first series in the m-ranking formula.  $R^2$  is the rank obtained by considering two terms in the first series and one term of the second series in the m-ranking formula. Similarly,  $R^3$  is the rank obtained by taking three terms of the first series and two terms from the second series in the m-ranking formula and so on. We compare the ranks of the nodes in subsequent steps. When we see same ranks repeat for the same nodes in adjacent steps we stop.

We find the correlation of the successive ranks, using Kendall’s tau (here denoted by  $\tau$ ) value of the rank obtained in each step with the rank obtained in the previous step. The Kendall’s tau value considers two sets of ranking values  $X$  and  $Y$ . Two pairs of observations  $(x_i, y_i), (x_j, y_j) \in (X, Y)$  are said to be concordant if the ranks of both elements agree:  $x_i < x_j$  and  $y_i < y_j$  or if both  $x_i > x_j$  and  $y_i > y_j$ . They are said to be discordant if  $x_i < x_j$  and  $y_i > y_j$  or if both  $x_i > x_j$  and  $y_i < y_j$ . If  $x_i = x_j$  or  $y_i = y_j$ , the pair is neither concordant or discordant. The Kendall’s correlation coefficient is defined as

$$\tau = \frac{n_c - n_d}{0.5n(n - 1)}$$

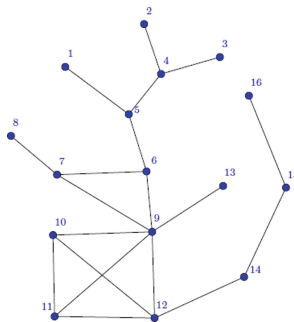


Fig. 1. Example network containing 16 nodes and 19 edges

where  $n_c$  is the number of concordant pairs  $n_d$  is the number of discordant pairs respectively. If the  $\tau$  value is near 1, the more accurate the ranked lists and if  $\tau$  is near 0 there is no correlation between the two ranks. If  $\tau$  value is near  $-1$ , the two ranks are negatively correlated. The approximation method is illustrated using an example network given in Fig. 1. This is an un-weighted network with 16 nodes and 19 edges.

As mentioned at the end of Sect. 2, we have calculated  $R^1, R^2, R^3$ , etc. and are tabulated in the Table 1.

**Table 1.** Ranking of nodes in the network given in Fig. 1.

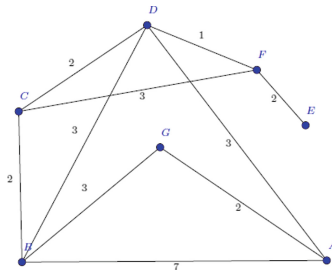
Rank	$R^1$	$R^2$	$R^3$	$R^4$	$R^5$	$R^6$	$R^7$
1	9	9	9	9	9	9	9
2	12	12	12	6	6	6	6
3	4, 5, 6, 7, 10, 11	6, 10, 11	6	12	12	12	12
4	14, 15	5, 7	10, 11	7, 10, 11	10, 11	10, 11	10, 11
5	1, 2, 3, 8, 13, 16	4	7	5	7	7	7
6		14	5	14	5	5	5
7		13	14	13	14	14	14
8		15	13	4	13	13	13
9		1	4	8	4	4	4
10		2, 3, 8	15	1	8	8	8
11		16	1	15	1	1	1
12			2, 3	2, 3	15	15	15
13			16	16	2, 3	2, 3	2, 3
14					16	16	16

Since the network in the above example is un-weighted we consider only degree of nodes. So in the calculation of  $R^i$ , we use  $A = 1$  and  $B = 2$ . In the sixth and seventh steps ranks obtained are same. As the ranks of the nodes repeat in three successive steps we complete the procedure. In the above example, nodes 2 and 3 are identical. So they have equal rank. Similarly, nodes 10 and 11 are identical and they also have equal rank in all steps (Table 2).

**Table 2.** Kendall's tau value for ranks in Table 1.

$\tau(R^i, R^{i+1})$	Value
$\tau(R^1, R^2)$	0.70
$\tau(R^2, R^3)$	0.84
$\tau(R^3, R^4)$	0.95
$\tau(R^4, R^5)$	0.96
$\tau(R^5, R^6)$	0.97
$\tau(R^6, R^7)$	0.97

From the table it is clear that tau values converge and the difference in successive ranking narrows down. So we take the seventh ranking as the final ranking on nodes. Next we proceed to calculate the successive ranks of a weighted network. This network contains seven nodes and ten edges. All the edges are weighted. The network is given in the Fig. 2.



**Fig. 2.** Example network containing 7 nodes and 10 edges

For this weighted network, we calculate total power  $T(i)$  of each node using the  $m$ -ranking equation with  $A = 0.5$  and  $B = 2$ .

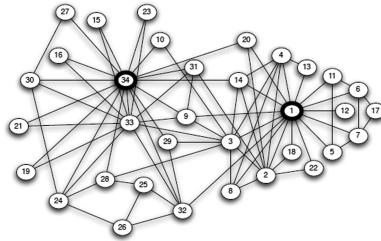
**Table 3.** Ranking of nodes in the network given in Fig. 2.

Rank	$R^1$	$R^2$	$R^3$	$R^4$	$R^5$
1	B, D	B	B	B	B
2	A, C, F	A	D	D	D
3	G	D	A	A	A
4	E	C	C	C	C
5		F	F, G	F	F
6		G	E	G	G
7		E		E	E

Ranks at each stage for the nodes in the network are in the Table 3. In  $R^4$  and  $R^5$  all the nodes are ranked with different ranks. Kendall’s tau are calculated for the above network as follows.  $\tau(R^1, R^2) = 0.33$ ,  $\tau(R^2, R^3) = 0.85$ , and  $\tau(R^3, R^4) = 0.90$  and  $\tau(R^4, R^5) = 1.0$ . Here,  $R^4$  and  $R^5$  are perfectly correlated and thus the rank  $R^5$  is taken as the final rank of the nodes.

### 3 Application of the Approximation Method in a Real Network

In this section we apply the approximation method in the ranking of a real network. We adopt the famous Karate club [20], network in our study. It describes a network of 34 members, documenting 78 pair wise links between members who interacted outside the club. This network signifies the interrelationship between the members of the Karate club from 1970 to 1972.



**Fig. 3.** The social network of friendships within a 34-person karate club.

There were two prominent figures in the network, who played key roles in the network dynamics. At the end, the network split into two. Network analysis is conducted on this network using the data available in [21]. Karate club network is given in the Fig. 3. Ranks of the nodes obtained in the successive steps are given in the Table 4.

**Table 4.** Ranking of nodes in the karate club network.

Rank	$R^1$	$R^2$	$R^3$	$R^4$
1	34	1	1	1
2	1	34	34	34
3	33	3	3	3
4	3	33	33	33
5	2	2	14	14
6	4, 32	9	32	32
7	9, 14, 24	14	9	9
8	6, 7, 8, 28, 30, 31	32	2	2
9	5, 11, 20, 25, 26, 29	4	20	4
10	10, 13, 15, 16, 17, 18, 19, 21, 22, 23, 27	31	4	20
11	12	24	31	31
12		8	29	29

(continued)

**Table 4.** (continued)

Rank	$R^1$	$R^2$	$R^3$	$R^4$
13		20	8	8
14		30	24	24
15		28	15, 16, 19, 21, 23	28
16		29	28	30
17		6, 7, 15, 17, 19, 21, 23	30	15, 16, 19, 21, 23
18		10	6, 7	6, 7
19		5, 11, 18, 22	10	10
20		13	18, 22	18, 22
21		27	5	5
22		26	11	11
23		25	13	13
24		12	26	27
25		17	27	26
26			12	12
27			25	25
28			17	17

The calculated Kendall’s tau values are  $\tau(R^1, R^2) = 0.677$ ,  $\tau(R^2, R^3) = 0.852$  and  $\tau(R^3, R^4) = 0.935$ . Clearly the correlation between  $R^3$  and  $R^4$  is very close to 1. So we take  $R^4$  as the final ranking of nodes of the network. In this network, nodes 6, 7, 15, 16, 19, 21, 23 are identical and have same rank in each step. Similar is the case of the nodes 6 and 7. There is one more pair of nodes having the same property. They are the nodes 18 and 22. Node 1 is ranked first. It is followed by the node 34. These are the most prominent players in the network.

## 4 Conclusion

In this paper we present an approximation method to the m-ranking method. Since m-ranking method takes into account all nodes and all edges in a network, this method takes more time to give a result. In practice we can obtain a better ranking without calculating all terms in the formula for m-ranking method. This is the motivation behind the study presented in this paper. We have explained the approximation method and illustrated it with suitable example. Finally we applied the method on a real network to obtain the ranking of the nodes. This method can be tested using many other real networks. It is proposed as an area for future research.

**Acknowledgements.** First author would like to acknowledge the research facilities extended by Institute of Mathematical Sciences, Chennai by granting the Associate Visitor-ship. A part of the research is completed during this period. He also likes to acknowledge the financial support of UGC in the form insert of a major research project No. 40-243/2011(SR). A part of this research is completed during this visit. The second author would like to thank the financial support given to him by UGC in the form of FDP (FIP/12th Plan/KLMG018 TF06).

## References

1. Zeng, A., Zhang, C.-J.: Ranking spreaders by decomposing complex networks. *Phys. Lett. A* **377**, 1031–1035 (2013)
2. Brin, S., Page, L.: The anatomy of a large- scale hyper textual web search engine. *Comput. New. ISDN Syst.* **30**, 107–117 (1998)
3. Easley, D., Kleinberg, J.: *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*. Cambridge University Press, Cambridge (2010)
4. Garas, A., Schweitzer, F., Havlin, S.: A k-shell decomposition method for weighted networks. *New J. Phys.* **4**, 083030 (2012)
5. Jaber, L.B., Tamine, L.: *Active micro bloggers: identifying influencers, leaders in micro blogging networks*. Springer (2012)
6. Jackson, M.O.: *Social and Economic Networks*. Princeton University Press, Princeton (2010)
7. Bae, J., Kim, S.: Identifying and ranking influential spreaders in complex networks by neighborhood coreness. *Phys. A* **395**, 549–559 (2014)
8. Li, Q., Zhou, T., Lu, L.: Identifying influential spreaders by weighted leader rank. *Phys. A* **404**, 47–55 (2014)
9. Bordons, M.: The relationship between the research performance of scientists and their position in co - authorship networks. *J. Inform.* **9**, 135–144 (2015)
10. Rosnow, R.L., Foster, E.K.: We should distinguish between rumors and gossip as each appears to function differently in its pure state. *Psychological Science Agenda*, American Psychological Science Association, April 2005
11. Reji Kumar, K., Manuel, S.: Spreading information in complex networks: a modified method. In: *Proceedings of the International Conference on Emerging Technological Trends*. IEEE Digital Explore Library (2016)
12. Reji Kumar, K., Manuel, S.: Personal influence on the spreading of information – a network based study. *Int. J. Math. Trends Technol.* **52**(8), 570–573 (2017)
13. Reji Kumar, K., Manuel, S., Sathesh, E.N.: Spreading information in complex networks: an overview and some modified methods. In: *Graph Theory Advanced Algorithms and Applications*. Intechopen (2017)
14. Reji Kumar, K., Manuel, S.: A centrality measure for directed networks: m-ranking method. Zyer, T., et al. (eds.) *Social Networks and Surveillance for Society*. *Lecture Notes in Social Networks*. Springer, Heidelberg (2019)
15. Reji Kumar, K., Manuel, S.: Collaborations of Indian institutions which conduct mathematical research: a study from the perspective of social network analysis. *Scientometrics*. <https://doi.org/10.1007/s11192-018-2898-0>
16. Reji Kumar, K., Manuel, S.: A network analysis of the contributions of Kerala in the field of mathematical research over the last three decades. In: *Proceedings of the International Conference on Computer Networks, Big Data and IoT (ICCBI 2018)* (2018)

17. Manuel, S., Reji Kumar, K.: An improved k-shell decomposition for complex networks based on potential edge weights. *Int. J Appl. Math. Sci.* **9**(2), 163–168 (2016)
18. Manuel, S., Reji Kumar, K., Benson, D.: The m-Ranking of nodes in complex networks. In: *Proceedings of 9th International COMSNETS 2017* (2017)
19. Lewis, T.G.: *Network Science: Theory and Practice*. Wiley, Hoboken (2009)
20. Zachary, W.W.: An information flow model for conflict and fission in small groups. *J. Anthropol. Res.* **33**, 452–473 (1977)
21. [www.personal.umich.edu/mejn/netdata](http://www.personal.umich.edu/mejn/netdata)



# Cloud Service Prediction Using KCFC Approach

K. Indira<sup>1</sup>, C. Santhiya<sup>1</sup>(✉), and K. Swetha<sup>2</sup>

<sup>1</sup> Department of Information Technology,  
Thiagarajar College of Engineering, Madurai, India  
csit@tce.edu

<sup>2</sup> Thiagarajar College of Engineering, Madurai, India

**Abstract.** Cloud computing is an emerging paradigm where the user can benefit many efficient services. Since many services resemble the same functionality, the user faces relevant and un-relevant information as data burden. So, Recommender System (RS) is getting used to suggest the user only the information that suits their search. Here (CFC)-Collaborative Filtering Coefficient is used as RS which functions by analyzing user history and similar service from neighbor users. Pearson coefficient is used to calculate the association between the services. But, it works for existing users not for new users because the further user details are not sufficient to recommend a service. To overcome this, the KNN approach is utilized to classify the recommendation from a k-nearest neighbor by finding the resemblance between various client ratings using Euclidean Distance measure. Thus, the KNN-CFC hybrid novel approach can create a new efficient RS framework which supplies the client a most relevant service information with low execution time for various data densities and different users and services.

**Keywords:** Quality of service · k-Nearest Neighbour · CFC-Collaborative Filtering Coefficient · Pearson coefficient · Recommendation system

## 1 Introduction

Cloud computing is an amounting mechanism that provides services based on user demand (computing power, storage resources, applications, etc.). It has become famous now, since it allows for plenty of nature with the purpose of improves internet people on the way to struggle it, for example reliability, security, agility, performance, etc. [1]. It provides three various services, Infrastructure as a service, Platform as a service and Software as a service via the internet with pay-as-you-go pricing. Many cloud services supply similar services which are the challenge designed for the users to decide a relevant repair so as to fits precisely with their needs. Due to the existence of several websites that provide an enormous quantity of information on the same items, the clients are overcharged with irrelevant and relevant service info. To find the suitable web services based on user request, the web service suggestions are used. Recommender systems take users' interest as input and apply certain methods to sieve the



available information and deliver the user with the enormous lump of information called recommendations. But, whenever a new user drives through the website, the recommender system is not able to predict a user's interest due to the lack of the user's details known as cold start problem [2]. Regarding the recommendation system, cold start issue with new user regarding no rating of new products new; those services will not have any ratings, therefore will not be able to suggest to other users. Since the majority work in recommendation system is based on nearest neighbors' information, this work helps the cloud providers to promote their services and cloud users in the direction of recognize services so as to assemble their QoS requirements (e.g., response time, security, availability, reliability, throughput, etc.). High QoS with services satisfies the client then some additional features are to be used such as user's ratings, service completing, revenue model and business methods, etc. [3]. CF approach with QoS based RS is used to suggest the relevant services by using Pearson coefficient. The approach is used to forecast in cooperation QoS category of cloud services. Reliable ranking can be attained through this approach using the Pearson coefficient. The Collaborative Filtering Algorithm (CF) is a known technique in the recommender systems that deal with the human making decisions through their previous search. Adding to the experience, decisions may be taken based on some knowledge they may come across from a group of associates. This set of knowledge can be taken for suggestions. CF-based RS allow users to give rating about a set of elements (hotels, theatres) in such a way that where every information is stored in the database which can be used for recommendation. The suggesting quality comes from the capacity to find the common number of users made that votes or ratings [4]. The CF faces the troubles of missing of data and enlargement of data. Data sparsity refers to the situation when available data (e.g., ratings) is not such client to conclude the region of the energetic user so, nearly all and sundry of the services resolve not encompass precise ratings or one ratings at all [5]. Many available services will not be used for this reason. To overcome this KNN-CFC (K Nearest Neighbour – Collaborative Filtering Coefficient) approach is used to attain more reliable rankings than a CF approach and also attain exactness and scalability. In kNN, resemblance metric such as Euclidean distance is used to study the relation of a query to the neighboring query. The association of training dataset with 1 – D distance space based on found similarities and labeling them [6].

## 2 Related Works

Mezni et al. [7] stated that the client could face large similar operating services due to the presence of many websites. So, the recommendation system was provided to solve this issue. Then the new user may suffer from low recommendations due to few votes and service ratings. This problem was called the cold start problem. To overcome this recommendation system was combined with unclear recognized notion examination. After Implemented the unclear recognized notion Analysis-based service proposal come up to the concert and the excellence of fashioned recommendations in judgment through on hand high-tech solutions.

Hayyolalam et al. [9] provided a numerical examination of the previous approach for QoS-aware cloud service composition/selection. QoS monitoring can provide the QoS of a cloud service (Client workstation monitoring, server-side monitoring, and third-party monitoring). The quality assessment checklist had been famed, and the quality of service was monitored. The selection for the recommendation was made based on the assessment report.

Ertuğrul et al. [10] proposed the KNN approach which was the machine learning technique finds the k-Nearest Neighbour by using the resemblance metric such as Euclidean distance. Based on the gradient between the query and each sample weight was given to the query similarity for differentiation. Mapping process kNN was carried out to predict the likeliness, with a question being positioned happening a location procession and supplementary samples were mapped to a 1-D distance line based on the expanse to the uncertainty.

Ortega et al. [11] proposed to beat the data burden problem recommendation System was used. It was better to use the recommendation framework that would function as to design and implement recommendation method, increasing the execution time. Here the proposed work was CF4 Opensource library intended en route for holdout CF based RS, which allows reading RS Dataset, jam-packed and easy entrée to figures.

Kumar et al. [12] made the comparison of many various machine learning algorithms to obtain the successful extraction of internet answer instance plus throughput events. Baking was the successful method for extracting the absent answer time and sequential minimum optimization regression be the achievement technique designed for extracting throughput values. The absent principles of the real world datasets was extracted using this two models for recommendation instances.

Hadeel et al. (2014) proposed the significance of digital knowledge, social network in addition to information withdrawal to individualize the social information withdrawal application inside stipulations of the instructor's and student's requirements. information withdrawal techniques such as classification, clustering of the post, comments given in the Facebook like social networks were discovered to improve the student's usage of e-learning.

### 3 Methodology

#### 3.1 Quality of Service

QoS defines the range of execution, consistency, and availability obtainable by an submission and by the proposal [14, 15]. QoS is extremely significant designed for users, who anticipate providers to distribute the superiority and meant for providers, encompass to switch the trade-offs among QoS levels and equipped expenses. Through this approach, the service promotion and identification of quality services are done. High QoS with services satisfies the client then some additional features are to be used in business model and completion time. The work deals with the QoS-based cloud service recommendation, and propose a CF approach using the Spearman coefficient to suggest cloud services. The scheme is new to estimate in cooperation place and QoS

rating for cloud services. QoS monitoring involves Client-side monitoring, server-side monitoring, and intermediary monitoring. The a range of excellence metrics like business plan, failure time and failure recovery etc. suggestions [16, 17, 18]. CF-based RS helps the client to give a rating for a set of services (hotels, theatres)in such a way that where every information is stored in the database which can be used for recommendation. The quality of advice comes from the capacity to find the typical number of users made that votes or ratings.

### 3.2 KNN-CFC (K Nearest Neighbor - Collaborative Filtering Coefficient)

Reliability, accuracy and scalability are attained through KNN-CFC approach. In kNN, the relative of a uncertainty to the neighboring query is learned from a parallel metric, Euclidean distance [20, 21]. The association of training dataset with 1 – D distance space based (Fig. 1).

$$d(x,y) = (i = 1 \text{ to } n) \tag{1}$$

Therefore in Eq. (2)  $(x, y)$  is the distance between the samples  $x$  and  $y$ , having  $n$  dimension. The decisions can be taken from the class of a sample based on the extracted similarity. The difference among the sample. KNN is largely used in the classification problems though it is effective for both classification and regression problems. Consider a spread of blue circle(bc) and blue square(bs) have to find the class of red star(rs). Here  $k$  is the nearest neighbor we wish to take a vote from. If  $k = 3$  then by placing the rs as a center it will group the bc and it comes under the class of bc Fig. 2.a, b.

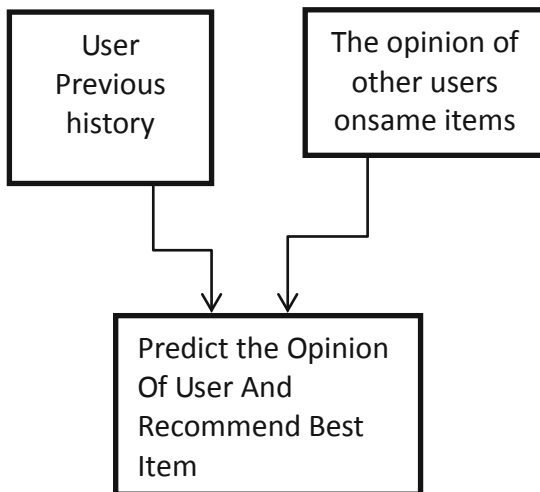
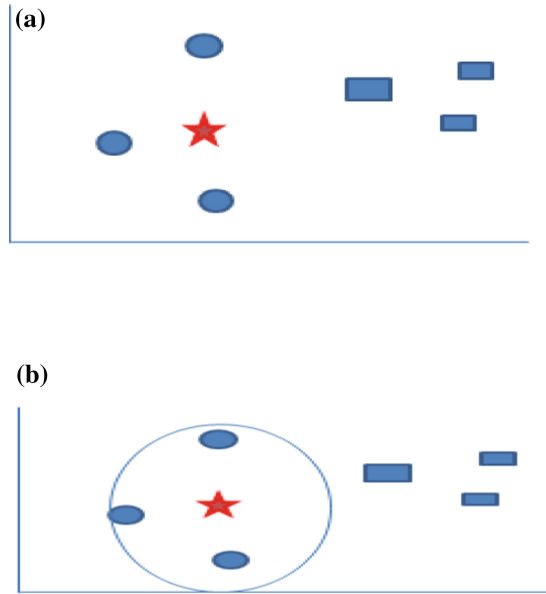


Fig. 1. Predicting recommendation



**Fig. 2.** a. The red star among the sparse particles. b. The red star belongs to the class blue circle.

#### **KNN-CFC algorithm steps:**

**Step 1:** Loading the dataset as input for preprocessing state.

**Step 2:** Set value of K for predicting number of clusters to be made.

**Step 3:** Predicted class iteration from 1 to no of the training set.

**Step 4:** Calculate Euclidean distance to predict the similarity among the dataset.

**Step 5:** Sort the distance in ascending order.

**Step 6:** Get the Top k rows that attain the most similar pattern.

**Step 7:** Get the frequent class of rows that represents the association among the dataset.

**Step 8:** Return predicted class from the observation.

### **3.3 System Architecture**

Figure 3 says that the user asks for a cloud service and the server recommends the user's search-related items by predicting the users' history and other users similar search topics. The recommendation system using Collaborative Filtering Coefficient filter and cluster the similar information and the result is listed with KNN classification approaches that predict the user service similarity from the k amount of adjacent nodes, the similarity is calculated from the Euclidean distance then predict the top frequently occurring services as a class to attain accuracy [22]. Then the novel recommendation system suggests the user the relevant information. Here Cloud provider may provide movie recommendation as a cloud service that is controlled by cloud administrator. This cloud service which contains multiple movie recommendation but for the perfect

service to the potential user, the recommendation engine will perform KNN classification which has the more impact on CFC. This Core CFC and KNN will provide the perfect service to the cloud users. Distance between the nearest cloud service users is calculated by various distance metrics and finally which has evaluated with real time cloud service providers. Here history of the users is very important essential keyword for the perfect services.

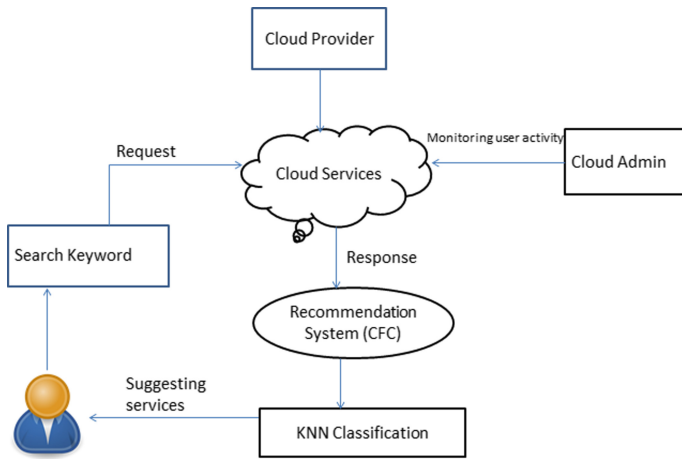


Fig. 3. System Architecture

## 4 Results and Discussion

The movie lens dataset is analyzed with 6000 users with 400 tags for timesharing nature in the hadoop framework environment to process the user information in a parallel manner. This service is deployed in the open source cloud platform (IaaS) to movie recommendation as a cloud service. With this setup the effective execution time and response time of the various users to be measured.

### 4.1 Precision, Recall and F-Measure

The new proposed system provides precision, recall and f-measure to evaluate the recommender system in a better way. The following table gives the values evaluation metrics (Figs. 4 and 5).

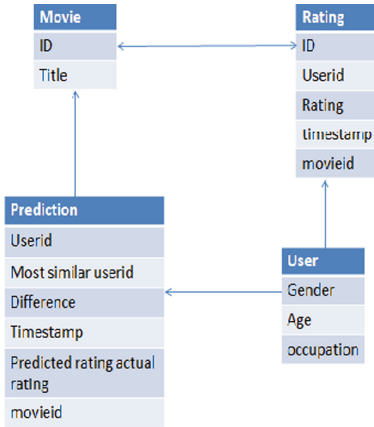


Fig. 4. Class diagram for a prediction

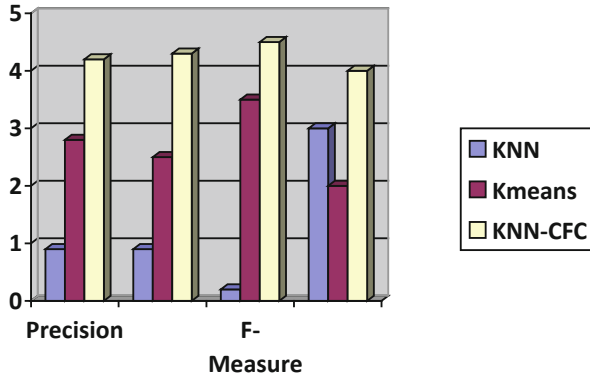


Fig. 5. Precision, Recall and F-measure

### 4.2 Evaluation Measure

We espouse the Mean Absolute Error (MAE) method and the Root Mean Squared Error (RMSE) method, which are broadly second-hand in a lot of recommendation systems, to appraise the routine of the new model. The terminology is as follows:

$$MAE = \frac{1}{N} \sum_{i=1}^N |q(i) - r(i)| \tag{2}$$

where  $N$  is the number of testing data samples and represents the prediction score according to Eq. (2).

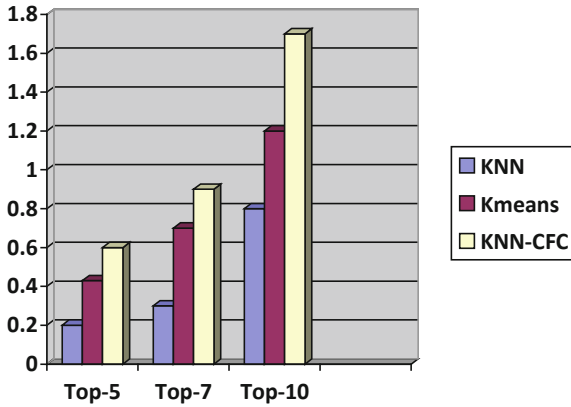


Fig. 6. Mean Absolute Error

### 4.3 Execution Time with Different no of Services

The experiment deals with the no of services and time in seconds for various data density in Fig. 6. Initially, the time is 100 s for 96 number of services for the data density 20%. And the time increases from 250–390 for the range 300–600 number of services for the density 40% and 60%. When there is a high data density, the recommendation time increases along with the improved number of services. It limits the search process to minimum data density. So, there commendation algorithm (collaborative filtering approach) can find parallel users and top-rated services.

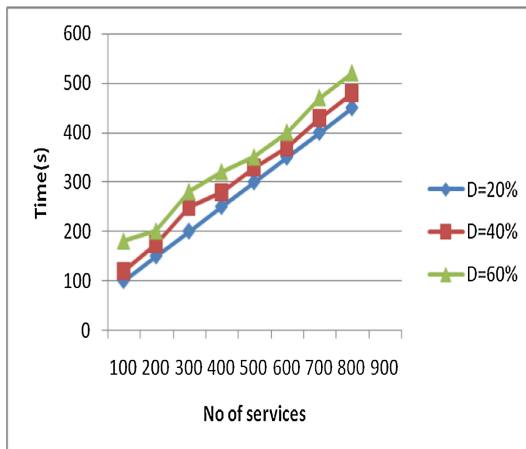


Fig. 7. Execution time comparisons

#### 4.4 Recommendation Time with Various no of Users

The experiment deals with the no of users and time in seconds for various data density in Fig. 7. Here the computation time is 110 s when the user’s count are less than 100 for rating density of 20% with top k recommendation [10]. Then the time varies from 190 to 350 for the user’s count is in the range of 400–700 for density 40% in top k = 10. So, the time increases with the user’s count and ratings as well. This helps to find the similarity in first few steps and works better with large ratings [24] (Fig. 8).

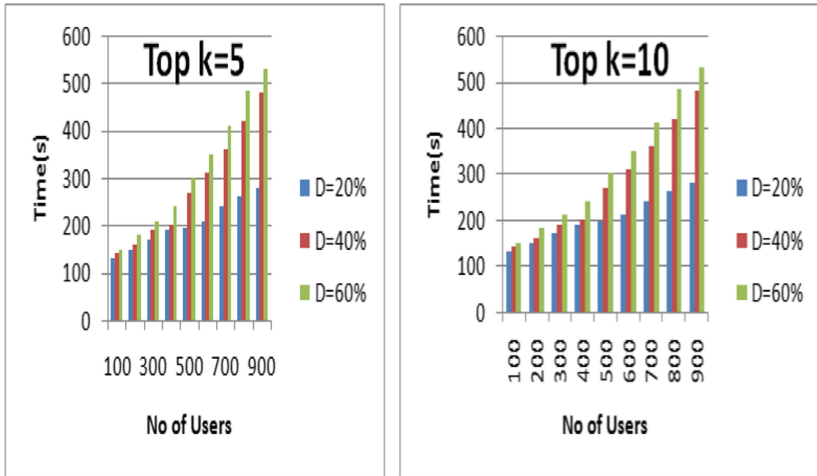


Fig. 8. Execution time comparisons

## 5 Conclusion

Recommendation system provides the service that the client looking for and overcome the challenge of correct service selection. Here we used a hybrid RS framework that combines the CFC clustering technique and the KNN technique. The CFC clustering technique is used to extract the active users relevant services based on the user history and similar neighbor user’s service votes. The KNN technique is suitable to find the recommendation even for the new user’s searching of services that reduce the service delivery time from cloud providers to the users. The user can also benefit the relevant service information. The execution time is low for predicting the large amount similar services from the cloud provider. The recommendation time is less when comparing with many cloud services even for large user rates. The recommendation framework performs with the help of QoS ranking and user rating. The research had been made with the small dataset and research on an actual social cloud will be the real test proposal in the future works.



## References

1. Jannati, H., Bahrak, B.: An improved authentication protocol for distributed mobile cloud computing services. *Int. J. Crit. Infrastruct. Prot.* **19**, 59–67 (2017)
2. Camacho, L.A.G., Alves-Souza, S.N.: Social network data to alleviate cold-start in recommender system. *Inf. Process. Manag.: Int. J.* **54**(4), 529–544 (2018)
3. Wang, S., Zhao, Y., Huang, L., Xu, J., Hsu, C.H.: QoS prediction for service recommendations in mobile edge computing. *J. Parallel Distrib. Comput.* (2017)
4. Wei, J., He, J., Chen, K., Zhou, Y., Tang, Z.: Collaborative filtering and deep learning based recommendation system for cold start items. *Expert Syst. Appl.* **69**, 29–39 (2017)
5. Salah, A., Rogovschi, N., Nadif, M.: A dynamic collaborative filtering system via a weighted clustering approach. *Neurocomputing* **175**, 206–215 (2016)
6. Li, J., Zhang, K., Yang, X., Wei, P., Wang, J., Mitra, K., Ranjan, R.: Category preferred Canopy-K-means based collaborative filtering algorithm. *Future Gener. Comput. Syst.* **93**, 1046–1054 (2018)
7. Mezni, H., Abdeljaoued, T.: A cloud services recommendation system based on Fuzzy Formal Concept Analysis. *Data Knowl. Eng.* **116**, 100–123 (2018)
8. Bobadilla, J., Ortega, F., Hernando, A., Bernal, J.: A collaborative filtering approach to mitigate the new user cold start problem. *Knowl.-Based Syst.* **26**, 225–238 (2012)
9. Hayyolalam, V., Kazem, A.A.P.: A systematic literature review on QoS-aware service composition and selection in cloud environment. *J. Netw. Comput. Appl.* **110**, 52–74 (2018)
10. Ertuğrul, Ö.F., Tağluk, M.E.: A novel version of k nearest neighbor: dependent nearest neighbor. *Appl. Soft Comput.* **55**, 480–490 (2017)
11. Ortega, F., Zhu, B., Bobadilla, J., Hernando, A.: CF4 J: collaborative filtering for Java. *Knowl.-Based Syst.* **152**, 94–99 (2018)
12. Kumar, S., Pandey, M.K., Nath, A., Subbiah, K., Singh, M.K.: Comparative study on machine learning techniques in predicting the QoS-values for web-services recommendations. In: 2015 International Conference on Computing, Communication & Automation (ICCCA), pp. 161–167. IEEE, May 2015



# Detection and Classification of Tumors Using Medical Imaging Techniques: A Survey

Sheetal Garg<sup>1,2(✉)</sup> and S. R. Bhagyashree<sup>3</sup>

<sup>1</sup> ATME College of Engineering, Mysuru, India

<sup>2</sup> Department of Computer Science and Engineering,  
MVJ College of Engineering, Bangalore 560067, India  
sheetal.garg@mvjee.edu.in

<sup>3</sup> Electronics and Communication Engineering Department,  
ATME College of Engineering, Mysuru 570028, India  
bhagyashreeraghavan@gmail.com

**Abstract.** Cancer (tumors) is the cause of every sixth death around the world. This makes cancer a second leading cause of death. Globally 42 million people across the world suffer from cancer and this figure is continuously increasing. In India around 2.5 million people are suffering from different types of cancer. If detected in early stage, then with proper treatment it can be cured. This paper presents details of a few methods used for detection of diseases like Breast cancer, brain tumor, liver cancer, lung cancer and Spine tumor. This paper also speaks about the different machine learning techniques used to classify the diseases into malignant & benign.

**Keywords:** Positron Emission Tomography/Computed Tomography (PET/CT) · Magnetic Resonance Imaging (MRI) · Artificial Neural Network (ANN) · Fuzzy c means classifier · Support Vector Machine (SVM) · Region of interest

## 1 Introduction

In spite of several developments in the field of diagnosis of cancer, still Cancer is one of the most dangerous diseases. Cancer is the second most popular reason of death not only in India, but across the world. Diagnosis of Cancer is a very crucial task. Due to this reason, detection and treatment of cancerous tumors is one of the major research areas. The rate of survival for the patients can be improved, only if the cancer is diagnosed at the early stage and if proper treatment is given soon after the detection of the disease. There are various techniques to capture different types of cancers, to name a few, CT scan, PET scan, Mammograms, Single Photon Emission Computed Tomography (SPECT), MRI, 3D Ultrasound etc. For breast cancer diagnosis, mammograms are used. CT scan, MRI and other techniques are used to detect brain tumors, liver cancer, lung cancer, spine tumors etc. Doctors inspect images to detect cancer.

If cancer tissues are identified, then a biopsy is done to confirm whether the tumor is cancerous or not. This human process is prone to errors. Hence, of late researchers are concentrating on automatic detection and classification of cancer. This paper presents various types of cancer, the medical imaging techniques that are used for diagnosis and the various classification techniques that are used for the purpose of classification.

In this paper, the various imaging techniques based on machine learning are used for cancer categorization are considered. For breast cancer, the imaging technique considered is mammogram and the classification techniques used are Feed forward back propagation, Extreme Learning Machine (ELM) ANN, back propagation ANN, Particle Swarm Optimized Wavelet Neural Network and CNN based on deep learning. For brain tumors, imaging technique used is MRI and CT scan and the classification techniques considered are Level Set, K means Algorithm, SVM, Fuzzy C-means, Adaboost, Naïve Bayes classifier and ANN classifier. For lung cancer medical imaging technique used is PET/CT and classification techniques considered are FCM classifier, ANN, Feed Forward ANN, SVM binary classifier and Entropy degradation method. For spine tumor detection medical imaging technique considered are MRI and classification methods used are ANN, SVM and Multilayer perceptron neural network.

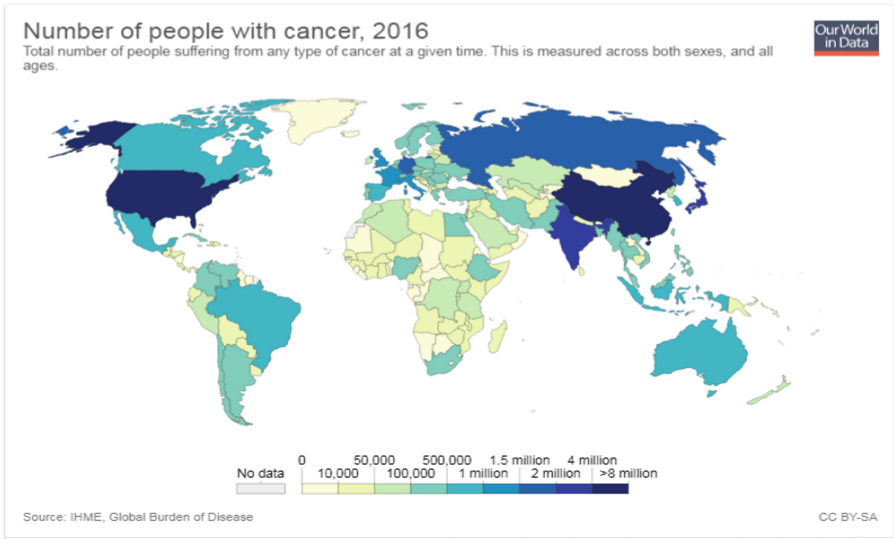
The remaining paper is structured as: Overall Literature Survey explored in Sect. 2. In Sect. 2, Sect. 2.1 gives the statistics of distribution of cancer worldwide and in India. Section 2.2 gives the survey for Breast Cancer Classification. Classification techniques used in diagnosis of Brain tumor is studied in Sect. 2.3. Section 2.4 gives an insight on classification techniques used in the diagnosis of Lung Cancer. Section 2.5 deals with Spine Tumor Classification techniques. Section 3 gives conclusion.

## 2 Literature Survey

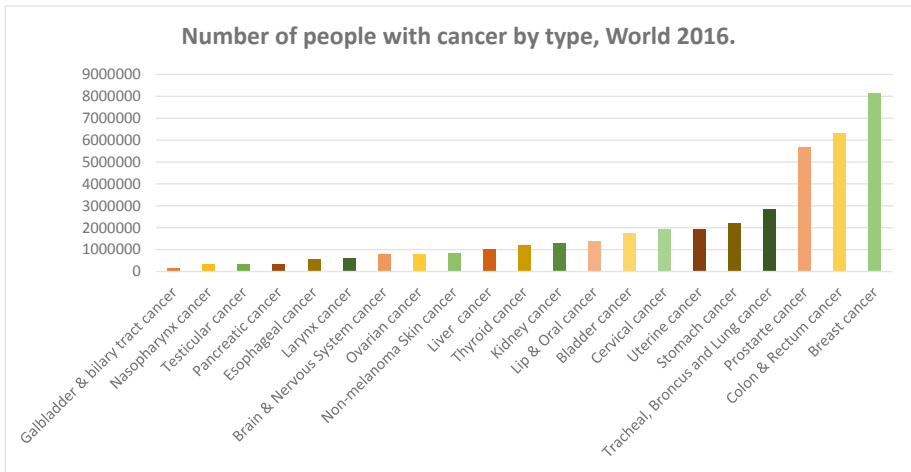
This part of the paper focuses on number of patients suffering from cancer across the country, the various types of cancers that they are suffering from, the techniques used in the diagnosis of these diseases, the techniques used in the classification of the subjects.

### 2.1 Statistics of Patients Suffering from Cancer

Even though there is a great advancement in the field of medical sciences we can find an exponential growth in the number of people affected from Cancer. According to a survey conducted in 2016 [1] globally 42 million people across the world are suffering from various types of cancers. Figure 1 provides the data on the number of people affected from cancer. From Fig. 1 it is clear that in China and in United States the number of people with cancer is more than 8 million, whereas Russia and India are the second leading counties with number of people exceeding 2 million.



**Fig. 1.** Number of people with cancer 2016 [1]



**Fig. 2.** Number of people with different types of cancer [1].

Figure 2 gives the breakup of number of people suffering from different types of cancers across the world [1]. This is measured across all ages and sex. Breast cancer, Colon & Rectum cancer have the highest number of patients i.e., around 8.5 million and 6.32 million respectively. Brain and Nervous system cancers like Spinal Cord tumors risk nearly 7,81,185 patients globally.

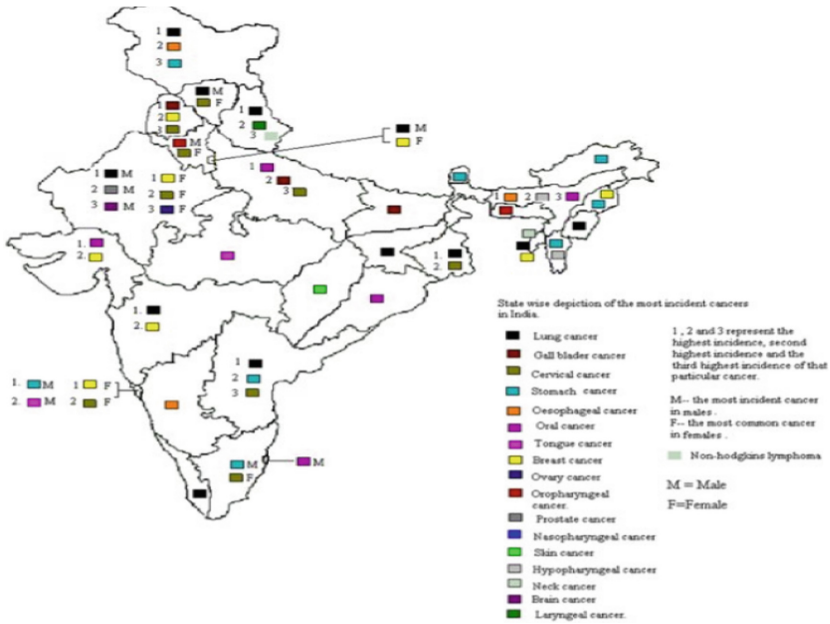


Fig. 3. Statewise distribution of different types of cancers [2].

As per the statistics, in India around 2.5 million people are suffering from different types of cancer [1]. Figure 3 gives the state wise distribution of cancer across India and this shows that cancer patients are distributed all over India. Few states have more types of cancer while others have a few. This may be due to the dietary habits, consumption of tobacco, alcohol, radiations and miscellaneous pollutants. In India states like West Bengal, Himachal Pradesh, Delhi, Uttarakhand, Rajasthan, Maharashtra, Jharkhand,

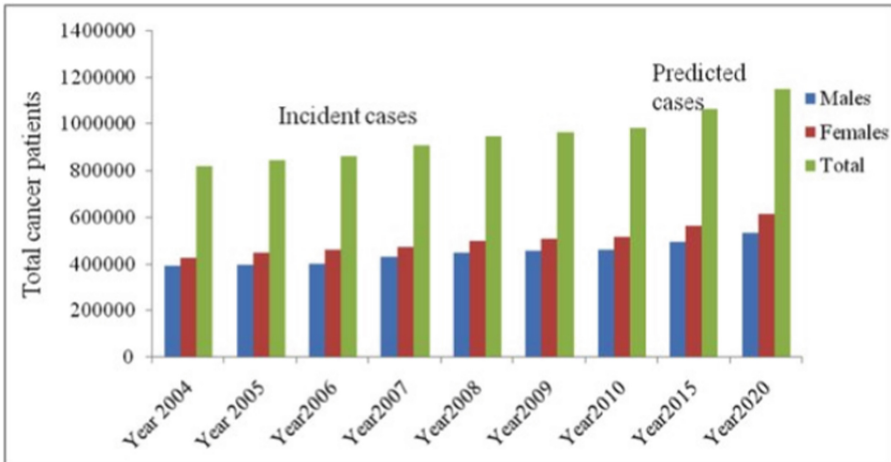


Fig. 4. Yearwise distribution of cancer cases [2].

Jammu & Kashmir, Andhra Pradesh, Kerala, Tripura and Manipur have more varieties of cancer compared to other states.

Figure 4 shows the year wise statistics of cancer in India. This depicts that the total number of patients suffering from cancer has increased with time [2]. The graph clearly states that the number of female patients is more in number compared to male patients.

Above statistics show that cancer is one of the major diseases globally and in India. This demands major advances in healthcare, specifically in cancer detection and classification. The mortality rate can be reduced if cancer is detected at early stage and is treated correctly.

## 2.2 Survey on Breast Cancer

Satish Saini et al. [3] developed a system for diagnosing Breast Cancer based on Image Registration. Artificial Neural Network enhanced the effectiveness of this system. The system was made up of Testing and Training Phase. Different features were extracted from 42 mammogram images using Gray Level Co-occurrence matrix (GLCM) technique. In a total of 42 images, 70:30 ratio of benign and malignant images. For training the images various features like Correlation, Sum Variance were calculated using varied angle values. Feed forward back propagation network for Artificial Neural Network (ANN) classified the images into cancerous and non-cancerous images. Levenberg–Marquardt back-propagation algorithm was used to Train the network and Mean Square Error (MSE) measured the performance. The system gave 98% accuracy.

Chandra et al. [4] used Artificial Neural Network for detecting breast cancer. Breast Cancer Wisconsin Dataset was used. The data had 699 instances consisting of 10 attributes along with the class attributes out of which 65.5% (458 instances) were benign and 34.5% (241 instances) were malignant. Features like Uniformity of Cell Size, lump Thickness, Uniformity of Cell Shape, Single Epithelial Cell Size, Marginal Adhesion, Bland Chromatin, Bare Nuclei, Mitoses, and Normal Nucleoli were considered. ELM could operate on both differentiable and non-differentiable activation function. K-fold cross validation method was used. ELMs learning process was slow compared to other method as it was found to be a complicated algorithm. In respect of accuracy and sensitivity ELM ANN outperformed Back Propagating ANN.

Dheeba et al. [5] developed a CAD system to help radiologists in finding cancer of breast. The diagnosis was done based on the texture of the 54 patients each two mammogram images. Particle Swarm Optimized Wavelet Neural Network (PSOWNN) was implemented to detect the abnormalities. A pattern classifier was used to extract and classify the abnormal regions. Masses and micro calcifications, the two powerful indicators of cancer were used in evaluating mammograms. 216 digital mammograms images were used. To extract the region of interest by removing the background intensity histogram was created. Receiver Operating Characteristic (ROC) curve was used to calculate the performance of the CAD system. The result depicted that the area under the ROC curve of the proposed algorithm was 0.96853. The system depicted sensitivity and specificity od near to 93%.

In this paper, the author Abdulkadir et al. [6] proposed automated mitosis detection using Deep learning for histo pathological images. MITOS dataset was used which contained nearly 748 mitotic and 180,000 non-mitotic images. In this system, for

training and test set equal size of non-mitotic and mitotic images were considered. PCA +LDA methods were combined for dimension reduction which increased the overall accuracy from 0.73 to 0.96. SVM was implemented for classifying mitotic and non-mitotic cells. Due to the proposed dimension reduction strategy, the precision, recall and F-measure values were increased to 1, 0.94, and 0.969. This system gave good results for balanced distribution of mitotic and normal cellular formation but the performance degrades for imbalanced distribution.

### 2.3 Survey on Brain Tumor

Mukambika et al. [7] performed the comparison of two methods to classify the malignant or benign brain tumors from a dataset from JSS Hospital. Image preprocessing was done using double threshold to remove the skull from the brain images. Image segmentation was performed by non-parametric Level set and K means segmentation algorithms. After segmentation feature extraction was done using DWT and GLCM. Next classification was done using SVM. From the different values of accuracy, sensitivity and Specificity for Level Set method and K means method it can be concluded that classifier Level set method outperforms K-means method for classifier.

Parveen et al. [8] proposed a hybrid technique to predict brain tumor by combining SVM and Fuzzy c-means methods. Image enhancement was achieved using contrast improvement and mid-range stretch. Skull stripping was performed by Double thresholding and morphological operations. Image segmentation was performed by FCM and feature extraction by Grey level run length matrix (GLRLM). Linear, Quadratic and Polynomial SVM techniques were used for classification phase. For training SVM classifier 96 MRI were used and for testing 24 images are used with total number of 120 images. The system depicted accuracy, Sensitivity and Specificity of 100%.

Astina et al. [9] proposed Adaboost machine learning algorithm for classification of brain MRI. Noise removal and conversion to gray scale were performed in image processing phase. Segmentation was done by median filter and thresholding. GLCM was applied for feature extraction and for classification Adaboost algorithm is used. The system gave good performance with the proposed Adaboost algorithm. The proposed system had the accuracy of 89.90%.

Garima et al. [10] devised a novel method for brain tumor classification using Normalization of Histogram and K-means Segmentation. Various filters were used for denoising the images. Histogram of preprocessed images were normalized using segmented K means algorithm. In classification phase SVM and Naïve bayes classifier were used. A dataset consisting of more than 100 images from Yatharth Hospital, Noida was considered. Efficiency of Naive Bayes Classifier is 87.23% and that of SVM Classifier is 91.49%. SVM gives better performance.

Rasel et al. [11] developed a Brain tumor classification system by implementing SVM and ANN. For preprocessing three techniques namely adjusted threshold, adaptive threshold and histogram imaging were carried out with weiner 2 and median 2 filter. TKFCM algorithm was used for segmentation. Feature extraction was done in two stages: static features and next stage was region property based static features. The first order statistic features for SVM and region property based features for ANN were extracted. Brain tumor stages were classified by ANN and types of tumors were

classified by SVM. The MRI dataset used consisted of 39 images from oncology department of University of Maryland Medical Center. The accuracy of categorizing tumor of brain was nearly 97% which was found to be better than other methods.

Harshavardhan et al. [12] interpreted brain tumor with the help of texture based methods. They have analyzed the texture based feature extraction methods such as histogram, Gray Level Co-occurrence Matrix (GLCM), Gray-Level Run-Length Matrix (GRLM). Depending upon their findings they proposed to combine these methods. SVM classifier was used to classify the tumors into cancerous or non-cancerous tumors on a dataset of 5500 digitized images. To measure the performance of the texture methods, statistical performance. The accuracy level was significantly increased by combination of various features produces. The percentage of accuracy of combined features was higher than the values obtained from others. The authors declared that best efficiency can be achieved by combining GLCM, Histogram, and GLRLM texture features.

Bhagyashree et al. [13] has mentioned that to detect brain tumors MRI are useful. She has also mentioned that brain MRI will also help to detect degenerative diseases like Alzheimer's.

## 2.4 Survey on Lung Cancer

Dhayanand et al. [14] pointed out that there are many challenges involved in data mining techniques to predict the diseases. To overcome some of these, the author proposed a system with SVM and Naïve Bayes classifier. The classification was performed on Indian Liver Patient Dataset (ILPD) from the UCI Repository. Dataset is made up of 167 non liver patient records and 416 liver patient records along with Liver Function Test details (LFT). In terms of accuracy SVM classifier outperformed Naïve Bayes classifier but in term of execution time, Naive Bayes classifier was faster than SVM classifier.

Shubhangi et al. [15] proposed a system for the detection of TB, pneumonia and lung cancer which fall under the category of lung diseases. The imaging technique used was chest radiographs. The texture classification of Chest was performed by artificial neural network. From the results, the author concluded that image preprocessing image segmentation have given good results for the chest radiographs. Feed forward artificial neural network for pattern recognition gave good results upto 92% accurate. 80 patients database was considered from Sasoon Hospital; Pune. System performance is affected if the position and size of x-ray changes. The solution for this problem is CT scan.

Moffy et al. [16] used CT images for lung cancer detection. For noise removal median filter was used. Features like Area, Perimeter and Roundness average intensity and Eccentricity are considered. Segmentation was performed using morphological operations. ANN as a classifier depicted a good amount of accuracy. The overall accuracy is 92%.

Alam et al. [17] came up with an efficient lung cancer classification system using Support vector machine classifier. UCI machine learning database with 500 infected lung scan images was used for the system. The author has developed a multistage classification algorithm. At each stage of this algorithm image enhancement and image segmentation is done separately. Features like kurtosis, entropy rms, Mean, smoothness,



standard deviation, variation, skewness, Idb, Contrast, energy, correlation, homogeneity were considered. Contrast enhancement is used to attend Image enhancement. Image scaling and color space transformation. Threshold and watershed based marker-controlled segmentation was used. SVM binary classifier performed the classification. For cancer identification the proposed system gave accuracy of 97%.

Wu et al. [18] came up with a unique Entropy Degradation Method to detect small cell lung cancer from CT images. The work aimed at detecting lung cancers at early stages. Lung CT Scans from the National Cancer Institute were used for training and testing the system. 12 CT scan images of lungs were considered comprising of 6 healthy lungs and 6 with patients. The system achieved an accuracy of 77.8%.

## 2.5 Survey on Spine Tumor

Asanambigai et al. [19] proposed a software tool for detection of tumor in vertebral column. The dataset of 160 images consisted of 112 images for training and 48 images for testing was considered. It involves Median filters for noise removal and gray scale conversion. Spatial fuzzy clustering was implemented for extracting the region of interest. 46 reduced statistical features along with 13 GLCM based texture features were extracted. ANN classifier was applied to classify the images in tumor or non-tumor images.

Kumar et al. [20] presented a Computer Aided Diagnosis system for differentiating between tumorous and non-tumorous bone lesions of spine in CT images with the help Support Vector Machine (SVM). A dataset consisting of 100 bone lesions, consisting of 50 benign and 50 malignant images was considered. To extract the region of interest Snakes or Active Contour Model was used for segmentation. Then from these images features were calculated. SVM used these features for classification of the tumors. In the results the author concluded that SVM in combination with RBF outperformed in terms of accuracy.

Huang et al. [21] author designed a CAD system to diagnose bone metastasis. From 35 patients 4,413 CT images were obtained among which 192 metastatic vertebrae and 392 normal vertebrae images were there. Image segmentation was performed to get the region of interest. From this ROI 33 features were extracted. These features were given to a multilayer perceptron (MLP) neural network for classification. Accuracy of 87.9% was achieved.

Alfonse et al. [22] proposed a classification system using SVM classifier. Dataset of 100 MR images, 80:20 ratio for cancerous and normal images. Image preprocessing was performed by Expectation Maximization (EM) algorithm along with adaptive thresholding. Fast Fourier Transform (FFT) implemented feature extraction, feature selection using Minimal-Redundancy-Maximal-Relevance criterion (MRMR) were used in image segmentation phase. Finally for classification SVM classifier was used. Experimental results demonstrate that system had 98.9% classification accuracy.

### 3 Conclusion

In this paper a survey is performed on the various types of cancer and the methods used to diagnose and classify these cancers. Four major types of cancer such as Brain Tumor, Breast cancer, Lung cancer and Spine tumors are studied. The various methods used to classify each of these diseases are studied. From the analysis of each method, it is found that Support Vector machine (SVM) technique yields more accuracy. Authors also found that the accuracy of the overall system depends on the methods used for preprocessing, image segmentation and feature extraction.

**Acknowledgement.** We would like to sincerely thank the management of MVJ College of Engineering, Bengaluru for their eternal help and support. We would also like to thank Principal and management of ATME College of Engineering, Mysuru for their eternal help and support.

### References

1. <https://ourworldindata.org/cancer>
2. Ali, I., Wani, W.A., Saleem, K.: Cancer scenario in India with future perspectives. *Cancer Ther.* **8**(8), 56–70 (2011)
3. Satish Saini, R.V.: Performance analysis of artificial neural network based breast cancer detection system. *Int. J. Soft Comput. Eng.* **4**(4), 70–72 (2014)
4. Utomo, C.P., Kardiana, A.: Breast cancer diagnosis using artificial neural networks with extreme learning techniques. *Int. J. Adv. Res. Artif. Intell.* **3**(7), 10–14 (2014)
5. Dheebea, J., Singh, N.A.: Computer-aided detection of breast cancer on mammograms: a swarm intelligence optimized wavelet neural network approach. *Biomed. Inform.* **49**, 45–52 (2014)
6. Albayrak, A., Bilgin, G.: Mitosis detection using convolutional neural network based features. In: 2016 IEEE 17th International Symposium on Computational Intelligence and Informatics (CINTI), pp. 335–340 (2016)
7. Mukambika, P.S., Uma Rani, K.: Segmentation and classification of MRI brain tumor. *Int. Res. J. Eng. Technol. (IRJET)* **04**(07), 683–688 (2017)
8. Parveen, A.S.: Detection of brain tumor in MRI images, using combination of fuzzy C-Means and SVM. In: 2nd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 98–102 (2015)
9. Minz, A., Mahobiya, C.: MR image classification using Adaboost for brain tumor type. In: IEEE 7th International Advance Computing Conference (IACC) (2017)
10. Singh, G., Ansari, M.A.: Efficient detection of brain tumor from MRIs using K-means segmentation and normalized histogram. *IEEE Issue* (2016)
11. Bhagyashree, S.R., Sheshadri, H.S.: An approach in the diagnosis of Alzheimer disease-a survey. *Int. J. Eng. Trends Technol. (IJETT)* **7**(1), 41–43 (2014)
12. Ahmmmed, R., Swakshar, A.S., Hossain, M.F., Rafiq, M.A.: Classification of tumors and it stages in brain MRI using support vector machine and artificial neural network. In: International Conference on Electrical, Computer and Communication Engineering (ECCE) (2017)
13. Harshavardhan, A., Babu, S., Venugopal, T.: Analysis of feature extraction methods for the classification of brain tumor detection. *Int. J. Pure Appl. Math.* **117**(7), 147–155 (2017)

14. Vijayarani, S., Dhayanand, S.: Liver disease prediction using SVM and Naïve Bayes algorithms. *Int. J. Sci. Eng. Technol. Res. (IJSETR)* **4**(4), 816–820 (2015)
15. Khobragade, S., Tiwari, A., Patil, C.Y., Narke, V.: Automatic detection of major lung diseases using Chest Radiographs and classification by feed-forward artificial neural network. In: *IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES)* (2016)
16. Vas, M., Dessai, A.: Lung cancer detection system using lung CT image processing. In: *International Conference on Computing Sciences* (2012)
17. Alam, J., Alam, S., Hossan, A.: Multi-stage lung cancer detection and prediction using multi-class SVM classifier. In: *International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2) IEEE Conferences*, pp. 1–4 (2018)
18. Wu, Q., Zhao, W.: Small-cell lung cancer detection using a supervised machine learning algorithm. In: *International Symposium on Computer Science and Intelligent Controls (ISCSIC) IEEE Conferences*, pp. 88–91 (2017)
19. Asanambigai, V., Sasikala, J.: ANN based computer aided diagnosis and classification of vertebral column images. *ARPN J. Eng. Appl. Sci.* **12**(5), 1521–1524 (2017)
20. Kumar, R., Suhas, M.V.: Classification of benign and malignant bone lesions on CT Images using support vector machine: a comparison of kernel functions. In: *IEEE International Conference on Recent Trends in Electronics Information Communication Technology*, p. 821 (2016)
21. Huang, S.-F., Chian, K.H.: Automatic detection of bone metastasis in vertebrae by using CT images. In: *Proceedings of the World Congress on Engineering 2012, WCE 2012, 4–6 July 2012, vol. II* (2012)
22. Alfonse, M., Salem, A.B.M.: An automatic classification of brain tumors through MRI using support vector machine. *Egypt. Comput. Sci. J.* **40**(03) (2016). ISSN 1110–2586



# Cab Service Communication in Transportation Classification Techniques

Prachi Singhal<sup>1</sup>(✉) and G. Vadivu<sup>2</sup>

<sup>1</sup> Big Data Analytics, SRM Institute of Science and Technology, Kattankulathur, Chennai, India

prachisinghal201@gmail.com

<sup>2</sup> SRM Institute of Science and Technology, Kattankulathur, Chennai, India

**Abstract.** This paper tries to analyze Uber data set, and would implement business intelligence using Hadoop framework. This means by reducing the overhead and focusing on the routing optimization paths for a popular destination. However, there is dependably absence of straightforward and realistic techniques for choosing prominent destination. The paper tries to solve this problem by defining a threshold mechanism in order search the popular places. By, finding the days on which each place has more trips and more number of active vehicles by performing analysis on the Uber dataset in Hadoop using [MapReduce](#) in Java. Based on the data, find the top 20 destinations people travel the most, top 20 cities that generate high revenues for travel, based on booked trip count.

**Keywords:** Map Reduce · Hadoop framework

## 1 Introduction

In India, there is a huge range of start-ups coming up every day to offer reliable cab services in both rural as well as urban areas. This brings up an issue of experiencing a conceivable ‘Taxi Revolution’? The intention is to build the overall industry and accomplish economic scale and by giving consumer loyalty. This article would focus on understanding the rapid change in the taxi market of India by analysing factors such as price, revenue and market share. By deeply understanding the internal motivating and demotivating factors that influence the decision of tourists in choosing their favourite destination, a Preference Analysis Model can be prepared. In this study it is found that the most favourite destination among 20 different destinations under study is San Francisco, California. Uber Technologies Inc. is a peer to peer transportation network company. It has been Established as the Uber Cab by Garrett Camp and Travis Kalanick in 2009. They created, advertised and worked the Uber application by permitting the customers to send a ride request. The request is then handled by the server and the driver who is nearest to the customer’s location is asked to accept the customer’s request. Once the request is accepted the driver is alerted about the location of the customer. In August 2016, Uber gave its taxi benefit in more than 66 nations and 545 urban communities around the world. The application is made in such a beautiful way that the fare of the ride is automatically calculated and when the customer makes a payment the funds are automatically shared with the driver. Since, other companies

have replicated Uber's business, a trend is referred as "Uberification". Previously, activity-based ride matching algorithm has been introduced for finding the alternative destinations. This paper tries to find the number of trips and active vehicles on the basis of place and trips each day by using Map Reduce Algorithm.

## 2 Literature Survey

The idea in progress work is to find the place trips and active vehicles for each place trip and on that basis finding the 20 popular destination. [1] As the traffic is largely scalable therefore it further limits its application in large networks due to high computational costs and routing overhead thereby making the selection of popular places a tough practical criterion. [2] By applying this criterion, we come to know the number of prefixes can be easily reduced to a smaller portion of the total number, and at the same time ensuring the stability in the traffic. Using the cab services, this would foster market share, achieve economies, provide customer satisfaction and would focus on India's taxi market by studying numerous factors such as pricing, revenue models, market share and customers demand. [3] Boosting the opportunities of ride-sharing based on the in depth knowledge and understanding of individual human activities and demands to lower down the quality of life due to pollution and traffic congestion in the cities. [4] Using Hadoop framework to analyse business intelligence and analysing the data from the provided dataset. [5] Use of IP-forwarding interchanging enabled by Open-Flow to realize quality-of-service (QoS) aware flexible traffic building (F-TE) in a hybrid network where IPv4 and IPv6 coincide. [6] The content delivery network (CDN) make use of the cache to send data close to end users. Over both traditional Internet architecture and emerging cloud-based framework, cache allocation has been the core problem that any CDN operator needs to address. Cache allocation problem has been the core problem that any CDN operator faces in both traditional and urban and cloud-based internet architecture. After studying the point of presence (POP) and temporal information in user's requests we provide a dynamic traffic-based solution to them. [7] a system to share cost and journey among the passengers. the taxi ones pick one passenger then based on other passenger's destination the taxi driver will take the route based on arbitrary shortest path algorithm. This technique saves the taxi driver's time, revenue and traffic on the road. [8] imbalance in taxi service i.e. in one area passengers waiting to long for a taxi and in other area taxis are roaming vacant. knowledge to where the taxi will become available will help us solve the issue of imbalance in taxi service. approach consists of 2 steps: first to use entropy and correlation to measure the unpredictability of the passengers and second is to identify which predictive algorithm can predict the maximum predictability of the passengers by implementing probability-based algorithm, sequence based and neural network machine learning based algorithm.

### 3 Proposed Model

#### UBER CAB:

#### DATA-SET DESCRIPTION:

The Uber dataset comprises of six segments: place\_id, date, active vehicles, place, trips and user\_id.

#### Uber cab use case 1:

1. Seeking for the number of trips in each place on various days.
2. The Mapper class, would accept the combination of the current day of week and place as key and the number of trips as value.
3. Now, after this operation, the combination of place\_id + Days of the week as key and the number of trips as value.
4. In the reducer, calculate the sum of trips for each place and for a particular day.

#### Uber cab use case 2:

1. Seeking the number of active vehicles in various places of consideration on different days of the week.
2. The Mapper class, would accept a combination of the day of week and place as its key and the number of active vehicles as their values.
3. Now, after this operation, the combination of place\_id and Day of week is generated as key and the number of active vehicles is generated as their respective value.

Presently, in the reducer, we will figure the whole of dynamic vehicles for every cellular and for every specific day.

### 4 Hadoop Framework and Map Reduce

**Hadoop** is a open source software framework that is used for storing data and running applications on the cluster of commodity hardware. It provides massive storage of all kind of data (structured or unstructured data) with good processing power and has the ability to work on many concurrent jobs or task simultaneously. Hadoop is a single framework out of many big data tools. Hadoop is mainly used for batch processing of the data.

The term **MapReduce** is a software for distributed processing of large dataset. It splits the dataset into number of parts and run a program on all data parts parallely. It consists of two jobs mapper job and reducer job:

- **The Mapper job:** is to process the input data. The input data is in the form of files and directory and this gets stored in the form of hdfs (Hadoop distributed file system). the input data is passed into the mapper function line by line. Mapper processes the data and creates small chunks of input data.

- **The Reducer job:** it processes the data that comes from the mapper i.e. output of mapper job is the input of the reducer job and combines those data chunks into smaller set of tuples. These tuples, produces the new set of output that is stored in hdfs.

Ordinarily, both the input and the output are put away in a record system. The structure deals with booking assignments, observing them and re-executes the fizzled tasks.

## 5 Dataset

Dataset has been collected through uci repository. It has 5 attributes in it i.e., user id which is unique, place trip is the trip of particular place, place, no. of active vehicles and no. of trips.

It has total 350 records of different place and unique user id.

user id	palce_id	date	trips	active vehicles	place
1	B02512	01-01-2015	190	1132	Kabul
2	B02765	01-01-2015	225	1765	Kandahar
3	B02764	01-01-2015	3427	29421	Herat
4	B02682	01-01-2015	945	7679	Mazar-i-Sharif
5	B02617	01-01-2015	1228	9537	Kunduz
6	B02598	01-01-2015	870	6903	Jalalabad
7	B02598	01-02-2015	785	4768	Lashkar Gah
8	B02617	01-02-2015	1137	7065	Taluqan
9	B02512	01-02-2015	175	875	Puli Khumri
10	B02682	01-02-2015	890	5506	Khost
11	B02765	01-02-2015	196	1001	Ghazni
12	B02764	01-02-2015	3147	19974	Sheberghan
13	B02765	01-03-2015	201	1526	Sari Pul
14	B02617	01-03-2015	1188	10664	Farah
15	B02598	01-03-2015	818	7432	Vienna
16	B02682	01-03-2015	915	8010	Lower
17	B02512	01-03-2015	173	1088	Upper Austria
18	B02764	01-03-2015	3215	29729	Styria 2

## 6 Result

By performing the map reduce we predicted the following result in Figs. 1 and 2. Through the output of map reduce framework we predicted the number of active vehicles and place where these vehicles travel the most. Through this result, we can try to predict the popular destinations where people travel the most.

This figure tells about the calculated number of trips for each place on a particular day and place.

This figure tells about the number of active vehicles present on each place for a particular day.

1	B02512	01-01-2015	Kabul	1132
10	B02682	01-02-2015	Khost	5506
100	B02765	1/17/2015	Sari Pul	2160
101	B02617	1/17/2015	Farah	12676
102	B02764	1/17/2015	Vienna	36318
103	B02512	1/18/2015	Lower	1521
104	B02598	1/18/2015	Upper Austria	9443
105	B02765	1/18/2015	Styria 2	2287
106	B02764	1/18/2015	Tyrol	35182
107	B02682	1/18/2015	Carinthia	11161

Fig. 1.



1	Kabul	B02512	01-01-2015	190
10	Khost	B02682	01-02-2015	890
100	Sari Pul	B02765	1/17/2015	252
101	Farah	B02617	1/17/2015	1306
102	Vienna	B02764	1/17/2015	3657
103	Lower	B02512	1/18/2015	177
104	Upper Austria	B02598	1/18/2015	869
105	Styria 2	B02765	1/18/2015	248
106	Tyrol	B02764	1/18/2015	3290
107	Carinthia	B02682	1/18/2015	1056
108	Salzburg	B02617	1/18/2015	1223
109	Vorarlberg	B02682	1/19/2015	883
11	Ghazni	B02765	01-02-2015	196
110	Burgenland	B02617	1/19/2015	992
111	Loer	B02765	1/19/2015	238
112	Aksu	B02764	1/19/2015	2958

Fig. 2.

## 7 Future Work

This work can be expanded further by finding the top 20 popular destination people travel by using the no. of active vehicles and trips for particular place by using some categorical and classification algorithm such as naive Bayes, k-mean clustering algorithm etc.

## References

1. Chaudhuri, S., Dayal, U., Nara-sayya, V.: An overview of business intelligence technology. *Commun. ACM* **54**(8), 88–98 (2011)
2. Watson, H.J., Wixom, B.H.: The current state of business intelligence. *IEEE Comput.* **40**(9), 96–99 (2007)
3. Sallam, R.L., Richardson, J., Hagerty, J., Hostmann, B.: *Magic Quadrant for Business Intelligence CT* (2011)

4. <http://hpccsystems.com>
5. Vailaya, A.: What's all the buzz around big data? In: IEEE Women in Engineering Magazine, pp. 24–31, December 2012
6. Feamster, N., Borkenhagen, J., Rexford, J.: Guidelines for interdomain traffic engineering. SIGCOMM Comput. Commun. Rev. **33**(5), 19–30 (2003)
7. Li, J.P., Homg, G.J., Cheng, S.T.: Intelligent ridesharing system for taxi to reduce cab fee. In: IEEE 12th International Conference, pp. 468–473 (2015)
8. Zhao, K., Kardashev, D., Freire, J., Silva, C., Vo, H.: Predicting taxi demand at high spatial resolution: approaching the limit of predictability. In: IEEE Conference, pp. 833–842 (2016)
9. Amin, M., Ho, K., Howarth, M., Pavlou, G.: An integrated network management framework for inter-domain outbound traffic engineering. In: Proceedings of the MMNS 2006, pp. 208–222 (2006)
10. Rekhter, Y., Li, T., Hares, S.: A Border Gateway Protocol 4 (BGP-4). RFC 4271 (Draft Standard), January 2006
11. Caesar, M., Rexford, J.: BGP routing policies in ISP networks. IEEE Netw. **19**(6), 5–11 (2005)
12. Dhamdhere, A., Dovrolis, C.: ISP and egress path selection for multi-homed networks. In: Proceedings of the IEEE INFOCOM 2006, Barcelona, Spain, November/December 2006



# Analysis on Emotion Detection for Infant Cry

M. Meenalochini, M. Janani<sup>(✉)</sup>, P. Manoj, and A. ShakulHameed

Department of CSE, Jai Shriram Engineering College, Tirupur, TN, India  
meenalochinicse@gmail.com, jananemuthusamy@gmail.com

**Abstract.** Crying is an infant behavior, a part of behavioral system in human which assures persuade of the helpless neonate by eliciting others to meet their basic needs. It is one of the way of communications and a positive sign of healthy life for the infant. The reasons involved for infant's cry includes hungry, unhappy, discomfort, sadness, stomach pain, has colic or any other diseased conditions. The health of new born babies are effectively identified by the analysis of infant cry. Researchers made a huge analysis of infants by using methods like spectrography, melody shape method, and inverse filtering etc. The paper proposes a procedure to detect the emotion of infant cry by using Feature Extraction techniques including Mel-frequency and Linear predictive coding methods. A statistical tool is used to compare the efficiency of the two techniques (Mel-frequency and linear predictive coding). Present work is carried out mainly for five reasons which includes infant crying, has colic, hungry, sad, stomach pain, unhappy.

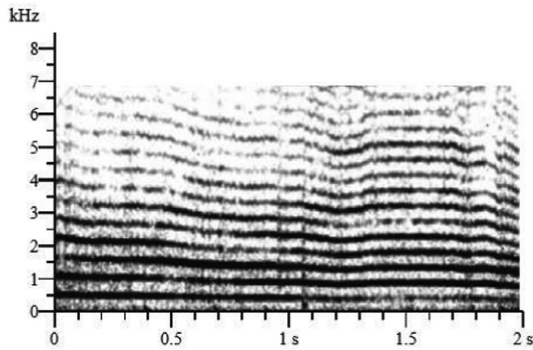
**Keywords:** Neonates · Feature extraction · Mel-frequency spectrum

## 1 Introduction

Infant Cry is wholly associated with the respiratory system and the nervous system. It forms the most only means of communication immediately after baby's birth. In respiratory system vocal cord and vocal tract are responsible to produce the crying sound of frequency range 250–600 Hz. We always wants to see a cute smiling baby rather than a Crying baby. And most of all have no reasons for which the baby cry's. At times mother can only understand their child's behavior. No two signals of an infant cry is found to be similar. The infant cry signal is always different for different emotional reasons like hungry, stomach pain, sad, happy, has colic, etc.

Infants cannot be able to express its discomfort or pain through verbal communication. In order to draw the attention from its potential care takers, infant's alert them through their cry [2]. From extracting various feature from the infant cry signal, lots of information is obtained. Thus this paper provides an alternative method to detect the reason for baby's cry by using various different signal extractions methods. Each method is statistically analyzed for its efficiency. Infant cry signal is analyzed for knowing reasons as well as for diagnosing pathological conditions because of it containing lots of information about both the physical and physiological conditions.

As stated earlier infant's cry is associated with the central nervous system, importance for the analysis of infant cry signal will increase the early detection of risk to infants. In the 1960s and 1970s, the sound spectrogram was the major tool for analyzing cry sounds [2]. Produced by an analog device, a spectrogram plots a time on x axis and frequency on y axis, and encodes the darkness of the frequency lines (Fig. 1).



**Fig. 1.** A (digitally produced) spectrogram of an infant cry [1].

In recent years, there are various simple techniques are used for analyzing the infant cry signal by using most effective methods such as Pitch frequency, Cross-Correlation, Mel frequency cepstral coefficients, Linear prediction coefficient. These methods are used in automatic classification of cry signal and produces highly efficient results. In this present work, a three different method has been proposed for analysis of the infant cry due to has colic, hungry, sad, stomach pain, unhappy.

Cry signal of the infant is directly acquired and stored in a folder. Another folder is created to store the database signals. These two signals are correlated by writing algorithms and their features are extracted to predict the final result by using various feature extracting methodology [4]. One picked signal from the test folder will be compared with all the database signals one by one and when the corresponding feature is matched, then the reason for which the infant cry will be displaced. As this paper deals with signal analysis, we made use of MATLAB software for easy computation. And also the signals are processed by using both time-domain and frequency-based signal processing.

## 2 Methodology

The infant cry signals are stored in test folder which are collected from the site (<http://www.soundJay.com>) and provided as an input voice to the simulating software MATLAB where it is compared with the databases [3]. Then the further analysis is computed and the results are classified according to the extracted feature by using their specific methods. In this present work, database folder contains 11 types of crying signal in which each signal has its own signal characteristics and defines the mood of

the infant like hungry, sad, pain, etc. In order to test the proposed algorithms, all the crying signals are collected randomly from different databases available on internet. In this paper different types of infant cry are analyzed for the following reasons.

### **2.1 Hungry**

If the infant cries because of hunger, then the caretaker have to feed them to stop crying.

### **2.2 Stomach Pain**

If the infant cries due to stomach pain, then the caretaker have to take some remedies to stop their baby's cry.

### **2.3 Unhappy**

If the infant cries due to unhappy, the caretaker should understand that they are feeling very uncomfortable with wet diapers etc.

### **2.4 Sad**

If the infant cries out of sadness, then the caretaker should demand more attention towards their infant and has to make them feel safer.

### **2.5 Has Colic**

If the infant cry was stated as has colic for more than three hours a day, then the caretaker should consider the health of their baby very seriously. This condition may leads to certain unhealthy conditions/Diseases. Normal routine behaviors of infants are only analyzed in this process and in future aspects several diseased conditions can also be processed by using pitch information or fundamental frequency etc.

## **3 Features Extraction Methods**

Various methods have been processed for the infant cry signals which includes 3 different methods of feature extraction.

### **3.1 Pitch Information**

As infants cry has some normal frequency range, the fundamental frequency ( $f_0$ ) is considered as classifier. Pitch and frequency components are detected by using the two different combinations of different algorithms.

Pitch is an important attribute of voice speech. It contains most specific information about the speaker [3, 5]. The estimation of fundamental frequency ( $f_0$ ) or pitch frequency is an important part in infant cry analysis. Initially, input voice push button is

pressed and the test cry signal is loaded [8, 10]. Then pitch of the signal is detected if the fundamental frequency ranks between 100 to 400 Hz and with the cry duration between 1 to 1.5 s. It is completely a time domain analysis (Fig 2).

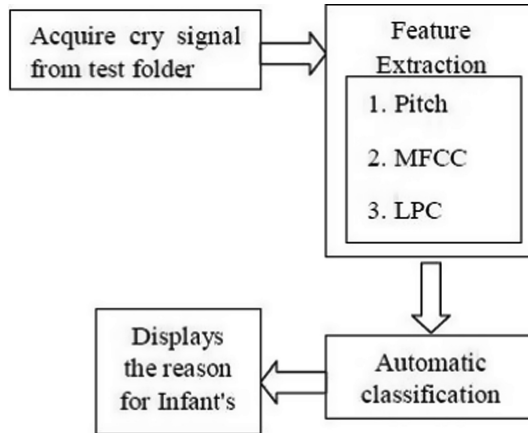


Fig. 2. Flow chart for infant cry analysis.

### 3.2 Mel Frequency Cepstral Coefficient and Cross Correlation Method

Pitch detection using time domain analysis has some limitations like that there may occur larger pitch signals which is not in the pitch period (T0). Thus we have implemented the same pitch detection algorithm in frequency domain by using the simplest cepstral analysis. Pitch feature by using Mel-frequency cepstral coefficient method can function only in combination with Cross-correlation method [6]. Total spectral energy contained in each filter is computed and a DCT is performed to obtain MFCC sequences (Fig. 4). Cry signal is loaded as an input voice through the software MATLAB coding and their corresponding feature is extracted using equation,

$$= \sum_{i=0}^{M-1} \log(E(i)) \cdot \cos\left(\frac{2\pi}{M} \left(t + \frac{1}{2}\right) \cdot t\right)$$

for  $l = 0, \dots, M - 1$ .  $E(i)$  is the total Spectral Energy.

### 3.3 Linear Prediction Coefficient with Auto-Correlation Method

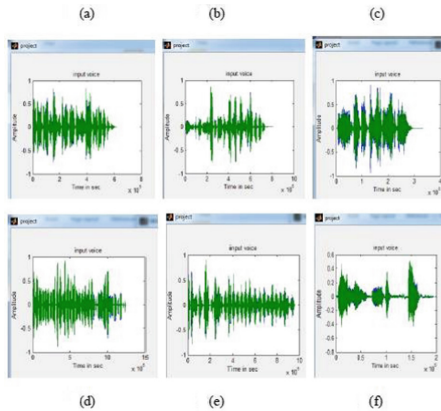
LPC can also be functioned in combination with the auto-correlation techniques. LPC analysis technique was used to extract the fundamental components of cry signal to understand and analyze the physiological conditions of healthy infant [10]. Many research are being done in this technique as it the most suitable technique for speech analysis procedures. In the recent analysis, neural network concepts are widely used in LPC cepstral pattern and different windowing concepts are integrated into this techniques which gives the most accurate results (Fig. 5).

### 3.4 Statistical Analysis

Feature extraction techniques MFCC and LPC are analyzed based on different feature concepts. In this paper, we have extracted the spectrum envelope and data values are exported to the Microsoft Excel for statistical analysis [8]. Statistical analysis process is drawn by using a simple line graph method. From the output graph (Fig. 6), the efficiency of two methods can be analyzed easily.

## 4 Results and Discussion

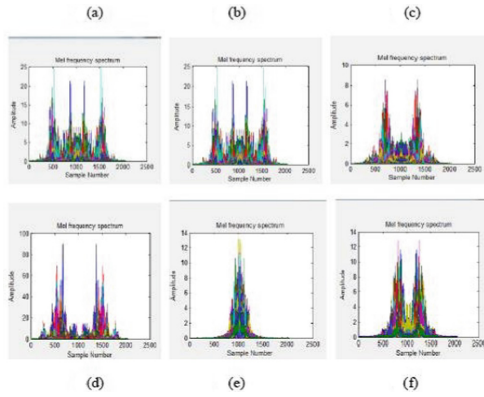
Crying signals are stored in the test folder. Then one by one push button on GUI is pressed and the process starts. The comparison takes place by using cross-correlation algorithm and resampling those signals, which are of different lengths the input signal will be loaded for further processing (Fig. 3).



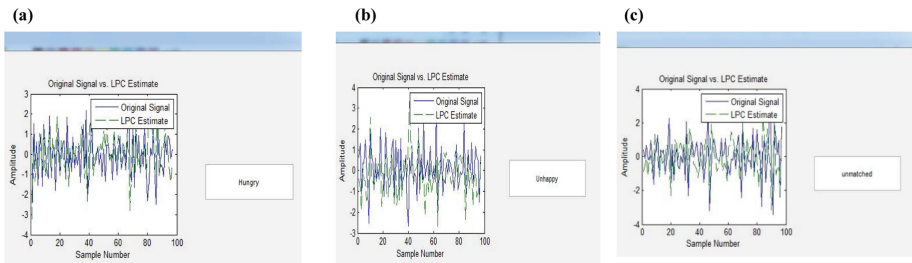
**Fig. 3.** Input Signals - 3(a) Has colic, 3(b) Hungry, 3(c) Sadness, 3(d) Stomach Pain, 3(e) Unhappy and 3(f) Unmatched Conditions.

Mel-frequency spectrum is a representation of the short-term power spectrum in sound processing. The human auditory system response more closely than the linearly spaced frequency bands used in the normal cepstrum.

Linear predictive coding is a tool in audio signal processing and speech processing and it is representing the spectral envelope of digital signal speech in compressed form. It is one of the most powerful speech analysis techniques, and one of the useful method for encoding.



**Fig. 4.** Mel Frequency Spectrum of 4(a) Has colic, 4(b) Hungry, 4(c) Sadness, 4(d) Stomach Pain, 4(e) Unhappy and 4(f) Unmatched Conditions.

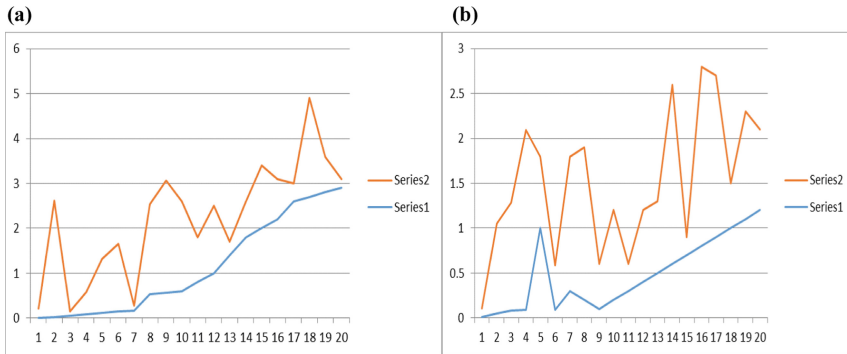


**Fig. 5.** Linear Predictive Coefficient spectrum of 5(a) Hunger 5(b) Unhappy 5(c) Unmatched Conditions.

**4.1 Statistical Analysis**

Statistical analysis is carried out between two different feature extraction methods like Mel Frequency Cepstral Coefficient and Linear Prediction Coefficient method. A line graph has Sample numbers in X-axis and Amplitude in Y-Axis. Thus the pitch of each method is analysed using an Excel as a tool. By observing the graph curve lines (Fig. 6) it is very clear that LP technique can give us an most accurate results in infant cry analysis. In the Fig. 6 Series 1 is Mel Frequency Cepstral Coefficient (MPCC) values represented in blue color and Series 2 is Linear Prediction Coefficient (LPC) values represented in red color.





**Fig. 6.** Statistical Analysis of 6(a) Has colic and 6(b) Hungry

## 5 Conclusion

Neonates cry can be a mode of communication, or a sign of mood and it is an acoustic signal to diagnose several diseases. In this paper, GUI and various databases are used to compared the crying signals by cross-correlation algorithm, Additionally the harmonics, pitch, frequency range of the cry signals are compared with the help of Mel-frequency spectrum and linear prediction coding methods. The efficiency of the two techniques has also been differentiated in the statistical data using excel.

## References

1. Varallyay Jr., G.: Future prospects of the application of the Infant Cry in the Medicine. *Per. Pol. Elec. Eng.* **50**(1–2), 47–62 (2006)
2. Lederman, D., Cohen, A.: Automatic Classification of Infants' Cry Ben-Gurion. University of the Negev. *Elec. and Comp. Eng.*, October 2002
3. Roopa, S.M., Anitha, S.G., Mohamed, D.R.: Analysis of infant cry through weighted linear prediction cepstral coefficient and probabilistic neural network. *Comput. Sci. Eng. IJCSMC* **4**(4), 413–420 (2015)
4. LaGasse, L.L., Neal, A.R., Lester, B.M.: Assessment of infant cry: acoustic cry analysis and parental perception. *Mental Retard. Dev. Disabil. Res. Rev.* **11**, 83–93 (2005)
5. Balandong, R.P.: Acoustic Analysis of Baby Cry. *Biomedical Eng. University of Malaya*, May 2013
6. How to Run Statistical Tests in Excel. Student Research. CBGS M&E Science
7. Dhanashri, U.S., Nayana Shenvi, T.: Analysis of cry in new born infants. *Electron. Telecommun. Eng. IJARCCCE* **4**(3), March 2015
8. Varallyay, G.J., Benyo, Z., Illenyi, A., Farkas, Z., Kovacs, L.: Acoustic analysis of the infant cry: classical and new methods. In: 26th Annual International Conference of the IEEE EMBS. San Francisco, CA, USA, pp. 313–316, 1–5 September 2004
9. Cohen, R., Lavner, Y.: Infant cry analysis and detection. In: IEEE 27th Convention of Electrical and Electronics Engineers in Israel, pp. 1–5 (2012)
10. Orgeron, H.: Method for extracting the frequency response of an audio system from a recording. *J. Undergraduate Res. Phys.*, 7th September 2011



# Computational Model for Hybrid Job Scheduling in Grid Computing

Pranit Sinha<sup>(✉)</sup>, Georgy Aeishel<sup>(✉)</sup>, and N. Jayapandian<sup>(✉)</sup>

Department of Computer Science and Engineering,  
CHRIST (Deemed to be University), Kengeri Campus, Bangalore, India  
{Pranit.sinha,  
Georgy.aeishel}@btech.christuniversity.in,  
jayapandian.n@christuniversity.in

**Abstract.** Grid computing the job scheduling is the major issue that needs to be addressed prior to the development of a grid system or architecture. Scheduling is the user's job to apropos resources in the grid environment. Grid computing has got a very wide domain in its application and thus induces various research opportunities that are generally spread over many areas of distributed computing and computer science. The cardinal point of scheduling is being attaining apex attainable performance and to satisfy the application requirements with computing resources at exposure. This paper posits techniques of using different scheduling techniques for increasing the efficacy of the grid system. This hybrid scheduler could enable the grid system to reduce the execution time. This paper also proposes an architecture which could be implemented ensuring the optimal results in the grid environment. This adaptive scheduler would possibly combine the pros of two scheduling strategies to produce a hybrid scheduling strategy which could cater the ever changing workload encountered by the grid system. The main objective of the proposed system is to reduce to overall job execution time and processor utilization time.

**Keywords:** Dynamic scheduling · Distributed computing · Grid Computing · Scheduling · Parallel computing

## 1 Introduction

The need for extensive computing power has been never been more required than now, which could enable human to find prime numbers up to ten million digits, or to find more effective drugs to fight AIDS. The recent developments in the field of networking and web-based technologies has powered a thought and enabled us to exploit the potential of using huge number of computer resources distributed geographically and belonging to different owners, which has been given the appellation "Grid Computing" [1]. This new paradigm is distributed system of a type that works on basic idea of parallelism and requires well integrated and synchronized use of resources. It has the potential to fulfill large demand of researchers requiring huge amount of communication and computational power to carry out state-of-art engineering and science application. Resource provisioning is the biggest task in grid computing [2]. The high

end technological application of grid computing is in domain of medical-drug discovery, meteorology-analysis and security of climate data for weather forecasting. The grid resources are not dedicated to a single user and hence can be accessed simultaneously [3]. Due to this the grid system is subjected to different load variations. The local task has higher priority, thus are dealt prior in comparison to other grid tasks. The variation in the availability of the resource due to different computational pace of hosts and link's bandwidth and other factors make the requirement of scheduler essential for the proper functioning of the grid system. To attain the full potential that grid computing has to offer, an efficacious scheduling algorithm is important. Scheduling has been implemented efficiently by our operating system to manage the processes and their allocation to the processor.

The grid scheduler is a device that places itself as an interface lying between the user and the grid resource. The task scheduling in distributed computing is a major challenge and the task of the grid scheduler is to schedule and manage the allocation of the grid resources to each requesting process and also maintaining the job dependencies and meeting other constraints [4]. Making sure for optimal performance will be there in continuously changing and capricious grid environment, need of adaptive scheduling can be the solution in which the scheduling strategy changes dynamically depending of the behaviour of the grid system to cater the fluctuations according to the availability of resource. Starting scheduling of all the work is carried out by a static scheduler and then the scheduling strategy changes to dynamic scheduling as and when required to meet the demand of unexecuted tasks. In parallel scheduling is also implemented in grid job scheduler, this author to use backfilling algorithm to solve grid computing [5]. The fundamental for above mentioned technique is the ability of the scheduler to find and analyse current face of system at running time. Online data storage is also deal with this scheduling algorithm [6]. Primary proposition by the paper is the development of a smart scheduler that could cater the needs of continuously changing grid environment by analysing the different scenarios encountered and switching between the scheduling policy depending of on the result generated during the analysis.

## 2 State of Art

Grid computing allows resource pooling and enabling large-scale resource collaboration for finding of solutions of advanced science and engineering application problems. Principle challenge of distributed computing is planning and synchronization of jobs to the grid assets [7]. Several advancements have been proposed in the recent years, contains static and dynamic methods. The static scheduler signs works to grid assets, before the runtime or implementation time and dynamic scheduler gives during the running phase. A recent study focus and develops a system which could adapt between these scheduling strategies, this system has been given appellation AWS, which stands for Adaptive workflow scheduling. Achieve the lowest running time on diversely spread grid's environment has been the prime motive for many searches conducted on the scheduling mechanism. The most favoured list based heuristic all around the globe is Heterogeneous Earliest Finish Time (HEFT), which is used to schedule scientific workflow. It arranges the workflow jobs depending on priorities assigned to each task

and it is also responsible for the assignment of tasks to acceptable assets to attain the optimum performance. Furthermore, a different study stated a different list based heuristics Min–min or Max–Min also known as Critical Path on a processor (CPOP) are analysed to get maximum performance. Grid resource management is mainly deal with min-min and max-min algorithm [8]. Another major development was by PCH algorithm, which uses hybrid clustering list scheduling strategies.

This strategy deals with tasks with more communicational costs. These are grouped together and are assigned to similar resource in a grid cluster. The primary aim being of reducing the communicational cost by the implementation of efficient scheduling algorithm to minimise the cost involved. The objective of this study is to abate the scheduler length by reduction in the communication price. In addition, this paper gives discretion on the blueprint, burgeoning and progress of Pegasus Workflow Management System (PWS), this System focuses on mapping theoretical workflow explanation onto grid computing infrastructures, with the goal of achieving trustworthy and scalable workflow implementation [9]. In static scheduling is the data pertaining to all contents of grid assets [10]. Task is to assign individually and it is handle with separate application program during scheduling time. In dynamic scheduling, task is allocated during the run time while the application is executing, hence finding the execution time is not possible. The scheduler has to work hard because tasks are entering dynamically hence decision making and resource allocation becomes a tedious task. Load balancing is a major deciding factor. Dynamic scheduling is more advantageous than static scheduling because the system does not require having the runtime behaviour, before it runs the application [11]. In grid computing many internal and external factors is affecting during job submission. Major factors are job communication cost and data storage process.

Then some time network transmission time and QoS also measured. In the part of resource allocation some time resource failure and recovery is also happened. Few traditional scheduling algorithms are first come first serve, Min-min, Minimum completion time, round robin technique, max-min. Current Grid computing provides a medium for an organized sharing of remote autonomous resources. Future Grid computing provides access to managed services, of which computing resources are most important. Advantages of grid computing are as follows ameliorating Operating Efficiency, Asset Optimization, and Accelerate Business. Resources Processes Enable Data Access, Integration and Collaboration, Enhance Employee Productivity, Strengthen Redundancy and Resiliency and quickly acclimate to fickle requirements, quickly respond to fluctuating requirements. The prime goal of task scheduling is to manage the incoming load effectively and efficiently [12]. It is also responsible allocation of the load to among different resources. The ulterior motive behind grid scheduling is minimization of the overall execution time, which also happens to be the main concern. Job scheduling and resource scheduling are the main requirements in grid computing. The task of the job scheduler is to find a specific resource for the job that is requested by the user. The Scheduler has to be smart to allocate the best machine pertaining to the given task. A grid comprises the local schedulers and grid schedulers. The work of local schedulers is in local computational environment and thus it ensures faster connections and reliability, Grid Schedulers also known as Meta scheduler's apex level scheduler available, charged for managing the resource that orchestrates the

different local schedulers. If dynamic information about the workload of the assets are know the jobs executing can be migrate. In grid, there is huge number of resources during the runtime of a job. Get the right assets for the job that is what is mean by scheduling jobs.

### 3 Problem Statement

The scheduler code is already in our control or already written. If any emergency situation occurs there is no chance in that thread or job will come front and get the processor. In this dynamic world it is very difficult to be static but static is useful in operating system jobs where the job should be done in an order and all the processes are done linked each other. It cares about thread dependencies and does not break the flow. Lots of issues and problems are there in grid scheduling task [13]. The factors they should look are user demand, communication time and that way they handle failure, and to reduce the total time from start to end. As we see most of through algorithms most of the algorithms does not care of the user satisfaction and fault tolerating systems. The complex factor of the grid increase by the size of the problem which is one of the areas to be takes care.

In this can see all the resource is under a single controlled domain and after starting that cannot control it as the scheduler take up the control to get a single image. Here the resource never changes. Major challenge here is adaptability and allocation of the resources; this is not still able to bring in grid in grid computing according to the resource request. This dynamic scheduling problem is mostly deal with online job shop scheduling [14]. That means during online job processing different type of jobs handled with in some time interval. This job is deal with the concept of basic queue structure, job sent to queue and deal with some heuristic algorithm. Dynamic scheduler has two major components that are named as estimating the different levels of states and another major one is decision making. In state estimating is the concept similar to operating system, major task of this module is to find the cost in grid system [15]. By this cost it finds want to do and plans accordingly for giving task to choose the resource from the set. And another advantage is that processor will not starve for data or sit ideal because when it find data is not available and understand that the data to get will take time, pose the current process and take up another process and continue with paused one if the data is available, Like wise it manages the processes and make the utilization of processing time. They are good in finding unknown links between the processes at the compile time.

### 4 Hybrid Grid Scheduling Model

The job is divided according to their properties and to propose the concept of hybrid static and dynamic scheduling methodology. The proposed method task is given according to the environment. In this proposed methodology is choosing static or dynamic scheduling based on current environment in grid. They give the jobs for a dynamic scheduler. By this approach the draw backs of both the static and dynamic

scheduling can be overcome, Like the issues where the starvation and if suddenly a dynamic process occurs or environment changes suddenly from static to dynamic then it can be cleared by just switching to each other. For understanding which job should give which type of scheduling and to understand the environment it should have an algorithm where it check out what type of job or process is this and how it is going to work, weather it is a static or a dynamic one. As seen there are a lot of parameters is to check it out.

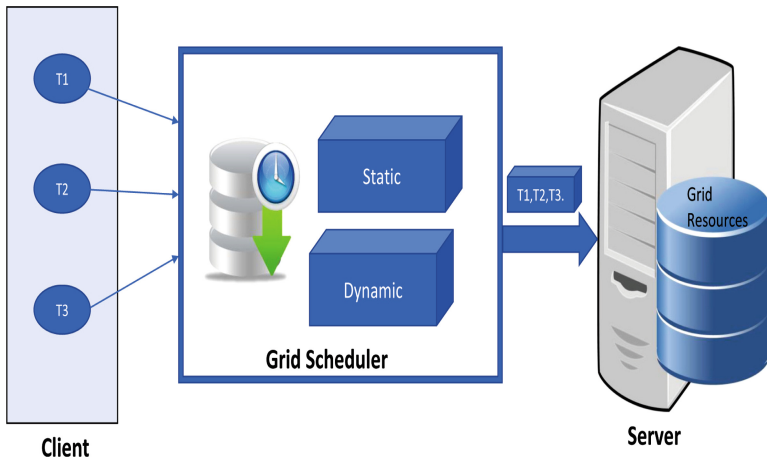
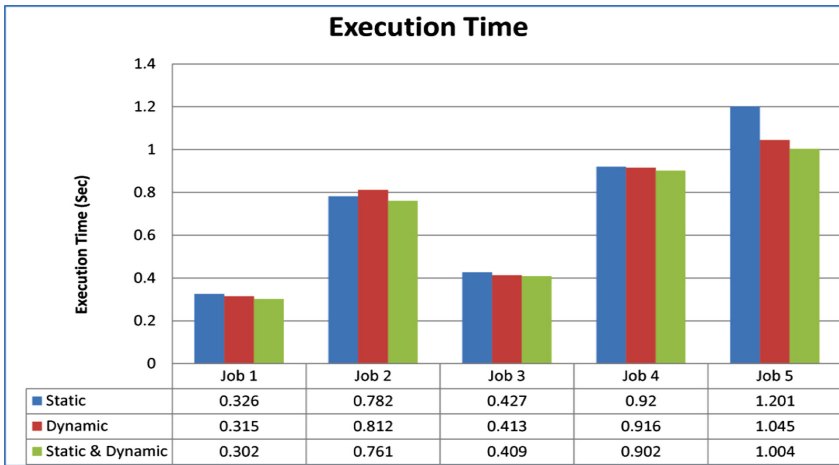


Fig. 1. Hybrid gid scheduling architecture

For checking and deciding whether to give static or dynamic scheduler they need to have a rough estimation of the cost of the job on the basis of number of jobs and there dependencies between each other Expected execution time. If there are lot of dependences and process then they go for dynamic scheduling. If the job has a dynamic environment where system cannot able to estimate the cost and execution time then it will go for dynamic scheduling. In Fig. 1 proposed architecture combination of static and dynamic scheduler the jobs are placed to it and the algorithm estimate the cost, dependencies and number of processes in the job and rate it with a static dynamic rating and decide which scheduler it should be given then as seen in the diagram the scheduler divide the job and accordingly allocate the resources to the processor for processing. For improve the efficiency if any conflict or any starvation or occurs in static scheduling system then suddenly the job is moved to the dynamic scheduler and it will be taking care of the next step and will be allocation the resource accordingly. This approach can avoid a lot of system crash and deadlocks.

## 5 Result and Discussion

The proposed system is initiating hybrid scheduling concept. This methodology is not using both static and dynamic method. Based on the situation to situation they select the method of static or dynamic. The simulation proposes take a different job and test in java platform. This experiment is taken from sample data set with Linux platform. The system requirement of this simulation is i3 processor and minimal storage space.



**Fig. 2.** Job execution time comparison

The proposed methodology is taken two major parameters; one is overall job execution time and processor utilization. Most of the time job execution time is depending upon processor speed. This processor speed is varying based upon number of jobs executed in a particular time. In some situation unwanted jobs take more processor space and wasting the processor time. The following graph is demonstrating the different jobs execution for with and without implementation of proposed hybrid method. The Fig. 2 is discuss about job execution time at the overall job execution time is gradually reduced in proposed method. The Fig. 3 is demonstrated processor utilization out of 5 job more than three job process utilization is reduced.

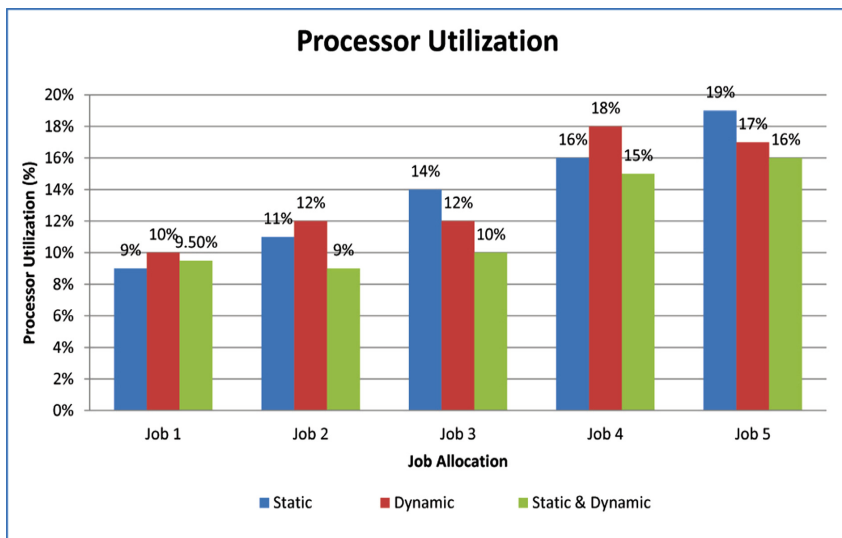


Fig. 3. Processor utilization time comparison

## 6 Conclusion

This paper tried to give a different approach on scheduling by combining the two major static and dynamic scheduling technique and tried to give a combined effect where it can overcome the issues or disadvantage of the each static and dynamic resource scheduling by switching each other accordingly understanding the environment with the help of certain heuristics and criteria and making the scheduling process more effective with respect of time and processing covering all the disadvantage of each scheduling procedure.

## References

1. Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud computing and grid computing 360-degree compared. In: International Workshop in Grid Computing Environments, pp. 1–10. IEEE (2008)
2. Jayapandian, N., Rahman, A.M.Z., Gayathri, J.: The online control framework on computational optimization of resource provisioning in cloud environment. *Indian J. Sci. Technol.* **8**(23), 1–5 (2015)
3. Deelman, E., Blythe, J., Gil, Y., Kesselman, C., Mehta, G., Patil, S., Livny, M.: Pegasus: mapping scientific workflows onto the grid. In: International European Across Conference in Grid Computing, pp. 11–20. Springer (2004)
4. Sheikh, S., Nagaraju, A., Shahid, M.: Dynamic load balancing with advanced reservation of resources for computational grid. In: International Conference in Computing, Analytics and Networking, pp. 501–510. Springer (2018)



5. Jayapandian, N.: Parallel queue scheduling in dynamic cloud environment using backfilling algorithm. *Int. J. Intell. Eng. Syst.* **11**(2), 39–48 (2018)
6. Jayapandian, N., Zubair Rahman, A.M.J.Md.: Secure and efficient online data storage and sharing over cloud environment using probabilistic with homomorphic encryption. *Clust. Comput.* **20**, 1561–1573 (2017)
7. Younis, M.T., Yang, S.: Hybrid meta-heuristic algorithms for independent job scheduling in grid computing. *Appl. Soft Comput.* **72**, 498–517 (2018)
8. Dai, Y.S., Xie, M., Poh, K.L.: Availability modeling and cost optimization for the grid resource management system. *IEEE Trans. Syst. Man Cybern.-Part A: Syst. Hum.* **38**(1), 170–179 (2008)
9. Cao, J., Jarvis, S.A., Saini, S., Nudd, G.R.: Gridflow: workflow management for grid computing. *Computers* **1**(1), 198–205 (2003)
10. Hamscher, V., Schwiegelshohn, U., Streit, A., Yahyapour, R.: Evaluation of job-scheduling strategies for grid computing. In: *International Workshop on Grid Computing*, pp. 191–202. Springer (2000)
11. Chen, H., Maheswaran, M.: Distributed dynamic scheduling of composite tasks on grid computing systems. In: *International Symposium on Parallel and Distributed Processing*, pp. 1–10. IEEE (2001)
12. Fang, Y., Wang, F., Ge, J.: A task scheduling algorithm based on load balancing in cloud computing. In: *International Conference on Web Information Systems and Mining*, pp. 271–277. Springer (2010)
13. Yu, J., Buyya, R.: A taxonomy of workflow management systems for grid computing. *J. Grid Comput.* **3**(3), 171–200 (2005)
14. Tang, M., Lee, B.S., Tang, X., Yeo, C.K.: The impact of data replication on job scheduling performance in the Data Grid. *Future Gener. Comput. Syst.* **22**(3), 254–268 (2006)
15. Opitz, A., König, H., Szamlewska, S.: What does grid computing cost? *J. Grid Comput.* **6**(4), 385–397 (2008)



# A Comparative Analysis of LEACH, TEEN, SEP and DEEC in Hierarchical Clustering Algorithm for WSN Sensors

Anitha Amaithi Rajan<sup>(✉)</sup>, Aravind Swaminathan, Brundha,  
and Beslin Pajila

Department of Computer Science Engineering, Francis Xavier Engineering  
College, Tirunelveli, Tamil Nadu, India  
{anitharajan1804, aravindcse2010, brundhasenthil,  
beslin.kits}@gmail.com

**Abstract.** Remote sensor system (RSS) is a framework formed with an extensive number of minimal effort micro-sensors. Number of messages can be sent to the base station (BS) by using this system. RSS includes ease hubs with affected battery power, additionally the battery swap isn't easy for WSN with thousands of physically inserted hubs, which suggests vitality productive steering convention to supply a long-labor of affection time. To accomplish the point, we require not just minimizing absolute vitality utilization additionally to adjust WSN load. Scientists have proposed numerous conventions, for example, LEACH, TEEN, SEP, DEEC. The elective Cluster Heads (CHs) communicate the base Station (BS) through beta elective nodes, by exploitation multi-hopping. We tend to logically divide the network into two elements, on the idea of the residual energy of nodes. The normal nodes with high initial and residual energy are going to be extremely probable to be CHs than the nodes with minor energy. The algorithms applied in a situation where initial energies of nodes are different from each other are called as mixed clustering schemes. It is difficult to implement an energy aware mixed clustering algorithm due to the complex energy design of the network.

**Keywords:** Remote sensor system · Cluster Heads · Base station · Wireless Sensor Network

## 1 Introduction

The multiplication of the usage for minimal effort, low-control, multifunctional sensors has made remote sensor systems (WSNs) an unmistakable information gathering worldview for extricating nearby proportions of interests. In such applications, sensors are commonly thickly conveyed and haphazardly dissipated over a detecting field and left unattended in the wake of being sent, which make it hard to energize or supplant their batteries. At the point when sensors around the information sink drain their vitality, arrange network and inclusion may not be ensured. Because of these imperatives, it is significant to structure a vitality proficient information gathering plan that expends vitality consistently over the detecting field to accomplish long system

lifetime. Moreover, as detecting information in a few applications are time-touchy, information accumulation might be required to be performed inside a predefined time period. Transfer steering is a straightforward and a powerful way to deal with directing messages to the information soak in a multi-bounce form. It considered the development of a most extreme lifetime information gathering tree by planning a calculation that begins from a self-assertive tree [2] and iteratively diminishes the heap on bottleneck hubs. Assess Collection Tree Protocol (CTP) by means of proving grounds. CTP processes [3] remote courses versatile to remote connection status and fulfills unwavering quality, heartiness and proficiency and equipment autonomy necessities. Proposed convention is contrasted and Low-Energy Efficient Clustering Hierarchy (LEACH), Stable Election Protocol (SEP) and Distributed Energy Efficient Clustering [4] (DEEC). Our reenactment results demonstrates that our proposed convention beats every one of these conventions as far as dependability and system lifetime.

## 2 Related Work

To help multicast transmission, a multicast tree is shaped on-request to incorporate all the gathering individuals and some non-individuals which are hand-off hubs [1]. The way toward building such a tree is like the course disclosure strategy in unicast directing: each time when a hub needs to join a multicast gathering or to send an information bundle to a multicast goal (while it doesn't have the best possible steering passage), a RREQ [5] message is communicated all through the MANET. The hubs in the multicast tree for this gathering send back a RREP message. The hubs sending RREQ and RREP record the way in reverse to the wellspring of parcel, as they will do in unicast directing. On receipt of various RREP parcels, the hub picks one part of the multicast tree and associates with it, in this manner a circle is stayed away from. At the point when a connection breakage is distinguished because of hub development, the hub which is more remote far from the gathering chief starts neighborhood fix [6]. Once more, it communicates a RREQ message and hangs tight for RREP from the gathering chief. By this implies the tree is reproduced to suit the topological change. WSN comprising of countless sensors [7] with low-control handsets can be a viable instrument for social occasion information in an assortment of situations. As sensor hubs are sent in detecting field, they can assist individuals with monitoring and total information. Analysts likewise endeavor to discover progressively proficient methods for using restricted vitality of sensor hub so as to give longer life time of WSNs [8]. System lifetime, versatility, and load adjusting are essential prerequisites for some, information gathering sensor arrange applications. Along these lines, numerous conventions are presented for better execution. Receptive systems, as opposed to latent information gathering proactive systems, react promptly to the progressions happening in the critical parameters of intrigue. They present another vitality proficient convention, TEEN (Threshold touchy Energy Efficient sensor Network convention) for responsive systems [9]. The execution of convention for a straightforward temperature

detecting application was being assessed. As far as vitality productivity, the convention has been seen to beat existing ordinary sensor arrange conventions. Youngster depends on a various leveled gathering where closer hubs frame bunches and this procedure goes on the second dimension until the BS (sink) is come to. Adolescent is a grouping correspondence convention that objectives a receptive system and empowers CHs to force a limitation on when the sensor should report their detected information these sensor hubs (or basically hubs) are generally conveyed arbitrarily and thickly in threatening condition. They team up to watch the environment and send the data back to the system chief (or base station) when unusual occasions happen [10]. It is alluring to make these hubs as vitality effective as could reasonably be expected and to depend on their expansive numbers so as to get fantastic outcomes.

The absence of physical remoteness leads to the performance vulnerability. For this reason it's suffer more so they can't share the resources for the more people only for the limited people [11]. Our implementation focused mainly on security and performance vulnerability occurs, all the authorized users can't use the SERVER resource as full fully and it's not support for a flexible strong environment for large-scale applications.

### 3 Proposed System

To beat this issue utilizing swiper a system it can without much of a stretch offer the speed. In the swiper outline work it basically focus on the three procedure co-area, synchronization and exploiting, co-area put the foe SERVER on indistinguishable physical machine from the unfortunate casualty SERVER synchronization distinguish whether the focused on application is running on the person in question and, provided that this is true, the condition of execution for the focused on abusing structure an antagonistic outstanding task at hand as indicated by the condition of the injured individual application, and dispatch the remaining task at hand to defer the person in question.

#### 3.1 Reliability Gain of Network Secret Writing in Thrashing Wireless Networks

In spite of the fact that these sensor hubs are not as incredible or precise as their costly full scale sensor partners, we can assemble a fantastic, blame tolerant sensor arrange by making a large number of sensor hubs cooperate. Through the collaboration of remote sensor hubs, WSN gathers a lot of data and sends them to the Base Station (BS). WSN has a wide scope of potential applications including military observation, debacle forecast, and condition checking, and so on. After sending, the system can't work legitimately except if there is adequate battery control. When all is said in done, WSN may deliver a significant considerable measure of information, so if information combination could be utilized, the throughput could be decreased. Since sensor hubs are conveyed thickly, WSN may produce excess information from various hubs, and the repetitive information can be joined to decrease transmission.

In this paper an Energy Efficient Clustering Scheme for Self-Organizing Distributed Wireless Sensor Networks (EECS). We considers a circumstance in which the system gathers data intermittently from a landscape where every hub constantly faculties nature and sends the information back to BS. Typically there are two definitions for system lifetime:

- (a) The time from the beginning of the system activity to the demise of the principal hub in the system.
- (b) The time from the beginning of the system task to the demise of the last hub in the system.

## 4 Experiment

### 4.1 Initial Phase

The steering tree and the calendar of the system by utilizing the EL and directions data. BS communicates a bundle to every one of the hubs to educate them of starting time, the time allotment space and the quantity of hubs  $N$ . At the point when every one of the hubs gets the parcel, they will process their own vitality level.

### 4.2 Tree Constructing Phase

BS can transmit every one of the information with indistinguishable length from its own, which results in considerably less vitality utilization. So as to adjust the system stack hub with the biggest leftover vitality is picked as root. The root gathers the information everything being equal and transmits the melded information to BS over long separation.

### 4.3 Self-organized Data Collecting and Transmitting Phase

TDMA and Frequency Hopping Spread Spectrum (FHSS) are both connected. This stage is separated into a few TDMA availabilities. In a vacancy, just the leaf hubs endeavor to send their DATA\_PKTs. After a hub gets every one of the information from its youngster hubs, this hub itself fills in as a leaf hub and attempts to send the combined information in whenever space.

### 4.4 Information Exchanging Phase

It might debilitate its vitality and kick the bucket. The withering of any sensor hub can impact the geography. So the hubs that will pass on need to illuminate others. The procedure is likewise separated into schedule openings. In each schedule opening, the hubs whose vitality will be depleted will figure an irregular postpone which makes just a single hub communicate in this vacancy. At the point when the deferral is finished, these hubs are attempting to communicate a bundle to the entire system. Here we use LEACH, TEEN and proposed EECS conventions for grouping idea. In the LEACH arrange has a large number of remote sensors are scattered that gathers and transmits

information. Additionally in these systems group takes are chosen off of the sensors to transmit the information gathered to the base station. Because of enormous control bundles it will make a lot of vitality be squandered. Here we use LEACH and TEEN conventions for bunching idea. In the LEACH organize has a huge number of remote sensors are scattered that gathers and transmits information. Additionally in these systems group takes are chosen off of the sensors to transmit the information gathered to the base station.

### 5 Flow Diagram

The following Fig. 1 shows the flow diagram of node death occurrence. It starts from the cluster formation and continuous with tree construction process and data gathering undergone in setup and transmission phase. Finally based on threshold value the node death will occur.

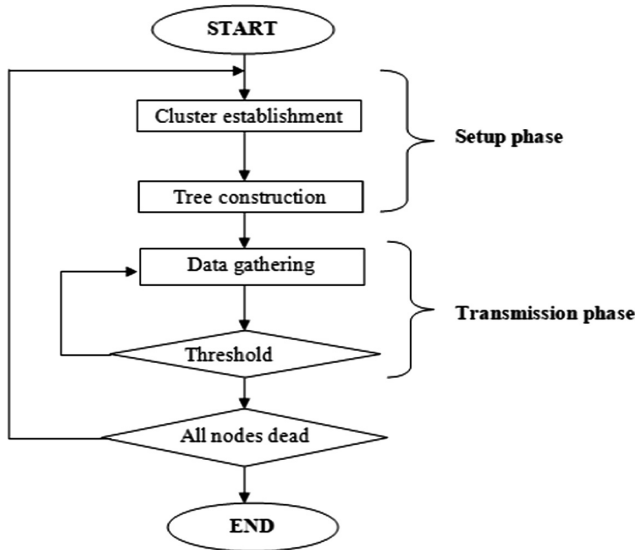


Fig. 1. Flow chart

## 6 Result Analysis

### 6.1 Performance Analysis of Heterogeneous Clustering Protocols Simulation and Results

In this section, the comparison is made between two heterogeneous clustering protocols, SEP and DEEC Simulation parameters (Table 1).

**Table 1.** Simulation parameters for heterogeneous clustering protocols

Simulation parameters	Values
Simulation area	100 × 100 m
Skin position	50 × 50 m
Number of nodes	100
Transmitter amplifier energy dissipation	$E_{fs} = 10 \times 0.0000000000001$ J $E_{mp} = 0.0013 \times 0.000000000001$ J
Channel type	Wireless
Cluster head selection probability	0.1
Data aggregation	5*0.000000001
Energy model	Battery
Initial energy	0.5 J
Transmit power	$0.5 \times 10^{-7}$
Receiver power	$0.5 \times 10^{-7}$
Maximum number of rounds	3000
Percentage of advanced nodes	0.1
Energy enhancement of advanced nodes	1

## 6.2 Performance Analysis

Figures show experimental comparison results of the two protocols, SEP and DEEC in the aspect of nodes dead, nodes alive and packet delivery ratio. The ratio of number of packets sent from the source to the number of packets received at the destination. The greater the value of PDR means the better the performance of the protocol (Table 2).

**Table 2.** Simulation performance for all protocols

PERFORMANCE	LEACH	SEP	DEEC	TEEN
Cluster stability	Lower than SEP and DEEC	Moderate	High	Medium High
Energy efficient	Low comparing SEP and DEEC	Moderate	High	High
Cluster head selection criterion	Moderate	LOW	LOW level variety	High
Network lifetime	Moderate	Moderate	Network lifetime than SEP and LEACH	Network lifetime than SEP and DEEC

Figure 2 indicates that the first node of SEP dies faster than the first node of DEEC which implies that the stable region of DEEC is greater than the stable region of SEP.

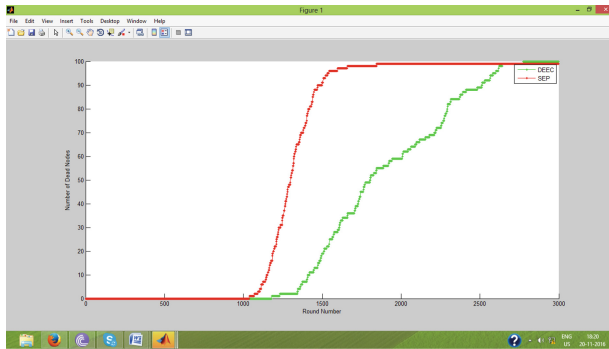


Fig. 2. Number of dead nodes versus rounds

Figure 3 implies that all nodes of SEP get drained merely from round 2000 but in case of DEEC all nodes get drained only after round 2600. So DEEC can withstand much more time than SEP. This will avoid bottleneck problem and may result in long life of the network by proper load balancing. This protocol degrades the energy of long distance sensor nodes early than nearer sensor nodes.

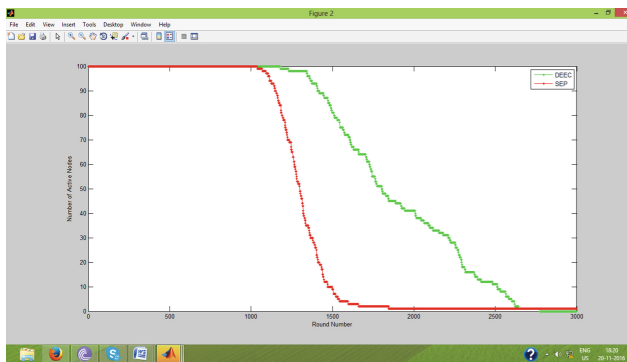
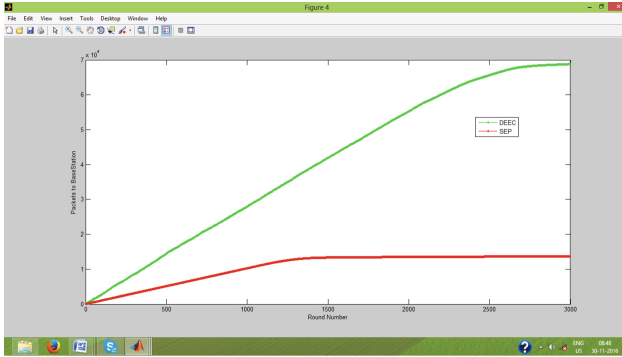


Fig. 3. Number of alive nodes versus rounds

In SEP and DEEC, first node dies at 922 and 965 respectively while in LEACH and TEEN, first node dies at 1487 and 2389 respectively. So, stability time of TEEN and LEACH is 35% and 60% better than DEEC respectively and 38% and 61% better than SEP due to inefficient energy utilization in these classical protocols.





**Fig. 4.** Packets to BS versus rounds

A base station receiving more data packets confirms the efficiency of clustering protocol. Throughput depends on network life time in a sense but not always. Considering the simulated results as shown in Fig. 4 we deduce that maximum throughput is achieved by DEEC.

## 7 Conclusion and the Future Work

One of the fundamental difficulties in the plan of bunching conventions for WSNs is vitality productivity. In this manner, grouping conventions proposed for WSNs ought to be as vitality effective as conceivable to delay the lifetime of the individual sensors and thus the system life time. Many grouping conventions have been proposed to settle this issue. This venture reenacts and examines Homogeneous bunching conventions, LEACH and TEEN and Heterogeneous grouping conventions, SEP and DEEC. Through the investigation made on LEACH and TEEN, it is reasoned that TEEN performs nearly well than LEACH since TEEN gives vitality effectiveness by having increasingly number of alive hubs in the later cycles and in this manner dragging out the existence time of the system. Furthermore, through the examination made on SEP and DEEC, it is presumed that DEEC performs similarly well than SEP on the grounds that DEEC gives vitality effectiveness by having higher steadiness area than SEP which prompts higher unwavering quality and in this manner drawing out the existence time of the system.

## References

1. Manjeshwar, A., Agrawal, D.P.: TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. In: Proceedings of 15<sup>th</sup> International Parallel and Distributed Processing Symposium (2009)
2. Chen, G., Li, C.: An unequal cluster-based routing protocol in wireless sensor networks. Springer (2007)

3. Marin-Perianu, R.S., Scholten, J.: Cluster-based service discovery for heterogeneous wireless sensor networks. *Int. J. Parallel Emergent Distrib. Syst.* **23**, 325–346 (2007)
4. Kumar, D.: Energy efficient heterogeneous clustered scheme for wireless sensor networks. *Comput. Commun.* **32**, 662–667 (2009)
5. Kim, K.T., Yoo, H.K.: EECS: an energy efficient cluster scheme in wireless sensor networks. In: *IEEE International Conference on Computer and Information Technology* (2010)
6. Chaurasiya, V.K., Rahul Kumar, S.: Traffic based clustering in wireless sensor network. In: *IEEE WCSN* (2008)
7. Mehrani, M.: FEED: fault tolerant, energy efficient, distributed Clustering for WSN. In: *Advanced Communication Technology (ICACT)*. IEEE (2010)
8. Kumar, A., Chand, N.: Location based clustering in wireless sensor network. *World Acad. Sci. Eng. Technol.* **5**, 1313–1320 (2011)
9. Wang, C., Liu, J.: An improved LEACH protocol for application specific wireless sensor networks. In: *IEEE: WiCOM 2009 Proceedings of the 5th International Conference on Wireless Communication Networking and Mobile Computing* (2009)
10. Saini, P., Sharma, A.K.: Energy efficient scheme for clustering protocol prolonging the lifetime of heterogeneous wireless sensor networks. *Int. J. Comput. Appl.* **6**, 30–36 (2010)
11. Ishmanov, F., Kim, S.W.: Distributed clustering algorithm with load balancing in wireless sensor network. In: *IEEE World Congress on Computer Science and Information Engineering* (2009)



# Investigation of Power Consumption in Microcontroller Based Systems

Rakhee Kallimani<sup>1</sup>(✉) and Krupa Rasane<sup>2</sup>

<sup>1</sup> Department of Electrical and Electronics, KLEDRMSSCET, Belgaum, India  
rakhee.kallimani@klescet.ac.in

<sup>2</sup> Department of Electronics and Communication,  
Jain College of Engineering, Belgaum, India  
kru\_ran@yahoo.com

**Abstract.** In this paper, the current consumption of microcontroller with varying frequency and voltage has been experimented in an attempt to understand the power consumption of microcontroller. The power consumption of microcontroller, when connected to an active load, is investigated. The microcontroller is experimented in sleep mode and analyzed the current consumption in its deepest sleep mode and active mode. Among the various wake-up sources, we have used an external input pin and watchdog timer method for the experimental setup. Using the obtained values the battery life is estimated.

**Keywords:** Embedded systems · Wireless Sensor Network (WSN) · Sleep/active · Low power · Microcontrollers · Battery life · Power management

## 1 Introduction

Designing an Embedded system is a challenging task and it requires several metrics to be considered while designing an embedded system. [1] Some of the design metrics are (1) Size: The physical size of the embedded system is of most important design metric, (2) Power: the amount of power consumed by the system is another challenging design metric, (3) Flexibility: the ability of the system to change the function without incurring loss to the system, (4) Cost: the Non Recurring and Recurring cost is to be decided while designing the embedded systems and (5) Safety, correctness, testability and manufacturability and many more. Out of the above metrics, power consumption is the major metric to be considered and is found of enormous scope in the field of research. Particularly in designing the portable embedded system, power consumption would be an important design metric to be considered at the early stage of the design.

Wireless Sensor Network has lately gained the attention of embedded system design researchers. Another parallel technology, the Internet of Things has also become very popular and as specified in [2], the author estimates that 99.4% of the existing objects are yet to be connected to the internet. Further the authors mention that it is all Internet of Everything (IoE), and reflects that there is an need to create intelligent connections by the year 2020. Both WSN and IoT are gaining the attention of Researchers to connect the devices across. Both WSN and IoT are gaining the interest of researchers and academicians in increasing processing power, storage and decreasing the cost of bandwidth

and many more. This encourages the researchers to think on power investigation of the processor/microcontroller such that we can handle the power of the connected devices optimally through internet.

Typically a WSN consist of numerous sensor nodes, a processing subsystem and a communication unit. And these nodes are found to be deployed at remote places and should be capable enough to maintain and organize the sensing capability without the human intervention in most of the application. This makes them to be self reliant and thus these nodes are required not to deplete the power faster over the period of time. This puts a great demand on the power management requirements of the nodes, the node size and the mode of deployment [15]. This is a big challenge to the researchers and much research is done on deployment setting i.e. for manually replacing the batteries or using rechargeable batteries. But this calls for a trade off in the design. Conventionally, batteries are connected to source these nodes. And researchers have made great efforts to limit the finite battery by different power control algorithm and topologies [3, 4]. In WSN, the rechargeable batteries are not considered and non rechargeable batteries are very costly thus this needs to manage power efficiently and increase the lifetime of battery. To extend the lifetime of the sensor node, it is very much required to know the power consumption of the nodes. As the battery life is important metric in the design of sensor node for a longer life.

## 2 Wireless Sensor Network

### 2.1 Architecture

A wireless sensor network basically consists of data processing unit, communication unit and information collection unit as shown in the block diagram, Fig. 1. The data processing unit employ strong ultra low power microcontroller or microprocessor, which can provide a feature to enable themselves to be put in low power down mode or idle mode when they are idle and communication unit is comprised of communication protocols such as inter-integrated Circuit(I2C), suitable for low speed communication (communication between ADC and processing subsystem), Serial Peripheral Interface (SPI) suitable for high speed communication. For the information/data collection is performed by sensor node, aim at collecting the physical data from the nature and send it to the processing unit for processing of information. All the components of WSN node requires power supply and has to be efficiently handled in a node [5].

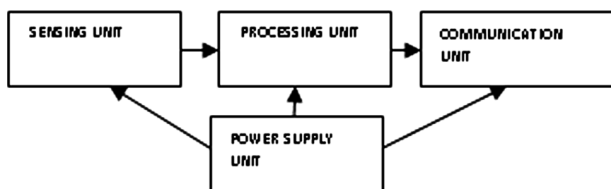


Fig. 1. A block diagram of wireless sensor node

### 2.2 WSN Standards and Components

In the recent years, there has been a great advance in developing WSN standards. IEEE has defined two standards, the IEEE 802.15 regarding the wireless communication interface between nodes and the IEEE 1451 that defines the interface between sensors and actuators.

One of the popular protocols in WSN is ZigBee [7], that defines the network and the application layers, built upon the IEEE 802.15.4 physical and MAC layers. In the ZigBee specification the network layer has different topologies namely tree, star, point-to-point (mesh). Each topology has three different kinds of nodes as shown in Fig. 2. They are (1) Network coordinator, which forms the root of the network and this is the one which gets all the data from the end devices in the network and as well as it can send information to the end device, thus it needs to be awake most of the time [10, 14]. (2) Router, it can act as an intermediate between a co-ordinator and an end device, passing on data from each other. It can get information from end device and send to co-ordinator as well as it can send the data from co-ordinator to the end device. (3) End device or Nodes, these are the devices which are the outer end of the network; it is only able to communicate with its parent (router or coordinator). The end devices are usually battery operated and deployed in inaccessible locations thus have gained the attention of research in the area of power consumption.

These devices can go to sleep and thus can be optimized for power consumption in the network. It is not mandatory to have all the three nodes, a network can drop a router depending upon the application. Network would be implemented by just connecting a co-ordinator and an end device only.

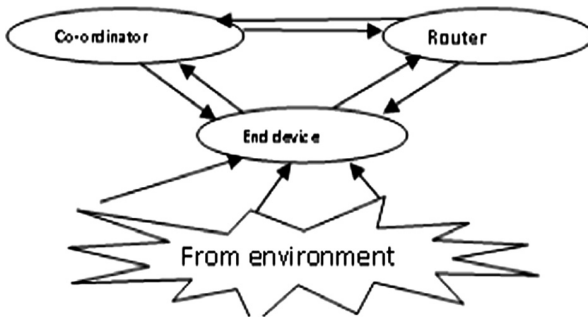


Fig. 2. Network nodes

### 3 Methods

The popular wireless sensor network nodes are built these days on the low power microcontroller. The low power and ultra low power microcontrollers are in demand for the feature provided on power saving. To mention few of them, researchers are using MSP430, ATmega328/P and many more as mentioned in [6]. The processing unit of Wireless sensor node is comprised of low power microcontrollers. The author in [11]

explains ATmega128L microcontroller in different sleep modes for processing sub-system. In this paper we have analyzed the ATmega328/P microcontroller [8] which provides six different configurations and this feature helps in establishing the processor in sleep modes, the different power dissipation profile.

**Table 1.** Six different sleep modes of ATmega328/P microcontroller with wake up sources

Sleep mode	INT AND PCINT	TWI address match	Timer2	SPM/EEPROM ready	ADC	WDT	Other I/O	Software BOD disable
Idle	Y	Y	Y	Y	Y	Y	Y	
ADC noise	Y	Y	Y	Y	Y	Y		
Reduction	Y	Y				Y		y
Power-down	Y	Y	Y			Y		Y
Power-save	Y	Y				Y		Y
Standby	Y	Y				Y		Y
Extended standby	Y	Y	Y			Y		Y

Table 1. display the different sleep mode of ATmega328/P and describes the different wake up sources and their oscillators and active clock domain.

### 3.1 Sleep Mode

ATmega 328P microcontroller has number of sleep modes that can be invoked to reduce the power consumption, this is a good feature for the application which are battery operated.

A number of wake up sources can be specified to wake the microcontroller from sleep mode and resume the operation. Some of the wake up sources:

- (a) External interrupt
- (b) Pin change interrupt
- (c) Timer interrupt
- (d) Watchdog interrupt
- (e) I2C address match and many more

### 3.2 Power Reduction Register

The Power Reduction Register (PRR) allows to turn off the clock to individual peripherals that are not in need and reduce power consumption when in active mode. For power saving PPR can be used when in the IDLE sleep mode. The PRR register bit is to be manipulated to use this function for power saving. PPR can Turn OFF or ON

the following (1) Analog to Digital Converter (ADC), (2) Serial Peripheral Interface (SPI) for communication, (3) 2 wire Serial Interface, (4) Serial Communication (USART) and (5) Timer/counter0, timer/counter1, Timer/counter 2.

### 3.3 Watch Dog Timer

The Microcontroller has an Enhanced Watchdog Timer (WDT). The WDT is a timer counting cycles of a separate on-chip 128 kHz oscillator. The WDT can be used as a stop watch for the system reset or as interrupt source. The WDT gives an interrupt or a system reset when the counter reaches a given time-out value. In normal operation mode, it is required that the system uses the Watchdog Timer Reset (WDR) instruction to restart the counter before the time-out value is reached. If the system doesn't restart the counter, an interrupt or system reset will be issued as mentioned in [8]. To set the interval of the WDT, we set "Prescalers bits" of the registers.

In Interrupt mode, the WDT generates an interrupt when the set timer expires its count. This mode is used to wake the device from sleep-modes, and also as a general system timer. One example is to limit the maximum time allowed for certain operations, giving an interrupt when the operation has run longer than expected. In System Reset mode, the WDT gives a reset when the timer expires. This is typically used to prevent system hang-up in case of runaway code. The third mode, Interrupt and System Reset mode, combines the other two modes by first giving an interrupt and then switch to System Reset mode. This mode will for instance allow a safe shutdown by saving critical parameters before a system reset.

### 3.4 Brown Out Detect

BOD is abbreviated in datasheet [8] detects when there is a drop in voltage VCC for a certain period of time and will reset the MCU. This function is used to ensure there is no unexpected behavior occurs when VCC is dropped for whatever reason. The BOD can be shut down if the Voltage drop is not a big concern in the design. The BOD is set by the Fuse Bits, these bits are in non-volatile memory and thus can be altered using IDE. ATmega328/P has three different fuse levels, high fuse, low fuse and extended fuse. The BOD is in extended fuse, in which there are three different level of triggering

## 4 Results

The microcontroller ATmega328/P has different power saving modes and can be invoked by the available wakeup sources. For measurement of current consumption the microcontroller is put in deep power down mode and is woke up by the two possible ways [9].

- (1) Periodically waking up the microcontroller by the internal watchdog timer and in sensor node, it is configured as transmission mode.
- (2) The other method is by using the external interrupt method and in sensor node, it is configured as reception mode in sensor node.

A summary of both the wake up methods of the microcontroller from deep sleep mode is performed using high precision multi-meter and is summarized in the Table 2.

#### 4.1 Power Down Mode

**Table 2.** Power down mode and current consumption

Current reading		
	External pin Interrupt	Watchdog timer
Active mode	22 mA	3.14 mA
Sleep mode	14.9 mA	0.1 $\mu$ A

#### 4.2 Changing the Crystal and Voltage

Power management is managing the power consumption of ATmega328/P microcontroller, when operated at different operating voltages and frequencies are studied. We have connected 16 MHz as external crystal and 8 MHz as internal crystal. Table 3. summarizes the reading of current consumption. The measurements are done using a high precision multi-meter and with regulated power supply.

**Table 3.** Current consumption with different frequency and voltage

Current reading (mA)			
Crystal	Voltage	Current	Power
16 MHz	5 V	22 mA	110 mW
16 MHz	3.3 V	12.2 mA	40.26 mW
8 MHz	5 V	6.6 mA	33 mW
8 MHz	3.3 V	3.4 mA	11.22 mW

#### 4.3 Estimation of Battery Life

With the measured values, an attempt is made to estimate the battery life of a node during both the wakeup sources [12, 13].

The node is made to go sleep and wake up after a regular interval of time using the watch dog timer. This concept of waking the microcontroller regularly to the set time of the watchdog timer is similar to the cyclic scheduling.

The following simple equations are used to estimate the battery life of a node [10].

Duty ratio is defined as ratio of the sleep/wake up cycle.

$$D = \frac{t_w[s]}{t_p[s]} \quad (1)$$

Where,  $t_w$  is the time period employed when the node is running active,  $t_p$  is the total time period, both in seconds.



We worked our watch dog timer for 1 s thus duty ratio was calculated to be 50%. Assume the battery capacity to be  $cap$  and to be derating factor of 85%, assuming  $I_a$  and  $I_s$  to be active currents and sleep currents consumed by the node. The node is assumed to constantly repeat to sleep and run with the fixed time durations.

Battery life is estimated using the following equation

$$\text{battery life} = \frac{cap[\text{Ah}] \times 0.85}{I_a.D + (1 - D)I_s} \quad (2)$$

## 5 Conclusion

In this paper, we have presented the two possible ways of wake up sources to be used to wake up the microcontroller from the deepest sleep mode and measured the current consumption, to calculate the power consumption of microcontroller. An attempt of understanding power consumption by varying the voltage and frequency is also made. The measured values aided us in estimating the battery life of a sensor node. This is estimated for the sensor node which is battery operated, especially for an end device in a Wireless Sensor Network. This can aid an embedded designer at the early stage of the design. The work can be further carried out with different current measurement methods and read the high dynamic range of current in microcontroller based systems and analyze the power consumption of the system, and manage the power accordingly without affecting the performance of the system.

## References

1. Vahid, F., Givargis, T.: A Unified Hardware/Software Introduction. Wiley, Hoboken (2002)
2. Bradley, J., Barbier, J., Handler, D.: Embracing the internet of everything to capture your share of \$14.4 trillion, Cisco, San Jose, CA, USA (2013)
3. Ahonen, T., Virrankoski, R., Elmusrati, M.: Greenhouse monitoring with wireless sensor network. In: IEEE/ASME, pp. 403–408(2008)
4. Deepti Goyal, S.: Power management in wireless sensor network. In: Computing for Sustainable Global Development. IEEE (2016)
5. Da silva, A.I., Pereira, F.D.: An based-FPGA dynamic power management technique for wireless sensor network. In: 3rd International Conference on e-Technologies and Networks for Development, pp. 189–194. IEEE (2014)
6. Jelicic, V.: Power Management in Wireless Sensor Networks with the Consuming Sensor (2011)
7. <http://www.intechopen.com/books/authors/ict-energy-concepts-towards-zero-power-information-and-communication-technology/power-consumption-assessment-in-wireless-sensor-networks>
8. Atmel-42735-8-bit-AVR-Microcontroller-ATmega328-328P\_Datasheet
9. Di Nisio, Attilio, Di Noia, Tommaso, Carducci, Carlo Guarnieri Calò, Spadavecchia, Maurizio: High dynamic range power consumption measurement in microcontroller-based applications. IEEE Trans. Instrum. Measur. **65**(9), 1968–1976 (2016)

10. Yamawaki, A., Serikawa, S.: Battery life estimation of sensor node with zero standby power consumption. In: IEEE International Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), pp. 166–172 (2016)
11. Dargie, W.: Dynamic power management in wireless sensor networks: state-of-the-art. *IEEE Sens. J.* **12**(5), 1518–1528 (2012)
12. Cornell, E.D., Lam, C.S., Sundar, S.: Humidity and temperature sensor node for star networks enabling 10+ year coin cell battery life, Texas Instruments, Technical report TIDU797B(2015)
13. Zhao, Q., Nakamoto, Y., Yamada, S., Yamamura, K., Iwata, M., Kai, M.: Sensor scheduling algorithms for extending battery life in a sensor node. In: *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E96-A, no. 6, pp. 1236–1244 (2013)
14. Santosh, K., Vishal, H., Rakhee, K.: Smart sensor system based smart sensor network system based on Zigbee technology to monitor grain depot. *Int. J. Comput. Appl.* **50**(21), 0975–8887 (2012)
15. Kallimani, Rakhee, Rasane, Krupa: A survey of techniques for power management in embedded systems. *IJETCSE* **14**(2), 461–464 (2015)



# An Analogical Study of Hyperledger Fabric and Ethereum

A. V. Aswin<sup>(✉)</sup> and Bineeth Kuriakose<sup>(✉)</sup>

Department of Computer Science and Engineering,  
Muthoot Institute of Technology and Science, Ernakulam, India  
aswinavofficial@gmail.com, bineeth@mgits.ac.in

**Abstract.** Hyperledger Fabric is one of the most popular blockchain framework which is hosted by the Linux Foundation. As a basis for the development of applications or solutions with a modular architecture, Hyperledger Fabric offers plug - and - play components such as consensus and membership services. Ethereum is a decentralized platform running smart contracts, applications running exactly as programmed without any possibility of downtime, censorship, fraud or interference from third parties. These apps are based on a custom built blockchain, an enormously powerful global shared infrastructure that can change value and represent property ownership. This study deals with comparison of Hyperledger Fabric and Ethereum platforms while covering various factors like architecture, performance, use cases, ease of algorithm etc.

**Keywords:** Blockchain · Hyperledger fabric · Ethereum

## 1 Introduction

Blockchain innovation is currently particularly well known in light of the fact that it gives another tool to explain problems in a way people couldn't previously. At the point when individuals consider blockchains, they in all likelihood consider Bitcoin, the most notable usage of a blockchain. There are numerous other blockchain usages also. Some of them are still being developed, while others are as of now running. Different implementations will vary in many ways such as their purpose, ease of participation, how governance is handled, and much more. To figure out which blockchain execution ought to be utilized for a given application, it is essential to be comfortable with the contrast between every usage. This paper discusses an overview of the blockchain technology and compares its different platforms which are commonly used, namely Ethereum and Hyperledger Fabric. The comparison is based on the conceptual design and is supported by identical implementations of one possible use case to cover additional development aspects.

## 2 Background

This section gives an overview of terms and technologies covered in this paper.

### 2.1 Blockchain

In general terms, a Blockchain is an immutable transaction ledger, maintained within a distributed network of peer nodes. Each node maintains a copy of the ledger through transactions validated through a Consensus Protocol, grouped into blocks with a hash which connects each block to the previous block [1].

### 2.2 Permissioned Vs Permissionless Blockchains

Permissionless blockchain networks are open to all and the identity of the participants are hidden. Virtually everybody can participate, and everyone is anonymous, in a permissionless blockchain. There is in this context nothing other than the state of the blockchain that offers participants trust. Permissionless blockchains usually have a native cryptocurrency which requires mining or transaction fees.

Permissioned blockchain only open to a selected group of verified participants operating under a governance model with partial trust exists between them. A permissioned blockchain provides a way of securing interactions between a group of entities that have a common goal but cannot trust each other completely. No costly mining is required and implementation of the native currency is not compulsory.

### 2.3 Smart Contracts

A Smart Contract is a virtual contract that is stored and executed by the blockchain like any other transaction. It acts as a regular contract between multiple parties but differs from the latter by not being approved by any central authority, such as notary or government, but by the network itself. It may contain any rules and therefore form any business logic that gets validated by every node. Basically said, it is a code, stored in the blockchain, that stipulates the conditions and waits for certain input to execute. For example, it is possible to set the code in smart contract to be executed at a certain time only.

## 3 Ethereum

Ethereum [2] is an open blockchain platform that allows everyone to build and operate decentralized apps using blockchain technology. Nobody controls or owns Ethereum just like Bitcoin, because it is an open-source project built by many people worldwide. But Ethereum was conceived as adaptable and flexible in contrast to the Bitcoin Protocol. New applications are easy to create on the Ethereum platform and now it is safe for anyone to use these applications with Homestead releases.

Ethereum [2] was created as a response to Bitcoin which is only focused on transferring monetary value between parties and has a limited programming language. Ethereum is a largest, decentralized software platform that enables designers to build decentralized applications over the blockchain using a built-in Turing complete programming language Solidity. Similar to Bitcoin, Ethereum has its own cryptocurrency called as *Ether*.

Ethereum platform is used to develop applications in a wide range of industries and services. Some of the applications are: Weifund, which offers an open crowdfunding campaign platform that make use of smart contracts. In Weifund, Contributions can be transformed into contractually supported digital assets which can be used, traded, or sold in the Ethereum ecosystem. Uport offers users a safe and convenient way of fully controlling their identity and personal information. Users control who can access and use their data and personal information rather than rely on government institutions and surrender their identities to third parties.

## 4 Hyperledger Fabric

Hyperledger Fabric is an open source business ready permissioned blockchain platform, designed for use in business environments and it has some unique features which are absent in other popular blockchain platforms. Hyperledger fabric was introduced by Linux Foundation which One key point of differentiation is that Hyperledger was established under the Linux Foundation, which has a successful track record of promoting open source initiatives under open governance that develop strong communities and prospering ecosystems. Hyperledger has various technical steering committees and a diverse range of managers from various institutions in charge of the Hyperledger Fabric project. Since its earliest commitment, it has a development community of over 35 organizations and almost 200 developers.

Hyperledger Fabric is an permissioned network framework with all participants knowing identities. A fabric network consists of “peer nodes” that execute chain code, access data, endorse transactions and application interface. “Orderer nodes” that ensure the consistency of the blockchain and deliver the transactions supported to the network’s peers and MSP services managing X.509 certificates which are used to authenticate member identities and roles.

## 5 Analysis

In order to compare the performance of both Ethereum and Hyperledger Fabric, an online voting system use case was taken and it was tested with two frameworks. This section explains how the use cases were implemented, what tools where used and what decisions were made.

### 5.1 Ethereum Application

The source code for this specific implementation is publicly available on GitHub [8]. The application is running using the *Truffle* framework [8] which makes the development of Ethereum applications easier providing smart contract compilation, deployment, binary management and automated testing which are effectively used while developing a given application. It is possible to develop applications right on the Ethereum blockchain, but as every transaction has its fee, it would be cheaper to test it locally before releasing it to the main Ethereum network. For that reason, *Ganache* [8] has been used as it provides a virtual Ethereum blockchain with fake accounts for testing. This application can be used to cast vote securely by making use of cryptography and this would ensure that people do not vote two times, because we have an immutable record of their vote and identity. Each voter has a public key-private key pair and private key is used by the voter to prove his identity and cast the vote (Figs. 1 and 2).

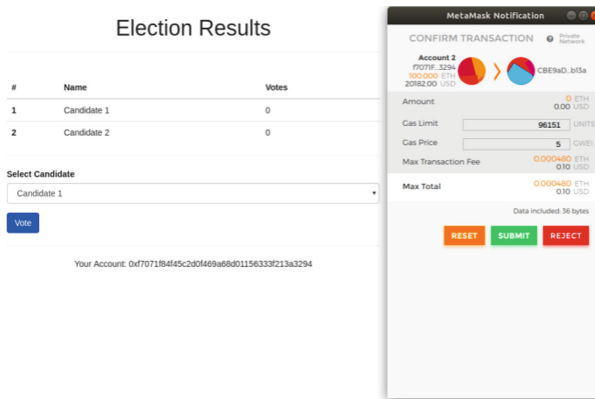


Fig. 1. Voting system DAPP

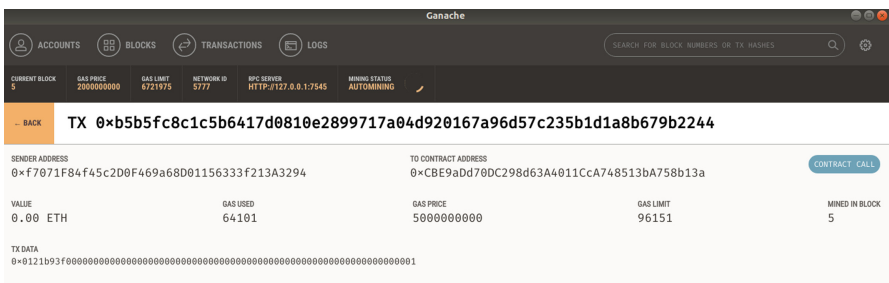


Fig. 2. Ethereum transaction details

### 5.2 Hyperledger Fabric Application

The source code for the Fabric implementation of the Voting app is publicly available at GitHub [9]. Implementation begins by providing a network with all the predefined participants in the configuration. Then a chaincode is created to interact with the ledger (Figs. 3 and 4).

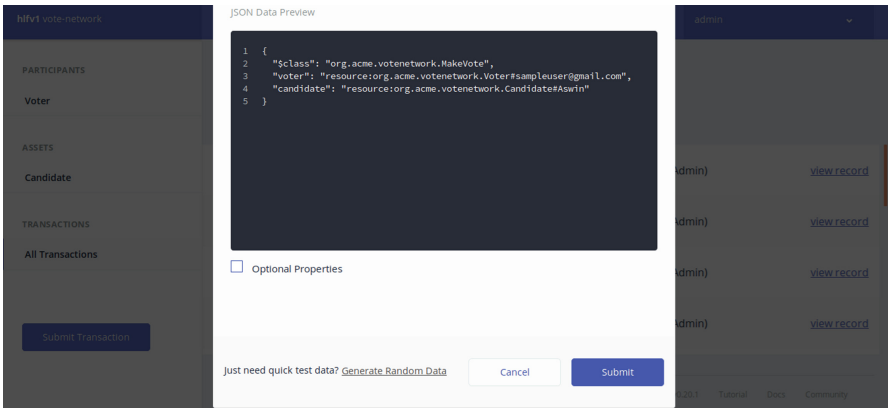


Fig. 3. Voting system Hyperledger Fabric app

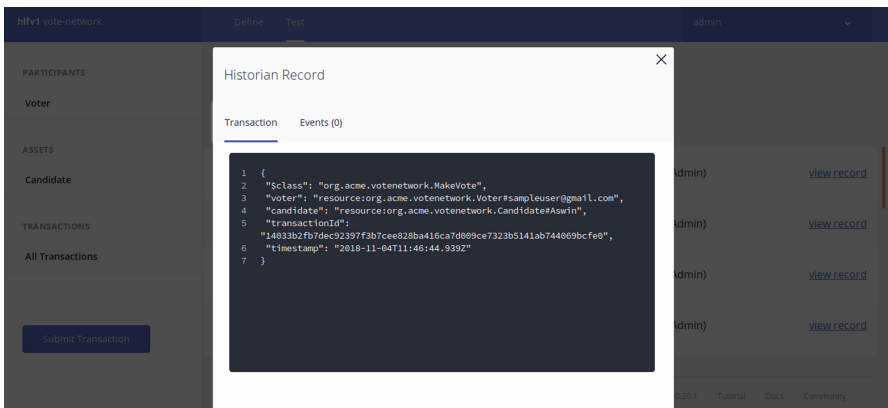


Fig. 4. Fabric transaction details

## 6 Comparison

This section compares Ethereum and Hyperledger Fabric platforms.

### 6.1 Architecture

Ethereum and Hyperledger Fabric have been designed to take into account different concerns. Since the idea of Ethereum is to be the public blockchain for all types of applications, it is designed to be permissionless and completely transparent. A shared ledger with universal access is used to store the data.

Hyperledger Fabric offers modular and flexible solutions for private blockchains that guarantee security and confidentiality. Channels provide independent ledgers which are accessible only to particular users provided by channels. Multiple channels can be created to connect only a particular group of users to it. Since the ledger is private, confidential data can be shared among a set of the participant without the notice of others participants.

Ethereum has native cryptocurrency implementation called *Ether*. Hyperledger Fabric doesn't have native cryptocurrency implementation.

### 6.2 Consensus Algorithm

Ethereum uses mining based proof of work consensus algorithm called *Ethash*.

In contrast, the Hyperledger fabric is modular and allows the use of various algorithms and also has different types of nodes on the consensus mechanism.

### 6.3 Ecosystem

Since Ethereum was one of the first Bitcoin blockchain platforms, it has become much more popular than Hyperledger Fabric. Many companies and developers have developed many tools and frameworks to facilitate the development of ethereum based distributed applications like Truffle framework, Ganache etc.

On the other hand, fabric has fewer tools besides Docker, which simplify the entire development process.

Hyperledger Fabric supports many common programming languages such as Go and JavaScript, in contrast to Ethereum that supports less popular contract-oriented language called as Solidity which is not popular among developers hence fewer libraries are available.

### 6.4 Use Cases

Ethereum is public and have open membership so it can be used as a cryptocurrency, in digital identity management, real estate etc. Another good use case for Ethereum could be online-gambling to make it more transparent while removing the need for trusted third party.



Fabric focusses on usecases which requires storage and handling of confidential data. Supply chain management, electronic health record management are some of the suitable usecases.

## 6.5 Language

One of the major parameter for comparison is language support. Ethereum supports languages that are specifically designed to be used for writing Ethereum smart contracts, such as Solidity and Vyper.

Hyperledger Fabric, on the other hand, supports multiple popular programming languages such as Go and JavaScript.

This brings us to a situation, where it is possible to write chaincode in Fabric without learning a new language. But, as Solidity is contract-oriented and designed specically for Ethereum, it can be more effective to use it.

## 6.6 Ease of Development

Ethereum uses Solidity, being an contract-oriented language it involves a learning curve but in case of fabric popular languages are supported and developer is not forced to learn a new language.

Even though Hyperledger Fabric development is docker based, it still requires lot of time for environment setup but in case of Ethereum Truffle framework, Ganache and Metamask makes Environment setup easier.

Ethereum is better than Hyperledger Fabric in case of developer community support.

## 6.7 Performance

Performance analysis [4] shows that Hyperledger Fabric performs in terms of throughput and latency consistently better than Ethereum. Evaluation also shows that when the workload is up to ten thousand transactions, Hyperledger Fabric achieves higher throughput and less latency than Ethereum. Transactions per second measure is used to compare the throughput because as the system grows larger it must have capacity to handle a greater number of transactions for increased speed and performance. Latency is one of the most important measure to compare performance of two blockchain platforms since for better performance latency should be minimum between transactions.

When number of transactions get increased to 10000, Hyperledger can handle 10 times more transactions per second than Ethereum and latency of Ethereum becomes 15 times greater than Hyperledger fabric.

Moreover, differences are growing as the number of transactions increases in execution and average delay between the two platforms. Hyperledger Fabric's average throughput also changes much faster than Ethereum's. However, Ethereum can manage more simultaneous transactions with similar computational resources (Fig. 5).

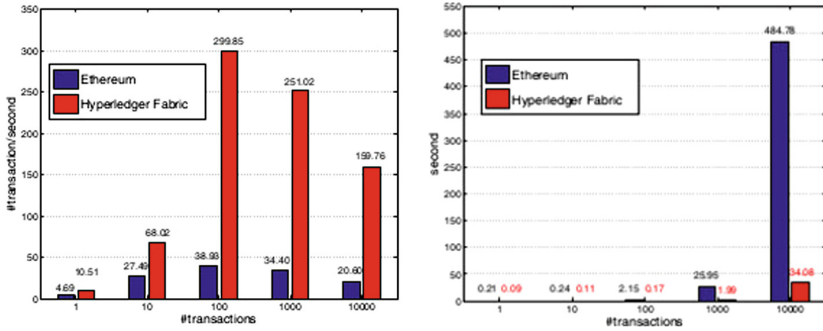


Fig. 5. Comparison of average throughput and latency between Ethereum and Hyperledger Fabric

## 7 Summary

Table 1 shows a comprehensive summary chart which compares the features and performance of both Ethereum and Hyperledger Fabric.

Table 1. Summary

Characteristics	Ethereum	Hyperledger Fabric
Description	Generic blockchain platform	Modular blockchain platform
Governance	Ethereum Developers	Linux Foundation
Mode of Operation	Permissionless, public or private	Permissioned, private
Consensus	Mining based on proof of work	Pluggable PBFT
State	Key-value database	Account data
Currency	Ether	None
Mining reward	Yes	None
Transaction	Anonymous or Private	Public or Confidential
Smart Contract	Solidity programming	Go, JavaScript
Throughput	Lower	Higher
Latency	More	Less
Learning Curve	More	Less
Environment Setup	Easier	Complex

## 8 Conclusion

The main goal of this paper was to compare Ethereum and Hyperledger Fabric in terms of its architecture and environment which they supports and then compare its performance using an implemented applications. Through this study it is found that Ethereum is public blockchain and therefore have all the data public, it suits well for applications that are designed to interact with a whole world such as insurance and peer-to-peer

gambling. Hyperledger Fabric, on the other hand, is designed for private use cases such as supply chain, where every chain participant should have data only relevant for him. For example, it allows possibility to sell goods with different prices without participants knowing about these deals. Analysis of same use case (Online Voting System) with Ethereum and Hyperledger Fabric was also done. It also demonstrates how to build applications on top of these platforms. Also it has found that as Ethereum is the most popular framework, its ecosystem is rich in different development tools but the supported languages are not that well-established and are thereby really limited. Hyperledger Fabric, in contrast, has only crucial tools but it supports popular languages that have already a lot of libraries to make development easier.

## References

1. Hyperledger Fabric Documentation. <https://hyperledger-fabric.readthedocs.io/en/release-1.3/>. Accessed 26 Dec 2018
2. Ethereum Homestead Documentation. <http://www.ethdocs.org/en/latest/>. Accessed 26 Dec 2018
3. Sajana, P., Sindhu, M., Sethumadhavan, M.: On blockchain applications: Hyperledger Fabric and Ethereum. *Int. J. Pure Appl. Math.* **118**(18), 2965–2970 (2018)
4. Pongnumkul, S., Siripanpornchana, C.: Performance analysis of private blockchain platforms in varying workloads. In: 26th International Conference on Computer Communication and Networks (ICCCN), Canada (2017)
5. Saraf, C., Sabadra, S.: Blockchain platforms: a compendium. In: IEEE International Conference on Innovative Research and Development (ICIRD), Thailand (2018)
6. Rouhani, S., Deters, R.: Performance analysis of Ethereum transactions in private blockchain. In: 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), China (2017)
7. Architecture of the Hyperledger Blockchain Fabric. [https://www.zurich.ibm.com/dccl/papers/cachin\\_dccl.pdf](https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf). Accessed 26 Dec 2018
8. Ethereum Voting DAPP Github. <https://github.com/dappuniversity/election>. Accessed 26 Dec 2018
9. Hyperledger Fabric Voting DAPP Github. <https://github.com/html5-ninja/hyperledger-vote-app.git>. Accessed 26 Dec 2018
10. Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>. Accessed 26 Dec 2018
11. Tasatanattakool, P., Techapanupreeda, C.: Blockchain: challenge and applications. In: 2018 International Conference on Information Network (ICOIN), Chaing Mai, pp. 473–475 (2018)
12. Ahram, T., Sargolzai, A., Sargolzai, S., Daniels, J., Amaba, B.: Blockchain technology innovations. In: 2017 IEEE Technology & Engineering Management Conference (TEMS-CON), Santa Clara 2017, p. 137 (2017)



# Smart City Traffic Control System

Kakan Adwani and N. Rakesh<sup>(✉)</sup>

Department of Computer Science and Engineering,  
Amrita School of Engineering, Bengaluru,  
Amrita Vishwa Vidyapeetham Amrita University, Bengaluru, India  
adwanikakan@gmail.com, n\_rakesh@blr.amrita.com

**Abstract.** Traffic light control systems are widely used to control the flow of the traffic in smart city. Due to rapid increase and continuous flow of the vehicles there is a lot of traffic congestion and people tend to break the traffic rules risking their life. Pedestrians are meant for the people to cross the road who are on foot but the vehicles are there on the pedestrians. At times breaking the traffic rule might lead to accidents. At night street lights are on even though the street is empty, which is a waste of energy and is a serious issue. So as to reduce the traffic congestion and make the people follow the traffic rules we propose “Smart City Traffic Control System”. It consists of a dynamic traffic light control system (based upon the density), a laptop camera (for monitoring and it will record the video in case if traffic rule has been broken, this recording will be stored and mailed to the traffic police department), a GSM module (to notify the traffic police department via SMS that a traffic rule has been broken, TSOP sensor, Arduino Mega Microcontroller, LEDs.

**Keywords:** Dynamic traffic light control system · Camera (lato) · GSM module · TSOP sensor · Arduino Mega Microcontroller · LEDs

## 1 Introduction

As wireless sensor network is a field of innovation we can automate each and everything in our surroundings with the help of sensors and thus making the devices smart and can be used in smart cities to control the traffic. In today’s life nobody wants to wait and so as to get rid from the fear of delay and to hurry up and reach to the destination on time people tend to break the traffic rules. Some people get caught hold by the police and are punished according to the law but some of them are not caught hold and they run away. Even though the pedestrians are meant for the people to cross the road but the vehicles are there and the people on foot cannot cross the road/fixed duration of traffic light signal increases the traffic as some of the lanes are empty and some of them are congested [1]. The number of vehicles are increasing day by day and thus, the traffic density is also increasing and as a result it slow down the speed and increases the delay to reach the destination and also increases the vehicle queuing [2].

Even today traditional circuits for traffic signal are used to control the flow of the automobiles and traffic light issue is one of the critical problems seen today [3]. As traffic congestion is a severe problem today then also the traffic signaling system is based on fixed time [4]. Also vehicular traffic control has been a problem at road crossings and has always been a matter of concern [5].

A lot of time is wasted at the signal even if there is no traffic because fixed time system is fixed for all lanes and is not concerned with the traffic density [6]. Vehicular density control is complicated and traditional approaches are not satisfactory [7]. The fears of getting delayed and to reach the destination on time people risk their life and break the traffic rules. Breaking the traffic rules not only risks the life but also it leads to accidents and sometimes people have to pay their life too.

To reduce the time and complexity we need traffic light switching [8], traffic light switching is the dynamic signal lighting which is dependent upon the density and is mostly implemented with IR sensors but we are using TSOP sensor which will enable us to create the dynamic traffic light switching based upon the density of the vehicles.

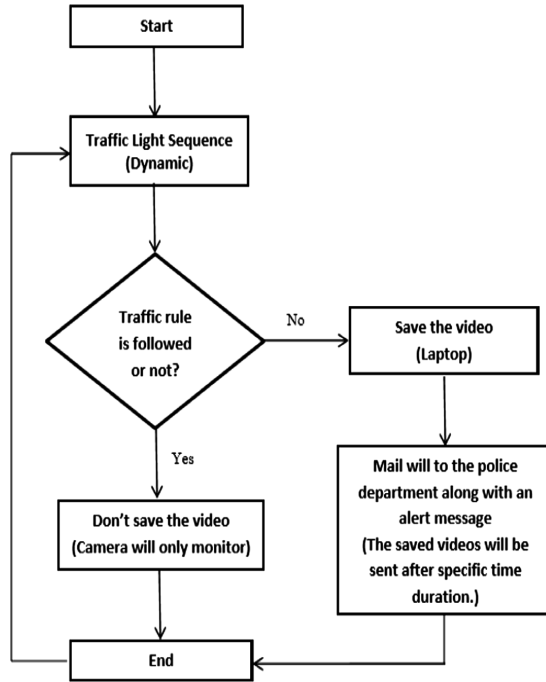
This project aims at developing a smart traffic control system which will help in making traffic rules disciplined for the people who do not follow the traffic rules. In case if someone breaks the traffic rule or if a vehicle is on the zebra crossing the video will be recorded and saved by the camera (laptop camera) and this stored video will be sent to the police department via mail. The police department will also be alerted via a message saying that the traffic rule has been broken kindly check the mail. For sending an alert message we have used a GSM900A module.

An alert message is sent to the police department using the GSM module. This execution is done using the ARDUINO ATmega2560 and is programmed using the ARDUINO IDE. The board is embedded with 16 digital input/output pins, 6 analog pins, a reset button, ROM is 32 kb; a 8 bit controller and a power jack. Tx and Rx are used for transmitting and receiving. Here we are using Rx for interfacing with GSM. The board requires 5 V of power and this power can be supplied to the board connecting a USB cable to the computer or with the help of a battery.

## 2 Methodology

The proposed system consist of dynamic traffic light control system, traffic rule violations are recorded by the camera and mailed to the police department and along with it an alert message is also sent so as to notify the police department if a rule has broken. In addition to this we have used Light Dependent Resistor (LDR) along with the LM358 IC OP-AMP for automated street lighting which is turned on and off automatically at night when it senses an object and will help in saving the natural resource. Figure 1 describes the block diagram of the system.

We have deployed the Thin Small Outline Packages (TSOP) sensors on the road so as to monitor the traffic density and instantly change another signal green if the density is low. TSOP sensor is also used at pedestrian incase if someone is crossing the road or not. This TSOP sensor is deployed at the zebra crossing which will help in detecting if the vehicles are standing on the pedestrian or not and if the vehicle is there it will be violation of the traffic rule as the pedestrians are meant for the people to cross the road safely.



**Fig. 1.** Block diagram of the system.

If the vehicle is standing on the zebra crossing and the signal is red or if someone is violating the traffic rule the video will be recorded by the camera and it will be sent to the police department along with the current date and time. Also, the police department will be notified via an alert message if the traffic rule has been violated. The alert message is triggered with the help of GSM module.

## 2.1 Arduino ATmega2560 Microcontroller

The ARDUINO ATmega2560 microcontroller has 14 digital input/output pins, 6 analog pins in addition to this it has a 16 MHz crystal, a 10k resistor, and two 18 to 22 picofarad (ceramic) capacitors. All the sensor pins are connected to the arduino board. The LED pins (traffic signal light) are also connected to the board which are controlled when to start and when to stop based upon the density of the vehicles in the lane. TSOP sensors re directly connected to the ARDUINO ATmega2560. Small PCB boards are also connected for common VCC and GND. The signal timing changes automatically with the density of the traffic and delay is provided with the help of microcontroller (Fig. 2).

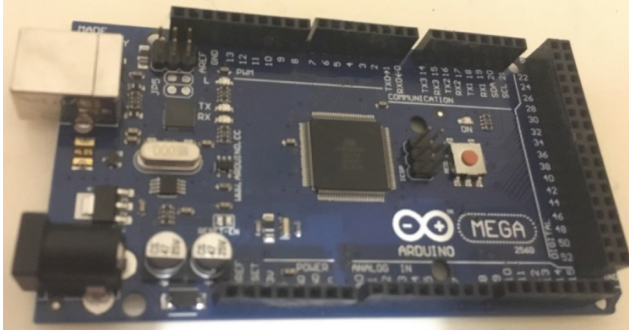


Fig. 2. Arduino ATmega2560.

### 2.2 TSOP Sensor

Sensors work in common anode way. It consists of IR LED and Photodiode IR LED continuously sends IR rays and photodiode receives the IR rays. Photodiode detects all the radiations of the light. So, in daytime IR sensor will not work accurately but in TSOP sensor, this wouldn't happen because it takes only the IR radiations and that too of particular frequency radiations. Thus TSOP sensor is used at the pedestrian, on the road to measure the density of the vehicle and is accordingly used for dynamic signaling in case if traffic is more or if there is less traffic. This will help in saving time and will help in reducing the traffic. When the traffic signal is red and the TSOP sensor detects a vehicle on the pedestrian, the ARDUINO ATmega2560 sends the command to the GSM module to send the message to the police department (Fig. 3).

### 2.3 LDR Sensor

The day and night mode can be identified by fixing a particular intensity value on LDR sensor and street light can be controlled [11]. LDR depends upon the intensity of the light and works accordingly based upon the intensity of the light falling on it.

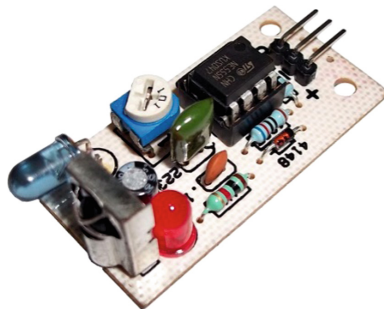
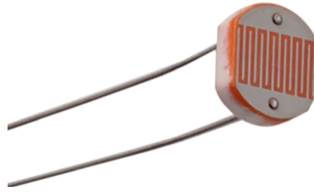


Fig. 3. TSOP sensor [12]

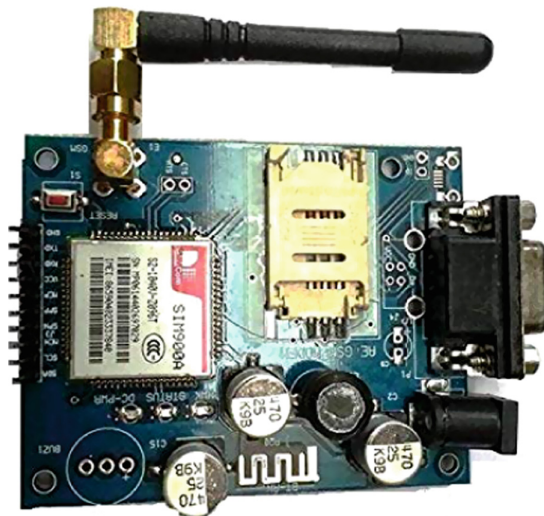


**Fig. 4.** LDR sensor [12]

We have used for automatic switching on and off the lights on the street so as to save the energy. Whenever an object is found at some distance the street light will be turned on automatically. With the help of LM358 which is an Op-Amp IC we have made a LDR circuit. This circuit is used for automatic switching on and off the lights on the street depending upon the intensity of the light as well as detecting the object (Fig. 4).

#### 2.4 GSM Module

The Global System for mobile communication (GSM) is a global standard and a widespread technology which enables us to connect to any mobile network over the globe. It makes the use of radio communication theory that depends upon the GSM frequency, transmitter power, height and gain of the antenna [9, 10]. GSM module can be interfaced with any microcontroller. This technology enables us to make calls and send messages over the network. To establish a connection we need a SIM and AT commands. It takes some time for the GSM to set the connectivity. Once the connectivity is set, a message will be sent at the starting stating that “Smart Traffic System



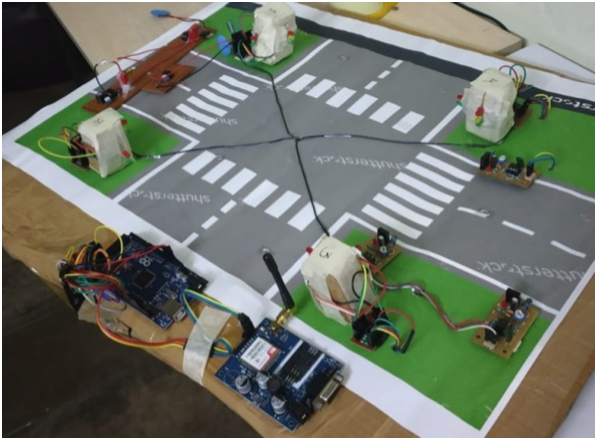
**Fig. 5.** GSM Module



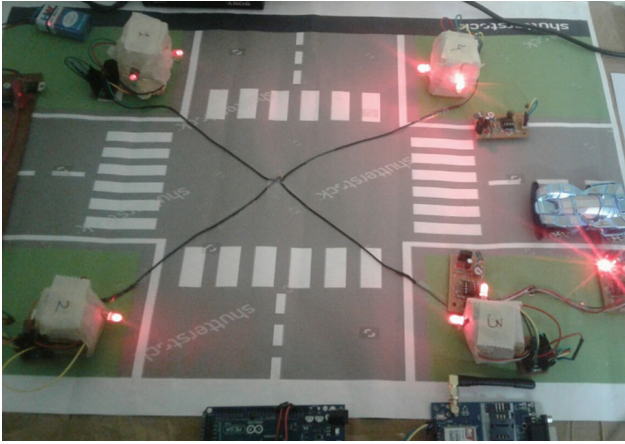
Power On: Check the mail at smartrafficnow@gmail.com”. As the traffic rule is broken the mail is sent to the police department in the meanwhile an alert message (SMS) is sent with the help of GSM module to alert the police department that a “Smart Traffic Signal Broken please check the mail” (Fig. 5).

### 3 Results and Discussions

The hardware implementation of the system is done with the help of microcontroller (Arduino Atmega), sensors, LED lights. As a result if someone violates the traffic rule video recording is saved and mailed to the police department, in the mean while an alert message is sent to the police department so as to notify them to check the mail when the traffic rule has been violated. TSOP sensor is used to check the density of the traffic and manage the traffic signal timings. It increases the signal timing if the density is high, it remains as it is if the traffic is moderate and if the traffic is low then it waits for a few seconds and changes to the signal in other direction. Also, the automated street lighting works based upon the intensity of the light and on the detection of an object which helps in saving the natural resource. Figure 6 shows the final setup of the system (Fig. 7).

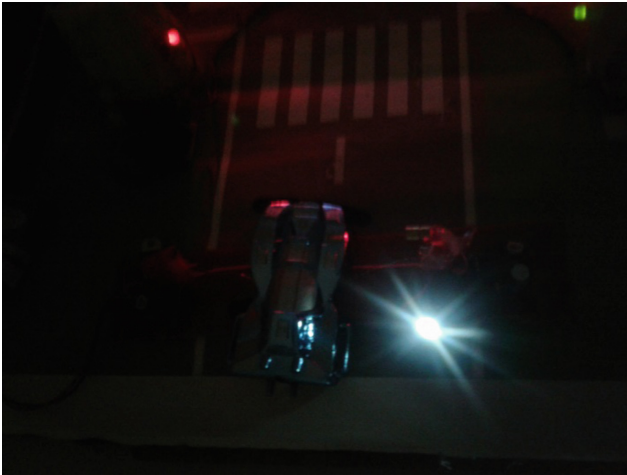


**Fig. 6.** Final setup



**Fig. 7.** Traffic density

The following Fig. 8 shows the automatic working of the street light at night when it detects an object. TSOP sensor is used along with the Op-Amp IC which enables the light to work at night automatically only when it detects an object.



**Fig. 8.** Automatic working of Street Light on detection of object.

Figure 9 shows the screenshot of the message sent to the police department to alert the police to check the mail when the traffic rule has been violated.

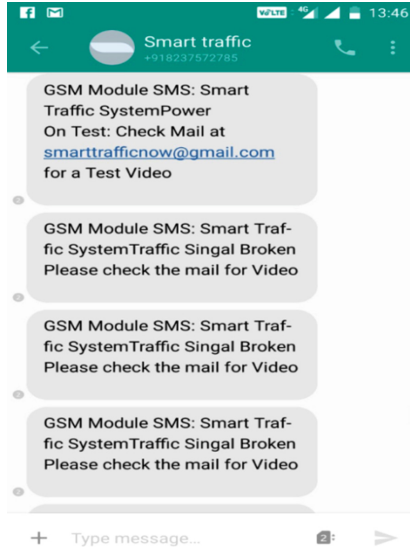


Fig. 9. Alert message (SMS) sent by GSM Module.

We have used Matlab for the video processing. Matlab is used to save the video and once the video is saved it is sent by the mail to police department ([smarttrafficnow@gmail.com](mailto:smarttrafficnow@gmail.com)). It has small resolution and this small resolution is fast to capture an image and is fast to send it. When the mail is sent over the network it uses SMTP. We select the camera (laptop) and the resolution. The selected camera is chosen as the source and is set in burst mode. We have the image color as RGB (Red, Blue, Green). Once the traffic rule is broken the camera starts taking the images in the background

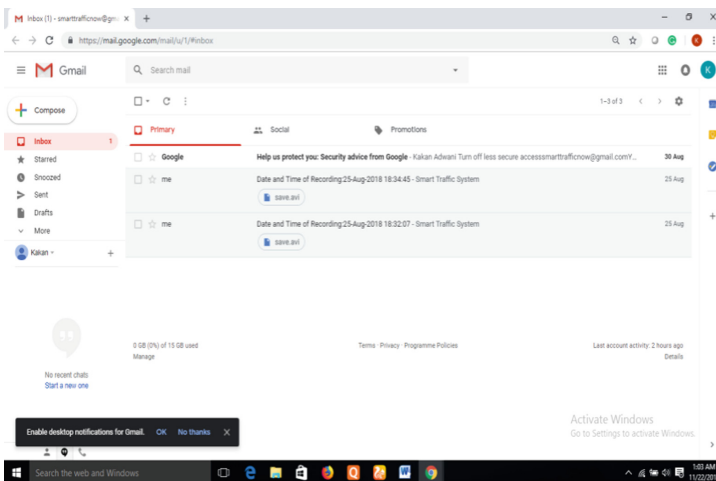


Fig. 10. Email received by the police department

and these images are captured into frames. Now these frames are converted into a movie frame and this frame is added into the AVI file. After the AVI file is ready it sent via the mail to the police department (smarrtraffic@gmail.com) along with the video the date and time is also sent.

Figures 10 and 11 show the email sent to the police department which consists of the video (when the traffic rule is violated) along with the current date and time. The Fig. 11 shows the screenshot of the email received at smarrtrafficnow@gmail.com which consists of the video (of the person who violated the traffic rule) in the form of avi file.

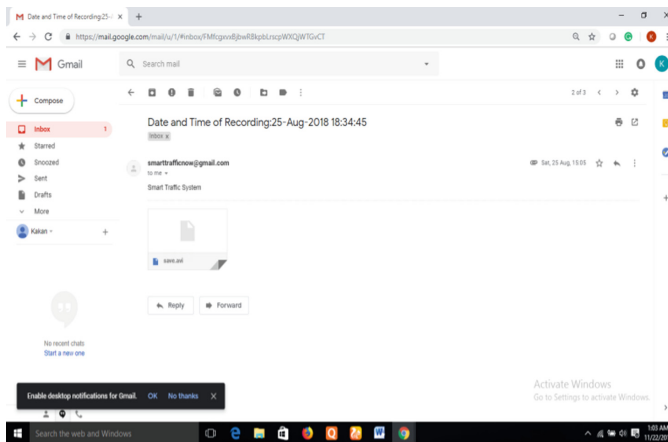


Fig. 11. Email consisting of the video in the form of avi file

## 4 Conclusion

This system helps in making the people follow the rule. In case if someone violates the traffic rule (i.e. breaking the traffic signal or the vehicle is on pedestrian) the video will be recorded and mailed to the police department and the police will be notified to check the mail via an alert SMS (with the help of GSM Module). The person who will break the rule will be punished according to the law. All the connections are made to the Arduino AtMega board which runs the program successfully. Also, we have developed dynamic traffic lighting which is based upon the density of vehicle which helps in saving time of the people in traffic. This system reduces the time of waiting in traffic jam and can help in reducing the accidents and making the people to follow the traffic rules in discipline. The proposed work is mainly considered to reduce the waiting time at the traffic and to make the people follow the traffic rules so as to avoid accidents. The future enhancement could be done by using surveillance camera for recording the video and sending it to the police department.

## References

1. Surya, S., Rakesh, N.: Traffic congestion prediction and intelligent signalling based on Markov decision process and reinforcement learning. In: Guru, D., Vasudev, T., Chethan, H., Kumar, Y. (eds.) Proceedings of International Conference on Cognition and Recognition. Lecture Notes in Networks and Systems, vol. 14. Springer, Singapore (2018)
2. Ramaprasad, S.S., Sunil Kumar, K.N.: Intelligent traffic control system using GSM technology. In: 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai (2017)
3. Ghazal, B., Khatib, K., Chahine, K., Kherfan, M.: Smart traffic light control system. In: 2016 Third International Conference on Electrical, Electronics, Computer Engineering and Their Applications (EECEA) (2016)
4. Chattaraj, A., Bansal, S.A.N., Chandra, A.: An intelligent traffic control system using RFID. *IEEE Potentials* **23**, 40–43 (2009)
5. Poyen, C.E.F., Bhakta, A., Manohar, B.D., Ali, I., Arghya, S., Rao, A.P.: Density based traffic control. *Int. J. Adv. Eng. Manag. Sci.* **2**, 1379–1384 (2016)
6. Halladmani, S., Radha, R.C.: Development of closed loop traffic control system using image processing. In: International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai (2017)
7. Liang, X., Fu, J., Yan, M.: Highway traffic density control based on the composite of CACMAC and PID Controller, 2657-2661. <https://doi.org/10.1109/cac.2017.8243225> (2017)
8. Jagadeesh, Y.M., Suba, G.M., Karthik, S., Yokesh, K.: Smart autonomous traffic light switching by traffic density measurement through sensors. In: International Conference on Computers, Communications, and Systems (ICCCS), Kanyakumari (2015)
9. Suryanarayanan, S., Rakesh, N.: Emergency human collapse detection and tracking system. In: International Conference On Smart Technologies For Smart Nation (SmartTechCon) (2017)
10. Rakesh, N., Nalineswari, D.: Comprehensive performance analysis of path loss models on GSM 940 MHz and IEEE 802.16 WIMAX frequency 3.5 GHz on different terrains. In: 2015 International Conference on Computer Communication and Informatics (ICCCI) (2015)
11. Saifuzzaman, M., Moon, N.N., Nur, F.N.: IoT based street lighting and traffic management system. In: IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka (2017)
12. Google images. <https://images.google.com/>



# An Investigation of Hyper Heuristic Frameworks

Rashmi Amardeep<sup>1</sup>(✉) and K. ThippeSwamy<sup>2</sup>

<sup>1</sup> Sri Siddhartha Academy of Higher Education, Tumkur, India  
rashmiamardeep@gmail.com

<sup>2</sup> Visvesvaraya Technological University, PG Regional Center Mysore,  
Mysore, India

**Abstract.** This article presents an emerging methodology in research and optimization called hype heuristics. The new approach will increase the extent of generality within which the optimization systems operate. Compared to heuristics (Meta) technology that works in a particular class of problems, hyper heuristics leads to general systems that manage extensive variety of issue area. Hype heuristics make an intelligent choice of the correct heuristic algorithm in a given situation. The article analyzes the absolute most recent works distributed in different fields.

**Keywords:** Hyper-heuristic · Meta-heuristic · Optimization search

## 1 Introduction

In the last decades, meta-heuristics has played a vital role in many different areas, such as data mining, machine learning, bioinformatics, imaging and many others. The meta-heuristics are specific to problems, simple, easy to implement and profitable and require a lot of knowledge to solve optimization problems. Throughout the following couple of years there will be an expansion in the dimension of sweeping statement in which meta-heuristic and optimization systems can work. The new research strategy is to work in a progression of related issues as opposed to in a thin class of issues.

Hyper Heuristics (HH) is a developing research innovation that is to a great extent inspired by the objective of expanding the dimension of all inclusive statement to which improvement in the optimization systems can work. The term has been characterized to portray comprehensively the way toward utilizing heuristics (Meta) to pick the heuristic (Meta) and to take care of the issue being referred to. The reports examine the utilization of these ways to deal with the issue.

The main motivation in the research community for the development of HH is that it is heuristics independent from the domain. Another inspiration for the advancement of HH originates from the way that singular heuristics can be especially powerful at specific phases of the arrangement procedure (i.e., when certain regions of the solution space are investigated) while poor execution on others stages. Along these lines, it is reasonable for expect that distinctive heuristics consolidated in a suitable way can deliver better arrangements whenever connected independently. Recent work in the field of machine learning approaches is to shrewdly choose heuristics dependent on the

present circumstance [2, 3]. There is extensive degree for hybridizing meta-heuristics with machine learning approaches for insightful heuristic selection [3].

Cowling et al. described HH [1] as follows: “Hyper Heuristics manages the choice of which lower-level heuristic method should be applied at any time, depending on the characteristics of the heuristic and the region of the solution space currently being explored”.

## 2 Concept of Hyper-Heuristics

Figure 1 shows the HH framework. HH knows how it will be called LHH. The results generated by the ‘n’ LHH obtained by execution of the evaluation function are passed to the solution space as decided by HH.

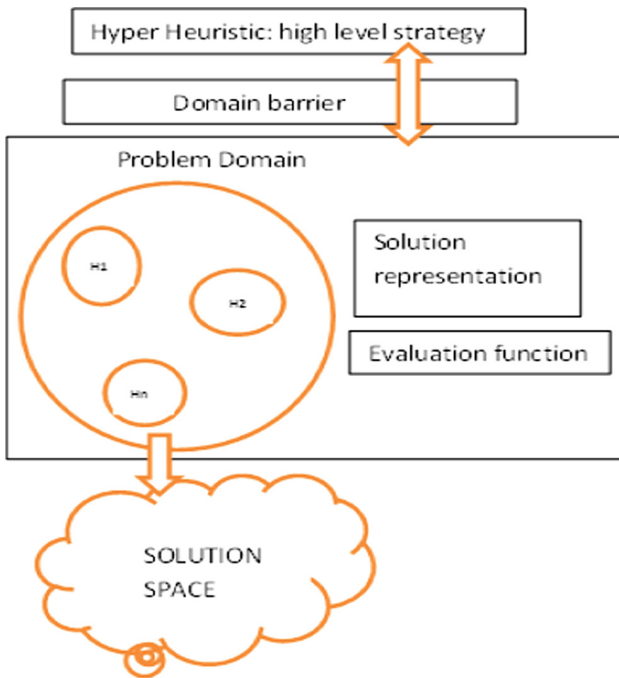


Fig. 1. Hyper-Heuristic framework

Hyper-Heuristic communicates with low-level heuristics via a standard interface. The thought is that HH calls any LLH that perform well to a specific arrangement. The Hyper Heuristics would then be able to choose which heuristic (or set of heuristics) ought to permit to refresh the arrangement in solution space.

The selection of which LLH to be called is decided by HH in one of the following ways:

Should it call the heuristics that led to the maximum improvement in the evaluation function?

Should it call the fastest heuristics?

Should it call the heuristics that has not been called for the longest period of time?

The internal state of Hyper Heuristics is a question for the designer, as is the process of deciding which heuristics to call after, but once there is adequate Hyper Heuristics, the hope is that it functions reasonably well in a wide range of problems and not just for the one originally implemented.

There is rapid development as Hyper Heuristics operates at a higher level of abstraction than a meta-heuristic approach. The approach begins to resolve the problem once it gets the evaluation function and the low-level heuristics from the user.

### 3 Classification Methods on HH

The Hyper Heuristics designer is to be thus ingenious and work within the limits. The Hyper Heuristics algorithm provides a different way to incorporate multiple heuristic algorithms into a one search algorithm.

The aim of HH is to supply solutions of acceptable quality at intervals in an inexpensive time. There's a good vary of recent heuristics illustrious within the literature that are specifically designed and tailored to resolve certain types of optimization issues. Below is a summary of HH applied in many decision and optimization problems that arise in the field of computer science in automatic planning systems, etc.

The DART logistics planning system [4] used in the Gulf War artificial intelligence surveys over the past 30 years. Minton's PRODIGY system [5], which uses explanatory learning to know what action, is best applied at every point of decision

The LR-26 programmer in the COMPOSER system [6] used to plan satellite communication programs involving several Earth orbit satellites and three earth stations. The issues concerned are nothing but trivial. For example, some satellites have to communicate several times a day with a ground station, with a predetermined maximum interval for message exchange, and yet the orbits of the satellites limit the windows of communication and the desire of earth stations.

Another example of applying a Hyper Heuristics approach [7], the problem is to gather and deliver live chickens from farms across Scotland and in the north of England to one of the two processing plants to meet all orders of supermarkets and different retailers. Client orders modification weekly and typically each day. The task was to set up the work done by a series of "capture teams" touring the country in minibuses and a series of trucks transporting from every park to industrial plant chickens. The main objective was to keep the work in the factories without the need for live chickens to wait too long in the industrial plant yard, vet and legal grounds. This has been sophisticated by several uncommon restrictions.



Hyper Heuristics a different kind of approach to tackling problem solving large-scale university exams [8]. There are a series of fixed time intervals in which the test can be done, and rooms of different dimensions. Any candidate appearing for two exams should not be scheduled at the same time. There has to be time intervals for some of the tests. Certain trigger actions may not be available and these can be violated if it is a soft constraint (Table 1).

**Table 1.** Study of classification methods based on HH

Sl. no.	Author	Data sets	Problem description	Result
1	Mitra Montazeri1 et al. [9]	Lung cancer dataset with 57 attributes and 32 patient records	The low-level hyper-heuristic approach (LLH) is a set of local search methods. Local search is a neighborhood search algorithm. GA chooses an LLH. In these LLH a different emphasis on probability is used, i.e. random probability, equal probability and probability of mutation in GA	An correct result of 80.63% using a 11 functions for HH in comparison to 5 Machine Learning Gain Ratio Algorithm, Major Components Algorithm, Relief Algorithm, Symmetric Deviation algorithm, Chi-square Algorithm is 60.94, 57.81, 68.75, 60.94 and 68.75
2	Limin Han, Graham Kendall [10]	Personnel scheduling to allocate 25 training staff to 10 training centers at 60 time slots	Tabu method assisted by hyper-GA was an improvement over computational time. The goal was to maximize the total priority of the courses taught during the period, minimizing the duration of the trip for each instructor	Comparison of hyper-GA with the HH-choice function led the hyper-TGA driven operator to obtain preferred outcomes over different forms of hyper GA

(continued)

**Table 1.** (continued)

Sl. no.	Author	Data sets	Problem description	Result
3	Graham Kendall and Mazlan Mohamad (2004) [11]	The channel assignment problem of networks sizes (21, 25 and 55) with different compatibility matrix, and traffic demand	Assigning channels considering the problem of the minimum interval (MS-CAP). They designed four simple local search methods of 2 options in low-level heuristics (LLH). The initial arrangement is produced utilizing an arbitrary helpful heuristic. This arrangement is then enhanced utilizing a hyper-specialized technique, the great deluge algorithm	The proposed algorithm has achieved promising results for all benchmark problems, although they have not been able to produce better quality solutions than earlier work of standard problems. However, the results have shown fair execution times
4	Chun-Wei Tsai, Hwei-Jyun Song, and Ming-Chao Chiang (2012) [12]	Considering the datasets from UCI performances of these algorithms are evaluated	Low-level heuristic algorithms considered are K-means, Tabu search, simulated annealing and genetic algorithm. The HH algorithm (HHCAD) first selects randomly from LLH. The selected algorithm was executed to group the data set and as an initial solution. HHCAD exits the loop after setting the number of iterations	The results of the proposed algorithm demonstrate that it can give a superior outcome than the other heuristic calculations as far as SSE

(continued)

**Table 1.** (continued)

Sl. no.	Author	Data sets	Problem description	Result
5	Sabihe Kabirzadeh, Dadmehr Rahbari, Mohsen Nickray [13]	Fog computing for planning and designating resources between fog nodes with the objective of maximizing the utilization of network resource's	The HH algorithm for the workflow planning problem in the fog processing environment using a test and selection rule. The designed algorithms in terms of average energy consumption, the utilization of the network are performance measures. The HH algorithm includes Genetic Algorithm, Particle Swarm Optimization Algorithm, Colony Optimization Algorithm and Simulated Cancellation Algorithm	The algorithm as far as average energy consumption 69.34% of the SA algorithm, 71.03% of the ACO algorithm and 69.60% of the PSO algorithm [13] Moreover, the average cost, in comparison with SA algorithm, is 58.84%, that of PSO algorithm is 59.39% and the ACO algorithm is a 60.65% improvement

## 4 Conclusions

The study reveals that hyper-heuristic, the state of the art, will assume an imperative job in research technology in the coming years. The hyper-heuristic structure finds development thanks to its general approach towards optimization, for large areas of application. The motivation to investigate the hyper-heuristic approach to traditional approaches adapted to problems is its re-applicability and robustness in different problem domains. The study shows that there is a potentially important direction in this field of research, as it satisfies an extensive variety of problems and is a more demanding task. Recent research till date gives just some encouraging beginning strides toward this path.

## References

1. Cowling, P.I., Kendall, G., Soubeiga, E.: A hyperheuristic approach to scheduling a sales summit. In: Selected Papers of Proceedings of the Third International Conference on International Conference on the Practice and Theory of Automated Timetabling. LNCS, vol. 2079, pp. 176–190. Springer, Heidelberg (2001)
2. Burke, E.K., MacCarthy, B.L., Petrovic, S., Qu, R.: Knowledge discovery in a hyperheuristic for course timetabling using case based reasoning. In: Proceedings of the Fourth International Conference on the Practice and Theory of Automated Timetabling (PATAT 2002), Ghent, Belgium, August 2002
3. Petrovic, S., Qu, R.: Case-based reasoning as a heuristic selector in a hyper-heuristic for course timetabling. In: Proceedings of the Sixth International Conference on Knowledge-Based Intelligent Information & Engineering Systems (KES 2002), Crema, Italy, September 2002
4. Cross, S.E., Walker, E.: Dart: applying knowledge-based planning and scheduling to crisis action planning. In: Zweben, M., Fox, M.S. (eds.) Intelligent Scheduling. Morgan Kaufmann, San Mateo (1994)
5. Minton, S.: Learning Search Control Knowledge: An Explanation-Based Approach. Kluwer, Boston (1988)
6. Gratch, J., Chein, S., de Jong, G.: Learning search control knowledge for deep space network scheduling. In: Proceedings of the Tenth International Conference on Machine Learning, pp. 135–142 (1993)
7. Hart, E., Ross, P.M., Nelson, J.: Solving a real-world problem using an evolving heuristically driven schedule builder. *Evol. Comput.* **6**(1), 61–80 (1998)
8. Terashima-Marín, H., Ross, P.M., Valenzuela-Rendón, M.: Evolution of constraint satisfaction strategies in examination timetabling. In: Banzhaf, W., et al. (eds.) Proceedings of the GECCO 1999 Genetic and Evolutionary Computation Conference, pp. 635–642. Morgan Kaufmann, San Mateo (1999)
9. Montazeri, M., Baghshah, M.S., Enhesari, A.: Hyper-Heuristic Algorithm for Finding Efficient Features in Diagnose of Lung Cancer Disease. <https://arxiv.org/pdf/1512.04652>
10. Han, L., Kendall, G.: An investigation of a tabu assisted hyper-heuristic genetic algorithm. In: IEEE 2003 Conference (2003)
11. Kendall, G., Mohamad, M.: Channel assignment in cellular communication using a great deluge hyper-heuristic. In: IEEE 2004 International Conference (2004)
12. Tsai, C.-W., Song, H.-J., Chiang, M.-C.: A hyper-heuristic clustering algorithm. In: IEEE International Conference on Systems, Man, and Cybernetics, COEX, Seoul, Korea (2012)
13. Kabirzadeh, S., Rahbari, D., Nickray, M.: A hyper heuristic algorithm for scheduling of fog networks. In: Proceeding of the 21st Conference of Fruct Association



# Detection of DDoS Attack Using SDN in IoT: A Survey

P. J. Beslin Pajila<sup>1</sup>(✉) and E. Golden Julie<sup>2</sup>

<sup>1</sup> Department of Computer Science and Engineering,  
Francis Xavier Engineering College, Tirunelveli, India  
beslin.kits@gmail.com

<sup>2</sup> Department of Computer Science and Engineering,  
Regional Campus, Anna University, Tirunelveli, India

**Abstract.** IOT: Internet of Things is a developing technique, it is the system of vehicles, home apparatuses, physical gadgets, and different things installed with hardware, programming, sensors, actuators, and system availability which empower these items to associate and trade data. IOT is made out of vast number of various end frameworks associated with web. Physical gadgets installed with RFID, sensor, etc. which enables item to communicate with one another. Security is a serious issue because all the heterogeneous end systems are communicated with each other through internet.

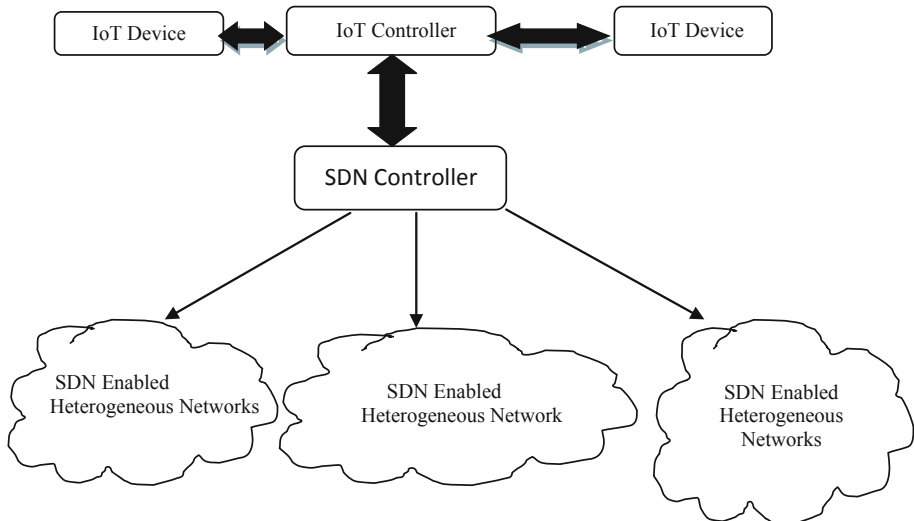
**Keywords:** RFID · Internet of Things IoT · DDoS · Security · DDoS attack · SDN

## 1 Introduction

The Internet of Things (IoT) is where physical articles can be associated with the Internet and furthermore have the capacity to recognize themselves to different gadgets [1]. IoT gadgets are firmly related to RFID, sensor innovations, remote advances. It makes the items to be detected and controlled remotely crosswise over existing system framework. Web is a medium that interface individuals over the world for messaging, gaming, conferencing, web based exchanging, etc. [2]. The universal things are apportioned with the capacity of solid data transmission, far reaching observation, and smart preparing. Here intelligent is consider as a significant feature. The intelligent IoT make it possible for distributed intelligent devices like sensors, actuators and data centers. The intelligent gadgets will go about as a smart information procurement, propelled data extraction, self-versatile control, dependable transmission, and clever choice help and administrations. The savvy IoT depend on the framework models, systems and correspondences, information preparing and omnipresent processing advances. Numerous applications administrations are expected to help smart administration and different business-related exercises, including blurring processing, enormous information, semantic web, learning coordination, and social registering [49]. IoT contains, for example, switching off the lights and automatic air conditioner in a room, which recognizes the availability of the person by sensing the temperature of the human. Internet of things moves the data over the web without individual conversation.

Traditional IP is not capable to connect various number of devices linked to the web, IPv6 is the right choice but it does not provide heterogeneity objects connectivity. SDN use IPv6 that allow various items from various systems to communicate [18]. Dos attack is one of the most intrusion that affect the end devices.

IOT gadgets are brilliant, the data are send to the brought together framework, which will screen and make a move as indicated by the undertaking given to it. IOT can be utilized in numerous areas like transportation, human services, savvy home, control matrices, shrewd structures etc. [13, 14]. Huge measure of gadgets connected to the web and huge information related with it, security is particularly concerned [3]. Most of the gadgets are effectively focused by interruption since they rely upon outside assets and are left unaddressed much of the time. Online apparatuses are effectively assault by the interruption. Two hundred million gadgets will be associated with the web constantly 2020, so there is a likelihood for programmers to utilize these gadgets through DOS attack, pernicious email and Trojan. An ongoing report expresses that 70% of Internet of the things gadgets is helpless against assaults. The secrecy, honesty and security of the information will be diminished and the clients will dishearten to utilize this innovation [4]. The security and protection issues in the cutting edge 5G versatile advances on IoT were unaddressed for quite a long time [5]. An IoT arrange is constrained by legitimately brought together controller and partitioned into zones. It is vital to consider the execution of disseminated SDN empowered IoT systems. to keep up administration quality. The normal design of joining of SDN and IoT is shown in Fig. 1 [64].



**Fig. 1.** Classical architecture that combine SDN and IoT, a high level view.

Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP) and Bluetooth Low Energy (BLE) are the communication protocols that are

used for the converse between the IoT devices. In this paper, we made a survey about the DDoS attacks and how to identify and reduce the attacks using Software Defined Networks.

## 2 Background

### 2.1 Distributed Denial-of-Service (DDoS) Attacks

The goal of the DDoS is to minimize or even crash and shut down, there by it deny the service or the legitimate users from the multiple compromised sources. Mostly the target of the DDoS attacks are a server, website or other network resource, it cause denial of service for users of the targeted sources. For launching large number of DDoS attack botnets are used, because compromised hosts (zombie) are available. Prevention against DDoS attack is the major concept to make our sources to get rid of DDoS attack. If the DDoS attack is not prevented and it will be detected and mitigated DDoS will flood the organization's servers with fake demand and deny the demand from authentic user [17] (Tables 1 and 2).

**Table 1.** Classification of DDoS attacks

1. Reflection-based flooding attacks	
Smurf Attack [26]	Smurf attack is a DDoS attack, huge ICMP parcels with the injured individual's fake source IP to a PC network. This cause illegitimate traffic on the network
Fraggle Attack [26]	Fraggle assault is same as smurf assault, yet it utilizes unapproved UDP traffic rather than ICMP traffic
Ping Flood	In a Ping Flood, attackers adopt "ping" which is a alternative of an ICMP and send IMCP echo requests (packets) at a very high rate and from random source IP ranges. Attackers can use all available network resources and bandwidth until the network goes offline. A PING attack is difficult to detect by deep packet inspection or other detection techniques
2. Protocol using flooding attacks	
SYN Flooding attack [26]	In TCP SYN Flood assault, the assailant sends SYN packets ceaselessly to each port on the focused on server, by utilizing a phony IP address. The server, not mindful of the attack, gets various, clearly real demands to build up communication
UDP Fragmentation attack [27]	In a UDP Fragmentation assault, assailants send enormous UDP parcels (1500+ bytes) to utilize more transfer speed with less packets
Slow Read Attack	This technique delay time to read the Web server response, even an attacker sends a legitimate HTTP request
3. Reflection and amplification based flooding attacks	
DNS amplification Flooding attack [28]	In Domain name System (DNS) intensification flooding assault, the zombies make little DNS questions with fake source IP address that makes tremendous system traffic coordinated toward the person in question
NTP amplification Flooding attack [29]	Network Time Protocol (NTP) enhancement Flooding assault is same as DNS intensification Flooding assault, yet it utilizes NTP servers in the interest of DNS servers

**Table 2.** Recent Popular DDoS attacks

Target	Description
Russian Defense Ministry's website, March 2018 [25]	DDoS attack targeted Russian Defense Ministry's website while they are polling for new weapons names
Boston Globe, November 2017 [24]	DDoS interrupt the news paper's telephone, disrupted editing system
UK National Lottery, September 2017 [24]	DDoS attack hitting vigorously lottery website and app, and prevent the customers laying lottery
Melbourne IT, April 2017 [24]	DDoS attack force the victim organization that their cloud hosting and mailing platforms service is unavailable for the customers
Client of US-based security vendor Sucuri. June 2016 [19]	Botnet produced to bargain CCTV-based botnet utilized for DDoS assaults. The botnet created 50,000 HTTP ask for every seconds to the server and the memory was involved by ill-conceived traffic
Bank of Greece Website [20]. May 2016	DDoS assault constrained the servers of Bank of Greece site to stay inert for 6 h
HSBC internet banking [21]. January 2016	DDoS assault constrained HSBC individual keeping money site in the UK to closedown for a long time
Irish government website [22], January 2016	Irish sites like Central Statistics office, the Courts Service, the Health Service Executive and Houses of the Oireachtas were briefly constrained disconnected by DDoS Attack
Thai government websites [23], October 2015	Thai government websites harmed by a DDoS attack, making them impossible to access

## 2.2 Software Defined Network

Secure communications network have some basic properties they are: integrity, confidentiality, availability of information, authentication and non-reputation. The most prominent technologies to deliver as key enablers for the IoT networks is Software Defined Network and Network Virtualization. Splitting of control Plane from the Data Plane is the main opinion in the background of SDN. To protect the network from malicious attack or unintentional damage, the information, the system resources and the conversation transaction should be protected by security professionals. SDN was introduced by the Clean Sate Research Group of Stanford University, originated in the Ethane project. SDN is a Network design Separate information plane and the control plane and make the programming straightforwardly on the control plane. SDN has a sensibly concentrated and programmable control plane. SDN have controllability and adaptability [48]. The Data plane and control Plane are autonomous in nature. At the point when Data Plane gets new parcels and it doesn't have enough information to deal with it. Data Plane asks the control Plane to make stream rules and the Control Plane reaction to the Data plane with the flow rules. Here Dos Attack happens when the Data Plane send more request to the Control Plane that makes hard to handle(control plane resource consumption) and also it happens when control plane generate more flow rules



unnecessarily due to the request of Data Plane and send to Data Plane (data lane resource consumption). There won't be any space to store all flow rules generated by Control Plane [13]. In [14] firewall prototype was developed for security purpose that maximizes the use of SDN. It is mainly used for two reasons: (i) New devices can be developed with the product quality, (ii) it allows end user flexibility when creating new devices. SDN is the latest technology that basically focused on quality of service and routing. The Concept behind the filtering is, it makes all the data to pass through the firewall due to the source and Destination IP addresses, set of rules, IP protocols (TCP or UDP) it allow or deny the data's. Basic algorithm is followed that sees all the incoming traffic, read the packet header information, check the rule list for matches and finally due to the set of rules allow or deny the packets. Network management, network function Virtualization; Accessing information from anywhere, Resource utilization, Energy management and Security and privacy are the essential key of IoT applications, which can fulfill by SDN technologies. Huge data that was originated from the gadgets must be handled in timely manner. Network Function Virtualization (NFC) that makes gadgets to perform various operations, depending on application specific requirement [34]. SDN is an emerging Technology, that is relevant to change the traffic arrangement, it has huge bandwidth, changing nature of today's application. Security is the essential feature of SDN, and it is mainly used to detect the attacks. The principal segments of SDN are controllers and switches. Controller will manage the entire network and the switches will forward the system traffic depend upon the data installed in the SDN controller. SDN understand clearly the flexible control of network traffic. SD comprises of Software defined ratio, Software defined networking, Software defined data centers, Software defined infrastructure and Software define World. Among all those technologies, SDN is the recognized technology to the greatest extent [46]. SDN is used to improve the new 5G wireless networks technology in its manageability and adaptability [47]. SDN have ability to program the system through a consistently programming characterized controller and it isolates the control path from the information plane. Stretching out SDN to remote systems is profitable [48]. The typical architecture of SDN is shown in the Fig. 2. By designing hybrid network architecture; SDN brings new opportunities in IoT. Utilizing bound together control convention SDN can possibly control circuit and parcel exchanging [64].

### 2.3 Characteristics of IoT

Low-control radios are utilized for the association of web, to limit the effect of such gadgets on nature and vitality utilization. WiFi, or entrenched cell arrange innovations are not utilized by such Low-control radios. IoT need higher-request figuring gadgets to perform heavier obligation assignments, it isn't just made out of inserted gadgets and sensors. Little gadget structure factor required for sensors, which restrains their preparing, memory, and correspondence limit [11].

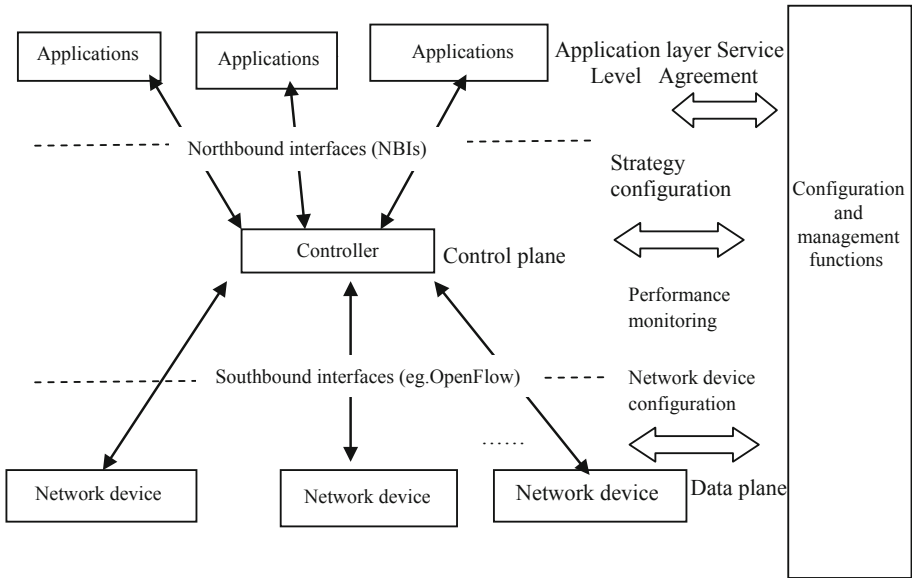


Fig. 2. A typical architecture of SDN

### 3 SDN Based Detection Techniques

#### 3.1 Machine Learning

Developing an automatic defense against DDoS attacks using machine Learning Techniques. Artificial Neural Networks algorithm is used to detect the anomaly. At the beginning System monitors the network traffic, to find whether the network is under intrusion or not. If it so actions will be taken to defence. Artificial Neural Network algorithm is used, it mimics the human brain. It is trained by giving the normal and malicious operations as inputs. It is also trained dynamically. The algorithm is split into two parts, first part is the training given to the algorithm with the given set of data and the second part is nothing but the evaluation of the result of the algorithm. Multiple ANN algorithms can be used for training the dataset because all the data are collected from different levels [15].

Filtering rules is used to filter the network traffic. After filtering the attack was detected and drops the attack packet. The filtered packets are stored in the database. The features like packet rate, protocol type etc. will be extracted, to speed up the training process the features are normalized. Machine learning algorithms like ANN is used to train the training data. Each packet is arranged as DDoS attack or authorized one. Once the DDoS packets are detected, the filtering rules will be updated. Deep Defense approach is relevant to Recurrent Neural Network (RNN) to identify DDoS attack. Dramatic rise in speech reorganization, language translation, speech synthesis etc. can be achieved by RNN. It is independent from input window size [16].

In [30] Unified Network Threat Management System (UNTMS) is constructed and installed at each site. It monitors the actual time traffic and filters the malicious traffic. The DDoS attack detection module analyzes the system traffic, identify the malignant traffic and generate signature for the malignant traffic. It follows four phases for the detection of DDoS attack i.e., Data collection, preprocessing, Classification and Response. RBP Boost is a classification algorithm used to classify, train and test the malicious traffic. RBP Boost division algorithm outcome with a high reveal accuracy of 99.4%.

DDoS attacks are detected using by Self-organizing map a neural network model. In this work six tuple (traffic flow features) are used to make decision, whether the traffic is ordinary or an intrusion. The appearances are Average of Packets per flow (APf), Average of Bytes per flow (ABf), Average of Duration per flow (ADf), Percentage of Pair-flows (PPf), Growth of Single-flows (GSf), Growth of Different Ports (GDP). Flow Collector module in a NOX based network is responsible for collecting the features and for the detection of illegitimate flows the collected features are moved to the classifier module. SOM will classify the network traffic and are useful for stream analysis. This task used for DDoS attack identification with huge rate, based on traffic flow features and less rate of fake alarms. This work does not mention about mitigation strategy and proposes about DDoS attack detection method [31].

Dotcenko et al. [32] proposed mamdani algorithm, fuzzy inference was carried out. This is a pragmatic approach based on fuzzy logic, fuzzy modeling problems are solved. Excessive computation was avoided. Decision making based on fuzzy rules was the results that were showed and it was better than using the security algorithms separately. Only the detection method has been proposed and no mitigation strategy.

Xin Xu et al. [33] Hidden Markov Models (HMMs) was proposed by the authors to detect the DDoS attacks. HMM method detect the DDoS attacks by origin IP invigilator in a single identification system. To take care of the issues of information preparing bottleneck and single point disappointment various identification operators are utilized in real applications. Hence the dispersed location system is consolidated with the HMM-based discovery technique utilizing source IP observing. Reinforcement learning (RL) is a machine learning strategy that takes care of consecutive choice issues by associating with nature. Reinforcing learning is more productive and appropriate than supervised learning in light of the fact that amid preparing RL agents don't have instructors' signs for watched states, they for the most part gets postponed, prizes or inputs from environment.

Dillon [35] Proposed DDOS mitigation method, detection and blocking of attacks was handled under the assist of OpenFlow. The complete mitigation process is done three stages. In the first stage, the abnormality is detected with the byte and packet counter. The second phase, two method were used, the first method is Packet symmetry, it is used to characterize legitimate and malignant traffic. The second stage is temporary blocking, it blocks the outgoing traffic. In the third stage, all the flows are dropped that are coming from malicious.

Machine learning procedures are utilized to recognize the vindictive action dependent on the strange behaviour that occurs in the system. The accomplishment of this strategy relies on the dataset, which has been utilized for training.

## 3.2 Traffic Analysis

[36] TAMD, a system that find host that was infected by stealthy malware that was available inside a network. By two ways malware writers avoid the detected techniques of TAMD, (i) they encrypt their malware traffic (ii) avoid by botnet architecture. The majority of the botnet today utilize unified IRC direction and-control server instead of P2P botnets and HTTP based botnets. An OpenFlow security application development framework, FRESCO was designed [37]. Another identification structure Botminar, distinguish the hosts that share comparable interchanges and malicious action designs by performing cross group correlations. This novel inconsistency based botnet recognition framework is free of the protocol and structure utilized by botnets. The framework achieve definition and properties of botnets i.e., bots inside the equivalent botnet have a similar communication malicious activity [38]. Malware in the mobile devices is detected using SDN architecture [39]. It detects the malware in the mobile devices through real-time traffic analysis. To extract the aggregation of malware communications features like, common destination, common connection time and common platforms are used.

## 3.3 Connection Oriented

### 3.3.1 Number of Connections

[40] POX Controller that was implemented on the SDN Controller that makes a secure communication between the server and DDoS Blocking applications that runs on a SDN controller. This was carried out mainly to protect the services against DDoS attacks. Because mostly DDoS attack will attack the services not the network components like switches, routers, links etc. [41] the Security of the host in the home networks was compromised, that host is used for many malicious activities without the user's knowledge. SDN provide the opportunity to detect the malicious activities. NOX Controller was implemented on the SDN Context for the detection of anomaly [32]. The identification algorithm connected with the basic leadership dependent on fluffy standards that is greatly improved than the security algorithm. Modules of the protected SDN includes processing modules, statistic collection and decision making, these have been implemented as applications for the Beacon controller [39]. By identifying the suspicious network, our system detects malware in the mobile devices. It analyzes the behavior of mobile malware and architecture and implements a malware identification system using SDN. Flood Light controller embeds our detection algorithm as independent modules.

### 3.3.2 Connection Rate

TRW-CB algorithm is useful in finding the anomalies on host. The probability of the connection being achievement is higher than a noxious one. The algorithm keeps up a queue for each new associations ask for (TCP SYN), if the connections got time out without any reply, the algorithm de-queue the connections from the queue, receives a TCP RST. Based on the connection success ratio the TRW-CB algorithm detects the anomalies [30]. Significantly fewer false positives results because of CBCRL algorithm [42]. The credit based association rate restricting and turn around consecutive theory

testing are joined together so worms are immediately related to a drawing in low false caution rate. By using the various controllers like NOX Controller [41], Beacon Controller [32], and Flood Light Controller [39] experiments are conducted and the attack detection are successful which were shown in the results (Table 3).

**Table 3.** Connection based DDoS attack Detection

Sl. No	Connection based DDoS attack detection	SDN Controllers
1	<i>Number of connections</i>	
	Lim. S and all [40]	POX Controller
	Mehdi and all [41]	NOX Controller
	Dotcenko and all [32]	Beacon Controller
	Jin. R and all [39]	Floodlight controller
2	<i>Connection rate</i>	
	Mehdi and all [41]	NOX Controller
	Dotcenko and all [32]	Beacon Controller
	Jin. R and all [39]	Floodlight controller

## 4 SDN Based IoT Frameworks

Lots of data and information are produced due to the rapid growth of IoT. This information are gathered by the enormous objects that are connected to it. In the event that we need to interface everything to the web it will be a basic issue in light of the fact that putting away, overseeing, controlling and verifying such bigdata is outlandish. Software Defined Systems (SDSys) will overcome all the challenges so it is considered as a vital solution. A structure is made for Software Defined Internet of Things (SDIoT) that misuses a few SDSys, for example, Software Defined Network (SDN), Software Defined Storage (SDStore) and Software Defined Security (SDNSec). Controller exists between the system applications and the sending components, its primary job is to control the system tasks. Controller act as a middleware to manage and transfer the communications. SDStore is mainly used to manage huge data in storage system, it separates data control layer and the data storage layer. SDSec provide secure virtual environment infrastructures from threats DoS attack, insider threats etc. [18].

Earlier Detection techniques are centralized detection so communication bottleneck has occurred because download and process will happen at the separate place. On the off chance that there is any blemish in the unified identification system, it won't work until it is recovered. Decentralized detection system is more popular now a day because the agents are placed in different location and it also overcomes the drawbacks of centralized detection mechanism. The multi-agent detection framework was mentioned for detecting DDoS attack. At edge routers multiple detection agents are placed of different transit networks among these detection agent there is a communication mechanism. Each and every agent observes only local information, to improve the detection efficiency; the information and decision among agents are combined together. Distribution detection system needed a cooperation mechanism to detect the abnormal changes in the traffic [33].

SD-IOT Framework which is the extended version of SDN architecture proposed in [46]. SD-IOT framework has controller pool which has SD-IOT controller and SD-IOT switches that were incorporated with the IOT gateway and IOT gadgets. A calculation with SD-IOT structure was proposed to recognize and alleviate the DDoS assault. The algorithm will detect the real DDoS attack by using some threshold value. By using the threshold value in the algorithm, it blocks the DDoS attack at the source itself. A novel framework is proposed in [48] that integrate caching, networking and computing technology that support energy proficient data recovery and registering administrations in green remote system. The system enhances the execution of coming generation green wireless systems. Software Defined Approach is utilized to deal with the assets of systems administration, computing and caching. But traditional SDN focus on networking resources alone. The resource like networking, computing and caching is managed efficiently to improve the resource utilization and user experience. The framework in [48] results in single point of failure, if anyone attacked it. Moreover if any attacker gets permission to access the controller, it will damage the entire wireless network. So an attack-tolerant system should be maintained to get rid of the framework from the attacker.

## 5 DDoS Attacks Mitigation Techniques Based on SDN

[43] Giotis and all proposed SDN architecture it has three components they are collector, anomaly detection and anomaly mitigation. Collector will gather the information; it gathers stream data and transports them to anomaly identification module. The anomaly detector will detect the anomaly for every time-window. The detection algorithm's like analytical abnormality identification, machine learning based abnormality identification and data mining based abnormality identification are used for the identification of the anomaly in the system traffic. Anomaly will be identified by the anomaly detection component and it is exposed to the anomaly alleviation module. The abnormality alleviation will kill recognized assaults; the stream sections will be embedded in the stream table to hinder the malignant traffic. To recognize and relieve the assaults, the ordinarily utilized activities are the forward, drop and change field activities. SDN-based DDoS defense mechanisms are integrated with the mitigation strategies. The commonly used mitigation strategies that are deployed in SDN are blocking ports, dropping packets and redirecting traffic [35, 40, 43, 44, 50, 51]. There are a lot more mitigation strategies that are implemented in SDN-based DDoS alleviation techniques, for example, profound bundle assessment, changing MAC and IP addresses and disengaging traffic [50, 51]. The straightforward and quick relief strategies that totally hinder the potential assault sources are dropping parcels and blocking ports. The above mentioned mitigation techniques will drop the legitimate traffic.

[44] Chin, T.; Mountroudou mention about two important features i.e., monitor and correlator. Monitor has dual functionality like messenger that sends alert and additional information and operates as a sensing node. Relate gets alert from the screen to the data kept up by the OVS switch for profound parcel examination. Some mitigation technique will clean the blacklisted IP address. It filters ill-conceived clients assaulting the server. These shield the server from DDoS. When we fail to pass judge

on the http request, regardless of whether the demand are sent by client or botnet, use CAPTCHA method to separate a human from the botnet. This technique used to find the differentiation between the human request and botnet request [45]. In some techniques mitigation of the attacks will be taking place due to blocking. Blocking by means of block flow that prevents DoS sources further communicating with host on the local. First of all it detect DDoS attacks, then it identify malicious attackers and at last it used to block the attack [35]. DDoS attacks mostly target specific service. SDN is used to overcome from the difficulty that occurs due to DDoS attacks. Usually the DDoS attacks are mounted by huge number of bots. The targeted services will be disabled by the DDoS attack but it won't affect the other network components. Servers that a present in the network need to be protected, SDN will provide sufficient protection for the servers [40].

## 6 Attacks in IoT Devices

Secret key from the substitution-box should be protected from correlation power analysis attack, light weight masked AES engine is used to protect data from this attack. Customary conceal AES execution is unreliable against high request control investigation assault. Equal or more number of masks should be used to protect against high order power analysis attack [6].

### 6.1 Attacks in Middleware

SDN-based IoT is defenseless against new stream assault; Smart Security Mechanism (SSM) is utilized to shield the middleware from the new stream assault. SSM used two methods for detecting the attack i.e., identification and mitigation. Identification method is used to identify the new stream assault and the mitigation method is used to redirect the attack [7]. Distribution middleware is utilized and is incorporated with a synchronization framework for the right appropriation, refresh utilization of strategies for the whole IoT condition [8].

## 7 Existing IOT Middleware Architecture

There are three types in existing Middleware architecture i.e., service based IOT middleware, cloud based IOT middleware and Actor based IOT middleware [9]. Internet security is provided by Public key cryptography. Light weight public key cryptography has been developed to overcome from new attack vectors. Security and Privacy is lack in IOT middleware. Middleware platforms like Hydra, Virtus and webinos addresses the security issues to some extent. The above middleware platforms use the following protocols for security purpose

Hydra utilizes SOAP/Web administrations for security, Virtus uses XMPP models and Webinos utilizes policy-based access control (XACML) and Federated Identity token (OpenID). These are excessively expensive in overseeing memory and time on the grounds that these conventions are not intended for the asset – compelled condition.

In [11], the middleware were gathered dependent on their structure approaches, they are Event based, Service arranged, Virtual Machine-based, Agent-based, Tuple-spaces, Database situated, Application explicit.

Event based Middleware: All the participants like components, applications are interacted with each other through events. An event system consists of large number of application components. Event based Middleware has a type called Message-oriented middleware (MOM). Event based middleware follows publisher-subscriber architecture model. Here we can survey some of the examples of Event based middleware. For Large-scale circulated applications, an event based middleware Hermes is utilized. It utilizes an adaptable routing algorithm and adaptation to internal failure components that defeat various types of disappointments in the middleware.

## 8 Issues and Suggestions

The gaps identified in the existing middleware platforms are: (i) Context-based security, (ii) lack of privacy-by-design, (iii) client driven model of access control and (iv) support for electronic character at the gadget level [10]. Denial of services attack occurs through resource exhaustion. There is no solution for this DoS Attack, but in [7] SSM is suggested to identify and reduce the DoS assault. Security and privacy in middleware is mandatory it should be enhanced with any new technologies [12]. EU FP7 project RERUM designed IoT architecture based on the concept of security and design. It is an open IoT middleware. Implementation of the middleware is at the central part of RERUM, it provides a high security and privacy.

## 9 Conclusion

Presently multi day in all fields everybody relies upon digital physical frameworks and upgrades in systems administration. Cloud innovations have appeared unique consideration for the insurance of system and figuring framework against DDoS assaults. The discovery and moderation of DDoS assaults is a incomplete job. By understanding this problem, we have made several clear collections.

In this paper, the aversion against DDoS assaults was talked about. Compelling DDoS assault identification strategy will react to the expanding malware traffic. What's more, adjusting and simplicity of the board the use of guidelines in identification, moderation and anticipation against DDoS assaults is likewise required. The SDN-based arrangements are ordered by the particular identification and moderation methods in this paper. The discussion about how the DDoS attacks is detected and mitigated using SDN-based techniques were made. SDN based framework also provide a protection against DDoS attacks.



## References

1. Chuah, J.W.: The Internet of Things: an overview and new perspectives in systems design. In: International Symposium on Integrated Circuits (2014). 978-1-4799-4833-8/14
2. Agrawal, S., Das, M.L.: Internet of Things – A Paradigm Shift of Future Internet Applications, Institute of Technology, Nirma University, Ahmedabad 382 481, 08-10 (2011)
3. Xu, X.: Study on security problems and key technologies of the Internet of Things. In: International Conference on Computation and Information Sciences (2013)
4. Kanuparthi, A., Karri, R., Addepalli, S.: Hardware and embedded security in the context of Internet of Things. In: CyCAR 2013: Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles, pp. 61–64 (2013)
5. Zhou, J., Cao, Z., Dong, X., Vasilakos, A.V.: Security and privacy for cloud-based IoT: challenges, countermeasures, and future directions, impact of next-generation mobile technologies on IoT: cloud convergence
6. Yu, W., Köse, S.: A lightweight masked AES implementation for securing IoT against CPA attacks. *IEEE Trans. Circ. Syst. I Regul. Pap.* **64**(11), 2934–2944 (2017)
7. Xu, T., Gao, D., Dong, P., Zhang, H., Foh, C.H., Chao, H.-C.: Defending against new-flow attack in SDN-based Internet of Things, special section on security and privacy in applications and services for future Internet of Things, vol. 5 (2017)
8. Sicari, S., Rizzardi, A., Miorandi, D., Coen-Porisini, A.: Dynamic policies in Internet of Things: enforcement and synchronization. *IEEE Internet of Things J.* **4**(6), 2228–2238 (2017)
9. Ngu, A.H.H., Gutierrez, M., Metsis, V., Nepal, S., Sheng, Q.Z.: IoT middleware: a survey on issues and enabling technologies. *IEEE Internet of Things J.* **4**(1), 1 (2017)
10. Fermantle, P., Scott, P.: A security survey of middleware for the Internet of Things. *PeerJ PrePrints* **3**, e1521 (2015)
11. Razzaque, M.A., Milojevic-Jevric, M., Palade, A., Clarke, S.: Middleware for Internet of Things: a survey. *IEEE Internet of Things J.* **3**(1), 1 (2016)
12. Moldovan, G., Tragosy, E.Z., Fragkiadakisy, A., Pöhlsz, H.C., Calvox, D.: An IoT middleware for enhanced security and privacy: the RERUM approach (2016). ISSN: 2157-4960
13. Shin, S., Gu, G.: Attacking software-defined networks: a first feasibility study. In: Proceedings of the 2nd ACM SIGCOMM Workshop Hot Topics Software Defined Networks, New York, NY, USA, pp. 165–166 (2013)
14. Pena, J.G.V., Yu, W.E.: Development of a distributed firewall using software defined networking technology. In: Proceedings of the 4th IEEE International Conference on Information Science and Technology (ICIST), Shenzhen, China, pp. 449–452 (2014)
15. Seufert, S., O’Brain, D.: Machine learning for automatic defence against Distributed Denial of Service attacks. In: IEEE International Conference on Communications (2007)
16. Yuan, X., Li, C., Li, X.: DeepDefense: identifying DDoS attack via deep learning. In: IEEE International Conference on Smart Computing (SMARTCOMP) (2017). 29-31 Electronic ISBN 978-1-5090-6517-2, Print on Demand (PoD) ISBN 978-1-5090-6518-9
17. Hoyos LI, M.S., Isaza E, G.A., Vélez, J.I., Castillo O, L.: Distributed Denial of Service (DDoS) attacks detection using machine learning prototype
18. Jararweh, Y., Al-Ayyoub, M., Darabseh, A., Benkhelifa, E., Vouk, M., Rindos, A.: SDIoT: a software defined based Internet of Things framework. Springer, Heidelberg (2015). Print ISSN 1868-5137, Online ISSN 1868-5145
19. CCTV-based botnet used for DDoS attacks (2016). <https://www.ddosattacks.net/a-massive-botnet-of-cctv-cameras-involved-in-ferocious-ddos-attacks>

20. DDoS Attack on Bank of Greece Website (2016). <https://www.hackread.com/anonymous-ddos-attack-bank-greece-website-down>
21. HSBC Internet Banking Services Down After DDoS Attack (2016). <http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/12129411/HSBC-online-banking-service-crashes-again.html>
22. Irish Government Websites temporarily offline due to DDoS-attack (2016). <http://www.bbc.com/news/world-europe-35379817>
23. Thai Government Websites hit by denial-of-service attack (2016). <http://www.bbc.com/news/world-asia-34409343>
24. <https://www.tripwire.com/state-of-security/featured/5-notable-ddos-attacks-2017/>
25. <http://ddosattacks.net/russian-defense-ministrys-website-suffers-ddos-attacks-during-poll-for-new-weapons-names/>
26. Zargar, S.T., Joshi, J., Tipper, D.: A survey of defense mechanisms against Distributed Denial of Service (DDoS). *IEEE Commun. Surv. Tutor.* **15**(4), 2046–2069 (2013)
27. Kaufman, C., Perlman, R., Sommerfeld, B.: DoS protection for UDP-based protocols. In: *Proceedings of the 10th ACM Conference on Computer and Communication Security—CCS 2003*, p. 2 (2003)
28. Peng, T., Leckie, C., Ramamohanarao, K.: Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Comput. Surv.* **39**(1), 3es (2007)
29. Czyz, J., Kallitsis, M., Papadopoulos, C., Bailey, M.: Taming the 800 Pound Gorilla: the rise and decline of NTP DDoS attacks. In: *IMC*, pp. 435–448 (2014)
30. ArunRaj Kumar, P., Selvakumar, S.: Distributed Denial of Service attack detection using an ensemble of neural classifier. *Comput. Commun.* **34**(11), 1328–1341 (2011)
31. Braga, R., Mota, E., Passito, A.: Lightweight DDoS flooding attack detection using NOX/OpenFlow. In: *LCN 2010 Proceedings of the 2010 IEEE 35th Conference on Local Computer Networks*, Washington, pp. 408–415. *IEEE* (2010)
32. Dotcenko, S., Vladkyo, A., Letenko, I.: A fuzzy logic-based information security management for software-defined networks. In: *16th International Conference on Advanced Communication Technology (ICACT)*, pp. 167–171. *IEEE* (2014)
33. Xu, X., Sun, Y., Huang, Z.: Defending DDoS attacks using hidden Markov models and cooperative reinforcement learning. In: *Proceedings of the 2007 Pacific Asia Conference on Intelligence and Security Informatics, PAISI 2007*, pp. 196–207 (2007). ISBN 978-3-540-71548-1
34. Bera, S., Misra, S., Vasilakos, A.V.: Software-defined networking for Internet of Things: a survey. *IEEE Internet of Things J.* **4**(6), 1994–2008 (2017). Electronic ISSN: 2327-4662
35. Dillon, C., Berkelaar, M.: OpenFlow (D)DoS Mitigation, February 2014. <http://www.delaat.net/rp/2013-2014/p42/report.pdf>
36. Yen, T.-F., Reiter, M.K.: Traffic aggregation for malware detection. In: *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 207–227. Springer, Heidelberg (2008)
37. Shin, S., Porras, P., Yegneswaran, V., Fong, M., Gu, G., Tyson, M., Texas, A., Station, C., Park, M.: Fresco: modular composable security services for software-defined networks. In: *Network and Distributed System Security Symposium*, pp. 1–16 (2013)
38. Gu, G., Perdisci, R., Zhang, J., Lee, W.: BotMiner: clustering analysis of network traffic for protocol- and structure-independent Botnet detection. In: *USENIX Security Symposium*, vol. 5(2), pp. 139–154 (2008)
39. Jin, R., Wang, B.: Malware detection for mobile devices using software-defined networking. In: *Proceedings of the 2013 Second GENI Research and Educational Experiment Workshop, GREE 2013*, Washington, pp. 81–88. *IEEE* (2013)

40. Lim, S., Ha, J., Kim, H., Kim, Y., Yang, S.: A SDN-oriented DDoS blocking scheme for Botnet-based attacks. In: Sixth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 63–68. IEEE (2014)
41. Mehdi, S.K., Khalid, J., Khayam, S.A.: Revisiting traffic anomaly detection using software defined networking. In: Proceedings of the 14th International Conference on Recent Advances in Intrusion Detection, pp. 161–180 (2011)
42. Schechter, S.E., Jung, J., Berger, A.W.: Fast detection of scanning worm infections. In: International Workshop on Recent Advances in Intrusion Detection. Springer, Heidelberg (2004)
43. Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., Maglaris, V.: Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. *Comput. Netw.* **62**, 122–136 (2014)
44. Chin, T., Mountrouidou, X., Li, X., Xiong, K.: Selective packet inspection to detect DoS flooding using software defined networking (SDN). In: 2015 IEEE 35th International Conference on distributed Computing Systems Workshops (ICDCSW), pp. 95–99. IEEE (2015)
45. Singh, K.J., De, T.: DDOS attack detection and mitigation technique based on Http count and verification using CAPTCHA. In: 2015 International Conference on Computational Intelligence and Networks (2015)
46. Yin, D., Zhang, L., Yang, K.: A DDoS attack detection and mitigation with software-defined Internet of Things framework. In: IEEE Access, Special Section on Security and Trusted Computing for Industrial Internet of Things, pp. 24694–24705, 30 April 2018
47. Zhang, J., Zhang, X., Imran, M.A., Evans, B., Zhang, Y., Wang, W.: Energy efficient hybrid satellite terrestrial 5G networks with software defined features. *J. Commun. Netw.* **19**(2), 147–161 (2017)
48. Huo, R., et al.: Software defined networking, caching, and computing or green wireless networks. *IEEE Commun. Mag.* **54**(11), 185–193 (2016)
49. Guest Editorial: IEEE Systems Journals Special Issue on “Intelligent Internet of Things”. *IEEE Syst. J.* **10**(3) (2016)
50. Chung, C.-J., Khatkar, P., Xing, T., Lee, J., Huang, D.: NICE: network intrusion detection and countermeasure. *IEEE Trans. Dependable Secure Comput.* **10**(4), 198–211 (2013)
51. Xing, T., Huang, D., Xu, L., Chung, C.J., Khatkar, P.: SnortFlow: a OpenFlow-based intrusion prevention system in cloud environment. In: Proceedings of the 2013 2nd GENI Research and Educational Experiment Workshop, GREE 2013, pp. 89–92 (2013)



# Impartial Clustering Algorithm to Increase the Lifetime of Wireless Sensor Networks

V. Asanambigai<sup>1(✉)</sup> and A. Ayyasamy<sup>2</sup>

<sup>1</sup> Department of Computer Engineering,  
Government Polytechnic College, Perambalur, Tamilnadu, India  
tradingbaskeran@gmail.com

<sup>2</sup> Department of Computer Engineering,  
Government Polytechnic College, Nagercoil, Tamilnadu, India  
samy7771@yahoo.co.in

**Abstract.** Wireless Sensor Networks (WSNs) have a large amount of real-time applications with tiny and energy utilized sensors. The network topology separates the sensors into several clusters. In this paper we propose an Impartial Clustering Algorithm, which enables the cluster formation without any requirement of set-up overhead. The proposed algorithm nominates one node called as Adjacent node to gather data from other sensor nodes. It also maintains the load balancing technique to ensure that all the sensor nodes will die only when they transmit all their data in the network within the time to live. The experimental results proved that the proposed work performed well when compared with all the other related works in terms of energy utilization and load balancing.

**Keywords:** Wireless Sensor Network · Cluster · Load balancing · Energy utilization

## 1 Introduction

The enormous enlargement of wireless networks like workstations, cell phones, and paging frameworks builds the demands what's more, request on infrastructure networks endeavors to produce inaccessible networks in all the designs [1], to be explicit, establishment networks, for example, cell structures [2], and framework less networks, for example, ad-hoc networks [3], that facilitate dissimilar mobile devices to operate their data collectively and productively. Owing to their lower establishment costs, flexibility, transmission ability, and flexibility, both structures of previously mentioned networks happened to an exceptional significance and therefore are by and huge conceded on [4].

It is necessary to construct orientation to that the gigantic improvement in distant advances prompted the improvement of little, brilliant, minimal effort, and multi-functional devices called sensors. Those sensors are typically outfitted with remote communication functionalities [5]. Obviously, sensors innovation is changing the method for how individuals are cooperating with the physical condition, particularly at the point when an accumulation of sensors frame a system that is normally managed to wireless sensor networks (WSNs) [6].

The rest of the paper is structured as follows. Section 2 details the work related to the model of the clustering based routing algorithm. The proposed work and its methodology are dilated Sect. 3. Section 4 presents the experiment and the discussion of evaluation results. Finally, conclusion of this work is Sect. 5.

## 2 Related Work

Utilizations of WSNs are boundless and length characteristic parts of our life from military applications, natural checking, and coordination augment, human-driven applications to mechanical technology applications [7]. Not quite the same as wired networks, WSNs are accountable to various kinds of requirements, for example, limited power assets, constrained correspondence separation, and restricted system correspondence transmission capacity [8].

Alongside these lines, assorted procedures are being familiar with use sensors qualities out of which those that look for limiting long-separate interchanges through having neighborhood cooperation between sensors also, stifling copy data by various collection systems. As directing in WSNs has an incredible effect on the system lifetime, it has numerous difficulties. In the previous works, analysts have proposed a lot of routing algorithms that contract with the constrained assets in WSNs [9].

In this paper, we propose a clustering based routing algorithm which adjusts the energy utilization and permits the WSN to the increased lifetime. WSN is dissimilar to other wireless networks. Cluster Head formation plays a vital role in Cluster based routing algorithms [10–12]. For every WSN nodes have the communication area and Base Station. LEACH protocol [12] is the basic clustering protocol which transmits the data directly to the Base Station. UCR protocol [14] is used to elect the cluster head based on the sensor capturing power is the result of having the reduced transmission overhead. RRCH protocol [13] is used to select the cluster head based on the Round-robin methodology which enables the efficient energy and improved load balancing technique.

## 3 Proposed Work

The significance of this work is as

- (i) Proposing energy utilized clustering algorithm to improve the lifetime of the network.
- (ii) Forming the proposed method which satisfies the objectives.
- (iii) Simulating the proposed algorithm with the related algorithms as LEACH, UCR and RRCH.

Energy plays a vital role for cluster formation.  $Energy_{Total}(q, dis)$  is the Total amount of Energy required for the bit  $q$  with the distance.  $Energy_{Total_{cir}}(q)$  is the total amount of energy required for broadcasting circuitry,  $Energy_{Total_{amp}}(q, dis)$  is the amount of energy required for the amplified the signal to discover the routing with bit  $q$  and distance.

$$Energy_{Total}(q, dis) = Energy_{Total_{cir}}(q) + Energy_{Total_{amp}}(q, dis) \quad (1)$$

$$Energy_{Required}(q) = Energy_{Required_{cir}}(q) \quad (2)$$

where  $Energy_{Required}(q)$  is the required energy for the broadcasting circuitry for the q-bits.

### 3.1 Algorithm – Impartial Clustering Algorithm

**Input:** Every adjacent sensor node A has finished the formation of clusters within the communication range.

**Output:** Feasible cluster formation.

Step 1: If the sensor node type is normal node then send data to the cluster head and update the order.

Step 2: If the sensor node type is adjacent node then receive the data from the cluster head and append the base station value.

Step 3: If the energy level of the adjacent node is less than the threshold value then adjacent node sends the transmission data and create the new cluster head.

Step 4: Analyze the condition of the sensor node's energy level.

Step 5: If the energy level is very low, then finish the network formation.

Step 6: Continue the Step 2 to 5 until the final result is achieved.

### 3.2 Network Topology Creation

The proposed algorithm creates a sensor field and separates the field into same sized fields. Every region has the adjacent node for creating and updating the gathered information from the cluster head. The deployment of the sensors is placed with the parameters of energy utilization. The sensor nodes can broadcast their data to the corresponding cluster head, then the cluster head aggregates all the received data and forwards the message to the nearest adjacent node. Figure 1 determines the network topology with the nodes is deployed in the sensor field. It is precious to declare that the proposed method does not need any setup overhead in every round. The sensor filed contains the actual nodes, Cluster heads and the adjacent nodes. Every cluster head forwards the updated data to the neighbor adjacent node within the path towards the cluster head.

A round robin rotation methodology is implemented to permit the cluster to have without any control overhead with more than one round is used. Every sensor node transmits a control message to all the base station with the cluster identification number. For this kind of available data, the entire sensor node can have the change to become the cluster head role in rotation. Each node in the particular cluster should guarantee that it recognizes the role of cluster head in any one round accordingly.

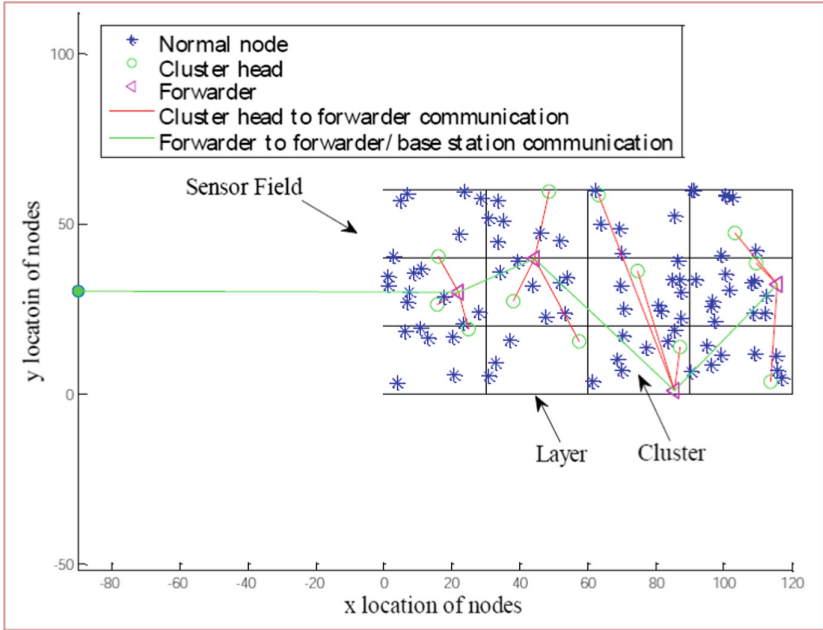


Fig. 1. Network topology

### 4 Performance Evaluation

The simulation has been done with the help of Network Simulator 2. In our simulation, 110 nodes were deployed with the sensor field in the network. Our aim for this simulation is to increase the network lifetime, for this purpose the utilization of network is the vital parameter also.

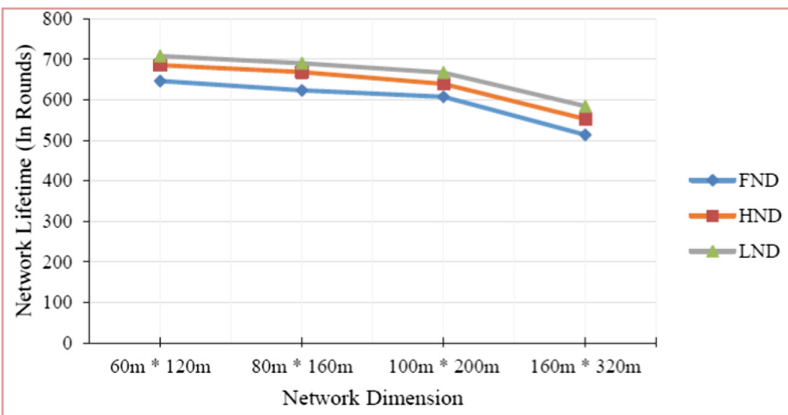


Fig. 2. Comparison of the network lifetime

The network lifetime is computed using the parameters FND, HND and LND. In this kind of simulation, the proposed algorithm can be performed in different network dimensions. The sensor field is separated in to several kinds of clusters with equal amount of sensor nodes. It can be proved from Fig. 2 that the lifetime of the network reduces as the sensor field improves and the distance is needed to broadcast the sensed data to the Base Station. The maximum dimension has the reduced amount of Network lifetime compared to other network dimensions.

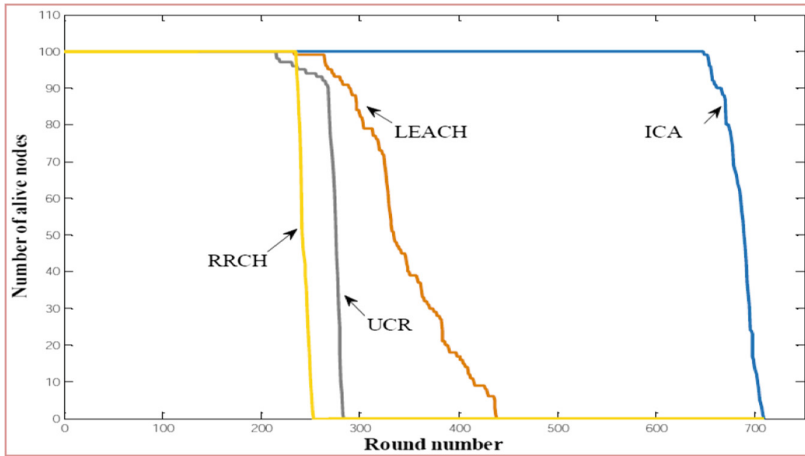


Fig. 3. Number of alive nodes in the network

In this simulation, the total amount of alive nodes in the network is observed in the round number. Figure 3 demonstrates that all the algorithms have the decreased amount of alive nodes whenever the round number is increased.

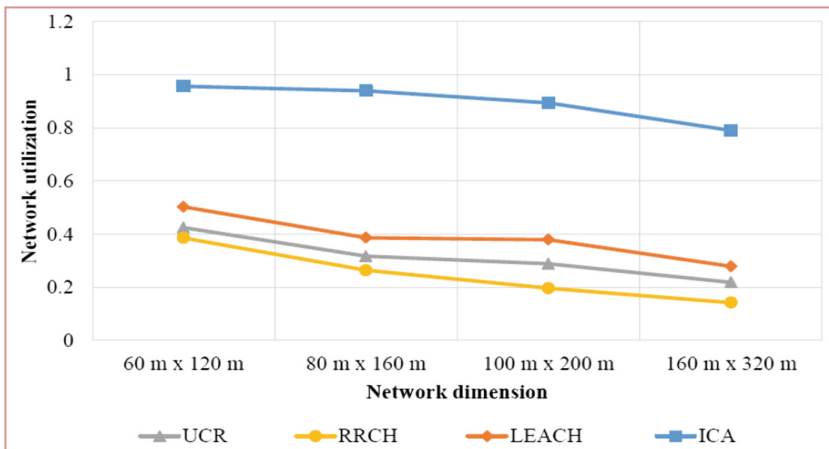


Fig. 4. Network utilization with network dimension



The utilization of the network is computed as the ratio between the energy utilized for data transmission and total energy utilized in the network. Whenever the communication range in the sensor field is increased, the utilization of the network is automatically increased. Whenever we need to increase the communication range, we should increase the sensor node in the deployment area. Figure 4 illustrates that the proposed ICA is utilized more network compared to the related methods UCR, RRCH and LEACH.

## 5 Conclusion

In this paper, we developed Impartial Clustering Algorithm with the formation of the network. The proposed network model is formed using the sensor field that is separated into several clusters in connection with the distance in the communication range. For this kind of cluster formation, the data loss is avoided. The simulation results proved that the proposed algorithm is performed well compared to the related algorithms.

## References

1. Darabkh, K.A., Alsukour, O.: Novel protocols for improving the performance of ODMRP and EODMRP over mobile ad hoc networks. *Int. J. Distrib. Sens. Netw.* **2015**, 1–18 (2015)
2. Akkaya, K., Younis, M.: A survey on routing protocols for wireless sensor networks. *Ad Hoc Netw.* **3**(3), 325–349 (2005)
3. Khalifeh, A., Darabkh, K.A., Kamel, A.: Performance evaluation of voice-controlled online systems. In: *Proceedings of IEEE/SSD 2012 Multi-conference on Systems, Signals, and Devices*, Chemnitz, pp. 1–6. IEEE press, Germany (2012)
4. Darabkh, K.A., Aygun, R.: Improving UDP performance using intermediate QoS-aware hop system for wired/wireless multimedia communication systems. *Int. J. Netw. Manage.* **21**(5), 432–454 (2011)
5. Al-Zubi, R.T., Abedsalam, N., Atieh, A., Darabkh, K.A.: Lifetime-improvement routing protocol for wireless sensor networks. In: *Proceedings of the 15th IEEE Multi-conference on Systems, Signals, and Devices (SSD 2018)* (2018)
6. Al-Zubi, R., Krunz, M., Al-Sukkar, G., Hawa, M., Darabkh, K.A.: Packet recycling and delayed ACK for improving the performance of TCP over MANETs. *Wireless Pers. Commun.* **75**(1), 943–963 (2014)
7. Darabkh, K.A., Judeh, M.S.E.: An improved reactive routing protocol over mobile adhoc networks. In: *Proceedings of the 14th International Wireless Communications and Mobile Computing Conference (IWCMC 2018)* (2018)
8. Darabkh, K.A., Aygün, R.S.: TCP traffic control evaluation and reduction over wireless networks using parallel sequential decoding mechanism. *EURASIP J. Wireless Commun. Network.* **2007**, 1–16 (2007)
9. Yaseen, H.A., Alsalam, M., Jarwan, A., Al-Mistarihi, M.F., Darabkh, K.A.: A secure energy-aware adaptive watermarking system for wireless image sensor networks. In: *Proceedings of the 15th IEEE Multi-conference on Systems, Signals, and Devices (SSD 2018)* (2018)

10. Harold Robinson, Y., Golden Julie, E., Ayyasamy, A., Archana, M.: Cluster based routing in sensor network using soft computing techniques: a survey. *Asian J. Res. Soc. Sci. Humanit.* **7**(3), 341–360 (2017)
11. Harold Robinson, Y., Golden Julie, E., Balaji, S., Ayyasamy, A.: Energy aware clustering scheme in wireless sensor network using neuro-fuzzy approach. *Wireless Pers. Commun.* **95**, 1–19 (2016)
12. Anguraj, D.K., Smys, S.: Trust-based intrusion detection and clustering approach for wireless body area networks. *Wireless Pers. Commun.* **104**, 1–20 (2019)
13. Shurman, M., Awad, N., Al-Mistarihi, M.F., Darabkh, K.A.: LEACH enhancements for wireless sensor networks based on energy model. In: *Proceedings of the 2014 IEEE International Multi-Conference on Systems, Signals & Devices, Conference on Communication & Signal Processing*, pp. 1–4 (2014)
14. Nam, D.H., Min, H.D.: An energy-efficient clustering using a round-robin method in a wireless sensor network. In: *5th ACIS International Conference on Software Engineering Research, Management & Applications*, pp. 54–60 (2007)
15. Chen, G., Li, C., Ye, M., Wu, J.: An unequal cluster-based routing protocol in wireless sensor networks. *Wireless Netw.* **15**(2), 193–207 (2009)



# Energy Efficiency Analysis of Cluster Based Routing in MANET

Parveen Kumari<sup>1</sup>(✉), Sugandha Singh<sup>2</sup>, and Gaurav Aggarwal<sup>3</sup>

<sup>1</sup> CSE, Jagannath University, Jhajjar, HR, India  
dahiyaparveen22@gmail.com

<sup>2</sup> CSE, G. H. Raisoni College of Engineering, Nagpur, India

<sup>3</sup> Computer Science Department, Jagannath University, Jhajjar, Haryana, India

**Abstract.** MANET is a set of non-identical mobile nodes, where all the nodes are under energy constrained environment. Here reduction in energy consumption is the main issue. This paper consists Energy Efficient Analysis Cluster based routing Protocol (EECP), in which the network coding is used along with cluster heads for reducing the number of transmissions and increasing the network lifetime. As the number of transmission is reduced, energy consumption is also reduced. Through simulation using NS-2, it has been shown that the performance of EECP is better than CBRP.

**Keywords:** Clustering · MANET · Network coding · CBRP

## 1 Introduction

In the absence of physical infrastructure, users can also communicate through mobile Ad-hoc network. In MANET, each node is considered as router and transfer the data packets. Managed energy resources have the responsibilities of network lifetime [2]. It is more beneficial to use the less power than to store the node battery power. This paper consists the technology of Network Coding (NC) for limiting the energy consumption. This technology is incorporated with cluster based routing protocol [3] for improving the output of mobile ad hoc network. Due to network coding, the packets at intermediate zone are combined and hence the number of transmitted packets reduced. Energy is consumed by each transmitted packets. Hence, with the increment of packets transmission, energy consumption is also increased [13]. The organization of this paper as follows: Sect. 2, explains CBRP with Network Coding aware routing. Section 3 consists of proposed EECP scheme. Section 4 shows Simulation and evaluation of result and Sect. 5 concludes the work and brief about the future work.

## 2 CBRP with Network Coding Aware Routing

Several individual approaches are used by previous researchers for developing the power aware routing protocol [14]. Active communication energy is minimized by transmission power control and load balancing methods where inactive communication energy is minimized by sleep power down mode [8].

## 2.1 Cluster Based Routing Protocol (CBRP)

CBRP is a upper level protocol which is strong and adaptable as compared to others used in MANETs. This protocol is used for the large mobile ad hoc network. The clusters are formed by separating the nodes of mobile ad hoc networks [3]. There is a cluster head in each cluster and all other nodes are considered as members node. ID is the selection criteria for electing cluster head (CH). CH is assigned to the node which has lowest ID. Every node has to maintain its respective neighbor table which is conceptual data structure and its helps in employing link status sensing and also for cluster formation [5]. Neighbor table is shown in Fig. 1.

Neighbor ID	Link Status	Role
Nbr 1	Uni/bidirectional?	Is1clusterhead?
Nbr 2	Uni/bidirectional?	Is2clusterhead?
Nbr N	Uni/bidirectional?	IsNclusterhead?

**Fig. 1.** Neighbor table

Each node also has to maintain cluster adjacency table that has the responsibility to keep information about adjacent clusters [6]. The structure of cluster adjacency table is shown in Fig. 2.

Cluster ID	Link Status
Adjacent Cluster 1	To/from/bi
Adj.Cluster 2	To/from bi
Adj.ClusterN	To/from/bi

**Fig. 2.** Cluster adjacency table

Node ID		Node Status	
Nbr ID	Nbr status	Link Status	
...	...	...	
Adjacent ID			

Fig. 3. HELLO message

Hello message as shown in Fig. 3 is used for updating neighbor table and cluster adjacency table.

On basis of source routing CBRP performance flooding traffic is minimized by making the cluster structure during route discovery phase. Cluster head is elected depending on the cluster membership status. Network connectivity is increased using the unidirectional links. Therefore intercluster links are dynamically discovered. At stage of route discovery, Route Request Packets (RREQ) carries the information of cluster head also to discover destination. RREQ packet is forwarded by each cluster head once only and once it is recorded in the route, it never forwards it [4]. Nodes in CBRP are organized in hierarchical manner and CH coordinates the data transmission between clusters. Intra cluster topological information is acquired by proactively sending the Hello message. The state information of link and neighboring nodes is kept by neighbor table and the information about neighboring clusters and members are kept by CH.

### 2.2 Network Coding Aware Routing

In Fig. 4(a), data is transferred between A and B through router and the transmitted data is represented by time slots of TDMA method and traditional method is used where 4 transmissions are required while in Fig. 4(b), Network Coding (NC) method is used where only 3 transmissions are take place which saves time and improves throughput.

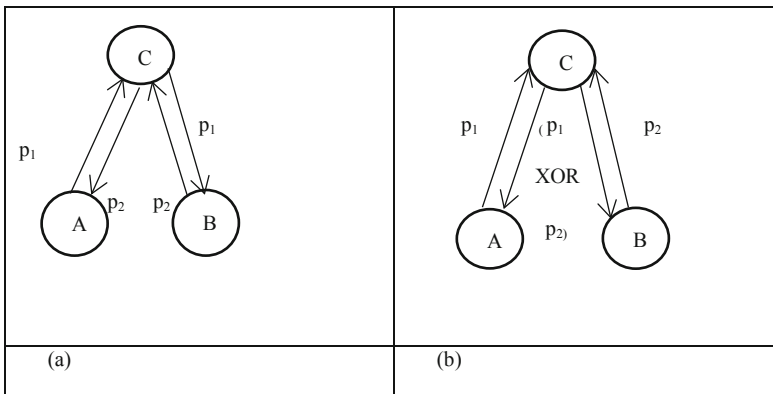


Fig. 4. (a) Traditional method (b) Network coding method

### 2.3 WCA for Saving Energy

High energy nodes are considered as cluster heads. If CHs and gateway nodes are in active state and all the member nodes are considered in sleep mode then more energy can be saved [11]. Clustering algorithm performs better with network coding in CBRP and cluster head is selected by WCA process in which overall weight is calculated on the basis of ideal degree of node, transmission power, mobility of nodes, battery power [1]. These 4 parameters are used for calculating the node weight as follows:

$$W_v = w_1.a + w_2.b + w_3.c + w_4.d \quad (1)$$

W: overall Weight of a clusterhead

a: neighboring nodes of a node (node degree)

b: total distance from neighboring nodes

c: mobility of the nodes

d: consumed battery power

In (1),  $w_1.a$  is used by cluster head for handling the limited nodes.  $w_2.b$  stands for energy consumption, more power is required for longer distance communication so total distance should be less.  $w_3.c$  stands for mobility, cluster stability improves with less mobility.  $w_4.d$  is the total time of a node acts as a cluster. Cluster heads consume more battery as compared to cluster member. As per network demand weighting factors can be changed [9]. At the combining stage of cluster heads, one having smaller weight becomes cluster head and the other having larger weight becomes cluster member.

## 3 Proposed Energy Efficient Analysis for Cluster Based Routing Protocol (EECP)

The approach based on cluster is used to reduce overall broadcast overhead [12]. Cluster heads help to avoid unnecessary network wide flooding in MANETs but EECP is better than CBRP such as, if there is route error in CBRP while transmitting the data then the upcoming node is removed from transmission range path while in EECP if the upcoming node is cluster head then it is replaced by next cluster head which also improves the performance and hence saves the energy [3].

### 3.1 System Model

Network coding is applied on CBRP to get advantage of clustering and reduce broadcasting overhead. The proposed system takes the input parameter like nodes, mobility, initial energy of the nodes and packets to be sent as shown in Fig. 5. It gives the output in terms of total number of delivered packets, simulation time and residual energy of the nodes [5].

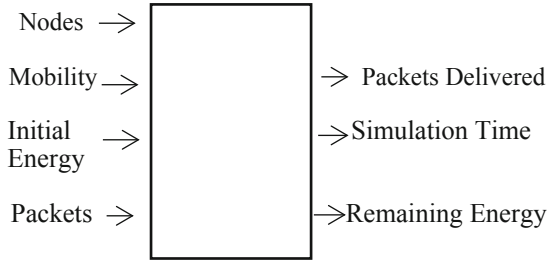


Fig. 5. System model

### 3.2 Packet Encoding Algorithm Based on Network Coding

Network coding is applied at the cluster heads of CBRP. Cluster head will be selected on the basis of smallest weight ( $W_v$ ) and by verifying its energy level and cluster head life time increases as well as increases the network life time [10]. For this, selection of cluster head is done by some threshold value on node energy levels 50. For packet encoding, two neighbour nodes  $u$  and  $v$  are considered. If neighbour reception table of  $u$  is accurate then  $u$  sends XOR - ed packet  $p$  based on the packet probability 0.5 and delay tolerance 0.7.  $p$  should be decoded by neighbor  $v$  by using stored native packets.

Some conditions should be fulfilled in this process: (i) the forwarded packets of each node is stored in FIFO queue known as the output queue. (ii) two virtual queues are maintained for each neighbour, first is small packets <100 bytes and second is large packets >100. (iii) each node consists a hash table where packet-id is the key of packet info. The hash table shows the possibility of having the packet by each neighbor in output queue.

```

Coding
{
let packet p at front of output queue
Createtopology(n);
UpdateNbrRecTable(T)
U=tdpFwdnode(n);
if u is not equal to Fwder(T) return;
if allNbrRecv(T) return;
if (Native(p))
{
if (prob(p)>0.3 and delaytolerance(p)>0.7)
{
if size(p)>100 bytes then
{
Queue=1
}
else
{
Queue=0
}
Obtaincodeset(C)
{
C=p //let p at front of output queue
for each remained packet r in the queue
{
for each neighbor v
{
if (cannot decode( $p \oplus r$ ))then
{
goto continue
}
}
}
C=C U r
p=  $p \oplus r$ 
continue
}
Return C
}
if(|C|>1) then
{
Send coded pkts(C);
}
elseif(!timeout(p))
{
Queue(p,t)
}
else
{
Send Native(p)
}
else
{
for each r=decode(T)
{
TDP_NC(T);
}}
}
}

```



### 3.3 Decoding Procedure

For decoding process, a native packet copy is kept by packet pool of each node where the packets are either received or sent out. Packet-id is the key of packets in hash table. On receiving a coded packet, a node checks the native packets id one by one and retrieve a corresponding packet from its packet pool. Decoding process is shown by Fig. 6. Suppose source S has to broadcast packets  $p_1, p_2, p_3, p_4$  then receiver  $R_1$  extract  $p_1$  packet,  $R_2$  extract  $p_2$ ,  $R_3$  extract  $p_3$ ,  $R_4$  extract  $p_4$  packet and  $R_5$  has all packets and  $R_6$  does not have the opportunities to decode the packet.

### 3.4 Route Discovery

There is no need to find out the route if packet destination is just its neighbor node or the route is present in the routing table else create the route request packet and broadcast it to the cluster head or gateway and perform network coding at CH then broadcast the coded packet to another cluster head or gateway. Finally update the route table according to the request reply [7].

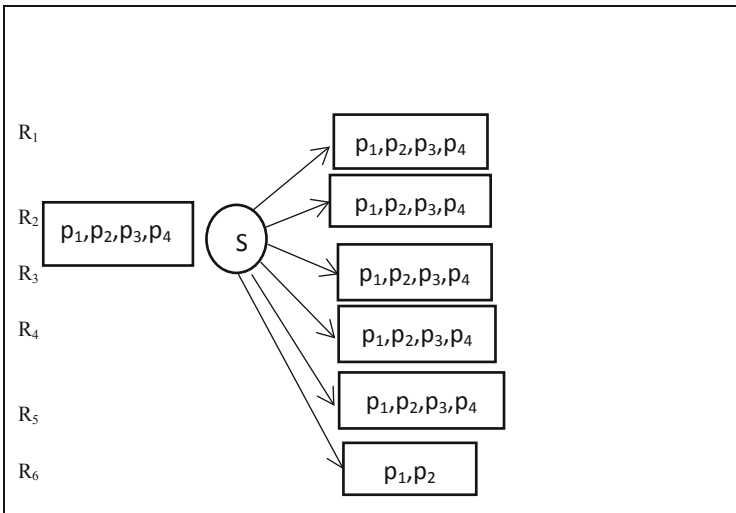


Fig. 6. Decoding process

## 4 Simulation and Evaluation of Result

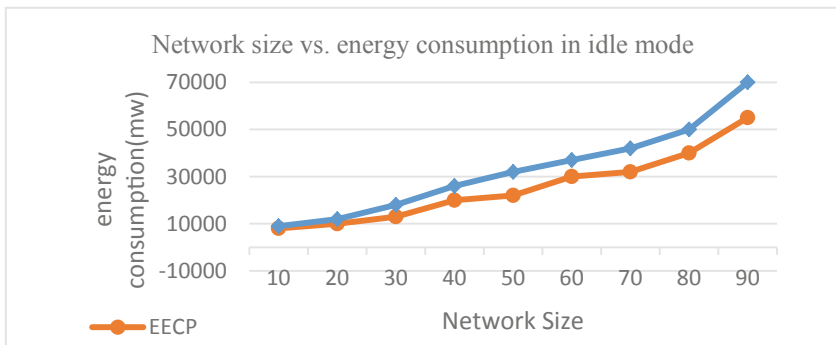
Energy consumption is considered in sending, receiving, idle and sleep mode [4]. The performance of proposed EECBP is compared with original CBRP by network simulator (NS-2) (Table 1).

**Table 1.** Simulation parameters

Background traffic - Constant Bit Rate (CBR)	Pause Time - 2 s
CBR maxpkts - 1100	Nodes number range - 5–30
Weight of clusterhead - 1	Sending rate - 0.20
Simulation Duration - 900 s	Broadcast interval - 2 s
Max connection - 16	Transmission Power - 600 mW
Seed - 1.0	Receiving Power - 300 mW
Max speed - 10 m/s	Area – 500 m × 500 m

#### 4.1 Network Size vs. Energy Consumption in Idle Mode

In Fig. 7, energy consumption increases with the increase of number of nodes and by simulation it is cleared that performance of proposed EECP is better than CBRP.

**Fig. 7.** Network size vs. energy consumption in idle mode

#### 4.2 Packet Delivered to Destination vs. Network Size

Initially 25 J energy was assigned to each node and simulations were run for 500 s to ensure that node ran out of energy. From Fig. 8. It is cleared that more number of packets are delivered as compared to CBRP.

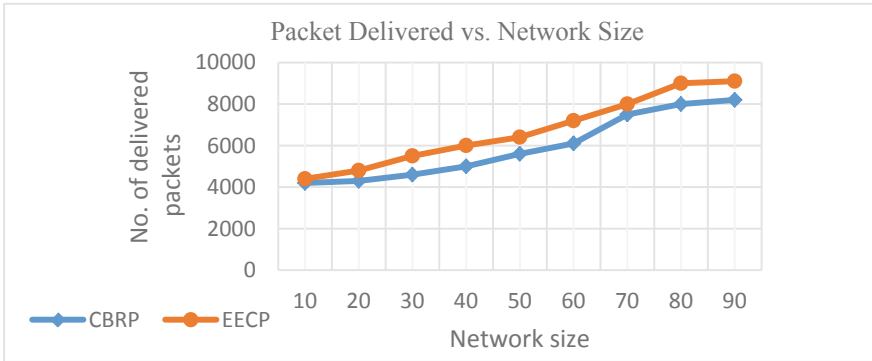


Fig. 8. Packet delivered vs. network size

### 4.3 Average of Saved Energy in EECP

Average of saved energy in different modes is shown in Fig. 9. During the simulation of 900 s more than 2100 mW significant value of energy is saved.

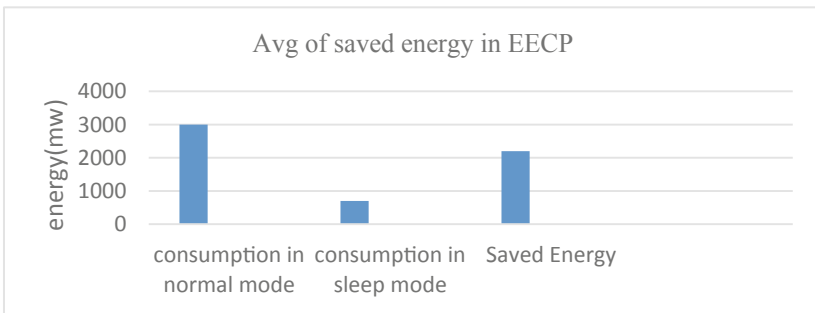


Fig. 9. Avg of saved energy in EECP

## 5 Conclusion and Future Work

This paper consists Network Coding (NC) in the proposed EECP scheme which improves the performance of CBRP for efficient energy along with WCA. Network coding is applied on cluster head which reduce the number of transmissions and energy consumption hence network lifetime increases. For the future work, other cluster based protocol can be used for improving the applied scheme (EECP) performance by considering the factors network size, mobility and transmission range.

## References

1. Kumari, P., Aggarwal, G., Singh, S.: Clustering in mobile ad hoc network: WCA algorithm. In: ICCNCT 2018 Organized by RVS Technical Campus, Coimbatore, India
2. Singh, S., Rajpal, N., Sharma, A.: Address allocation for MANET merge and partition using cluster based routing. <http://www.springerplus.com/content/3/1/605>
3. Kanakala, S., Ananthula, V.R., Vempaty, P.: Energy efficient cluster based protocol in mobile adhoc networks using network coding. *J. Comput. Netw. Commun.* **2014**, 12 (2014)
4. Hosseini-Seno, S.-A., Wan, T.C., Budiarto, R.: Energy efficient cluster based routing protocol for MANETs. In: 2009 International Conference on Computer Engineering and Applications IPCSIT, vol. 2 (2011) © IACSIT Press, Singapore (2011)
5. Abolhasan, M., Wysocki, T., Dutkiewicz, E., Liu, C., Kaiser, J.: A review of routing protocols for mobile ad hoc networks. *Ad Hoc Netw.* **2**, 1–22 (2004)
6. Liu, C., Kaiser, J.: A Survey of Mobile Ad Hoc network Routing Protocols, Tech Report Series, Nr.2003-08 (2003)
7. Tan, L., Yang, P., Chan, S.: An error-aware and energy efficient routing protocol in MANETs. In: ICCCN 2007, pp. 724–729 (2007)
8. Toh, C.K.: Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks. *IEEE Commun. Mag.* **39**, 1–11 (2001)
9. Wang, S.Y.: Reducing the energy consumption caused by flooding messages in mobile ad hoc networks. *Comput. Netw.* **42**, 101–118 (2003)
10. Schiele, G., Becker, C.: SANDMAN: an Energy-Efficient Middleware for Pervasive Computing, Report (2007)
11. Zhenxin, F., Layuan, L.: Advanced save-energy mechanism of ad hoc networks. In: Sixth Annual IEEE International Conference on Pervasive Computing and Communications, vol. 00, pp. 657–662. IEEE Computer Society, Washington, DC (2008)
12. Vijay, S., Sharma, S.C., Sharma, S.C.: An analysis of energy efficient communication in ad hoc wireless local area network. In: First International Conference on Emerging Trends in Engineering and Technology, pp. 140–144. IEEE Computer Society (2008)
13. Singh, S., Raghavendra, C.S.: PAMAS- power aware multi access protocol with signaling for Ad Hoc networks. In: Proceedings of the ACM SIGCOMM Computer Communication Review, July 1988
14. Yaun, P., Wang, H.: A multipath energy efficient routing protocol for ad hoc networks. In: ICCAS, June 2006



# Efficient and Secure Data Storage CP-ABE Analysis Algorithm

V. SenthurSelvi<sup>(✉)</sup>, S. Gomathi, V. Perathu Selvi,  
and M. Sharon Nisha

Department of Computer Science and Engineering, Francis Xavier Engineering  
College, Anna University, Tirunelveli, Tamilnadu, India

Senthurselviv@gmail.com, Gomathyrajah@gmail.com,  
Perathuselvi@gmail.com, sharonnishafxec@gmail.com

**Abstract.** In the contemporary digital environment, secure search over encrypted data is necessary to prevent the unauthorized data usage practices. To provide data privacy and security fine grained access control is important. For having data privacy data have to be stored onto the cloud in an encrypted form and have to be decrypted before retrieving the message. Encrypting the information is a tedious process for mobiles and also its recovery is a significantly challenging task since the mobile devices have limited bandwidth and battery life. Searching the encrypted data over mobile cloud is a tedious process. To tackle this issue, Cipher text Policy Attribute Based Encryption (CP-ABE) mechanism is proposed. The proposed system will perform computation in cloud rather than the mobile device. This mechanism could effectively prevent malicious searching and decrypting of files. Also, the proposed system support many number of attributes and flexible multiple keyword search patterns in which query file order will not affect the search result. This indicates CP-ABE scheme to improve the efficiency and security.

**Keywords:** Multiple keywords search · Attribute based encryption · Mobile cloud

## 1 Introduction

Cloud computing provides convenient, accessible and storage services from a common pool of shared resources. This makes the individuals and companies to store their data onto the cloud server. On the other hand, mobile devices can store their data on Mobile Cloud Storage(MCS) [1, 2]. Mobile devices store and receives their information from MCS utilizing remote correspondence [3]. This makes the document sharing procedure simple without depleting the mobile resources [4].

To secure the information, the proprietor encrypts the information in the cloud. During recovery, the required encoded file can be got by search method from MCS. Mobile devices are also facing security dangers like computers [5, 6]. Since the files are encrypted in a mobile cloud storage the challenges facing here are different over the conventional encoded search method. This could be because of limited energy capacity and calculating capacity of the mobile devices. Information encryption and its recovery

could also be the reasons. Henceforth the objective is ought to have versatile cloud storage which is better in vitality utilization and system traffic. It gives information security by means of wireless communication.

At here, we present CP-ABE architecture for distributed storage applications. CP-ABE accomplishes the efficiencies through utilizing and altering the ranked keyword search, which has-been broadly utilized in distributed storage framework as the search encrypted premise. Efficient search of the encrypted information is of two ways: Firstly, Ranked keyword search method provides significant scores [7] to the document searched by the keyword. This then sends the best-n required files to the user. This method is more appropriate for distributed storage than compared to the Boolean search [8–11]. Because Boolean keyword search instead of sending required file will return all matched files to the user when a keyword is typed. This will cause system traffic and heavy computations the mobile devices.

CP-ABE with ranked keyword search method is efficient for computation on the cloud server and also it saves energy for furthermore calculation in small devices like mobiles. CP-ABE is proficient in decrypting message in cloud by using search encrypted method. While implementing CP-ABE, the security is increased to ensure the data leak and the associated keyword file leak is lessen by altering the encoded search method [12, 13].

It is to be seen that CP-ABE is securely executed with improvement based on TF-IDF approach [13–16], yet the basic security imperfection of the encryption method could not be totally settled. However there is no powerful method exist other than this. But we can assure that CP-ABE is good to have in an improved encrypted search method. It is good to have the distributed storage provided is atleastly of trustable and wont intrigued with assailants in CP-ABE in many parts of the works. CP-ABE utilized the engineering upgrade over the customary search method. Our thorough examination demonstrates that CP-ABE has the below preferences in correlation with encoded search system:

1. Energy utilization is diminished between 35% and 55% by CP-ABE. This is done by offloading calculations of pertinent scores on the cloud server. As a result, mobile computation is decreased. In the mean time, mobile speed of the file access is increased.
2. CP-ABE lessens the system traffic for the correspondence required document and also its recovery time is decreased between 23% and 46% in our demonstrations.
3. By modifying the search method which is encrypted, CP-ABE again distributes the index. This is done because to prevent any data leak. Also CP-ABE wraps the keywords together with noise so as to make them indistinct to the assailants. Security examination demonstrates that security feature of CP-ABE is maintained and improved for MCS remote systems.

## 2 Related Works and ETAPR-VOD

In the real world, the access for our secured data in a trusted manner will be given to the recipients without knowing who the specified individual is. To tackle this issue, ABE comes into existence. ABE is more scalable approach than the existing system. ABE provides trusted sharing and information accessing. With ABE, decryption can be given to a specified person by specified identities. ABE is a form of public key and it is based on IBE where identity can be based upon many more set of attributes. Here the information is encrypted based on arbitrary attributes. The attributes are formalized in ASCII strings. These strings will be parsed and tokenized thereby creating a policy and it also verified lately. The intended recipient individual can decrypt the information only if the keys are matched according to the attributes during the cipher text generation.

There are two methods of ABE: (i). In Key policy method, where the cipher text will be related with many more attributes of the individual. The recipient's key will be encoded with the defined attributes. Information can be decrypted with the recipient's key only when the policy defined is matched. (ii). In CP-ABE method, the recipients have set of attributes and the related keys. The cipher text here will be encoded with the defined policy. The recipients attribute have to be matched with the defined policy. Only then decryption is done. CP-ABE is more proficient because it is similar to Role Based Access Control method. In this plan, we proposed another enhancement of ABDS method to solve insufficiencies of existing works. It likewise brings down the intricacy of capacity and correspondence.

A novel method called Efficient Tracing Attributes Proxy Reencryption with Verifiable Outsourcing Decryption ETAPR-VOD is introduced here only the authorized users are granted permission based on access policy for keyword searching of an encrypted data. The syntax and security definition are formally defined. In ETAPR-VOD two methodologies are used key-policy and ciphertext-policy. This method of approach has three properties (i) Searching by keyword is done on encrypted data by the information proprietor. (ii) The information proprietor allows only approved clients to have searching by keyword only when access control policy are satisfied. (iii) There exist no communication between data owners and the users and no violation of data privacy occurs.

## 3 Proposed System

In Proposed System, we propose CP-ABE transmission capacity and vitality proficient searching mechanism of encrypted data over mobile cloud. The proposed framework will have effective communication between clouds and clients by having workloads on the cloud. In this framework, the information security won't influence when any improvements are finished. Our tests demonstrate that CP-ABE decreases the calculation time and spare the vitality utilization for per record recovery; in the interim the system deals amid the document recoveries are additionally fundamentally diminished (Fig. 1).

During encryption, initially preprocessing of data is carried out followed by indexing as shown on Fig. 2. Selected files have to be stored on the cloud by the information proprietor [17]. Stemming will be carried out for each word in these files. To entry the data in the index, hashing and encrypting of every word stem is done. Index generation by the information proprietor is the next step. Atlas, encrypting the index altogether with file set and stored it on the cloud server is done. Order Preserving Encryption (OPE) is generally used procedure for the file index encryption. TF values of a TF (Term Frequency) table are of a file index. For finding word relevance in files TF-IDF table is used. The user can search the file by the keyword. Then the chosen file will be decrypted for the user.

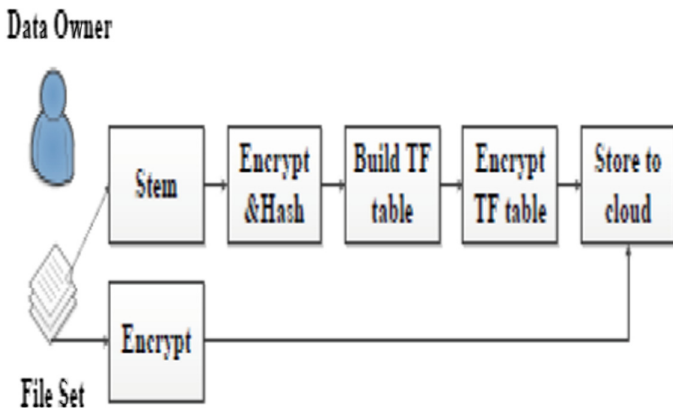


Fig. 1. Uploading files by information encryption.

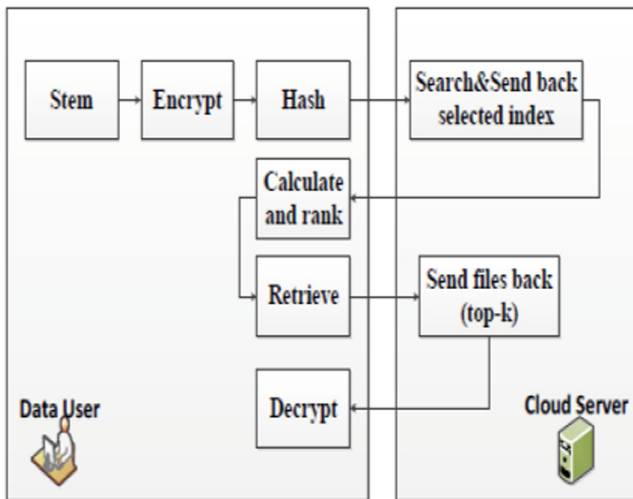


Fig. 2. System model



**ADVANTAGES:**

- Encrypted file Store and Retrieve
- Encrypted Keyword Search
- User Authentication using Verification key
- Index term encryption
- Ranked keyword Search

**4 Result Analysis**

**Key generation center:** It acts as a key centre for public and secret key generation by CP-ABE method. It issues and updates keys for the clients. It gives permission to distinct clients according to their attributes for file access. Hence its executes file access in a secret manner. But somehow it would know encrypted data. Therefore it is wise to prevent the knowing of plain text of the data from KGC.

**Data storing center:** It act as a data storing center. It prevents the unauthorized access of the data from the unknown individuals. It provides fine grained access control to the individuals by generating client key with KGC based on the clients attributes. It is similar to KGC and half trusted.

**Data owner:** It is the one who uploads and in charge of the data in data storing centre for data sharing purpose. He is the one who defines access policy and makes data restricted by encryption.

**User:** It is an individual who gains the data if his individual attributes set matches the encrypted information access policy. Only then he will able to decrypt the data (Table 1).

**ALGORITHM:**

```
$ cpabe-keygen -o sara.priv.key pub.key master.key \  
  sysadmin it.department 'office = 1431' 'hire.date = 'date +%s'  
  
$ cpabe-keygen -o kevin.priv.key pub.key master.key \  
  business.staff strategy.team 'executive.level = 7' \  
  'office = 2362' 'hire.date = 'date +%s'  
  
$ cpabe-enc pub.key security_report.pdf  
  (sysadmin and (hire.date < 946702800 or security.team)) or  
  (business.staff and 2 of (executive.level >= 5, audit.group, strategy.team))
```

**Table 1.** The symbol descriptions of cloud CP-ABE

Symbol	Description
KGC	Key generation center
SP	Security proxy
SA	Security attribute
EXPIRATION	Expiration attribute
PK	Public key
MK	Main key
SK	Private key
U	Attribute set
M	User data
CT	Cipher text

## 5 Conclusion

In this system, a new framework called CP-ABE proposed. It is the first system to have an energy proficient effective searching method over encrypted information in a mobile cloud. Initially here previous encryption searching mechanism has been compared with the proposed system. The disadvantages in existing and the reason to go for proposed system is detailed. Also effective execution of search method by keyword is done. The proposed method have the following: (i) By specifying fine grained access policy on the user, the authorized user can have search capability. (ii) the encryption can be done on the cloud without compromising information privacy.

The demonstration of CP-ABE about the security showed it is beneficial to have computations on mobile cloud computing. CP-ABE saves time and energy compared to the conventional system. Multi-keyword search method on the information encrypted is executed to have convenient document recovery.

## References

1. Vaquero, L., Roderer-Merino, L., Caceres, J., Lindner, M.: A break in the clouds: towards a cloud definition. *ACM SIGCOMM Comput. Commun. Rev.* **39**(1), 50–55 (2008)
2. Yu, X., Wen, Q.: Design of security solution to mobile cloud storage. In: *Knowledge Discovery and Data Mining*, pp. 255–263. Springer, Heidelberg (2012)
3. Huang, D.: Mobile cloud computing. In: *IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter* (2011)
4. Mazhelis, O., Fazekas, G., Tyrvaenen, P.: Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage. In: *2012 IEEE 5th International Conference on Cloud Computing (CLOUD)*, pp. 646–653. IEEE (2012)
5. Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J., Jahanian, F.: Virtualized in-cloud security services for mobile devices. In: *Proceedings of the First Workshop on Virtualization in Mobile Computing*, pp. 31–35. ACM (2008)

6. Oberheide, J., Jahanian, F.: When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments. In: Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, pp. 43–48. ACM (2010)
7. Moffat, A., Bell, T.: Managing Gigabytes: Compressing and Indexing Documents and Images. Morgan Kaufmann Publishers, San Francisco (1999)
8. Song, D., Wagner, D., Perrig, A.: Practical techniques for searches on encrypted data. In: Proceedings 2000 IEEE Symposium on Security and Privacy, 2000. S&P 2000, pp. 44–55. IEEE (2000)
9. Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Advances in Cryptology Eurocrypt 2004, pp. 506–522. Springer, Heidelberg (2004)
10. Curtmola, R., Garay, J., Kamara, S., Ostrovsky, R.: Searchable symmetric encryption: improved definitions and efficient constructions. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 79–88. ACM (2006)
11. Chang, Y., Mitzenmacher, M.: Privacy preserving keyword searches on remote encrypted data. In: Applied Cryptography and Network Security, pp. 391–421. Springer, Heidelberg (2005)
12. Zerr, S., Olmedilla, D., Nejd, W., Siberski, W.: Zerber +r: top k retrieval from a confidential index. In: Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology, pp. 439–449. ACM (2009)
13. Wang, C., Cao, N., Ren, K., Lou, W.: Enabling secure and efficient ranked keyword search over outsourced cloud data. *IEEE Trans. Parallel Distrib. Syst.* **23**(8), 1467–1479 (2012)
14. Wang, C., Cao, N., Li, J., Ren, K., Lou, W.: Secure ranked keyword search over encrypted cloud data. In: 2010 IEEE 30th International Conference on Distributed Computing Systems (ICDCS), pp. 253–262. IEEE (2010)
15. Cao, N., Wang, C., Li, M., Ren, K., Lou, W.: Privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE Trans. Parallel Distrib. Syst.* **25**(1), 222–233 (2014)
16. Wang, B., Yu, S., Lou, W., Hou, Y.: Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. In: INFOCOM, 2014 Proceedings IEEE (2014)



# An Adaptive Thresholding Approach Based on Improved Harris Corner Detection for Estimation of Built up Region from Remote Sensing Images

N. M. Basavaraju<sup>1(✉)</sup>, T. Shreekanth<sup>2</sup>, and L. Vedavathi<sup>3</sup>

<sup>1</sup> Department of Electronics and Communication, Sri Jayachamarajendra College of Engineering, Mysore 570006, Karnataka, India  
basavaraju.nm880@gmail.com

<sup>2</sup> L&T Technology Services, Mysore, Karnataka, India  
speak2shree@gmail.com

<sup>3</sup> Department of Electronics and Communication, JSS Polytechnic for Women's, Mysore 570006, Karnataka, India  
ecveda@gmail.com

**Abstract.** This paper proposes an approach to estimate the possible built-up areas from high-resolution remote sensing images covering different scenes for monitoring the built-up areas within limited time and minimal cost. The motivation behind this work is that the frequently recurring patterns or repeated textures corresponding to common objects of interest (e.g., built-up areas) in the input image data can help in discriminating the built-up areas from others. The proposed method consists of two steps. First step involves extracting a large set of corners from the input image by employing an improved Harris Corner detector. The improved Harris Corner selects the local maxima from the extracted corners by performing the gray scale morphological dilation operation. It then finds those points in the corner strength image that matches the dilated image and is greater than the threshold value. In the second step, an adaptive global thresholding is applied to the corner response image and binary morphological operations are performed to obtain the candidate regions. Experimental results show that the proposed approach outperforms the existing algorithms in the literature in terms of detection accuracy.

**Keywords:** Harris corner · Spectrum clustering · Global thresholding

## 1 Introduction

Remote sensing technologies play a vital role in sourcing the information in fields like geography, surveillance, city planning etc., It is instrumental in gauging the distribution, evolution and characteristics of built up area and it can be of great help in updating the land maps and draw city Plans. One of the most important steps in Remote sensing Technologies is extraction of the built up Regions/Urbanized regions from the satellite images. Most current techniques that are used to find urbanized areas are based on

texture analysis [5]. The built up area represents both manmade and Natural objects since the texture of the scene is often not clear from that of the natural objects.

While accessing the urban information, it is often seen that there are repeated patterns or textures, which makes it difficult in discriminating the built-up area and the natural objects, hence an unsubstantiated approach was proposed to detect built up regions using high-resolution satellite images. It is often observed that urban areas exhibit a multitude of straight line features. The numerical measurement of these straight lines help in analyzing the measurement of length, orientation and locality [1].

A new segmentation method used on the connected section in images based on syntactic characteristics was proposed which make use of the semantic leveling and range for defining the characteristics. This may result in producing an elaborate effect, a border effect and vagueness in discriminating the object from the background [2].

The mathematical semantic methods are used for the high phantom of data to classify the shadowy data with high altitudinal resolution to investigate the urban areas. This approach helps in bringing the transformations in isolation of the bright and dark structures in the images which means that the images are brighter or darker than the adjacent features in the images. The two high semantic urban datasets are further classified and used for visual network and are compared with other methods of numerical components and feature extractions [3]. The high resolution satellite images provide vital information to the remote sensing devices in monitoring the urban regions. Hence these high resolution aerial satellite images helps in optimum results and was tested on various three dimensional aeriels and Satellite image data set [6].

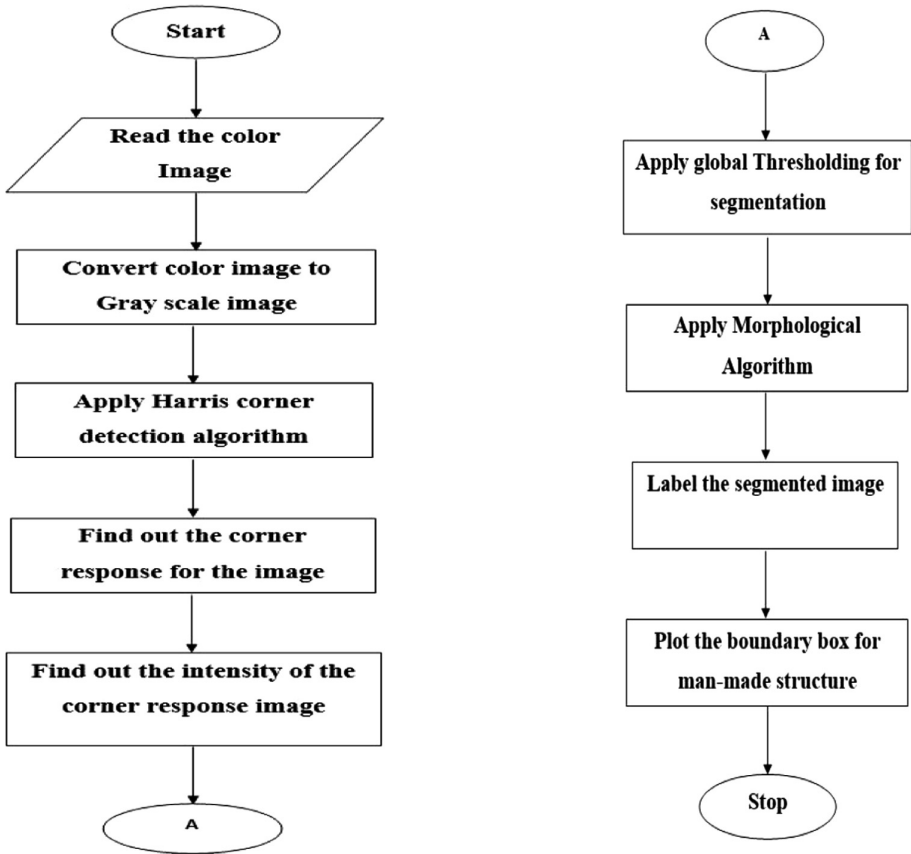
The challenges of detecting the built-up area images is hence proposed through high resolution satellite images under the perception that the built up areas often detected through these images can be measured by the geometrical structures [7, 8]. This method proposes a systematic beginning through this approach for gauging the built up area estimation.

This work proposes a use of adaptive global thresholding approach for built-up area estimation. The remainder of this article is segmented into different sections: Sect. 2 discusses about the proposed method and its step by step implementation process, Sect. 3 provides the discussion about the results obtained and Sect. 4 provides the conclusion about the present work and the scope for future enhancements.

## 2 Proposed Method

This work proposes a framework towards discovering built-up regions from high-resolution satellite images. The process flow of the proposed method is depicted in Fig. 1. The proposed method have two components:

1. A likelihood function based method to extract candidate built-up regions in which an upgraded Harris corner detection operation is proposed.
2. Adaptive global Thresholding based algorithm for the Built-up area detection.



**Fig. 1.** Flowchart

**Step-1.** In the first step, the high resolution satellite color image as shown in Fig. 2 is converted to gray scale image as depicted in Fig. 3. The conversion of color image to gray scale image is done using the expression (1):

$$0.2989 * R + 0.5870 * G + 0.1140 * B \quad (1)$$

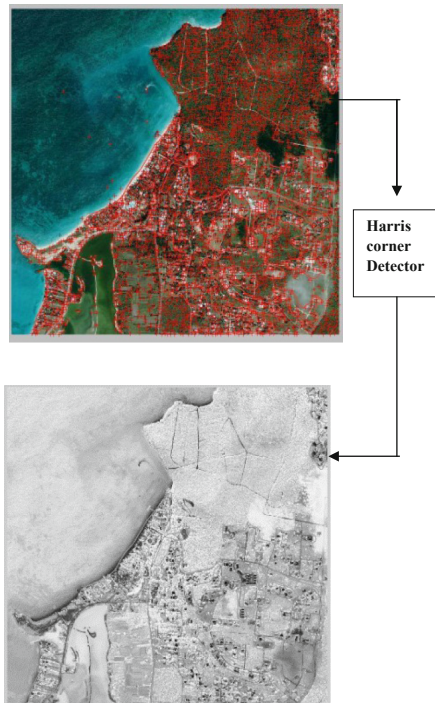


**Fig. 2.** Original image



**Fig. 3.** Gray scale image

**Step-2.** Figure 4 is an example of Corner detector on the gray scale converted image and the symbol '+' defines the corners detected. Harris Corner Detector is based on the autocorrelation of image gradient values or image intensity values. The gradient covariance matrix is given by:



**Fig. 4.** Corner detection by Harris Corner detection

$$G_{x,y} = \begin{bmatrix} (\frac{\partial I}{\partial x})^2 & \frac{\partial I}{\partial x} \frac{\partial I}{\partial y} \\ \frac{\partial I}{\partial y} \frac{\partial I}{\partial x} & (\frac{\partial I}{\partial y})^2 \end{bmatrix} = \begin{bmatrix} I_x^2 & I_x I_y \\ I_x I_y & I_y^2 \end{bmatrix}$$

Where  $I_a$  and  $I_b$  denote the image gradients in the a and b directions. Harris Corner Detector considers the minimum and maximum Eigen values,  $\alpha$  and  $\beta$ , of the image gradient covariance matrix  $G_{a,b}$  in developing corner detector. A ‘corner’ is said to occur when the two Eigen values are large and similar in magnitude. Harris devises a measure using the determinant and trace of the gradient covariance matrix.

The steps involved in the Harris corner detection algorithm are described below:

1. Compute a and b derivative of image  $I_a = G\sigma^a * I$   $I_b = G\sigma^b * I$
2. Compute products of derivatives at every pixel

$$I_{a2} = I_a \cdot I_a \quad I_{b2} = I_b \cdot I_b \quad I_{ab} = I_a \cdot I_b$$

3. Compute the sums of the products of derivatives at each pixel

$$S_{x2} = G\sigma * I_{x2} \quad S_{y2} = G\sigma * I_{y2} \quad S_{xy} = G\sigma * I_{xy}$$

4. Define at each pixel (x,y) the matrix  $H(a, b) = \begin{bmatrix} S_{a2}(a, b) & S_{ab}(a, b) \\ S_{ab}(a, b) & S_{b2}(a, b) \end{bmatrix}$
5. Compute the response of the detector at each pixel

$$a. R = \text{Det}(H) - k(\text{Trace}(H))^2$$



**Fig. 5.** Corner response



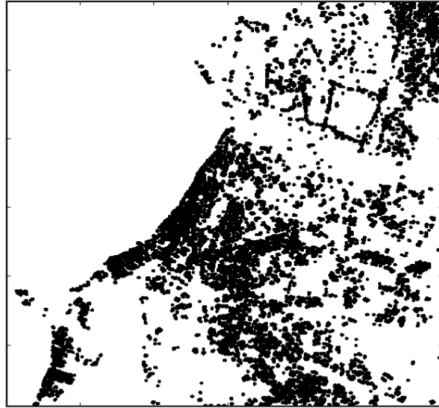


Fig. 6. Adaptive global thresholding binary image

Harris corner detector is a mathematical approach for defining which case holds. First consider the measure of corner response  $R$  as shown in Fig. 5, which is required to be a function of  $A$  and  $P$  alone, on grounds of rotational invariance [4]. It is attractive to use  $\text{Tr}(M)$  and  $\text{Det}(M)$  in the formulation, as this avoids the over eigen value decomposition.

Grouping the Built up regions using spectral cluster is used to solve the grouping problem. Spectral clustering algorithm can be used [10].

Typically adaptive thresholding takes a gray scale or color image as input operation and produces an output in a binary image. It represents the segmentation. Each pixel in the image, a threshold has to be calculated [9]. Binarization Processing is the simplest method of image segmentation converting gray scale image to binary image.

The Global Thresholding algorithms have following steps.

1. Selecting an initial estimate for the global threshold,  $T$ .
2. Segmenting the image using which will produce two group of pixels  $G_1$  consisting of all pixels with intensity values  $>T$ , and  $G_2$  consisting of all pixels with values  $>T$ .
3. Calculating the mean intensity values  $m_1$  and  $m_2$  for pixels in  $G_1$  and  $G_2$
4. Compute a new threshold value:  $T = 1/2(m_1 + m_2)$ .
5. Repeat steps 2–4 until the mean values and in successive iterations do not change.

The field of scientific morphology contributes a wide-range of operators to image processing, all concepts are taken from set theory. The operators can be useful for edge detection, noise removal, image enhancement and image segmentation and analysis of binary images. Morphological techniques image itself is a structuring element. Hence the structuring element is positioned at all possible locations (Fig. 5).

Morphological opening is carried out on the threshold binary image to remove false positive urban areas, and owing to the fact that urbanized areas have high concentration of corners; the opening enhances the clustering and groups the built-up areas together. Figure 6 shows the morphological opening applied on the threshold binary image. Figure 7 shows the grouping based on the opened binary image.



Fig. 7. Adaptive global thresholding method output

### 3 Results and Discussion

The proposed method has been evaluated on the dataset consisting of five high resolution remote sensing images with varied spatial resolution. The performance parameter considered is the number of segments and the area of segments. The performance comparison of the proposed method is done with the Otsu thresholding and Graph cut method. In order to compare the system performance, built-up regions in the original image are marked manually and are compared against the system output. The results of the proposed method, Otsu thresholding and Graph cut method are indicated for few randomly selected images from the dataset. Figure 8, shows the randomly selected original image from the dataset, Fig. 9 shows the manually marked built-up areas, Figs. 10, 11 and 12 depicts the output of proposed, Graph cut and Otsu method respectively. Further Figs. 13, 14 and 15 indicate that the difference between the manually marked images and the output obtained from the adaptive threshold method on the corresponding panchromatic satellite image is negligible. Table 1 compares the segmentation of proposed method with competing methods, such as graph cut and OTSU.

First row against each method in the Table 1 indicates the number of segments and the second row indicate pixel count corresponding to built-up region. It is observed from the result and images of Table 1 that the proposed method is considerably accurate, and is able to segment built-up areas well. In doing the comparison, a



Fig. 8. Original image: random sample 1



Fig. 11. Segmented image of the graph-cut method

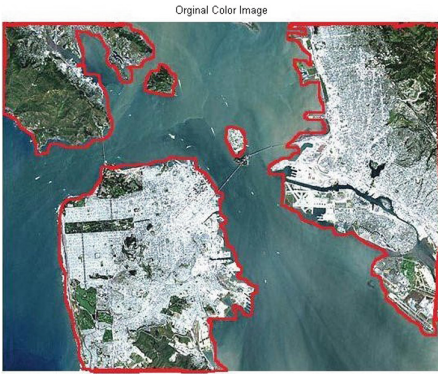


Fig. 9. Manually marked built-up regions of Fig. 8

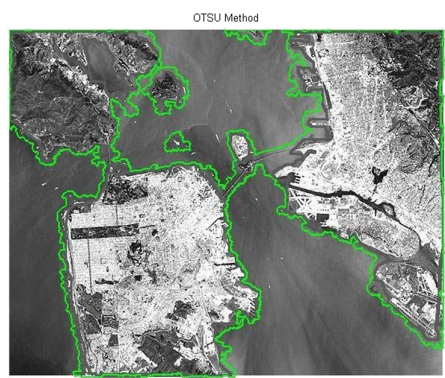


Fig. 12. Segmented image of the Otsu method

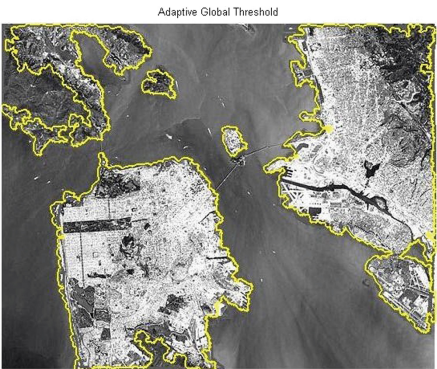


Fig. 10. Segmented image of the proposed method



Fig. 13. Manually marked built-up regions: random sample 2

quantitative measure of the number of segments deciphered by the newly proposed method and manual method has been used. It is observed that the proposed method results are visually more accurate. While the proposed method is robust in most scenarios, it produces false positives, in cases where there are prominent corner features in natural habitat, such as the “forest road” areas as depicted in Fig. 7.



Fig. 14. Manually marked areas vs. Areas marked using proposed method for random sample 2



Fig. 15. Manually marked areas vs. Areas marked using proposed method for random sample 3

Table 1. Performance comparison

Algorithm/Data	1	2	3	4	5
Manual marked image	5	3	7	2	1
	122647	17544	81244	84657	887036
Graph cut	3	5	2	2	1
	144699	36738	111558	109597	887253
Otsu method	3	2	1	1	1
	141892	120637	145787	122773	816632
Proposed	5	5	6	2	1
	120930	21472	82895	90661	823307

## 4 Conclusion

This work presents a framework for estimating the built-up regions from satellite images. The proposed method includes two major components, first being a likelihood-function to extract candidate built-up regions, in which an improved Harris operation is proposed, and the second being adaptive Global-Thresholding based algorithm for the final built-up area detection. Based on the results obtained, the proposed approach demonstrates increased accuracy when compared to the existing works in the literature. Future work in this direction is to improve the detection using machine-learning classification models, which would not only allow segmenting the urban areas in a much cleaner way, but also allow reading the city texture in a much detailed way.

## References

1. Ünsalan, C., Boyer, K.L.: Classifying land development in high resolution panchromatic satellite images using straight-line statistics. *IEEE Trans. Geosci. Remote Sens.* **42**(4), 907–919 (2004)
2. Pesaresi, M., Benediktsson, J.A.: A new approach for the morphological segmentation of high-resolution satellite imagery. *IEEE Trans. Geosci. Remote Sens.* **39**(2), 309–320 (2001)
3. Benediktsson, J.A., Palmason, J.A., Sveinsson, J.R.: Classification of hyperspectral data from built-up areas based on extended morphological profiles. *IEEE Trans. Geosci. Remote Sens.* **43**(3), 480–491 (2005)
4. Pesaresi, M., Gerhardinger, A., Kayitakire, F.: A robust built-up area presence index by anisotropic rotation-invariant textural measure. *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.* **1**(3), 180–192 (2008)
5. Sirmacek, B., Ünsalan, C.: Built-up-area and building detection using SIFT keypoints and graph theory. *IEEE Trans. Geosci. Remote Sens.* **47**(4), 1156–1167 (2009)
6. Sirmacek, B., Ünsalan, C.: Built-up area detection using local feature points and spatial voting. *IEEE Geosci. Remote Sens. Lett.* **7**(1), 146–150 (2010)
7. Harris, C.G., Stephens, M.: A combined corner and edge detector. In: *Proceedings of 4th Alley Vision Conference*, pp. 147–151 (1988)
8. Fonte, L.M., Gautama, S., Philips, W., Goeman, W.: Evaluating corner detectors for the extraction of man-made structures in urban areas. In: *Proceedings of IEEE Conference IGARSS*, pp. 237–240 (2005)
9. Sezgin, M., Sankur, B.: Survey over image thresholding techniques and quantitative performance evaluation. *J. Electron. Imag.* **13**(1), 146–165 (2003)
10. Luxburg, U., Planck, M.: A tutorial on spectral clustering. *J. Stat. Comput.* **17**(4), 395–416 (2007)



# Sentiment Classification Using Recurrent Neural Network

Kavita Moholkar<sup>(✉)</sup>, Krupa Rathod<sup>(✉)</sup>, Krishna Rathod<sup>(✉)</sup>,  
Mritunjay Tomar<sup>(✉)</sup>, and Shashwat Rai<sup>(✉)</sup>

Department of Computer Engineering,  
JSPM's Rajarshi Shahu College of Engineering, Pune, India  
kavita.moholkar@gmail.com,  
krupa.rathod13011998@gmail.com,  
rathod.krish1301@gmail.com, mritunjai88@gmail.com,  
raishashwat3@gmail.com

**Abstract.** Sentiment basically represents a person's attitude, expressing thoughts or an expression triggered by a feeling. Sentiment analysis is the study of sentiments on a given piece of text. Users can express their sentiment/thoughts on internet which may have impact on the user reading it [7]. This expressed sentiment are usually available in unstructured format which needs to be converted. Sentiment analysis is referred to as organizing text into a structured format [7]. The challenge for sentiment analysis is insufficient labelled information, this can be overcome by using machine learning algorithms. Therefore, to perform sentiment analysis we have employed Deep Neural Network.

**Keywords:** Sentiment analysis: sentiment polarity · Deep Neural Networks · RNN · LSTM

## 1 Introduction

Sentiment refers to Attitude, Thoughts, or judgement Triggered by a feeling through a text/of the person [8]. In Sentiment analysis Basically opinion mining is done Which is used to study sentiments on certain entities [8]. Sentiment polarities categorization is a major/fundamental problem in Sentiment analysis. Internet is a resource to get sentiment information. The main problem in sentiment classification is to categorize text into a specific polarity. People can post their sentiments, feelings through various social media sites, forums [8]. Almost in every Social and Business Domains sentiment analysis are in use because people's perspective is a very important aspect.

One of the Major Techniques in Natural language Processing is Sentiment Classification (NLP) applied in many Fields like Movie Review, stock analysis, Election analysis etc. [3] for analyzing the contents of the text i.e. if they are positive or negative [3]. Sentiment analysis can also be applied on twitter data to determine the overall sentiment of the post. MNCs and brands use sentiment analysis to analyze brand reputation across different platforms. Neural Networks are used for finding labels of sentiments by their ability to learn through test data set. The sentiments can be in the form of sentence-level or paragraph-level.

Sentiment analysis is computationally identifying and categorizing opinions expressed in a piece of text [8]. Sentiment Analysis must be able to Determine and Express the direction of data [8]. Typically, text classification includes sentiment analysis. The expression of the data maybe positive, negative, Neutral, Non-Neutral, thumbs up, thumbs down, etc. [7]. Sentiments contains wide variety of varied values. Neural networks are used and implemented in sentiment analysis to compute the belongingness of labels [7].

Deep Learning is a part of machine learning methods. Machine learning is a technique in computer science which allows data to drive and guide the execution of algorithm [10]. Using a training dataset, the algorithm develops a model which is used to compare against the expected output [10]. Algorithms that uses deep learning go through much the same process. Each hierarchy applies a transformation on the training input and forms it as a model [10]. This process is repeated until output has reached and an acceptable level of accuracy [10]. Learning can be supervised, unsupervised and semi-supervised [8]. Deep Learning includes many deep neural networks, some of them are CNN (Convolutional Neural Network), RNN (Recurrent Neural Network), Recursive Neural Network [7]. These networks are basically algorithms.

Among these techniques, Recurrent Neural Network can handle such sequences better because RNN's uses memory and can take context sequence into account. Recurrent Neural Network (RNN) is a network that remembers its input, due to internal memory, which enables them to predict very precisely [9]. Unfortunately, the problem with RNN's are that during training When Long texts Sequence are taken as an input then the Components of gradient vector can vanish.

LSTM is an addition to features of RNN [9]. It basically extends their memory of RNN's. LSTM's are capable of Providing long term Reliance's [8]. Therefore, LSTM's can be used to learn from experiences that have long lags in between. LSTM's are explicitly designed to avoid long term dependencies. Remembering information for a longer if their default behavior. Therefore, Long-Short Term Memory can be used to predict the labels for unlabeled data.

Convolutional Neural Network is a neural network made from group of neurons. It has learnable weights and biases [8]. In CNN, each neuron receives some input. These inputs are in the form vector magnitude. It will then perform the dot product on the received input and follows non-linearity.

## 2 Related Work

For detecting the presence of cardiac arrhythmia [1]. Recurrence neural network is used to diagnose whether arrhythmia is present or not. This can be done by classifying ECG signals [1]. Deep learning techniques like Convolutional Neural Network, Recurrent Neural Network, Long-Short Term Memory-Recurrent Neural Network are used to detect the presence of arrhythmia [1]. RNN for classifying the relation in clinical notes [2]. RNN finds the sequential relation between data and accordingly classifies the data [2]. Here data can be in the form of text, image or longitudinal data [2]. Sentiment classification aims on recognizing sentiment labels in a document [3]. LSTM is a type of recurrent neural network which handles the problem of gradient diffusion and

explosion [3]. It also deals with exploiting the relation between sentences in document level sentiment classification [3]. A technique called RNN-RTs is used to accommodate flood-based prediction [4]. Based on past rainfall and flood conditions, conclusions are drawn [4]. Recurrent Neural Network is used to predict the rainfall that can occur in future. Regression techniques are then used to determine number of human and animal deaths that can occur because of rainfall [4].

Workload in cloud datacenters can be predicted using LSTM-RNN [5]. First step involves prediction of workload [5]. Then further LSTM-RNN technique is used to predict future workload and check if they systems will be capable enough to handle the workload or scale the systems [5]. Activity reorganization and abnormal behavior detection can be done using RNN [6]. The first comprises of slicing the raw data collected via sensors into segments using sliding window approach [6]. Then certain feature and patterns are identified from the data and RNNs are trained to recognize daily activities and normal behavior [6]. The trained model is then used to detect the deviation in normal behavior [6]. Sentiment analysis can be done using deep learning techniques [16]. The main challenge in sentiment classification is lack of labelled data [16]. Different deep learning techniques like deep neural network, convolution neural network, recurrent neural network is used to overcome the problems like cross lingual problems, sentiment classification, textual analysis and visual analysis [16].

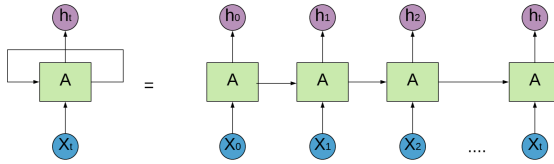
### 3 Literature Review

Our Central problem in sentiment analysis is categorization of sentiment polarity. Given a piece of written text, major problem arises in finding the sentimental polarity of the text i.e. positive, negative or neutral. Sentiment Analysis is one of the most used techniques in NLP and in domains like stock analysis, e-commerce etc. for analyzing the contents of the text or documents.

Sentiment classification tasks can be done by implementing many Deep Neural Networks like Recurrent Neural Network (RNN), Convolutional Neural Network (CNN), Recursive Neural Network (RNN) and Deep Belief Network (DBN). This section describes how Neural networks can be implemented for Recurrent Neural Networks.

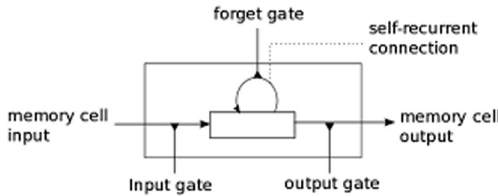
The idea behind Recurrent Neural Network is to make use of sequential information. In a traditional neural network, we assume that all inputs are independent to each other. But if we need to predict the next word, we need to know which words have come before it. RNN's perform tasks in sequential manner, that is it performs the same task in sequential manner. The input of next layer is dependent on previous layer output. Another way to think about RNNs is that they have memory which stores information about previous layers. There is a hidden layer present in Recurrent Networks which is used as memory of the network. This hidden layer captures information about what has happened in previous states. Unlike traditional feed forward network RNN shares the same parameters across all the states. This reduces the number of parameters required to train a model. This reflects that we are performing the same task in each step. The Fig. 1 shows the working of basic RNN.





**Fig. 1.** Basic RNN

The most common type of RNN is Long-Short Term Memory (LSTM), which is much better in capturing long-term dependencies than simple RNNs. LSTMs are essentially the same thing as RNN but they have a different way of computation for the hidden state. The LSTM layer comprises of memory which is known as LSTM cell that takes in account the previous state and current input. Figure 2 shows a basic LSTM gate.



**Fig. 2.** Basic LSTM

Training an RNN is similar to training a feed forward neural network because the parameters are shared among all the steps in the network.

## 4 Proposed System

The data set used for the proposed system is IMDB movie dataset. **This dataset** contains reviews of 14,762 movies. The dataset is preprocessed and encoded using word2Vec embedding. Word2Vec model converts the words in sentence into embedding matrix placing words in same context together. In any language the meaning of words depends on the word before and after it. RNN helps to cater to this need. Let's consider an example

“The movie was boring”

$x_0 \ x_1 \ x_2 \ x_3$

$t = 0 \ t = 1 \ t = 2 \ t = 3$

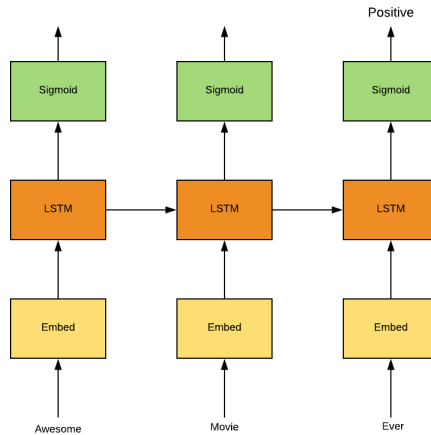
Hidden state vector  $h_t$  is associated with each time step.

$$h_t = \sigma(W^H h_{t-1} + W^X x_t)$$

$$\sigma(x) = \frac{1}{1 + e^{-x}}$$

$x_t \rightarrow$  vector  $x$  containing information of specific word  
 $h_t \rightarrow$  vector containing information of previous step  
 $w \rightarrow$  weight metrics

Activation function used is sigmoid. The hidden vector contains the summary of the sentence. Back propagation through time optimizes the weight metrics.



**Fig. 3.** Proposed system

The Fig. 3 shows the proposed system for sentiment classification using RNN deep neural network. Long Short-Term Memory (LSTM) cells receive representations from the embedding layer. Long-range dependencies for sentiment analysis are modeled through LSTM. It adds input, output and forget gates to a recurrent cell thereby adding recurrent connections to the network to include information about the sequence of words in the data. For the  $t$ -th word in a sentence, the LSTM takes as input the word embedding  $x_t$ , the previous output  $h_{t-1}$ , and cell state  $c_{t-1}$  and computes the next output  $h_t$  and cell state  $c_t$ . Both  $h$  and  $c$  are initialized with zeros. With each time step a hidden state vector  $h_t$  encapsulates and reviews all of the information from the previous time steps. The current state is given by  $h_t$  and output by  $y_t$ :

In this model,  $\sigma$  is the sigmoid activation function,  $\tanh$  the hyperbolic tangent activation function,  $x_t$  the input at time  $t$ ,  $W_i$ ,  $W_C$ ,  $W_f$ ,  $W_o$ ,  $U_i$ ,  $U_C$ ,  $U_f$ ,  $U_o$  are weight matrices to regulate the input and  $b_i$ ,  $b_C$ ,  $b_f$ ,  $b_o$  are bias vectors. For the  $t_{th}$  word in the sentence, the LSTM takes as input the word embedding  $x_t$ , the previous output  $h_{t-1}$  and cell state  $c_{t-1}$  and computes the next output  $h_t$  and cell state  $c_t$ . Both  $h$  and  $c$  are initialized with zeros. Back-propagation, an optimization process used for updating the weight matrices with the time.

The hidden state vector at the final time step is fed into a binary softmax classifier through LSTM layer. The softmax classifier multiplies the hidden state vector with another weight matrix and output is fed to a softmax function which produces values between 0 and 1 probabilities. The learning rate is set to default 0.001. Adam optimizer is used for optimization.

## 5 Challenges

The system has few challenges that need to be addressed.

1. When similar words are encountered, it can be treated as either Subjective or Objective depending upon the context in which it is said, thus it becomes difficult to identify only the subjective portions of text.
2. Meaning of sentence change with respect to domain.
3. Difficult to identify Sarcastic sentences.
4. Order of words are important
5. Internationalization.

## 6 Applications of Sentiment Analysis

Few applications of the system are

1. Analysis of website reviews
2. Business Intelligence
3. Cross Domain application like medical, sociology
4. Smart homes

## 7 Conclusions

Sentiment analysis or Emotion AI is an Area of study where people's sentiments, their attitudes, thoughts, their views or emotions towards certain entities are analyzed and on basis of it Predictions are made. Sentiment analysis is implemented using different deep learning techniques. Basic Problems of sentiment analysis, sentiment polarity categorization using Deep Neural Networks is tackle in the paper. Sentiment classification helps to classify text according to labels associated with sentiments, e.g., favorable or unfavorable, positive or negative. Sentiment Analysis analyses texts, like posts and reviews, uploaded by users on social media like twitter, Facebook etc., forums, like Quora and electronic businesses, regarding the reviews they have about a product or service. Depending on the dataset, Sentiments can be classified into binary classes or multi-class problem. Binary class problems can be either positive or negative and multi class problems can 3 or more classes.

## References

1. Swapna, G., Soman, K.P., VinayKumar, R.: Automated detection of cardiac arrhythmia using deep learning techniques. *Procedia Comput. Sci.* **132**, 1192–1201 (2018)
2. Luo, Y.: Recurrent neural network for classifying relations in clinical notes. *J. Biomed. Informat.* **72**, 85–95 (2017)

3. Rao, G., Huang, W., Feng, Z., Cong, Q.: LSTM with sentence representation for document-level sentiment classification. *Neurocomputing* **208**, 49–57 (2018)
4. Khosla, E., Ramesh, D., Sharma, P.P., Nyakotey, S.: RNN's-RT: flood based prediction of Human and animal deaths in Bihar using recurrent neural networks and regression techniques. *Procedia Comput. Sci.* **132**, 486–497 (2018)
5. Kumar, J., Goomer, R., Singh, A.K.: Long short-term memory recurrent neural network (LSTM-RNN) based workload forecasting model for cloud datacenters. *Procedia Comput. Sci.* **12**, 676–682 (2018)
6. Arifoglu, D., Bouchachia, A.: Activity recognition and abnormal behavior detection with recurrent neural networks. In: *The 14th International Conference on Mobile Systems and Pervasive Computing*
7. Ain, Q.T., Ali, M., Riaz, A., Noureen, A., Kamran, M., Hayat, B., Rehman, A.: Sentiment analysis using deep learning techniques: A review. *IJACSA* **8**(6), 424 (2017)
8. <https://towardsdatascience.com/recurrent-neural-networks-and-lstm-4b601dd822a5>
9. <https://searchenterpriseai.techtarget.com/definition/deep-learning-deep-neural-network>
10. Islam, J., Zhang, Y.: Visual sentiment analysis for social images using transfer learning approach. In: *2016 IEEE International Conference on Big Data Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing Communications*, pp. 124–130 (2016)
11. Ouyang, X., Zhou, P., Li, C.H., Liu, L.: Sentiment analysis using convolutional neural network. In: *2015 IEEE International Conference on Computer and Information Technology Ubiquitous Computing and Communications Dependable, Autonomic Secure Computing Pervasive Intelligence Computing (CIT/IUCC/DASC/PICOM)*, pp. 2359–2364 (2015)
12. Silhavy, R., Senkerik, R., Oplatkova, Z.K., Silhavy, P., Prokopova, Z.: Artificial intelligence perspectives in intelligent systems. In: *Proceedings of the 5th Computer Science On-line Conference 2016 (CSOC2016)*, vol 1, *Advances in Intelligent Systems and Computing*, vol. 464, pp. 249–261 (2016)
13. Vateekul, P., Koomsubha, T.: A study of sentiment analysis using deep learning techniques on Thai Twitter Data (2016)
14. Yanagimoto, H., Shimada, M., Yoshimura, A.: Document similarity estimation for sentiment analysis using neural network. In: *2013 IEEE/ACIS 12th International Conference on Computer and Information Science*, pp. 105–110 (2013)
15. Ain, Q.T., Ali, M., Riaz, A., Noureen, A., Kamran, M., Hayat, B., Rehman, A.: Sentiment analysis using deep learning techniques: a review.
16. Pang, B., Lee, L.: A sentimental education: sentiment analysis using subjectivity summarization based on minimum cuts. In: *42nd Meeting of the Association for Computational Linguistics (ACL 2004)*, 271–278 (2004)
17. Luo, Z., Osborne, M., Wang, T.: An effective approach to tweets opinion retrieval. *World Wide Web* (2013). <https://doi.org/10.1007/s11280-013-0268-7>
18. Socher, R., et al.: Recursive deep models for semantic compositionality over a sentiment Treebank. In: *Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP)* (2013)
19. Taboada, M., Brooke, J., Tofiloski, M., Voll, K., Stede, M.: Lexiconbased methods for sentiment analysis. *Comput. linguis.* **37**(2), 267–307 (2011)
20. Wan, X.: A comparative study of cross-lingual sentiment classification. In: *Proceedings of the The 2012 IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technology-Volume 01* (pp. 24–31). IEEE Computer Society (2012)
21. Bollegala, D., Weir, D., Carroll, J.: Cross-Domain Sentiment Classification using a Sentiment Sensitive Thesaurus. *IEEE Trans. Knowl. Data Eng.* **25**(8), 1719–1731 (2013)



# Secure Data Transmission in VANETs Using Efficient Key-Management Techniques

Mahalakshmi Gopalakrishnan<sup>(✉)</sup> and Uma Elangovan

Department of Information Science and Technology, College of Engineering,  
Guindy, Anna University, Chennai, India  
{mahalakshmi, umaramesh}@auist.net

**Abstract.** A Vehicular Adhoc Network (VANET) is a sub-class of Mobile Adhoc Network (MANET) which provides vehicle to vehicle communication and vehicle to infrastructure communication, i.e., between vehicles and Road-Side base stations. The presence of Vehicular technology in the present automotive industry owes to its increasing number of applications with a good resource for the Intelligent Transportation System. The designed system uses the road side unit (RSU) to ensure the originality of the vehicles which is sending messages and also to prevent redundant messages. With large computing power, it stores all information about the vehicle and provides a pseudo id to the vehicle for communication, thereby anonymity is preserved. The RSU verifies the vehicle id, and the freshness of the message is verified by using timestamp. Once the details are verified, it finally broadcast the message to all vehicles and other RSUs that may need the information, thereby arresting redundant messages. Cryptographic algorithm is applied for encryption and decryption of messages, ensuring secure messages.

**Keywords:** VANET · Road Side Unit (RSU) · On-Board-Unit (OBU) · Trusted Authority (TA)

## 1 Introduction

**VANET:** A VANET is the acronym of Vehicular Ad hoc NETWORK, which is a self-organized network of vehicles on roads and other Road Side Units (RSUs). VANET is a wireless technology which is developed on the basis of mobile ad hoc network (MANET). An ad hoc network is a wireless connectivity that consists of individual devices capable of communicating with each other in a direct way. Being a Local Area Network (LAN), which can be formed instantly, it obviates the need to build a main serving access point. A MANET is capable of changing its locations and is characterized by the ability to self-arrange without wires. VANET network enables communication between the other vehicles for sharing vital messages. With the ceaseless increase in vehicular traffic on roads, this translates to the creation of human lifesaving applications. This, coupled with VANETs open access medium, makes the security of information exchange a vital concern in VANETs. A typical VANET environment is shown in Fig. 1.

The applications of VANET are broadly categorized into two, namely, non-safety and safety ones. Non-safety applications include the comfort of drivers and passenger, besides improving the overall management of traffic system. Examples of non-safety applications include finding the nearest filling station, availability of parking lots, and weather information. Safety applications, on the other hand, warrant error-free and secure information. Security is of utmost importance owing to the fact that even the slightest disconnection can be highly problematic to the users. This warrants uninterrupted network availability. Since a malicious/fake node can render the network inaccessible, security is of paramount importance.

While considering the security issues, authenticating the sender node is necessary in a VANET system to avoid impersonation. This indicates that the incoming data are from a legitimate node of the network. The messages sent by the legitimate user should be highly intact so as to ward off the action of an attacker to change the information contained in the message. Privacy of a legitimate node must be protected against any unauthorized node. This results in a reduction in message delay attacks. And moreover, there is need for cryptographic algorithms to ensure a secure communication.

The objective of this work is to deliver integrated, authenticated, and secure messages to vehicles in VANETs. These messages should aid in free flow of traffic by helping drivers to avoid traffic by taking alternate routes and aid in avoiding accidents. While communicating, the identity of the participating vehicle should be preserved, but when needed by authority their real identity should also be obtainable.

The responsibility of disseminating messages to vehicles or other RSUs lies with the roadside unit (RSU). With the help of its stored table, it verifies the identity of the vehicle from which the messages are received, decrypting and checking the integrity of the messages received, after which it encrypts the messages and sends the encrypted message to other vehicles in its region and other RSUs.

The rest of the paper is organized as follows: Sect. 2 describes the existing work relevant to this topic and merits & demerits are analyzed and highlighted. Section 3 discusses the overall system design with detailed module description. Section 4 provides the analysis for obtained results and conclusion with future enhancements of this work is given in Sect. 5.

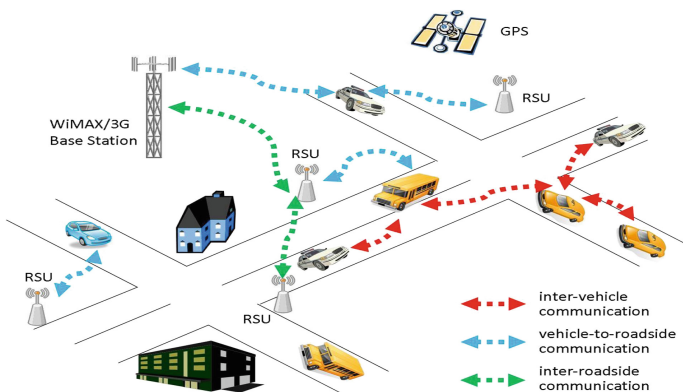


Fig. 1. A typical VANET environment

## 2 Literature Survey

Some works which related with the proposed secure VANET system is discussed in this section. The 802.11p standard specification enables to support wireless or adhoc communication between the vehicle to vehicle and between vehicle to infrastructures to perform the short-duration exchanges required in communication between a high-velocity vehicle and a stationary roadside unit [1]. Known as WAVE (wireless access in vehicle environments), this mode of operation operates in a 5.9-GHz band and support the Dedicated Short Range Communications (DSRC) standard for secure communication of messages between the vehicles and other vehicle applications. DSRC protocol is used for ensuring the safety communication to avoid vehicle crashes [2].

In this work [3], the secure communication for message transmission between the vehicles is providing by using Elliptic Curve Digital Signature Algorithm for message authentication.

VANET required a trustable routing mechanism for secure communication between the vehicles and the between the vehicle and infrastructure. As described in [4] a message fabrication detection approach for Beaconless Routing is proposed. By using this approach the malicious nodes are detected and prevented from interception of packets during transmission.

A secure routing mechanism for vehicular communication is necessary for sharing the information. In [5], a secure position-based routing scheme is proposed in order to improve the network stability.

In order to provide security in vehicular communication, it is necessary to verify the originality of the message and to authorize the vehicles which are sending messages, for which a secure protocol is needed. To authenticate vehicles needs to be authenticated for the receivers [9]. This can be done by having a set of private keys and public keys. If more number of public/private keys is used in vehicles, it is necessary to store the keys in the vehicles OBU which is having limited storage space.

The vehicular communication networks has a unique requirements, in order to fulfill the requirements security protocol based on group signature and identity-based signature scheme was explained in Ref. [10]. Privacy issues with traceability were addressed by this protocol, the identities of vehicles is used for tracing a vehicle for resolving a dispute. Due to increase in the traffic density, the verification of each group signature may result in high computation overhead. A spontaneous privacy-preserving protocol was defined on the basis of revocable ring signature with a feature for authenticating safety messages locally [11]. As a result, this scheme provided unscalable because it makes all to participate in message verification process.

In order to circumvent attacks in the network, authentication of the vehicles needs to be guaranteed. In [12], Identity based authentication framework is proposed with adaptive privacy preservation scheme. The framework proposed in this paper enables reusability. To ensure and provide authentication, the ID-Based Signature (IBS) scheme and the ID-Based Online/Offline Signature (IBOOS) schemes are used.

To reduce the computation burdens involved in verification process of the vehicles, a cooperative message authentication protocol (CMAP) is presented. In this protocol,

vehicles share their verification results with each other in a cooperative way, this greatly reduces the number of safety messages that each vehicle needs to verify [13].

In multi-hop applications a bogus signature may spread out quickly and impact a significant number of vehicles. Selective authentication scheme is used to overcome this problem. Selective authentication scheme works well even under a dynamic topology by providing fast isolation of malicious senders. The consumption of computation resources is only 15%–30% compared to other schemes [14].

An efficient cooperative authentication scheme which greatly eliminates the redundant authentication efforts on the same message send and received by different vehicles, thus reducing authentication overhead on individual vehicles and shorten the authentication delay in [15]. This scheme reduces the authentication efforts of other vehicles' in the future and also reduces its own workload.

### 3 Proposed System

Figure 2 shows the architecture diagram of VANET. This architecture diagram consists of three main modules: Trusted Authority (TA), Road Side Units (RSUs), and On Board Units (OBUs). Trusted authority does not involve much in the communication. Its purpose is to verify and issue certificate. The actual road communication happens mainly between RSU and OBU, and also among vehicles.

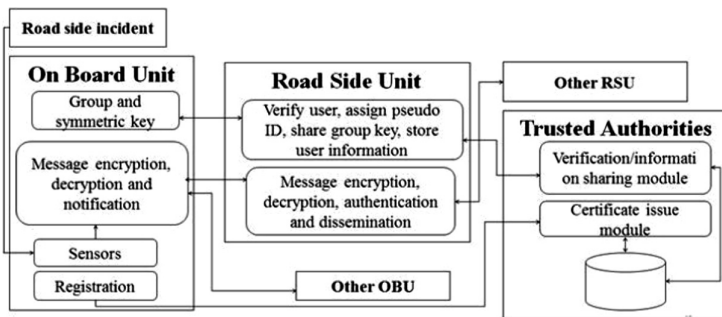


Fig. 2. Architecture diagram of vehicle ad hoc network

The role of TA is to issue the authorization certificate for the vehicles. This certificate issue will happen by checking the private information of the vehicles, this private information is provided by the vehicles at the time of registration with the RSU. So, the TA will maintain all this information for its certificate issuing process and also it will share the secret information with the RSUs when it is required.

The vehicles are equipped with the OBU which is having the central control module, communication module, interface module for human-machine interaction and Position tracking module. Processing of information will be carried out in central control module. The data which is received from other vehicles and the processed data are all stored in memory unit for decision making process.



An OBU installed vehicle often sends its basic information using GPS. A vehicle that has to send messages uses the human-machine interface module. The details are given for general understanding, and this system does not deal with either the hardware parts or how the messages are created in the OBU, but simply assumes a message from the OBU.

The proposed protocol consists of three phases:

Phase 1: Symmetric key and Group Key and Establishment

Phase 2: Vehicle RSU Message sharing for Propagation

Phase 3: RSUs Message verification and Propagation

### **3.1 Key Establishment**

Once a vehicle starts move from one location to another location, which is outside the coverage area of the present RSU, then it is necessary for the vehicle to get connect with the new RSU which is present in the current location of the new coverage area. After the connection is established by the vehicle with the new RSU, the vehicles can start sharing their symmetric key with the current RSU which is present within the coverage area of the vehicle to send an encrypted message using Group key and random ID from the Road Side Unit.

RSU makes use of group key for their message encryption process and sends the encrypted message to the vehicles that are connected with the RSUs.

The pseudo ID is used by the vehicles for all their communications with the RSU which is present within their transmission range.

### **3.2 Vehicle RSU Message Sharing for Propagation**

The message sending process can be occur between the vehicles to RSU only after the key generation process is completed. A vehicle makes use of the symmetric key which is shared between the vehicle and RSU to encrypt the message and also to compute the message digest which it sends.

With the help of the message digest which is send by the vehicles, the RSU can able to verify the authenticity and integrity of the messages.

Consider, the case that vehicle which is sending message to the RSU is not present within the coverage are of the RSU, then we need use the routing protocol to send the message to the nearby RSU through multi-hop nodes.

### **3.3 RSUs Message Verification and Propagation**

The main job of RSU is to verify the originality, authenticity and integrity of the message which has been sent by the vehicles of that are present within the range of transmission with the RSU.

Once after the completion of verification of the message, then it will forward that message to the other RSU and to other vehicles. If, the RSU finds any discrepancy in the message, it will check for the authentication of sender by verifying the details of the sender which is available in a table. These details are given by the sender at the time of registering with the RSU.

### 3.4 System Implementation

Node configuration is defining the different node characteristics before creating them. The Wireless Channel class function is used to deliver packets from a wireless node to the neighboring nodes within its sensing range. The ad hoc routing protocol is DSR Class Mac802.11 has two functions: it uses CSMA/CA channel access mechanism on sending and it adopts a SNR threshold based capture model on receiving. The Drop Tail class maintains a queue which implements FIFO scheduling and drop packets when the queue length exceeds 100. The omni Antenna propagates radio waves symmetrically.

The NAM window opens once the node configuration setup and initialization is completed. The system is implemented by creating 25 nodes. Node 3, green in color, combined acts as TA and RSU. Nodes 0, 1, and 2 shown in color red, chocolate, and pink, respectively, act as three RSUs. The TA-RSU (node 3), RSU1, RSU2, and RSU3 are static nodes; they do not change their position at any point in the simulation. Every RSU covers a certain range. The remaining 21 nodes (4, 5, ..., 24) acts as vehicles. These 21 nodes are dynamic nodes; they change their position over time.

Initially every node scans/sends control messages in its transmission range to identify the neighboring nodes. A vehicular node saves two neighboring nodes id: a preceding node that sends packets and a following node that receives packets. The TA-RSU and other RSUs stores every other RUSs and TA/RSU ids, and those vehicles ids in their covered region.

Once the network is formed, the vehicles are double-circled: blue-colored circle will identify it as vehicle and the other-colored (red, green, chocolate, and pink) circle identify the vehicle with the RSU that it is connected to. In Fig. 4, nodes 4, 5, 6, and 12 (red colored that of node 0) are connected to RSU1; nodes 10 and 11 (green colored that of node 3) are connected to TA-RSU; nodes 7, 9 and 19 (chocolate colored that of node 1) are connected to RSU2; and nodes 8, 13, and 14 (pink colored that of node 2) are connected to RSU3. Nodes 20–24 that are yellow-circled are not in the coverage area of any of the RSU. Nodes 15–18 were at a time in the simulation is connected to some RSU and had two circles, but now it is moving away. Therefore, the one circle that indicates the RSU-color has vanished.

In Fig. 3, source S1 (node 4) sends message to RSU1, and RSU1 verifies the sender and the authenticity and the integrity of the message. Once the verification process completed it sends the message to the destination D1 (node 6). The same procedure is followed for transmitting message from S2 to D2 in the TA-RSU region.

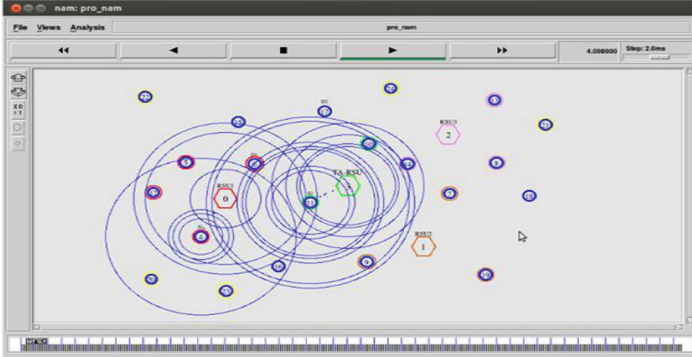


Fig. 3. Single message transmission in the same region.

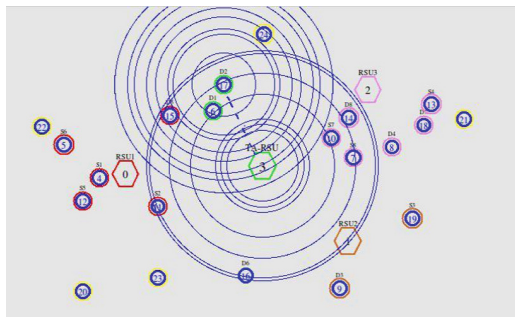


Fig. 4. Single message transmission from a source in one region to a destination in another region.

Figure 4 shows communication from one region to another region, also it shows communication in single region. Vehicles S1, S2, and S6 in RSU1 region send messages to D1 and D2 in TA-RSU region. D6 is not currently connected to any region. The message is held until this vehicle is connected to any RSU. The messages are maintained in queue and transmitted in first-in first-out manner.

## 4 Performance Analysis

The simulated results are stored in the trace file. Using this trace files, delay ratio, loss ratio and throughput can be shown by projecting the results in the graph, by using xgraph.

Figure 5 shows the graph for delay ratio. The x-axis reading is time in millisecond, and the y-axis reading shows the delay ratio. High delay ratio is shown by the red curve which is the existing system. Low delay ratio is shown by the green curve which is the proposed system.

At approximately 0.5 min, the curve of the existing system shows high delay ratio. The curve as suddenly fall and raise cannot give the opportunity for predicting the delay beforehand. Whereas, the proposed system, which shows very low delay ratio, is a steady curve giving an opportunity to predict the future delays.

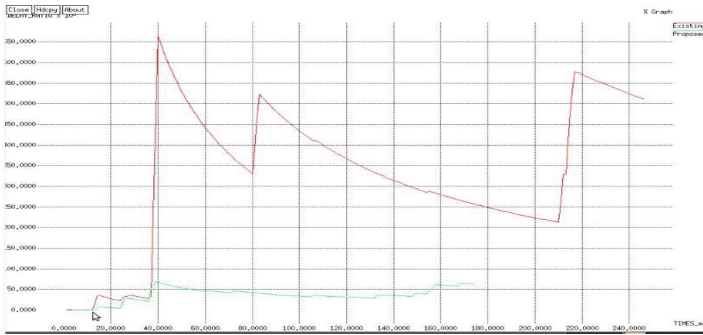


Fig. 5. Delay ratio of messages in the proposed system over existing system.

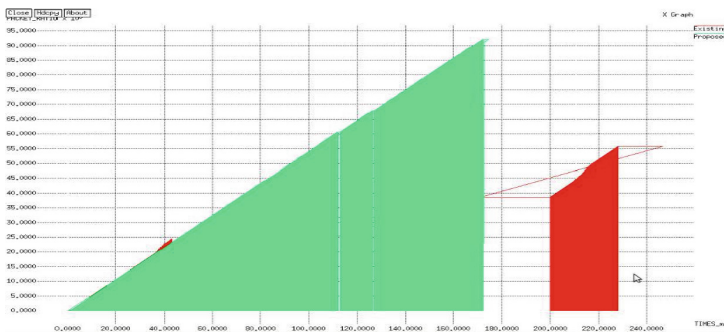


Fig. 6. Throughput of messages in the proposed system over existing system.

Figure 6 shows the graph for throughput. The x-axis reading is time in millisecond, and the y-axis reading shows successful delivery of packets. High throughput is shown by the green bars which is the proposed system. Low throughput is shown by the red bars which is the existing system.

The proposed system from the time of  $t_0$  seconds till the end of simulation at  $t_f$  seconds (here  $f$  represents final) shows a steady throughput, whereas the existing shows an irregularity in throughput. Apart from uneven throughput, at some time  $t_m$  seconds (here  $m$  represents some in between time in the simulation) the existing system produce a very throughput or hardly any throughput.

## 5 Conclusion

VANET is a technology which is used in vehicle to vehicle (V2V) or vehicle to infrastructure communication (V2I) to share the real situations (like road accidents, road condition, weather, security issues) etc., This messages will be sensed by the vehicles which are present in VANET network. The secure transmission system is adopted for message transmission between the vehicles and RSU and RSU to another RSU. The RSU will check the authentication of the sender from which message is sent. Our approach is used to identify and prevent the anonymity of the senders and to provide secure transmission.

In future, this work can extended with more number of nodes and also to improve the efficiency of the message transmission and time efficiency with respect to reaching the destination node.

## References

1. Armstrong, L., Fisher, W.: Status of project IEEE 802.11 task group p: Wireless access in vehicular environments (WAVE). [http://grouper.ieee.org/groups/802/11/reports/tgp\\_update.htm](http://grouper.ieee.org/groups/802/11/reports/tgp_update.htm). Accessed 1 April 2018
2. NHTS Administration. Vehicle safety communications project, final report. Technical report of the U.S. Department of Transportation, April 2006
3. Manvi, S.S., Kakkasageri, M.S., Adiga, D.G.: Message authentication in vehicular ad hoc networks: ECDSA based approach. In: Proceedings of International Conference on Future Computer and Communication, ICFCC 2009, pp. 16–20 (2009)
4. Chhoeun, K., Ayutaya, S.A.: A novel message fabrication detection for beaconless routing in VANETs. In: Proceedings of the International Communication Software and Networks, ICCSN 2009, pp. 453–457 (2009)
5. Harsch, P.P.C., Festag, A.: Secure position-based routing for VANETs. In: Proceedings of the IEEE Vehicular Technology Conference, VTC 2007. IEEE (2007)
6. Aslam, C., Zou, B.: Distributed certificate and application architecture for VANETs. In: Proceedings of IEEE Military Communications Conference, MILCOM 2009, pp. 1–7 (2009)
7. Biswas, S.: Proxy signature-based RSU message broadcasting in VANETs. In: Proceedings of 25th Biennial Symposium Communications, QBSC 2010, pp. 5–9 (2010)
8. Kim, J., Song, J.: A pre-authentication method for secure communications in vehicular ad hoc networks. In: Proceedings of 8th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM, Shanghai, China, September 2012, pp. 1–6 (2012)
9. Raya, M., Hubaux, J.: Securing vehicular ad hoc networks. *J. Comput. Secur.* **15**(1), 39–68 (2007)
10. Lin, X., Sun, X., Ho, P.H., Shen, X.: GSIS: a secure and privacy-preserving protocol for vehicular communications. *IEEE Trans. Veh. Technol.* **56**(6), 3442–3456 (2007)
11. Xiong, H., Beznosov, K., Qin, Z., Ripeanu, M.: Efficient and spontaneous privacy-preserving protocol for secure vehicular communication. In: Proceedings of 2010 IEEE International Conference on Communications, ICC, pp. 1–6 (2010)
12. Lu, H., Li, J., Guizani, M.: A novel id-based authentication framework with adaptive privacy preservation for VANETs. In: Proceedings of Computing, Communications and Applications Conference, ComComAp, Hong Kong, January 2012, pp. 345–350 (2012)

13. Hao, Y., Han, T., Cheng, Y.: A cooperative message authentication protocol in VANETs. In: Proceedings of Global Communications Conference, GLOBECOM, Anaheim, CA, pp. 5562–5566, December 2012. IEEE (2012)
14. Wang, X., Tague, P.: Asia: accelerated secure in-network aggregation in vehicular sensing networks. In: Proceedings of the 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON, pp. 514–522. IEEE (2013)
15. Lin, X., Li, X.: Achieving efficient cooperative message authentication in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **62**(7), 3339–3348 (2013)



# Proof of Shared Ownerships and Construct A Collaborative Cloud Application

S. Ganesh Velu<sup>(✉)</sup>, C. Gopala Krishnan, K. Sivakumar,  
and J. A. Jevin

Department of Computer Science and Engineering,  
Francis Xavier Engineering College, Anna University,  
Tirunelveli, Tamilnadu, India

ganeshvelu4796@gmail.com, skywarekrish@gmail.com,  
shivakumaresan@gmail.com, xaviernega75@gmail.com

**Abstract.** Distributed storage stages guarantee advantageous applications to clients for sharing records and cooperate with coordinated efforts. The main challenge in a shared cloud-based application is the security and privacy of sensitive information stored by a particular user. For instance, Cloud users has the ability to erase documents and disavow them without counselling the alternate cloud associates. To handle this drawback, Proof of Shared belonging (PoSW) is proposed, a particular PoSW is subjected to execute information protection mechanism, confirmation and information reduplication. Furthermore, PoSW tends to utilize the diagonal cryptography equation to ensure the security of the mutual data records in order to provide a common information sharing approval, document ownership, and develop an absolutely particular relation between the document holders. Hence, integrating PoSW into the cloud server assists it to check the common belonging and overcome the data reduplication challenges in the common cloud-based data records.

**Keywords:** Shared possession · Proof of shared possession · Focussed encoding algorithmic rule · Reduplication

## 1 Introduction

Distributed computing is perceived as an effective alternative to hold the rank innovations [1, 2] because of its inborn asset sharing capability and low-support attributes. In distributed computing, the cloud Service Providers (CSPs), like Amazon, can convey fluctuated administrations to cloud clients with the assistance for incredible data focuses. By moving the local data into cloud servers, clients can get delight from fantastic administrations and spare imperative speculations on their local foundations. The unique and ubiquitous administrations offered by cloud providers is data stockpiling license. An organization will allow its employees to store and share records in a common storage platform called the cloud. PoSW enables the cloud applications for employees to securely store and share the sensitive data on the shared platform. In particular, the cloud servers are overseen by cloud providers and are not much reliable to the clients as the data documents kept at interims the cloud is also touchy and

classified, which is similar to the field-tested strategies. To save the withdrawn data, an essential goal is to compose data documents and at that point of exchange the data becomes encoded onto the cloud [3]. Tragically, concocting a financially savvy and to secure data sharing topic for gatherings at interims the cloud is certainly not a basic undertaking in many applications. In spite of the fact that the cloud ensures an advantageous procedure for clients to share documents and easily communicate in joint efforts, despite everything it holds the idea of individual record ownership. That is, each document kept at interims, the cloud is firmly held by one client, world association office can singularly choose to give or deny any entrance that demands to that record. Be that as it may, the element ownership isn't worthy for different cloud-based applications and joint efforts. Think about a situation where the kind of study associations and mechanical accomplices needs to arrange a common store at interims of the cloud to work together on a joint examination. On the off chance that all members blessing their examination endeavours to the task, they might want to share the ownership over the joint effort documents so as that each and every access decisions are set among the property holders. There are two fundamental contentions why this could be wanted to a singular belonging. To begin with, in the event that there is a sole proprietor, he can manhandle his rights by singularly settling on access the board decisions. The people group decisions kind of stories where noxious clients renounce access to shared records from various teammates. This disadvantage is a great deal of maddening by clients increasingly putting away a large portion of their data at interims the cloud though not keeping local duplicates, and getting to them through helpful gadgets that have limited stockpiling ability. Second, regardless of whether or not mortgage holders are eager to choose and confide in one in all them to make get to the executives decisions, the elective proprietor may not might want to be order in direction of collection and appropriately assessing diverse proprietors' strategies. For instance, mistaken assessments would conceivably increase negative name or money punishments. The thought of shared belonging inside a record get to the executives display named PoSW, and utilizations it to stipulate a novel access the executives move back of circulated gathering activity of shared belonging in existing mists. To existing an essential goals, called Commune, that distributive authorizes PoSW and could be sent in A rationalist cloud stage. Collective guarantees that (I) a client can't check a document from a common storehouse except if that client is built up output access by at least  $t$  of the mortgage holders, and (ii) a client can't compose a record to a mutual vault except if that client is allowed compose access by at least  $t$  of the property holders. To propose a second goals, named Comrade, this use helpfulness from the blowfish in this way on achieve accord on access have control over choice. Confidant enhances the execution of Commune, however wants that the cloud is set up to interpret get to the board decisions that achieved accord at interims the blowfish into capacity get to the executives rules, in this way requiring minor alterations of existing mists.

In an individual cloud, the interchanges is overseen and firmly held by the customer and set on-preface (i.e., at interims the buyers locale of control). Fundamentally, this infers access to customer data is underneath its administration and is simply allowed to parties it trusts. In a surpass open cloud the framework is firmly held and overseen by a cloud specialist organization and is found o\_-commence (i.e., at interims the specialist organization's area of control). This suggests customer data is outside its administration



and can no doubt be allowed to untreated gatherings. Capacity administrations upheld open mists like Microsoft's Azure stockpiling administration and Amazon's S3 furnish clients with versatile and dynamic stockpiling. By moving their data to the cloud clients can stay away from the expenses of building and keeping up a private stockpiling framework, selecting rather to pay a specialist co-op as a perform of its needs. For a few clients, this gives a few edges likewise as availability (i.e., having the ability to get to data from anyplace) and unwavering quality (i.e., not fussing with respect to reinforcements) at a fairly low worth, though the advantages of utilizing an open cloud framework are clear, it presents fundamental security and protection dangers. Truth be told, it appears that the premier imperative obstacle to the seizing of distributed storage (and distributed computing when all is said in done) is worry over the secrecy and uprightness of information. While, up until now, customers are eager to exchange protection for the accommodation of code administrations (e.g., for electronic email, date-books, photographs and so on), this is regularly not the situation for endeavors and guideline.

## 2 Problem Statement

The issue of coursed gathering activity of shared belonging among Associate in Nursing skeptic cloud. By focused gathering activity, we have a tendency to mean gathering activity where access to documents in an exceedingly} exceptionally shared archive is settled if and on condition that  $t$  out of  $n$  householders severally underpins the concede choice. To handle this drawback, we have a tendency to introductory present the Shared-Ownership record get to the board Model (POSW) to stipulate our idea of shared belonging, and to formally express the given gathering activity drawback.

## 3 Related Work

To the best of our data, regularly the primary work to (I) plan and tackle the matter of dispersed gathering activity of shared belonging approaches. Among the ensuing we have a twisted to overview applicable associated include the zones of data scattering, win big or bust change, and access the board. Mystery Sharing and information scattering Secret sharing plans [4] enable a merchant to circulate a mystery among kind of investors, such solely affirmed subsets of investors can remake the key. In limit mystery sharing plans [5, 6], the merchant characterizes an edge  $t$  and each arrangement of investors of cardinality equivalent to or bigger than  $t$  is reasonable to recreate the key. Mystery sharing ensures security (i.e., the key can't be recouped) against a non-approved arrangement of investors; in any case, they bring about a high calculation/stockpiling value, that makes them unfeasible for sharing substantial documents.

Incline plans [7] speak to an exchange off between the security certifications of mystery sharing and therefore the productivity of data scattering calculations. A slope topic accomplishes higher "code rates" than mystery sharing and decisions two edges  $t_1$ ,  $t_2$ . at least  $t_2$  shares are required to remake the key and less than  $t_1$  shares give no

data with respect to the mystery; kind of offers somewhere in the range of  $t_1$  and  $t_2$  spill “PoSW” data. Win big or bust changes (AONTs) were starting presented in [8] and later researched in [9–11]. most of AONTs use a mystery key that is inserted among the yield squares. When all yield shut are out there, the key are ordinarily recouped and single squares are commonly returned.

Access the executives Systems Current dynamic access the board frameworks, for example, SecPAL [12], Keynote and Delegation Logic—can in principle clear cut t out of n approaches. These dialects, be that as it may, depend on the nearness of an incorporated PDP part to guage their arrangements. also, their PDPs can’t be conveyed among an outsider cloud stage. As clarified in Sect. 2, these entrance the executives frameworks depend on partner chairman to stipulate and alter get to the board strategies. In our setting, this suggests a gaggle of proprietors should choose one collaborator authoritative body has one-sided controls over their records.

### 4 System Architecture

In the proposed framework, they considered the structure in nearness of every hub and connection assault. They toward the begin arranged Associate in Nursing decide noted as JLNA that is acclimated reduced the  $\beta$ -disruptor issue. Anyway they require utilized the circulated cut system that has extra undesirable cuts. Henceforth they propose Associate in Nursing rule noted as mixture meta-heuristic (HMM) rule. It’s utilized administration the greatness between the property inside the lingering chart and afterward the objective property. Inside the arranged framework, we have a tendency to will in general understand the recreated system to appreciate the most extreme transmission while not loss of the data and time utilization for the transmission. Here the move happens with the high connection worth and after that the less separation between the each show hubs (Fig. 1).

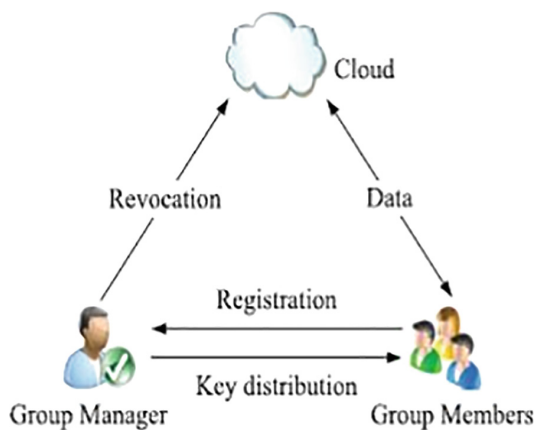


Fig. 1. System architecture

## 5 Proposed System

A cloud figures style by consolidating with Associate in Nursing precedent that an organization utilizes a cloud to change its staffs at interims the indistinguishable group or division to share documents. The framework display comprises of three all totally extraordinary elements: the cloud, a bundle chief (i.e., the organization administrator), and an outsized digit of bunch individuals (i.e., the staffs) as delineated. Cloud is worked by CSPs and furnishes evaluated very much endowed with space for putting away administrations. In any case, the cloud isn't totally sure by clients since the CSPs are extremely well on the way to be outside of the cloud clients certain area. about like [4, 8], we will in general will in general expect that the cloud server is straightforward yet inquisitive. That is, the cloud server won't perniciously erase or change client data due to the insurance of data examining plans, yet will endeavor to get familiar with the substance of the keep data and also the personalities of cloud clients. to all guarantee that the information respectability and spare the cloud clients calculation assets in like manner as on-line load, it is essential expecting to change open examining administration for distributed storage, a far a lot of less demanding and moderate strategy for the clients to make certain their stockpiling rightness at interims the cloud. The outcome from the TPAS would even be useful for the cloud benefit providers to help their cloud based administration stage, even once fill for independent mediation need.

## 6 Modules

### 6.1 Secure Dynamic Auditing

In distributed storage frameworks, information property holders will powerfully refresh their insight. As partner inspecting administration, the evaluating convention ought to be intended to help the dynamic information, extra because of the static chronicle information. Nonetheless, the dynamic activities may assemble the examining conventions uncertain. In particular, the server may lead a couple of following assaults: (1) Replay Attack The server may not refresh legitimately the proprietor's information on the server and will utilize the past form of the data to pass the reviewing. (2) Forge Attack once the data proprietor refreshes the data to the present form, the server may get enough learning from the dynamic activities to manufacture the data tag. In the event that the server could fashion the data tag, it'll utilize any information and its strong information tag to pass the evaluating.

### 6.2 Algorithms for Auditing Protocol

Assume a document  $F$  has  $m$  data segments as  $F = (F_1, \dots, F_m)$ , every data part has its physical implications and ought to be refreshed progressively by the information property holders. For comprehension segments, the information proprietor does not must write it, beside individual data part, the information proprietor needs to engrave it with its relating key.

### 6.3 Service Provider (SP)

SP is to boot trustable and has fundamental assets and screens live distributed computing frameworks. When a client gets to a cloud ADPS, as Associate in Nursing precedent, perusing/composing a document, SP will initially verification the client and fabricate the framework assets open once the client confirmation is passed key age equation. KGen: it's Associate in Nursing equation go past SM, that takes as information the last open parameters params, key and Associate in Nursing picture of either a client  $U_i \in U$  or the SP, and yields a comparing private key ski. This equation are normally either probabilistic or settled.

## 7 Result Analysis

Based on the feedback received, there is giant support for the potential introduction of a Cloud vogue service by UIS. aside from a combine of researchers. World Health Organization were entirely endowed in exploitation Cloud skilled and didn't believe there was any real profit to them in adopting another answer, nearly everyone else was very interested by the prospect (with many creating an effort to push for any details of potential choices, quotas and a launch date). The only real completely different exceptions were a combine of Postdoctoral analysis associates World Health Organization were to boot presently exploitation Cloud skilled as some way of storing and backing up all of their data, and notably likeable the particular indisputable fact that they weren't tied to the University in any suggests that - and would still have full access to any or all or any of their data if/when they emotional on from Cambridge at some purpose at intervals the long run. although the potential for inclusion in associate extremely proof of plan wasn't a matter raised throughout the discussions until fairly late at intervals the project, everyone World Health Organization was asked regarding this indicated they could be very happy to participate - that underlines the proper good craving for such a solution.

## 8 Conclusion and Future Enhancement

Despite the fact that current cloud stages are utilized as agreeable stages, cloud applications still employs some challenges in utilizing the shared belongings that are available in the public storage platform. By effectively integrating the Proof of Shared belonging [PoSW] approach in cloud applications the data reduplication and unknown access to the cloud resources has been drastically reduced. So, the matter of forcing shared belonging inside the cloud is significantly secured since a PoSW based cloud stage does not permit the readiness of an outsider gathering the actively available cloud data part.

## References

1. Charnes, C., Pieprzyk, J., Safavi-Naini, R.: Conditionally secure secret sharing schemes with disenrollment capability. In: ACM Conference on Computer and Communications Security (CCS), pp. 89–95 (1994)
2. Shamir, A.: How to Share a Secret? In: Communications of the ACM, pp. 612–613 (1979)
3. Alon, N., Kaplan, H., Krivelevich, M., Malkhi, D., Stern, J.: Scalable secure storage when half the system is faulty. In: ICALP (2000)
4. Adya, A., Bolosky, W., Castro, M., Cermak, G., Chaiken, R., Douceur, J., Howell, J., Lorch, J., Theimer, M., Wattenhofer, R.: FARSITE: federated, available, and reliable storage for an incompletely trusted environment. In: OSDI, pp. 1–14, December 2002
5. McDaniel, P.D., Prakash, A.: Methods and limitations of security policy reconciliation. In: Proceedings of SP2002 (2002)
6. Yu, T., Winslett, M.: A unified scheme for resource protection in automated trust negotiation. In: Proceedings of SP2003 (2003)
7. Kallahalla, M., Riedel, E., Swaminathan, R., Wang, Q., Fu, K.: Scalable secure file sharing on untrusted storage. In: Proceedings of FAST2003 (2003)
8. Yao, D., Fazio, N., Dodis, Y., Lysyanskaya, A.: Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption. In: 2004 Proceedings of 11th ACM Conference on Computer Communication Security, pp. 354–363 (2004)
9. Li, J., Li, N., Winsborough, W.H.: Automated trust negotiation using cryptographic credentials. In: Proceedings of CCS2005 (2005)
10. Rivest, R.L.: All-or-nothing encryption and the package transform. In: International Workshop on Fast Software Encryption (FSE), pp. 210–218 (1997)
11. Waters, B.: Efficient identity-based encryption without random oracles. In: 2005 Proceedings of 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 114–127 (2005)
12. di Vimercati, S.D.C., Foresti, S., Jajodia, S., Paraboschi, S., Samarati, P.: Over-encryption: Management of access control evolution on outsourced data. In: Proceedings of VLDB2007 (2007)
13. Anderson, J.: Computer Security Technology Planning Study. Air Force Electronic Systems Division, Report ESD-TR-73-51 (1972). <http://seclab.cs.ucdavis.edu/projects/history/>
14. Sterling, T., Stark, D.A.: High-performance computing forecast: Partly cloudy. *Comput. Sci. Eng.* **11**(4), 42–49 (2009)
15. Sahai, A., Seyalioglu, H., Waters, B.: Dynamic credentials and ciphertext delegation for attribute-based encryption. In: 2012 Proceedings 32nd Annual Cryptology Conference of Advanced Cryptology, pp. 199–217 (2012)
16. Nieto, J.M.G., Manulis, M., Sun, D.: Forward-secure hierarchical predicate encryption. In: 2013 Proceedings of 5th International Conference on Pairing-Based Cryptography—Pairing, pp. 83–101 (2013)
17. Lynn, B.: PBC library: The pairing-based cryptography library (2014). <http://crypto.stanford.edu/pbc/>



# Life at Ease with Technologies-Study on Smart Home Technologies

M. S. Meghana, K. Pavithra, S. Sahana, N. Shubha<sup>(✉)</sup>,  
and K. Panimozhi

Computer Science and Engineering, BMS College of Engineering,  
Bangalore, India  
msmeghana07@gmail.com, kpavithra1998@gmail.com,  
sahanaprakash234@gmail.com,  
shubha.nagendrakumarm@gmail.com,  
panimozhi.cse@bmsce.ac.in

**Abstract.** Internet of Things is the network of physically connected devices, which enables these devices to communicate with real world appliances. Home Automation is a beneficial technology for automatically controlling the activities done at home. The different technologies like Bluetooth, WIFI and Zigbee are used to implement the Home Automation System (HAS) where various devices like smart phone, tablet and laptops are used for controlling various household appliances. In this paper we evaluated the capabilities and behaviours of the WSN technology on home automation systems mainly regarding the power consumption and also the advantages of integrating solar panel to the system to enhance the power consumption ratio.

**Keywords:** Zigbee technology · Wireless sensor network · Solar panel

## 1 Introduction

A Wireless Sensor Network is a network which can configure by itself and interact among themselves which can be monitored and understood by the physical world. WSN acts as a backbone between the physical and virtual worlds.

WSN system is composed of nodes or independent devices with a central gateway and router. The nodes wirelessly communicate with a central gateway, which in turn provides a connection to external devices where you can analyse and process your measured data. The router is used to gain a communication link between end nodes and also extending distance and to maintain accuracy in a wireless sensor network. The whole system is networked with more scalability and requires little power capability.

## 2 Need

Wireless Sensor Network has a most important advantages over a traditional communication systems used in today's electric power consuming systems. Recently, WSNs with its best implementations have been recognized and can be used to enhance

various features like utilization of power, delivery rates and has various generations. Hence plays a important role in today's electric efficient power systems.

Home automation system usually needs less cost, less power consumption and do not require high speed data rates, hence the Zigbee would be a best implementation technology for it.

### 3 Scope

IOT is a concept where a device has its unique IP address and thus communication is made by the specified IP address. IOT has various new technology based solutions in all the major fields like Education, Medical, Transportation and in Security.

Today world is facing issues with an irregular power supply, hence we need a latest technologies which is self-charging and remotely controlled by the usage of Renewable Energy resource solar system and WSN.

### 4 Different Wireless Technologies

With the continues development of various communication technology, varieties of short-range wireless communication technologies have been originated. Presently available technologies like Bluetooth technology, WI-FI technology and Zigbee technology are widely used in different applications.

- 4.1 **Bluetooth** is a wireless technology used to send and receive the data between the different electronic devices. Data transmission is very small compared to the other technologies of wireless communication. Bluetooth uses a radio technology called FHSS. Bluetooth uses master/slave architecture.
- 4.2 **WI-FI** is a IEEE 802.11 protocol, is another short-range wireless data transmission technology with the help of the internet access radio frequencies only within a few rooms to as many square kilometres.
- 4.3 **ZigBee** is an IEEE 802.15.4-based protocol which is used in communication protocols. It is used to build PAN's with a small and less-power such as for home automation and many other less-power less-bandwidth needs, designed for small scale projects with the help of wireless connection. Hence, Zigbee has a less-power consumption, less data rate and long battery life and it uses 128 bit symmetric key for security.

### 5 Why WSN? How Is It Useful?

In existing systems the manual intervention had many problems and drawbacks such as power consumption and time consuming as switches are located in different places in home and in garden areas. It is difficult to keep track of Intrusion, Accidents, Water level in the tank and Moisture level of the soil and uses wired communication so, cannot have a long range communication wirelessly.

WSN is the network of physical devices, sensors and many other electronic software's which enables devices to connect and exchange data with efficient improvements, economic benefits and reduced human intervention. IOT play's a major role in Home Automation which automatically control and monitor electrical and electronic home appliances and also compute data in cloud. Home Automation System consists of Door Lock System, Magnetic Gate Lock, Water level Monitoring, Alert System and control of Lights.

Our project aims to increase safety and security for the homes and to reduce human intervention, power consumption and cost by using latest technologies such as renewable energy resource and ZigBee wireless sensor network by organizing the collected data at a central location wirelessly and perform necessary actions by doing analysis on the data.

## **6 Related Study**

### **6.1 Role of WSN in Fire/Gas Leakage**

Wireless Sensor Network (WSN) can also be used to detect gas leakage in a large area. The early discovery of the gas/fire leakage helps to reduce the risk and effects of an accidental event which enhances the safety of home. Explosion prevention system works based on alarm/buzzer. If any gas leaks found, the sensor will send the data wirelessly to Arduino then the system will be activated. The system will ON the alarm/buzzer and also allow the air to vanish with the exhaust fan.

The gas leakage is detected by using gas sensor and notified by GSM Module [1–5]. When there is gas and fire leakage, the relay turns on the alarm, exhaust system and water system by using ZigBee [6, 7]. The paper consists of number of modules i.e. Alert system, Lightening system, Water level and Gardening, the data is sensed and managed by relay, ZigBee, DC motor [8].

### **6.2 Role of WSN in Smart Door**

Importance for the home security systems has been increased due to the growth of crime rates. The Digital door lock system in home automation which enables the user to have the controlling power and manipulate the condition of home before he enters or leaves the house. The system provides the security by ensuring the user identity and if and only if the authenticated person tries to open the door, the door is opened.

When the authenticated person encounters, the door opens and the message is displayed on the LCD [10, 11].

### **6.3 Role of WSN in Smart Gardens**

By using the concept of WSN we make sensors to communicate with each other which are powerful in automation. The important aspect while using the WSN is that it saves cost. When people try to make plantings and set up their own garden, they were cautious in maintenance at only in their early stages. As days goes on due to lack of



maintenance the plants get destroyed. This module will help people to automatically monitor the moisture level of the soil and ensures maintenance of the garden. It plays a major role and serves as a good companion for plants.

IR sensor used to know the temperature of environment based on that water spray motor is switched ON [9]. The flow and level sensors sense data is sent from Zigbee to server and data is received by the end user [12, 13]. Gardening System monitors wind speed, soil moisture, light, temperature and humidity and sends the data to the base station based on that garden is watered [14]. The work about smart irrigation system using Zigbee technology in WSN's is monitoring the quality of crop fertilization by different sensors [15]. The main aim of this implementation is to reduce water usage and Photovoltaic powered irrigation system which consists of a network of soil moisture and temperature sensors [16]. Moisture content of the soil is sensed by the sensors in agriculture and monitoring the quality of crop which can be developed by using ZigBee Technology [17]. Precision farming and ZigBee applications in agriculture, actuation and control decision is based on sensed data [18]. Monitoring the parameters of moisture i.e., temperature and humidity for obtaining high-quality environment [19]. Sensors are used to measure the temperature, humidity and moisture so that information is stored and converted into digitized with the help of ADC and it is transmitted to ZigBee using UART [20].

#### **6.4 Role of WSN in Society**

The wireless sensor networks is most probably used to control various physical appliances. WSNs plays a important role in assuring the security by instantly sensing conditions in the real world and ZigBee is one of the main communication technologies to provide security with the minimal expenditure and also provide solutions for various problems and it allows things to be sensed or controlled remotely in networking. The main advantage by this system is to help the old age people in there day to day life and also to reduce electricity consumption.

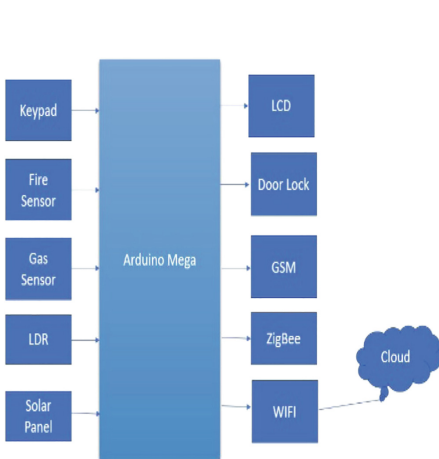
#### **6.5 Role of WSN in Lighting**

Energy efficiency or saving energy is one of the centre of attention throughout the world as the price of energy is increasing day by day and friendly environment thinking will be more important among the people. Wireless sensor network for lighting control is of adding intelligence to the lighting systems, hence reducing energy consumption. But not just energy efficiency, intelligence in lighting systems brings many other improvements to people's everyday life.

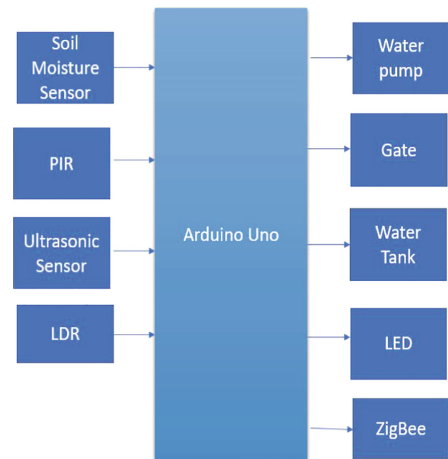
On each lamp post there is an monitoring station which helps to take an independent decision to activate light automatically, based on the data received by the sensors such as Light, PIR and Hall sensor and sends the data to the base station wirelessly, In case of any failure an message is sent to the Service Engineers using GSM module to take necessary actions. Remotely streets lights are controlled through GUI. Overall design reduces power consumption as it uses an Renewable source energy [21–24]. Temperature of an LED is maintained by decreasing the current flow through LED when it crosses the safe level [25].

## 7 Description of the Proposed Work

The sensor network includes number of sensors namely Flame sensor, Gas sensor, Door sensor, Ultrasonic sensor, Soil moisture sensor and PIR sensor. The sensors data is received by the Arduino and accordingly the actions are taken. ZigBee plays a very important role in communication between the two modules which is located inside and outside the house wirelessly. The solar power is used as the main source of power supply to the home appliances and if any shortage in the solar power supply while serving the devices the normal power supply is supplied to it. The comparisons of number of devices which were ON by using the solar and normal power supply is stored in the cloud and analyzed. The data stored in the cloud for each month is retrieved and analyzed for generating the monthly electricity bill. The graph is generated based on the monthly power consumption of analyzed data (Figs. 1 and 2).



**Fig. 1.** ZigBee Network inside the house



**Fig. 2.** ZigBee Network outside the house

## 8 Conclusion

As per now the home automation was only focused to ON or OFF the devices with the help of mobile phone, but the things have been changing rapidly, the automation combined with the smart wireless sensor networks has started to understand the human manipulations. Sensors like motion sensors, temperature sensors, light intensity sensors, smoke detectors, humidity sensors etc. are being used to implement the home automation systems and the sensed data is analysed and controlled by devices only when they are capable of doing it.

The proposed system is self-charging and as remote control by using latest technologies using Renewable solar energy and Zigbee wireless sensor network which reduces power consumption, cost and human intervention. By combining both ZigBee and solar system we are optimizing home energy usage.

Secure Door lock system and automated way of monitoring the gas leakage and fire explosions helps to take necessary measures to overcome accidents and we are reducing human intervention by automating the water monitoring and magnetic gate system which provides safety and security for the home.

**Acknowledgement.** We are very thankful for BMS College of Engineering and TEQIP III for the support and encouragement.

## References

1. Gokula Kaveeya, S., Gomathi, S., Kavipriya, K., Kalai Selvi, A., Sivakumar, S.: Automated unified system for LPG using load sensor. In: International Conference on Power and Embedded Drive Control (ICPEDC) (2017)
2. Fuzi, M.F.M., Ibrahim, A.F., Ismail, M.H., Ab Halim, N.S.: A dedicated fire alert detection system using ZigBee wireless network. In: IEEE 5th Control and System Graduate Research Colloquium, UiTM, Shah Alam (2014)
3. Ransing, R.S., Rajput, M.: Smart home for elderly care, based on wireless sensor network. In: International Conference on Nascent Technologies in the Engineering Field (2015)
4. Nimbai, M.S., Kulkarni, G.A.: Monitoring of home security using GSM and Zig-Bee network. In: International Advanced Research Journal in Science, Engineering and Technology (2016)
5. Ganesh, D., Anilet Bala, A.: Improvement on gas leakage detection and location system based on wireless sensor network. *Int. J. Eng. Dev. Res.* **3**, 407–411 (2015)
6. Saravanan, R., Vijayaraj, A.: Home security using ZigBee technology. *Int. J. Comput. Sci. Inf. Technol. Secur. (IJCSITS)* **1** (2011)
7. Chen, D., Wang, M.: A Home Security ZigBee Network for Remote Monitoring Application ICWMMN (2006)
8. Rawate, S.V., Patil, M.D.: Smart sensor network for monitoring and control of society automation. *Int. Res. J. Eng. Technol. (IRJET)* **3**, 912–915 (2016)
9. Rashid, S., Haider, N., Iqbal, M.: Gas management and disaster system using ZigBee. *Int. J. Eng. Res. Technol. (IJERT)* **2** (2013)
10. Park, Y.T., Sthapit, P., Pyun, J.-Y.: Smart Digital Door Lock for the Home Automation, University Gwangju, South Korea (2009)
11. Krishna Kanth, B.B.M.: An effective water quality and level monitoring system using wireless sensors through IoT environment, vol. 7. Anurag Engineering College (2017)
12. Balaji, V., Akshay, A., Jayashree, N., Karthika, T.: Design of ZigBee based wireless sensor network for early flood monitoring and warning system. Earwari Engineering College (2017)
13. Kanagamalliga, S., Vasuki, S., Vishnu Priya, A., Viji, V.: Security monitoring using embedded systems. *Int. J. Innovative Res. Sci. Eng. Technol.* **3** (2014)
14. Caetano, F., Pitarmaa, R., Reish, P.: Intelligent management of urban garden irrigation, UBI – University of Beira Interior
15. Esakki Madura, E., Venkatesa Kumar, V.: Smart agriculture system by using ZigBee technology. *Int. J. Curr. Eng. Technol.* **6** (2017)
16. Parvatkar, S.A., Bhagat, V.B.: Producing more crops in automated irrigation system using WSN with GPRS and ZigBee. *Int. J. Curr. Eng. Technol.* **5** (2015)
17. Sahitya, G., Balaji, N., Naidu, C.D.: Wireless sensor network for smart agriculture. In: 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (2015)

18. Kalra, A., Chechi, R., Khanna, R.: Role of ZigBee technology in agriculture sector. In: National Conference on Computational Instrumentation, CSIO Chandigarh (2010)
19. Sathish Kannan, K., Thilagavathi, G.: Online farming based on embedded systems and wireless sensor network. In: International Conference on Computation of Power, Energy, Information and Communication (TCCPEIC) (2019)
20. Chikankar, P.B., Mehtra, D., Das, S.: An automatic irrigation system using ZigBee in Wireless Sensor Network (2015)
21. Srinath, V., Srinivas, S.: Street light automation controller using ZigBee network and sensor with accident alert system. *Int. J. Curr. Eng. Technol.* (2015)
22. Mingxia, S.U., Yixin, S.U.: Design of the wireless monitoring system of solar lamps based on ZigBee and GPRS, WuHan University of Technology Huaxia College
23. Santhosh Kumar, R., Prabu, D., Vijaya Rani, S., Venkatesh, P.: Design and implementation of an automatic solar panel based led street lighting system using ZigBee and sensors. *Middle-East J. Sci. Res.* (2015)
24. Mhaske, D.A., Katariya, S.S.: Smart street lighting using a ZigBee & GSM network for high efficiency & reliability. *Int. J. Eng. Res. Technol. (IJERT)* **3** (2014)
25. Yoon, S., Kim, H.: Development of self-powered LED street light and remote controller utilizing the ZigBee and smart devices, Andong National University



# Data Analysis in Social Networks Based on Similarity Measurements on Multi-attribute Trajectories

K. Monica Rachel<sup>(✉)</sup>, D. C. Joy Winnie Wise, K. Raja Sundari,  
and N. Raja Priya

Department of Computer Science and Engineering,  
Francis Xavier Engineering College, Anna University,  
Tirunelveli, Tamilnadu, India

rachelpraveen27@gmail.com, monicarachel.k@gmail.com

**Abstract.** The headway of overall arranging development, sensor systems and versatile terminal, an extensive number obviously information are amassed. Bearing information contains an abundance of information, including directionality, time game-plan, and other outside expressive qualities. The examination obviously likeness estimation is the prelude of heading information the board and excavation, which acknowledge a fundamental occupation in bearing getting ready. Most course likeness work just spotlights on the dimensional-normal highlights. The augmentation of multi-credits to the heading changes the course furtiveness. MELD (Most extraordinary Least Direction Separation) and TLDS (Total of least Direction Separation) and inspect the association among the direction-common furtiveness and scholarly similarity. The headings including the zones, accurate location, and obvious characters are called multi-qualities bearings.

**Keywords:** Dimensional similitude estimation · Bolster direction · Direction figuring

## 1 Introduction

In the current conditions, it very well may be seen that the cloud has taken the authority over the IT business with its incalculable advantages. Cloud processing is permitted to as PaaS (Programming as an Administration) since it renders the applications as organizations over the Internet and the equipment and frameworks programming in the server farms that offer those organizations. The equipment of server farm and programming is known as a cloud. Today the mists can be open/open and moreover private. Private mists are related to the internal datacenters of a business or other affiliation, not made open to the general open. Distributed computing as such can be packed as a mix of PaaS and utility registering, booting out the server farm (little + medium assessed).

The advancement of remote correspondence innovation, worldwide situating framework, and keen versatile remote station, large indefinite quality or even terabyte

direction information collects quickly. DiDi1 declared that more than 70 GB dimension-transient information is produced every day and the preparing information examine is to 4500 GB day by day [1]. Meanwhile, with the ubiquity of web based life, for example, Twitter, Face book and Foursquare, an abundance of outside data are installed into the directions. Therefore, the crude directions are improved by a broad assortment of substances. For instance, the literary items in directions are related with the area name (i.e., eateries, exhibition halls) and so forth.

The semantics2 as the properties of the directions into the type of an accumulation of printed catchphrases. This isn't handy. Dubious information or incorrectly spell information to be sure exist in reality (i.e., theatre and theater). Here does not think about period course of action, where the measurement estimation and the common estimation are secluded. The two measurements rely upon one another. To beat the impediments, propose two rough similitude measures on directions (that is, MELD and TLDS) [2]. The two estimations settle the issue of direction time arrangement, and bolster surmised closeness utilizing the alter separate. Break down the relationships among the dimension-fleeting comparability and the printed similitude utilizing a genuine data set. Find that the dimension-fleeting comparability and the printed similitude are feeble relationship. So as to check the viability of MELD and TLDS contains the two similitude estimations in a traditional bunching calculation and imagine the grouping results.

## 2 Related Works

The likeness estimations on multi-traits directions can be isolated into three sorts: spatial-transient comparability, spatial-printed similitude, and spatial-fleeting literary closeness.

### **Spacial-Textual Likeness Estimations**

Considering the direct-fleeting furtiveness of directions has the Longest Normal Subsequence (LNSS) the quantity of coordinating point's sets as the direction remove overlooking the distant focuses. LNSS needs a manual coordinating edge to decide the separation. Discrete Fréchet Separation (DFS) [3] considers the areas and requesting of the focuses along the bend utilizing the "most limited puppy rope remove". Dynamic Time Traveling (DTT) [4] enables rehashing a few points to accomplish the best arrangement.

### **Spacial-Printed Similitude Estimations**

Concerned both the dimensional and printed similitude on two directions. [5] Processes the direction separation utilizing Euclidian separation and the printed separation by Alter remove. In [6], the dimension separations comprise of direction geometric focus remove, direction length distinction, and course. The literary separations depend on the longest basic subsequence of visited focuses, which just think about the full match. Considers the pair directions are comparative on the off chance that they share a typical focuses arrangement with the comparative travel time. Their methodology is not the same as the current similitude measures due to thinking about the visit recurrence.

**Spatial-Worldly Textual Similarity Estimations**

Consider the direction separate from the spatial viewpoint, the transient perspective and the printed angle at the same time. The comparability estimation is a direct blend of the Euclidian separation, the time interim crossing point, and the quantity of full coordinating pair. A classification tree is characterized for the content characterization, and distinctive loads are allocated to the hubs for building up the significance. Considering pair of new comparability estimations for multi-qualities directions. The pair of new likenesses bolster direction period arrangement and the surmised literary similitude.

- The least point-to-point remove
- The greatest point-to-point remove
- The total min separate
- The aggregate max separate

**3 Dataset Tables**

Pick 10 directions haphazardly from 1,290 reproduced directions as the seed directions. 50 directions are created by the direction change approach in [7, 8] with the distinctive changed rates and the changed kind (for example expansion of inserted focuses, expansion of arbitrary focuses, focuses expelling, focuses arrange change, and focuses substitution). For instance, in the event that we expel focuses from the seed direction with 10 points and  $r = 0.2$ , 2 points will be expelled from the seed direction. Looking at the comparability between the seed direction and the changed direction is for assessing the effect of each change on the diverse furtive estimation.

STATISTICS OF REAL DATA SETS

	Before time division		After time division	
	LA	NYC	LA	NYC
Number of Trajectories	31,544	49,062	18,024	29,784
Number of Check-in points	267,579	424,649	157,931	247,660
Number of keywords	395,738	630,691	372,422	596,312
Max number of points/ trajectory	200	200	199	199
Min number of points/ trajectory	1	1	3	3
Average number of points/ trajectory	9	9	8.7	8.3

1,200 directions are chosen by the straightforward arbitrary example. The spatial-worldly closeness and the printed similitude between any two directions are processed as MELD and TLDS [8]. The relationship network is created from SPSS. The speculation test with the certainty level  $\alpha = 0.01$ .

SPATIAL-TEMPORAL AND TEXTUAL CORRELATION ANALYSIS(MMTD)			
		Spatial-temporal similarity	Textual similarity
Spatial-temporal similarity	Correlation Coefficient	1.00	0.30**
	Sig.(2-tailed)		0.00
	Correlation Coefficient	0.30**	1.00
Textual similarity	Sig.(2-tailed)	0.00	

\*\* correlation is significant at the 0.01 level (2-tailed).

Sig (2-0.01): There is no noteworthy impact between the spatial-worldly closeness and the content likeness.

Sig(2-0.02): There is a noteworthy impact between the spatial-worldly closeness and the content likeness.

In Table Spatial and textual analysis, the Pair sided test Sig = 0.00 < 0.03 contains the speculation H0. As such, the spatial-transient comparability and the content likeness have a huge impact.

## 4 Proposed Work

In the proposed framework, the normal similitude change incline when  $r$  interjected focuses are included. Select pair back to back focuses from the seed direction and utilize the straight introduction technique to include another point. The new point takes the crossing point of the watch words from the pair of back to back focuses. In the wake of embeddings inserted focuses [9, 10], Expecting, that the likeness of pair of directions is high and the furtiveness changes little with  $r$  expanding. From Fig. 1 represents the similitude scores of MINT, MELD, TLDS decline, while the furtiveness score of MSS stays steady as the changed rate increments. Since MSS utilizes, the most coordinated concentrate the figure of separations without period arrangement, embeddings introduced concentrate to the directions has no impact on MSS. In any case, since MSS requires the correct counterpart for figuring content furtiveness, the likeness scores are least among the four techniques.

The furtiveness scores of MELD, TLDS and MINT decline coming about because of the expansion of the dimensional separations. For the three estimations, the printed likenesses between the seed direction and the changed direction don't change since the entire word sacks for pair directions are same the MSS occupies the entire space.



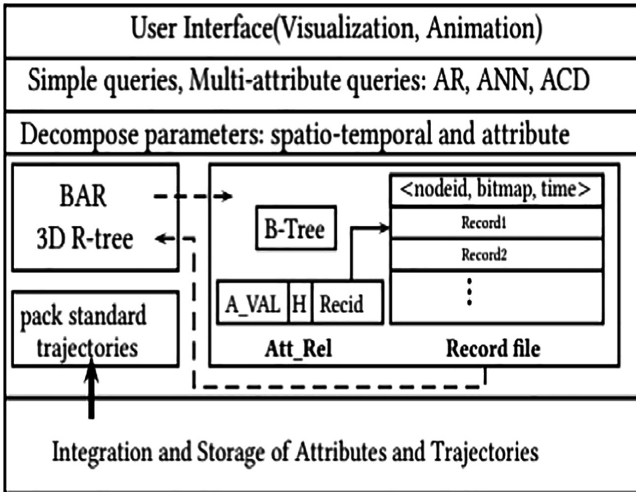


Fig. 1. Procedure for ANN range queries

Figure 1 represents the external range and the internal range covers all points with removes not exactly the span  $r$ . Since the internal range contains at any rate  $k$  focuses, there are at any rate  $k$  closest neighbors to the question concentrate with separations less than the sweep  $r$  [10]. Along these lines, the  $k$  closest neighbors must be in the external range. The areas of new focuses are created from the dimensional range and the transient range arbitrarily.

The new traits are arbitrarily chosen from the stored information expect the catchphrases set on the direction. Since MINT and MSS separate the dimensional comparability figuring, the fleeting similitude registering and the printed likeness processing, the point which adds to the last furtiveness are not similar sets. Therefore, the bunches in MINT and the ones in MSS disperse over the entire space.

Name	Domain
$A_1 = Color$	RED, SILVER, BALCK
$A_2 = Brand$	BENZ, BMW, FORD, TOYOTA

(a) Attributes

Id	Trip	Att
1	(((116.310, 39.938), 20121031095536), ((116.359, 39.949), 201211031095634), ((116.318, 39.937), 20121031095746))	(BLACK, BENZ)
2	—	(RED, BMW)

(b) An Integration

Fig. 2. Multi attribute trajectories

Figure 2 demonstrates the multi-directions have double surmised likeness measure on ways (that is, MELD and TLDS). The pair of estimations settle the issue of direction period arrangement, and bolster surmised comparability utilizing the alter remove. Break down the relationships between the dimensional-worldly furtiveness and the literary comparability utilizing a genuine dataset. The direction-fleeting likeness and the printed similitude are frail connection. Check the adequacy of MELD and TLDS [11], apply the twice furtiveness estimations in a traditional grouping calculation (for example k-distance of the locations) and imagine the bunching results.

- Two direction furtiveness measures, MELD and TLDS, for multi-traits directions which bolster estimated likeness.
- To demonstrate the dimensional-transient similitude and the literary likeness are powerless associated with one another utilizing the connection investigation.
- The adequacy of proposed furtive measurements in the k grouping utilizing a reenacted dataset and a genuine data set.

Multi-quality directions, give the information portrayal and characterize another question. Cross breed list structure and a proficient calculation to answer run inquiries on multi-quality directions together with a productive refreshing strategy for the list [11]. Query advancement calculation is utilized to recover the information from the database in a quick way. This calculation is utilized to decrease the time utilization.

## 5 Advantages

The technique has the favorable position that one can

- (i) Use existing direction administrators and social administrators to define questions, and
- (ii) Concentrate standard directions from multi-property directions, bringing about an adaptable method to control the information.
- (iii) More easy to understand.

## 6 Result Analysis

Analyzing the measurements of MELD and TLDS through the exact point locations of the user. Clustering techniques to reduce the time utilization.

### Grapples Pair Change

Both MSS and MINT utilize the separations between any double points, which moderate the lessening pattern. Concentrate the expelling adjusted focuses sets and the grapples sets change [11, 12]. In this manner, TLDS and MELD get a handle on the change. The progressions of TLDS is somewhat clear than the one of MELD.

### **Perception with the Simulated Data**

MINT and MSS separate the dimensional similitude processing, the transient comparability registering and the printed likeness figuring, adds to the last furtive are not similar sets. Thus, the groups in MINT and the ones in MSS convey over the entire space.

### **Perception with the Real Data**

The direction length in one set is four, and the one in the other set is between four to twenty. Like the outcomes of MINT and MSS is frail recognize. Consequently, in this segment, imagine the consequences of MELD and TLDS its demonstrate the bunching performance. Each shading (i.e., Blue, Black, Orange) speaks to a bunch to assess the furtiveness dissemination of the bunches, tried the discrete coefficient.

## **7 Conclusion**

In this paper, the blasting internet based life enhance the directions with many objects including dimensional data, fleeting data and other outside data. The greater part of works just spotlight on the comparability measures on the direction-transient element. Proposed two direction likeness estimations that measure the spatial transient printed direction comparability in the meantime. MELD assesses the most exceedingly bad of the best instances of direction, while TLDS is the normal comparability of directions. Both of MELD and TLDS resolve the issue of direction time arrangement and bolster inexact likeness for multi traits directions. After the arrangement of the trials, TLDS is best to different direction changes. Demonstrate the worldly directional comparability and the semantic printed furtively are powerless relationship. In future work, take a shot at the new similitude estimation out and about system utilizing multi-source information combination and supporting a hierarchal semantics among directions into a city.

**ALGORITHM:**

Input: Estimate the routing path in dynamic way

**Algorithm:**

- Identify different path for routing and optimization
- Estimate based on cost, time and performance
- Define the routing way along with some alternate path

**Pseudocode :**

**Input:** A set of base station routers to the broadcast network, an interference model. To estimate the packed delivery ratio

**For each routers do**

Construct a routing hash table for routing tree;

**For each th instance of each base station router do**

**For each node do**

**If is a complete set packet in node then**

Adds the data to be transmission routing table plan;

**If is an incomplete set packet in node then**

Remove the node in routing table list;

**Else**

Assign the packet not received

**For router in ( the packet for pending nodes) do**

Assign time;

**For each (node weight and length) do**

**For packet at (th packet to send to the node) do**

Include assigns time:

**Return** Time to transmit for each packet to particular router will send to source node/base station.

**if**  $R_o = \min$  **then**

Send the packets from neighbour node

**Else if** rebroadcast packet for all the node connected to router **then**

Rebroadcast to all nodes in the router

**End if**

**Output:**

Output will send estimates best way to route the packet without delay to improve the better performance

## References

1. Alokawatve, T.: Topological transformation approaches to database query processing. In: ACM SIGMOD Conference, vol. 9, no. 3, pp. 18–25 (2017)
2. Chen, K., Guo, S., Kavuluru, R.: ACM Data and Application, vol. 3, pp. 18–25 (2011)
3. Chen, K., Liu, L.: Geometric data perturbation for outsourced data mining. *Knowl. Inf. Syst.* **5**(6), 965–981 (2012)
4. Xu, H., Liu, K., Mitchell, L., Sun, G.: Building confidential and efficient query services in the cloud with RASP data perturbation. In: SIAM Data Mining Conference, vol. 10, no. 3, pp. 18–25 (2017)
5. Zhu, H.S.R., Konwinski, A.: Range based neighbor queries with complex shaped obstacles. Technical Report, University of Berkeley (2015). vol. 12, no. 3, pp. 18–25 (2015)
6. Shen, H.J., Mitchell, J.C.: Leveraging a compound graph based DHT for multi attribute range queries with performance analysis. *IEEE Secur. Privacy* **9**(3), 18–25 (2013)
7. Wen, M.I., Vandenberghe, L.: A PARQ-preserving range query scheme over encrypted metering data for smart grid, vol. 13, no. 3, pp. 18–25 (2016)
8. Qijun Zhu, M.K., Goldreich, O., Kushilevitz, E.: Querying distributed partial data sets with unknown region. *ACM Comput. Surv.* **45**(6), 965–981 (2017)
9. Li, R.P.: Fast and scalable range query processing with strong privacy protection for cloud computing. In: INFOCOMMDC, vol. 4, no. 2, pp. 18–25 (2014)
10. Xin range Qijunreich, J., Mitchell, J.C.: Skyline queries in mobile environments. *IEEE Secur. Priv.* **9**(3), 18–25 (2016)
11. Furtado, A.S., Kopanaki, D., Alvares, L.O., et al.: Multidimensional similarity measuring for semantic trajectories. *Trans. GIS* **20**(2), 280–298 (2016)
12. Arboleda, F.J.M., Fernández, S.R., Bogorny, V.: Towards a semantic trajectory similarity measuring. *Indian J. Sci. Technol.* **10**(18), 1–14 (2017)



# Defender Vs Attacker Security Game Model for an Optimal Solution to Co-resident DoS Attack in Cloud

S. Rethishkumar<sup>(✉)</sup> and R. Vijayakumar

School of Computer Sciences,  
Mahatma Gandhi University, Kottayam, Kerala, India  
rethishsnair3@gmail.com, vijayakumar@mgu.ac.in

**Abstract.** Virtual Machines (VM) are considered as the fundamental components to cloud computing systems. Though VMs provide efficient computing resources, they are also exposed to several security threats. While some threats are easy to block, some attacks such as co-resident attacks are much harder even to detect. This paper proposes Defender Vs Attacker Security Game Model otherwise called Two-Player security game approach based defense mechanism for minimizing the Co-resistance DOS attacks by making it hard for intruders to initiate attacks. The proposed defense mechanism first analyzes the attacker behavior difference between attacker and normal users under PSSF VM allocation policy. Then the clustering analysis is performed by EDBSCAN (Enhanced Density-based Spatial Clustering of Applications with Noise). The partial labeling is done depending on the clustering algorithm to partially distinguish the users as legal or malicious. Then the semi-supervised learning using Deterministic Annealing Semi-supervised SVM (DAS3VM) optimized by branch and bounds method is done to classify the nodes. Once the user accounts are classified, the two-player security game approach is utilized to increase the cost of launching new VMs thus minimizing the probability of initiating co-resident DOS attack.

**Keywords:** Co-resident DOS attack · PSSF · EDBSCAN · DAS3VM · Branch and bound method

## 1 Introduction

Cloud computing has showed the means for “long-held dream of computing as a utility” [1]. Commercial third party cloud facilitates organizations to eliminate their resources provisioning and have to give a small amount for computing, which they need. Virtualization plays a vital role for this model. By providing numerous virtual hosts on single physical machine cloud providers can competent to profitably balance economic scale and statistical multiplexing for computational resources. When numerous models exists in cloud computing, Infrastructure-as-a-Service (IaaS) model

utilized by providers like Amazon's Elastic Compute Cloud (EC2) service facilitates a pool of virtualized hardware configurations for clients [2]. By sharing the generic physical platform between several virtual hosts, moreover, presents novel bottlenecks to security, since the client's virtual machine (VM) may be co-located with un-trusted and unknown parties. Their outcomes provide that hypervisors give new attack surface via isolation and privacy assurances could face a compromise. Moreover, protection mechanisms against those dangers are already examined in various literature [5].

Virtual machine (VM) generally uses resources from cloud computing environments. For the advantage of cloud providers, VMs assist in increasing utilization rate of the hardware platforms beneath. For cloud clients, it facilitates outsources the maintenance and on-demand resource scaling of computing resources. Moreover, besides all the available advantages, it also asks a novel security menace [6]. Theoretically, VMs functions on similar physical server (i.e. co-resident VMs) that are logically separated from one another [7].

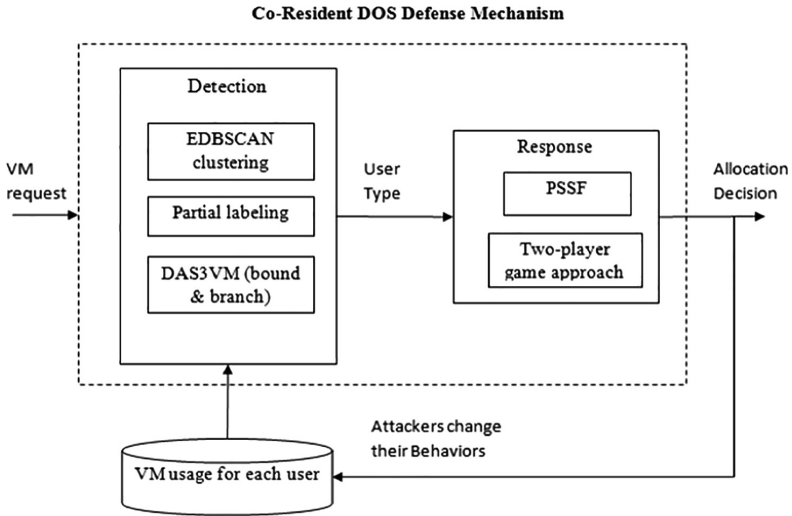
## 2 Related Works

Yinqian Zhang et al. [9] depicts about Home Alone, system that makes tenant verification of exclusive utilization of VM's over physical machine. The primary concept behind Home Alone is to reverse the essential application of side channels. Indeed of making the best advantage of side channel to be vector of any attack, Home Alone utilizes a side-channel (in L2 memory cache) as a new protective detection tool. By examining the utilization of cache while the period in which "friendly" VMs collaborate to eliminate segments of cache, tenant with home Alone can identify co-resident activity of "foe" VM.

Adam Bates et al. [10] depicts about Co-resident watermarking, traffic analysis attack, which facilitates dangerous co-resident VM to introduce watermark signature over the internet flow of target instance. The final examination illustrates that there is a careful hardware design to be utilized in the cloud environment. Similarly, there has been many techniques developed for the security of cloud computing.

## 3 Proposed Methodology

In the initial stages of the proposed methodology, the analysis of the attacker behavior is done and compared with that of the legitimate user. The attacker behavior is analyzed in three different scenarios namely under no security mechanism, with presence of PSSF VM allocation policy and the proposed defense mechanism. Under no defense mechanism, the behavior of the normal users can be found. Under PSSF policy, the new VMs will be assigned to lightly loaded servers (Fig. 1).



**Fig. 1.** Proposed defense mechanism architecture

The defense mechanism comprises of two important parts: the detection module and the response module. If a user requests to begin a new VM, the detection module loads historical data from the database, classifies the user into one of the three types: low/medium/high risk, and sends the result to the response module. The latter limits the available servers according to the result, so that VMs of any user only co-locate with VMs started by users of the same type. In addition, the response module sets the parameter in the VM allocation policy PSSF (also based on the classification result), which finally selects a server within the limited set. It is likely that attackers will adapt the way they start VMs according to the allocation decisions. Meanwhile, the defense system will also update the database of VM usage regularly, which in turn may change the allocation decision. Therefore, in order to analyze how to optimize this adversarial learning problem, we model the problem in the form of a two-player security game ( $G$ ) between the attacker ( $A$ ) and the defender ( $D$ ). Before studying about the security model, let us know about co-resident and DOS attacks.

**Co-resident Attacks:** In cloud computation, co-resident takes the malicious and influenced adversary into account, which isn't subsidiary with cloud provider. Victims are authentic cloud clients who are propelling Internet-directed instances of virtual servers to perform tasks for their business. Adversary who maybe a business contender, desires to utilize the new capacities conceded to him by cloud co-residency in order to find significant data on his objective's the target business. It is essential for the common utilization of some third-party cloud, cloud infrastructure is a trusted component. Co-residency detection via virtualization side channels is dangerous, which was initially revealed by Ristenpart et al. [3]. This investigation provides mechanisms for providing instance placement routines corresponding to Amazon EC2 cloud infrastructure in order to probabilistically attain co-location with the target instance. From that, co-residency can be identified with cross-VM covert channel in the form of ground truth.



Camouflaging in the form of legit client, an attacker is capable to place numerous instances, carry out co-residency check, stop, and repeat till the necessary placement is attained. Numerous cross-VM information leakage attacks are briefed, in the form of keystroke and load profiling timing attacks. Moreover, independent outcomes ensured that numerous techniques in previous work, like usage of simple network probes, which is no more suitable on EC2.

**Defense Action Set:** From the attacker action set, it can be found that the attacker is capable of triggering their targets to launch new VMs, capable of compromising a low risk account, and only starts same type of VMs. Hence based on these attacker behaviors, the defense process is defined. The defense process begins with determination of attacker behavior. Then the user accounts are clustered using EDBSCAN and then labeled partially as low, medium or high risks. Finally the accounts are classified using semi-supervised learning-DAS3VM with branch and bound method. Based on the classified results, the cost for the initialization of new VMs through new accounts is maximized making it hard for the attacker to co-locate the target VMs.

**EDBSCAN Clustering:** DBSCAN clustering has been previously used for clustering the user accounts. There are two parameters in the DBSCAN algorithm,  $\epsilon$  and *MinPts*, where  $\epsilon$  is the maximum distance between two neighbors, and *MinPts* refers to the minimum number of points present in a cluster. However, once *MinPts* is fixed,  $\epsilon$  can be determined by drawing a *k*-distance graph ( $k = \text{MinPts}$ ) as introduced in [16]. In other words,  $\epsilon$  can be considered as a function of *MinPts*. *MinPts* should not be too small; otherwise noise in the data will result in spurious clusters.

In EDBSCAN, the parameters Eps and MinPts are determined differently from DBSCAN. The procedure is given in the following algorithm:

**Algorithm 1: EDBSCAN**

<p><b>Input:</b> List of points pointList and depth</p> <p><b>Output:</b> KD Tree</p> <p><b>Function</b> kdtree(pointList, depth)</p> <p>Step 1: Chose axis sourced on depth so that axis cycles via all valid values (axis=depth mod k)</p> <p>Step 2: Sort point list and select median as pivot element</p> <p>Step 3: Generate node and construct sub-trees</p> <p style="padding-left: 40px;">node location := median;</p> <p style="padding-left: 40px;">leftChild := kdtree(points in pointList before median, depth+1);</p> <p style="padding-left: 40px;">rightChild := kdtree(points in pointList after median, depth+1);</p>
---

The algorithm given above is utilized in EDBSCAN procedure to eliminate the time complexity. Let ‘d’ refer to the distance of point ‘p’ to its  $k^{\text{th}}$  closest neighbor, then d-neighborhood of ‘p’ comprises exactly  $k+1$  points for almost all ‘p’ points. D-neighborhood of ‘p’ comprises more than  $k+1$  points merely if numerous points have precisely similar distance ‘d’ from ‘p’ that is moderately impossible. Moreover, [4–6] modifying, ‘k’ for point in cluster does not outcome in huge changes of ‘d’. This merely occurs if  $k^{\text{th}}$  nearest neighbors of ‘p’ for  $k = 1, 2, 3, \dots$  are positioned suitably on straight line that usually does not hold true for point in cluster. For certain k, function k-dist from database D is provided by the mapping of every point to distance from its  $k^{\text{th}}$  closest neighbor. While sorting database points in descending order of their k-dist values, the graph of this function provides certain clues relating density distribution in database. This graph is termed sort k-dist graph. In case a random point ‘p’ is selected, parameter Eps is set to k-dist (p) and parameter MinPts is set to k, all the points with an equal or lesser k-dist value will become the core points. Moreover, as specified k-dist graphs for  $k > 4$  do not appropriately vary from 4-dist graph and they require significantly more computations. Suitability of value 4 to MinPts was confirmed by numerous suggestions [6–10]. Henceforth, parameter MinPts is fixed to 4 while experimentations. 4-dist value of threshold point is utilized as Eps value for DBSCAN. These estimated values are provided to DBSCAN algorithm. Time necessity of BScan algorithm is  $O(n \log n)$ , where ‘n’ refers to the size of dataset and as of this it is not appropriate for huge datasets. This is merged with k-distance graph to automatically choose MinPts and Eps values, rises to  $O(n^2 \log n)$ . This current investigation utilizes KD Tree (space partitioning tree) to diminish time complexity to  $O(\log n)$  time. When utilizing KD-Tree attaining k closest neighbors for every ‘n’ data point complexity is  $O(kn \log n)$ . k value is extremely trivial and henceforth does not make huge varies and therefore time complexity turns to be  $O(n \log n)$ . MinPts and Eps factors are described, they are used in clustering of user accounts.

**Partial Labeling:** Once the list of clusters is obtained, the next step is to compare them with the attacker’s potential behaviors, and mark those clusters that are highly likely to be malicious or legal [11, 12]. After the labeling process is completed, the semi-supervised learning method is employed for user account classification.

**DAS3VM:** The last step of the classification is to apply semi-supervised learning techniques on the partially labeled dataset obtained from the previous step. The algorithm has three parameters [12–15]. The regularization parameters  $\lambda$  controls the tradeoff between maximizing the hyper plane margin, and minimizing the misclassification rate. The second parameter  $\lambda'$  controls the influence of unlabelled data, and reflects the confidence in the cluster assumption. The third parameter  $r$  is estimated based on the clustering result. In order to classify each node into one among the three types (low, medium or high risk), the “one-vs-all” approach is adopted:

- For each of the three types of labels –  $H1$ ,  $H2$  and  $L$ , we build the corresponding SVM, and then use it to test all the nodes.
- Each node is given three scores –  $SH1$ ,  $SH2$  and  $SL$ . A node is finally labeled as  $H1$  ( $H2$ ,  $L$ ) if and only if  $SH1$  ( $SH2$ ,  $SL$ ) is positive while the other two scores are negative. Otherwise, the node is labeled as  $M$  (medium risk).
- Nodes labeled as  $H1$  and  $H2$  are combined to  $H$ .

This process of account classification is very efficient as the account classification is highly accurate. But it cannot be termed as 100% accurate, as the clever attackers will adapt their behaviors accordingly. However, it should be noted that the objective of the proposed classification approach is not accurately labeling high risk accounts, but rather carefully choosing the hyper plane corresponding to  $L$ , so that it is difficult or expensive for attackers to be classified as low risk. Once this objective is achieved, the two-player security game approach is evaluated. However, the classification scheme provides sub-optimal solutions which are needed to be enhanced in order to avoid maximum activities of clever attackers.

**Branch and Bound for DAS3VM:** The classification function  $f$  corresponding to  $L$  over the space  $\chi$ , where  $\chi$  is usually discrete has to be minimized. Branch and bound algorithm exhibits two significant components:

**Branching:** Region  $\chi$  is partitioned recursively into smaller sub-regions. This offers a tree structure where every node is associated to a sub-region.

**Bounding:** Assume two (disjoint) sub-regions, that is, nodes  $A$  and  $B \subset \chi$ . If an upper bound on the best value of  $f$  against  $A$  is recognized and a lower bound (consider  $b$ ) on the best value of  $f$  against  $B$  is also recognized and if  $a < b$ . After that, there exists an element in subset  $A$  that is superior to every element of  $B$ . Therefore, while searching for global minimization, carefully remove the elements of  $B$  away from search: the sub-tree associated to  $B$  gets pruned.

$$D(\alpha, yU) = \sum_{i=1}^n \alpha_i - \frac{1}{2} \sum_{i,j=1}^n \alpha_i \alpha_j y_i y_j \left( K(x_i, x_j) + \frac{\delta_{ij}}{2C} \right)$$

Dual feasibility is  $\alpha_i \geq 0$  and  $\sum_{i=1}^n \alpha_i y_i = 0$

Vector  $\alpha(yU)$  must be attained that fulfills as dual is maximized.

$$D(\alpha(yU), yU) \leq \max D(\alpha, yU) = J(yU)$$

Subsequently, the branching procedure is carried out. Let  $s(L)$  refer to the SVM objective function that is trained on the labeled set.

$$s(L) = \min \frac{1}{2} w^2 + C \sum_{(x_i, y_i) \in L} \max(0, 1 - y_i(w \cdot x_i + b))^2$$

Lower bound  $s(L)$  is utilized for the branching method which comprises selection of an appropriate point in  $U$ ,

$$\arg \max_{x \in U, y \in \pm 1} s(L \cup \{x, y\})$$

**Algorithm 2: Branch and bound for DAS3VM**

```

Function:  $(Y^*, v)$  DAS3VM( $Y, ub$ )
Input:  $Y$ : Partially labeled vector (0 for unlabeled)
          $ub$ : upper bound on optimal objective value.
Output:  $Y^*$ : optimally complete labeled vector
          $v$ : objective function.
If  $\sum \max(0, Y_i) > ur$  then
return
end if
 $v \leftarrow SVM(Y)$  //Evaluate SVM
objective function over labeled points
if  $v > ub$  then
return //lower bound is
superior than upper bound
end if
if  $Y$  is completely labeled then
 $Y^* \leftarrow Y$ 
Return
end if
Attain index  $i$  and label  $y$  //Identify
subsequent unlabeled point to label
 $Y_i \leftarrow -y$  //Initiate first by
most likely label
 $(Y^*, v) \leftarrow DAS3VM(Y, ub)$  //Identify
(recursively) best solution
 $Y_i \leftarrow -Y_i$  //Switch label
 $(Y^*, v) \leftarrow DAS3VM(Y, \min(ub, v))$  //Explore
other branch with revised upper-bound
if  $v_2 < v$  then
 $Y^* \leftarrow Y^*_2$  and  $v \leftarrow v_2$  //Maintain best
solution
End if

```

Thus the optimal solutions for the DAS3VM classification are obtained and hence the user accounts are classified accurately.

**Two-Player Security Game Approach:** As stated [8], once the user accounts are classified, the game approach is employed for enhancing the defense mechanism. The attacker's behavior, as found earlier, when the attacker starts their first VM (there is no incentive for attackers to start more than one VM at first, as none of them will co-locate with the targets), they are labeled as medium risk. In order to be reclassified as low risk, the attacker has to keep the first VM running before starting more VMs. This is called

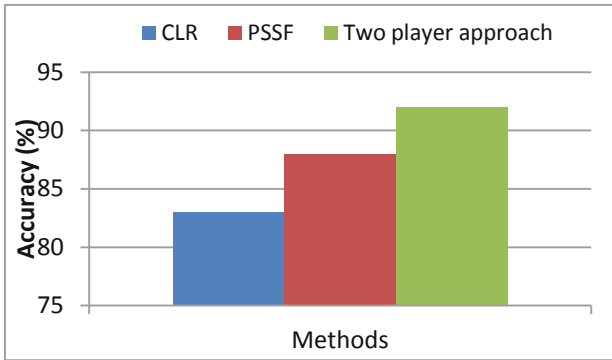
the initial cost. After being labeled as low risk, the attacker can create as many VMs as they want. However, they have to carefully control the pace, so that they will not be reclassified as medium or even high risk.

## 4 Performance Evaluation

The performance of the proposed two-player game approach based defense mechanism (referred as Two-player approach in graphs) is evaluated in CloudSim.

**Classification Accuracy:** Accuracy is the percentage corresponding to the correctly done classification of user accounts as legal and malicious users.

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{FN} + \text{FP} + \text{TN})} * 100$$

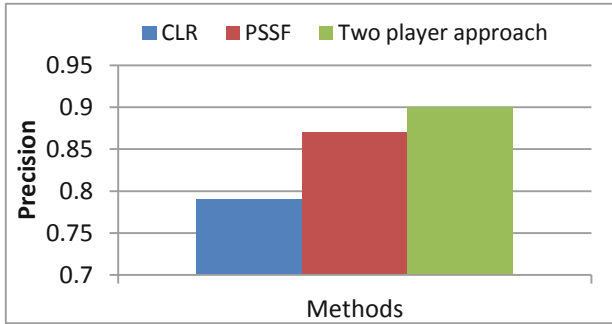


**Fig. 2.** Accuracy comparison

Figure 2 shows comparison of defense mechanisms based on accuracy. From the graph, it can be found that the proposed Two-player approach provides highly accurate classification.

**Precision:** Precision is the correctness of the classification of the user accounts (Fig. 3).

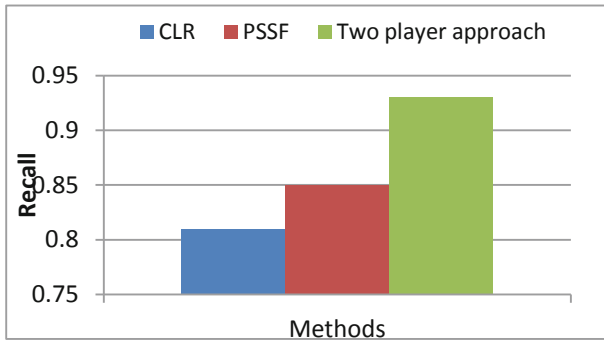
$$\text{Precision} = \frac{\text{TN}}{(\text{TP} + \text{FP})} * 100$$



**Fig. 3.** Precision comparison

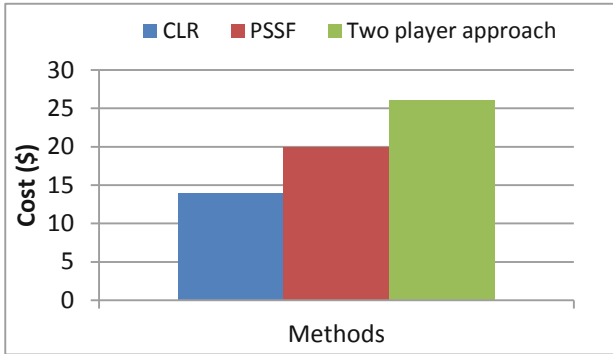
**Recall:** Recall is the completeness of the classification done in the cloud user accounts (Fig. 4).

$$\text{Recall} = \frac{\text{TN}}{(\text{TP} + \text{FN})} * 100$$



**Fig. 4.** Recall comparison

**Attacker's Overall Cost:** This parameter helps in evaluating the cost incurred for initiating an attack i.e. creating a new account for initiating a new VM. The cost is represented in US dollars (\$) for common cost evaluation (Fig. 5).



**Fig. 5.** Attacker's overall cost comparison

From the graph, the cost incurred by the attacker to initiate a co-resident DOS attack is higher in proposed two-player approach than the other methods. It is evident that the proposed defense mechanism makes it difficult for an attacker by making an attack process highly expensive.

## 5 Conclusion

This paper demonstrates an efficient two-player game based defense mechanism to minimize the attackers from launching co-resident DOS attacks. Though many game based methods have been developed previously, most of them focus on eliminating the side channels to avoid attacks.

## References

1. Bedi, H.S., Shiva, S.: Securing cloud infrastructure against co-resident DoS attacks using game theoretic defense mechanisms. In: Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp. 463–469. ACM (2012)
2. Han, Y., Alpcan, T., Chan, J., Leckie, C.: Security games for virtual machine allocation in cloud computing. In: International Conference on Decision and Game Theory for Security, pp. 99–118. Springer, Cham (2013)
3. Han, Y., Alpcan, T., Chan, J., Leckie, C., Rubinstein, B.I.: A game theoretical approach to defend against co-resident attacks in cloud computing: preventing co-residence using semi-supervised learning. *IEEE Trans. Inf. Forensics Secur.* **11**(3), 556–570 (2016)
4. Kwiat, L., Kamhoua, C.A., Kwiat, K.A., Tang, J., Martin, A.: Security-aware virtual machine allocation in the cloud: A game theoretic approach. In: 2015 IEEE 8th International Conference on Cloud Computing, pp. 556–563. IEEE (2015)
5. Do, C.T., Tran, N.H., Hong, C., Kamhoua, C.A., Kwiat, K.A., Blasch, E., Ren, S., Pissinou, N., Iyengar, S.S.: Game theory for cyber security and privacy. *ACM Comput. Surv. (CSUR)* **50**(2), 30 (2017)

6. Chen, J., Zhu, Q.: Security as a service for cloud-enabled internet of controlled things under advanced persistent threats: a contract design approach. *IEEE Trans. Inf. Forensics Secur.* **12** (11), 2736–2750 (2017)
7. Njilla, L.Y., Pissinou, N., Makki, K.: Game theoretic modeling of security and trust relationship in cyberspace. *Int. J. Commun. Syst* **29**(9), 1500–1512 (2016)
8. Wu, H., Wang, W.: A game theory based collaborative security detection method for internet of things systems. *IEEE Trans. Inf. Forensics Secur.* **13**(6), 1432–1445 (2018)
9. Hasan, M.G.M.M., Rahman, M.A.: Protection by detection: a signaling game approach to mitigate co-resident attacks in cloud. In: 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), pp. 552–559. IEEE (2017)
10. Rethishkumar, S., Vijayakumar, R.: Two-Player Security Game Approach Based Co-Resident Dos Attack Defence Mechanism for Cloud Computing (2017)
11. Annapoorani, S., Srinivasan, B., Mylavathi, G.A.: Analysis of various virtual machine attacks in cloud computing. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 1016–1019. IEEE (2018)
12. Jebalia, M., Letaïfa, A.B., Hamdi, M., Tabbane, S.: A secure data storage based on revocation game-theoretic approaches in cloud computing environments. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 435–440. IEEE (2017)
13. Abdul Wahab, O.: Game-theoretic foundations for forming trusted coalitions of multi-cloud services in the presence of active and passive attacks. Ph.D. dissertation, Concordia University (2017)
14. Njilla, L.L.Y.: Modeling Security and Resource Allocation for Mobile Multi-hop Wireless Networks Using Game Theory (2015)
15. Shoaib, Y., Das, O.: Pouring cloud virtualization security inside out. arXiv preprint [arXiv: 1411.3771](https://arxiv.org/abs/1411.3771)(2014)
16. Zhang, Y., Reiter, M.K.: Düppel: retrofitting commodity operating systems to mitigate cache side channels in the cloud. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp. 827–838. ACM (2013)





# Fuzzy Systems: A Human Reasoning Approach Using Linguistic Variables

Shama Parveen<sup>(✉)</sup>, Suraiya Parveen, and Nafisur Rahman

Department of Computer Science and Engineering, School of Engineering  
Sciences and Technology, Jamia Hamdard, New Delhi, India  
alamshama92@gmail.com, husainsuraiya@gmail.com,  
nafis@gmail.com

**Abstract.** The term “Fuzzy” means vague or imprecise or uncertain or inexact. Fuzzy Sets enable us to accept the vagueness and lack of precision. Fuzzy Sets are used when classical/crisp representation cannot make the decision for a problem. Fuzzy Set Theory is a vast field and relies heavily on mathematical equations. This paper is an attempt to capture its essence without getting overwhelmed by the complexity of details. In this paper, we have confined our discussions about Fuzzy Sets and its operations in contrast to Classical Sets. We have started with Classical Sets followed by a discussion on how a Classical Set fails in some of the problems and how Fuzzy Sets overcome those issues. Then we have briefly discussed the Linguistic Variables and how it is more practical and realistic than a binary reasoning. For the sake of simplicity and understanding, we have tried to avoid mathematical equations wherever possible.

**Keywords:** Fuzzy Sets · Membership function · Classical Sets · Linguistic Variables

## 1 Introduction

Fuzzy [1–3] Sets deal with the information that is vague, imprecise, uncertain, ambiguous, inexact, or probabilistic [4] in nature. *Fuzzy Sets* are associated with the membership function whose range is between 0 and 1. *Fuzzy Sets* are used in the development of Fuzzy Control Systems to make the appropriate decision. *Fuzzy Sets* differs from classical/crisp sets with the help of membership function and its operations. A *Linguistic Variable* [6] is a variable whose value is given by a word or a sentence rather than a numeric value.

In this paper, we have compared *Fuzzy Sets* with *Classical Sets* and established its superiority in terms of practical usage. We have documented the theoretical foundations of the subject matter after going through some notable works in the field. This work is aimed at presenting a lucid overview of the concepts to a naïve reader.

After this brief Introduction in Sect. 1, Sect. 2 contains a discussion on *Classical Sets* followed by the formal discussion on *Fuzzy Sets* in Sect. 3. Section 4 contains a discussion on *Classical Sets* Operations in comparison with a *Fuzzy Sets* Operations in Sect. 5. In Sect. 6 there is a brief discussion on Linguistic Variable and last Sect. 7 is our conclusion.

## 2 Classical Sets

Before starting with *Fuzzy Sets* let us first take a brief look at classical/crisp sets. A set is defined as a collection of well-defined objects.

For example:

- Collection of even integers.
- Collection of prime numbers.
- Collection of vowels.

The *Classical Set* is defined in such a way that the universe of discourse (X, as a collection of objects all having the same characteristics) is divided into two groups: member and non-member.

Suppose an object x in a *Classical Set* A. This object x is either a member or a non-member of the given set A.

Let the universe of discourse be A. A collection of elements within a universe are called sets and collection of elements within a set is called subsets.

For a *Classical Set* A in universe X:

- An object x is a member of set A ( $x \in A$ ), i.e., x belongs to A.
- An object x is a non-member of set A ( $x \notin A$ ), i.e., x doesn't belong to A.

The *Classical Set* allows membership of elements in binary form i.e. 0 or 1.

Mathematically, the *Classical Set* can be defined as:

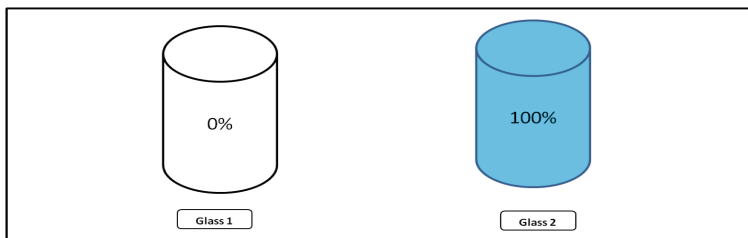
Let U be the universal set.

A *Classical Set* 'A' of the set U is characterized by

$$A = \{x, x \in U\}$$

Where A = *Classical Set*, x = value, and U = universal set.

Let us take an example of two glasses where one is empty and another is full of water. By looking at Fig. 1 below, we can easily identify which glass is full and which one is empty. There is no ambiguity in the decision.



**Fig. 1.** Classical Sets example

### 3 Fuzzy Sets

*Fuzzy Set* [1] Theory was first proposed by Lotfi A. Zadeh in 1965. The word “fuzzy” means “ambiguous”. The *Fuzzy Set* Theory is a generalization of a Classical or Crisp Set Theory. A *Fuzzy Set* is a class of object with the continuity of value of membership. This set is characterized by a membership function which is assigned to each object with a different membership value ranging from 0 to 1.

Let us take an example where we have four glasses of equal size. Each of these glasses, are respectively 0%, 20%, 80%, and 100% filled with water. Looking at the Fig. 2 below, we cannot decide whether a glass is full or empty. There is an ambiguity. The glass 1 which has 0% water is empty and the glass 4 which is 100% filled with water is full. But the glass 2 which is 20% filled and the glass 3 which is 80% filled is neither full nor empty. So, we can’t say that both are full or empty; there is an ambiguity.

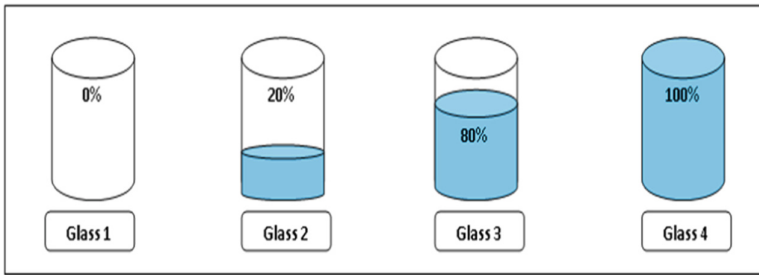


Fig. 2. Fuzzy Sets example

So, *Fuzzy Sets* viz. ‘Empty’ and ‘Full’ will allow the ambiguity with the help of degrees or grades of membership as follows:

Full {Glass 1(0), Glass 2(0.2), Glass 3(0.8), Glass 4(1)}

Empty {Glass 1(1), Glass 2(0.8), Glass 3(0.2), Glass 4(0)}

Here, Glass 1(0), Glass 2(0.2) ... Glass 4(1) form a membership function which contains membership value like 0, 0.2, 0.8 etc. lying between 0 & 1(including 0 & 1).

It can be graphically represented as (Fig. 3):

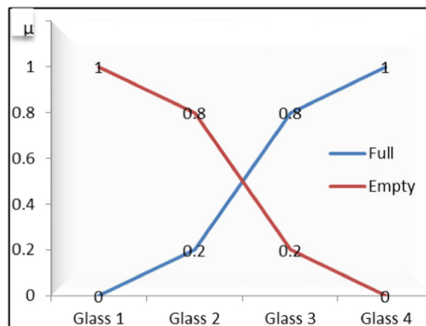


Fig. 3. Graphical representation

Mathematically, *Fuzzy Set* can be defined as:

Let  $U$  be the universal set.

A *Fuzzy Set* 'A' of the set  $U$  is characterized by its membership function  $\mu$  defined by

$$A = \{(x, \mu(x)) : x \in U\}$$

Where  $A = \text{Fuzzy Set}$ ,  $x = \text{value}$ ,  $\mu(x) = \text{membership function}$  and  $U = \text{universal set}$ .

It means that for every  $x \in U$ ,  $x$  does also belong to  $A$  by an amount  $\mu(x)$  where  $0 \leq \mu(x) \leq 1$ .

## 4 Classical Set Operations

Before understanding a *Fuzzy Set* operation lets briefly overview the basic *Classical Set* operations (Fig. 4).

The basic operations of the *Classical Set* are as follows:

### Union

It contains all the elements of set  $A$  or set  $B$ . It is also called as Logical 'OR'.

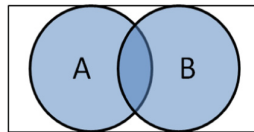
$$A \cup B = \{x | A \text{ or } x \in B\}$$

Example:

Set  $A = \{a, b, c\}$

Set  $B = \{c, d, e\}$

Set  $A \cup B = \{a, b, c, d, e\}$



**Fig. 4.** Classical union operation

### Intersection

It contains the common elements that are present in set  $A$  and set  $B$ . It is also called as Logical 'AND' (Fig. 5).

$$A \cap B = \{x | x \in A \text{ and } x \in B\}$$

Example:

Set  $A = \{a, b, c\}$

Set  $B = \{c, d, e\}$

Set  $A \cap B = \{c\}$

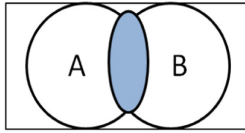


Fig. 5. Classical intersection operation

**Complement**

It contains the entire element but accepts the elements which are present in set A. It is also called as Logical ‘NOT’ (Fig. 6).

$$\bar{A} = \{x|x \notin A, x \in X\}$$

Example:

Set X = {a, e, i, o, u}

Set A = {a}

Set  $\bar{A}$  = {e, i, o, u}

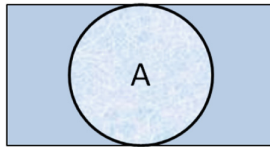


Fig. 6. Classical complement operation

**5 Fuzzy Set Operations**

Now the basic operation of *Fuzzy Set* is similar to the *Classical Set* but there is a difference in calculating the value of operations.

Basic operations of *Fuzzy Set* are:-

**Union**

The membership function of Union of two *Fuzzy Set* A and B ( $\mu_{A \cup B}$ ) is a maximum of membership function of  $\mu_A$  and  $\mu_B$ .

The Union operation of *Fuzzy Set* is equivalent to the Binary operation ‘OR’.

$$\mu_{A \cup B}(x) = \max[\mu_A(x), \mu_B(x)] \text{ for all } x \in U = \mu_A(x) \vee \mu_B(x);$$

Here  $\vee$  is the symbol for maximum (Fig. 7).

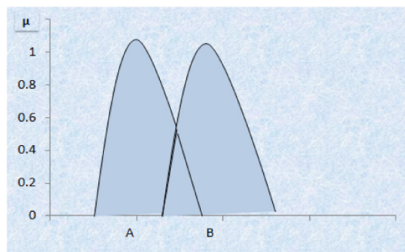


Fig. 7. Fuzzy union operation

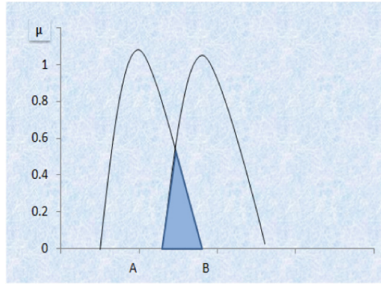
**Intersection**

The membership function of Intersection of two *Fuzzy Set* A and B ( $\mu_A \cap B$ ) is a minimum of membership function of  $\mu_A$  and  $\mu_B$ .

The Intersection operation of *Fuzzy Set* is equivalent to the Binary operation ‘AND’.

$$\mu_{A \cap B}(x) = \min[\mu_A(x), \mu_B(x)] \text{ for all } x \in U = \mu_A(x) \wedge \mu_B(x);$$

Here  $\wedge$  is the symbol for minimum (Fig. 8).



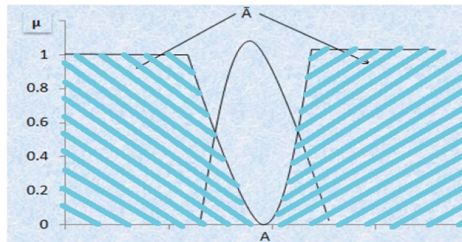
**Fig. 8.** Fuzzy intersection operation

**Complement**

The membership function of Complement of a *Fuzzy Set* A ( $\mu_{\bar{A}}$ ) is a negation of membership function of  $\mu_A$ .

The Complement operation of *Fuzzy Set* is equivalent to the Binary operation ‘NOT’ (Fig. 9).

$$\mu_{\bar{A}}(x) = 1 - \mu_A(x)$$



**Fig. 9.** Fuzzy complement operation

**6 Linguistic Variables**

It is one of the important concepts in *Fuzzy Logic* which played a vital role in the Fuzzy System. The *Linguistic Variable* [6] means a variable whose values are in words or a sentence in a natural language instead of numerical value. For example, a word like

Temperature is the *Linguistic Variable* if its value is linguistic rather than a numerical value i.e. very cold, cold, warm, hot, very hot, etc., rather than 5, 15, 25, 35, 45... Here *Linguistic Variable* temperature represents the temperature of a room.

*Linguistic Variable* can also be defined by:  $(x, T(x), U, M)$  where  $x$  is the name of the variable,  $T(x)$  is term-set i.e. the set of linguistic values assigned to  $x$ ,  $U$  is the universe of discourse, and  $M$  is the semantic rule associated with each variable (membership) i.e. it defines the membership function of each fuzzy variable; for example  $M(\text{cold}) =$  the fuzzy set for temperature below 25 with membership of  $\mu_{\text{cold}}$ .

Consider an example where  $x$ : temperature is defined as a *Linguistic Variable*,  $T$  (temperature): {very cold, cold, warm, hot, very hot},  $U$ : {0, 60},  $M$ : define the membership function ( $\mu$ ) of each variable, for instance,  $M(\text{hot}) =$  Fuzzy Set for temperature above 35° with membership of  $\mu_{\text{hot}}$  (Fig. 10).

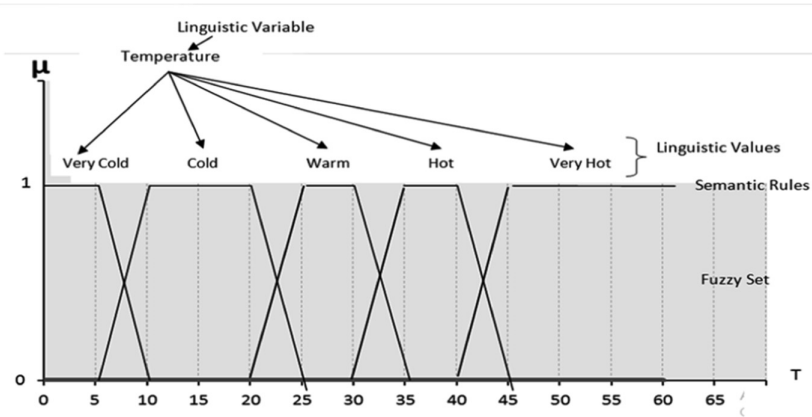


Fig. 10. Linguistic Variables

In the above example Linguistic Variable, Temperature is having a Linguistic values such as very cold lies between the range [0, 10], cold lies between the range [5, 25], warm lies between the range [20, 35], hot lies between the range [30, 45], and very hot lies between the range [40, 60].

The concepts of Linguistic Variable provide a mean of approximate characterization of concepts which are complex or not well-defined to be responsive to describe in quantitative terms. When the information which is not exact nor very in exact than *Linguistic Variable* offer a more realistic framework for human reasoning than the two valued logic i.e. true or false.

The main applications of the *Linguistic Variable* is especially in the fields of artificial intelligence, human decision processes, pattern recognition, psychology, law, medical diagnosis, information retrieval, economics and related areas.

## 7 Conclusion

In the above discussion, we have presented the theory of *Fuzzy Sets* in contrast to the classical/crisp set in simple terms. Also, we have discussed the *Linguistic Variables* that make things more realistic. The concepts of *Fuzzy Sets* pave the way for various advanced theories [7, 8] and implementations that has been documented extensively. Though the works related to these areas are widespread now, they are still grabbing the attention of the researchers and are frequently being cited. The industry is coming up with various kinds of innovative implementations based on *Fuzzy Logic*.

## References

1. Zadeh, L.A.: Fuzzy sets. *Inf. Control* **8**(3), 338–353 (1965)
2. Bellman, R., Kalaba, R., Zadeh, L.A.: Abstraction and pattern classification. *J. Math. Anal. Appl.* **13**(1), 1–7 (1966)
3. Halmos, P.R.: *Naive Set Theory*. Van Nostrand, New York (1960)
4. Zadeh, L.A.: Fuzzy Sets as a basis for a theory of possibility. *Fuzzy Sets Syst.* **1**(1), 3–28 (1978)
5. Zadeh, L.A.: The concept of a linguistic variable and its application to approximate reasoning —I. *Inf. Sci.* **8**(3), 199–249 (1975)
6. Zadeh, L.A.: The concept of a linguistic variable and its application to approximate reasoning —II. *Inf. Sci.* **8**(4), 301–357 (1975)
7. Zadeh, L.A.: Calculus of fuzzy restrictions. In: *Proceedings of US-Japan Seminar on Fuzzy Sets and their Applications*, pp. 1–39 (1975)
8. Bellman, R.E., Zadeh, L.A.: Local and fuzzy logics. In: Dunn, J.M., Epstein, G., Reidel, D. (eds.) *Modern Uses of Multiple-Valued Logics*, Dordrecht-Holland, pp. 103–165 (1977)





# Graph-Based Denormalization for Migrating Big Data from SQL Database to NoSQL Database

V. Rathika<sup>(✉)</sup>

Department of Computer Science, Mother Teresa Women's University,  
Kodaikanal, Tamil Nadu, India  
rathirajaphd2013@gmail.com

**Abstract.** In this big data era, the data storing methods are vary based upon the data type and the technologies upgradation. Due to the increase of voluminous data, the traditional Relational Database Management Systems (RDBMS) are immature to handle the unstructured data. To overcome this issue, NoSQL databases are used to store and process the unstructured data. The big data migration from SQL to NoSQL database is more complex. The SQL databases are well-normalized database. Denormalization plays a major role in retrieving the data more efficiently. This work is carried on migrating the big data from SQL to NoSQL database using the Graph-based Denormalization method. The proposed method is more efficient for big data migration and post-migration process.

**Keywords:** Big data · Data migration · Denormalization · Map Reduce · NoSQL database

## 1 Introduction

In the earlier days, it was very difficult to scale the disk space for data storage. Nowadays, in the big data era, it is easy to increase the disk space with help of new techniques and technologies. Thus, the big data is not more challengeable part in the data storage. But the massive data is more challengeable for the database administrators for migrating the big data from one database to another database. Due to the incredible growth of technologies, the normal structured database is not well suited to store the unstructured data. To overcome this problem the NoSQL database is introduced. Denormalization is a methodology which can be utilized on a formerly standardized database for the fastest data retrieval. In database computation, denormalization is the way toward attempting to enhance the read execution of a well-normalized database [1]. Sometime this will result in loss of some execution, due to the data redundancy [2].

Regularly, a well standardized database is planned to store varied data in distinct independent entities by linking each entity with some relations. In the event, these relations are put away physically as isolated circle of files in distinct disk. By carrying out a database query that draws data from a few relations (by using join query) which can be reduce the execution performance. The relations among the entities are numerous, then the read and write performance will be slow by the join query.

There are two methodologies that are practicing to address the above issues, they are as follows:

- i. Normalization allowing less redundant data
- ii. Denormalization methodology for efficient read/write execution

The first methodology is to keep the logical schema in normalized way and yet permit the DBMS to store extra repetitive data on circle to streamline for inquiry reaction. The second methodology is to denormalize the legitimate information plan. A denormalized information is not equivalent as an information display that has not been standardized. Denormalization should just happen after an agreeable level of standardization has occurred and that any required limitations as well as principles have been made to manage the irregularities in the plan. For instance, every one of the relations are in third ordinary shape and any relations with join and multi-esteemed conditions are dealt with properly. Denormalization strategies are regularly used to enhance the adaptability of Web applications [3].

### Types of Denormalization<sup>1</sup>

If the database is to be de-normalized, then there are several options that can be consider are represents in the Table 1:

**Table 1.** Methods for denormalization

S. No	Types	Description
1	Pre-joined tables	It can be used when the join is prohibitive
2	Report table	If the critical reports are too expensive, report table can be used
3	Physical denormalization	To take advantage of specific DBMS characteristics
4	Speed table	To support hierarchies like bill-of-materials or reporting structures
5	Combined tables	To consolidate one-to-one or one-to-many relationships into a single table
6	Split tables	The split could be tuples-wise or attribute-wise depending upon the needs of the accessing applications
7	Mirror table	When tables are required concurrently by two types of environments

<sup>1</sup> <https://datatechnologytoday.wordpress.com/2015/08/03/optimizing-database-performance-part-2-denormalization-and-clustering/>.

## 2 Related Works

Because of the fame of NoSQL databases, a great deal of works were examined and broke down the SQL and NoSQL databases. For instance, the researchers had examined issues about complex information structures in the NoSQL database [4]. The authors broke down the execution among SQL and key-esteem NoSQL databases [5]. In an article the author [6] thought about Oracle, i.e., the standard SQL database, and MongoDB, i.e., the NoSQL database from hypothetical contrasts, include confinements and framework design. Moreover, [7] distinguished issues and difficulties in taking care of enormous information utilizing MapReduce. The author [8] had considered the correlation among HBase and other NoSQL databases, e.g., BigTable, Cassandra, CouchDB, MongoDB, and so on. In this article the author [9] gave a way to deal with migrating information among various section between SQL and NoSQL databases. The meta model was proposed to state the information in a typical arrangement and in charge of the interpretation from a source database to the targeted database.

For instance, the author had [10] proposed and built a connection system for migrating the data using Sqoop into the HBase. HBase is a NoSQL database, [11] that consolidated every single related table into various segment families. The connections between the all SQL tables in the source database was migrated into one single NoSQL table. As to table settling conditions, [12] proposed a graph based migration. The author [13] had created Open PaaS Database API (ODBAPI) that is a streamlined and REST-based API to execute the CRUD activities, i.e., make, perused, refresh and erase, on the SQL and NoSQL databases. In this article the authors [14] had proposed an approach for migrating the data from RDBMS to NoSQL database using the query-oriented data model.

The author [15] had proposed a hypothetical model to actualize the HBase and get the created outcomes earlier. It was [16] actualized a middleware layer called Cloud TPS to empower join queries and keep solid value-based consistency over NoSQL databases, e.g., SimpleDB and HBase. With respect to report NoSQL database, the authors [17] had introduced a virtualization framework which migrated the data from SQL to MongoDB seamlessly. The author [18] had used MapReduce for reading the information from the SQL database. With respect to develop prerequisite of huge information, an ever increasing number of research scientists concentrate on how to incorporate SQL and NoSQL.

## 3 MR-DNORM<sub>GB</sub> Technique for Big Data Migration

The proposed method is built based on the column-joined denormalization technique. The column-joined technique is used to reduce the one-to-one or one-to-many relationships into single column. Three procedures are given below for the proposed Denormalization Approach. The main goal of the proposed technique is to increase the post-migration execution performance. Meanwhile, another responsibility is to reduce the total migration time taken between the data migration from RDBMS to NoSQL database. The meta-data are retrieved from the Meta database of the source database. Later, the constraints of the tables and attributes are listed to find the foreign keys of the

entities. For this proposed work, MySQL is taken as the RDBMS database whereas MongoDB is taken as the NoSQL database. Algorithm 1 presents the overall migration process of the proposed denormalization technique.

The relationship in between one entity to another entity is made up with the link of foreign keys. Here, it resembles by using the vertex-edges concept. The proposed technique is to delink the linked chains and merge the attributes to form as single document. To achieve the above said statement, the proposed denormalization technique is built based on the popular depth-first search method.

**Algorithm 1: Enhanced Denormalization Technique**

```

Input: D1          // D1 data from Source Database
Output: D2        // D2 data into Target Database
Extract()
1. Start
2. Extract_MD1 = {Table, Attributes} // Extract from Meta Database
3. Denorm_link() // Denormalizing for speedup the performance
4. Set_D2 = {Collections, fields} // Create entities in Source Database
5. ST ← {t1, t2, t3, ..., tn}
6. MapRed() // Parallel processing for record migration
7. End

```

### Entity and Attribute Level Denormalization

A basic technique for denormalize the database is at Entity and Attribute (EA) level. The EA level denormalization is the reverse process of the table normalization. This method would join the tables by mapping with the help of essential key constraints. Using the edge and vertices concept the one-to-one and one-to-many relationships are identified. This could be performed by using the narrow search method. Initially the foreign keys are identified to find the root table by using the child node. Here the parent node and child node are root table and referenced table respectively.

#### Definition 1

For a given Relational Schema,  $RS$ , the schema graph  $G = (C, K)$  with  $n$  vertices. A vertex  $c \in C$ , for  $\sigma = (c_1, c_2 \dots c_n)$  be the list of distinct elements of  $C$  which corresponds to an entity  $e \in RS$ . An edge  $k \in K$  corresponds to a primary and foreign key relationship between the separate tables and the tree is linked from the foreign key entity to the primary key entity.

In some cases, the foreign key may be a subclass of alternative composite-foreign key, then the above relational schema definition does not have an edge for the previous foreign key. To overcome this situation the column-level denormalization is used by the following definition.

**Definition 2**

For a given Relational Schema  $RS$ , the schema graph  $G = (C, K)$  with  $n$  vertices. Let us assume a transaction query  $q$ , then the transaction graph is defined as follows: A vertex  $c \in C$  corresponds to entity  $e$  mentioned in  $q$ . Entities with the similar term are named by their instance variables. Vertex  $v$  has attribute that may seem in NPFK join (Non-primary foreign key) predicates on entity  $e$ . An edge  $k \in K$  links to an inner join predicate between entity  $e$  on a primary key and entity  $d$  on a foreign key and is the graph structure directed from  $d$  to  $e$ . Here,  $e \neq d$ , the edge is labeled with foreign key.

From the above definitions it is clearly explained the applications of entity and attribute level denormalization. The attribute level denormalization is applied if there is need to undo the atomic principles.

**Algorithm 2: A Schema Migration Algorithm that uses Entity-Level Denormalization**

Input: SQL schema

Output: NoSQL schema

- 1: Generate a relational schema graph  $G$  from  $RS$
- 2: Make  $G$  acyclic or non-acyclic
- 3: Convert  $G$  into a set  $ST$  of schema trees
- 4: for (each schema tree  $T \in ST$ ) {
- 5:     create a collection for the root of  $T$
- 6:     for (each non-root vertex  $v$  of  $T$ ) {
- 7:         embed  $v$  into the parent node  $v_p$  of  $v$
- 8:         remove the foreign key in  $v_p$  that refers to  $v$
- 9:         for (each query  $q \in Q$ ) {
- 10:             build a transaction-query graph  $G(V, K)$  for  $q$
- 11:             add the columns of the vertex  $d$  to the entity  $e$
- 12:             }
- 13:         }
- 14:     }

The entity-attribute level denormalization for schema migration is given in the Algorithm 2. The SQL schema is given as input and the NoSQL schema is produced as output. As per the Definition 1, step 1 generates the graph for the relational schema. Based on the database structure, the cyclic or non-cyclic graph is generated. The generated graph is converted in schema trees which helps to identify the links between the entities. Delink the linked entity by using the entity-level denormalization. If foreign key presents with composite key, then step 9 will be executed. This algorithm produces the uninterrupted schema migration from SQL database to NoSQL database. The big data migration is carried out by using the Map Reduce algorithm which is given in the Algorithm 3. For the proposed technique, the standalone database server is utilized and experimented in the Linux based machine with 8 GB Ram and core i7 processor.

**Algorithm 3: Map Reduce based Data Migration from SQL to NoSQL Database**

Input: MySQL database  
Output: MongoDB Database

- 1: Start
- 2: Mapper function: *// input data*
- 3: Set the number of mappers
- 4: Set number of nodes
- 5: Assigns the entity and attribute as key
- 6: Assigns the instance as the value of the keys
- 7: If keys  $\neq$  0: go to step 9
- 8: else go to step 15
- 9: Sort function: *// data arrangements*
- 10: Obtained the rank of entity and attributes from MR-DENORM<sub>GB</sub>
- 11: Sorted based on the high relevancy to low
- 12: Reduce Function: *// output data (migrated)*
- 13: Create appropriate collections and fields in target database
- 14: Migrate data based on the key-value pairs
- 15: Stop

## 4 Results and Discussions

The proposed graph-based denormalization technique is evaluated using the two datasets. The comparative results are provided below. Results of proposed MR-DNORM<sub>GB</sub> is compared with the results of baseline MetaDatabase (API) techniques. From the results, it is easily observed that the migration time of the proposed work is slightly reduced when compared with the existing methods. Table 2, reveals the comparison between proposed technique and existing MetaDatabase (API) techniques for the Employees DB. It is noted that the denormalization takes more time than the usual schema conversion. Since the denormalization is performed on the entity and attribute levels. The time taken for the schema conversion using proposed technique is high when compared to the metadatabase technique. But it will reduce the data migration time, since the collection of tables are written into a single collection of the source database.

**Table 2.** Comparisons of MR-DNORM<sub>GB</sub> and MetaDatabase(API) migrating time for Employees DB

Techniques	# of rows				
	10000	40000	80000	120000	160000
MetaDatabaseAPI	80	170	410	1158	3256
MR-DNORM <sub>GB</sub>	67	121	256	491	1117

Figure 1 represents the comparisons of graphical chart of the data migration taken by the MR-DNORM<sub>GB</sub> and MetaDatabase (API) techniques. The X-axis denotes the number of the seconds and Y-axis denotes the number of records.

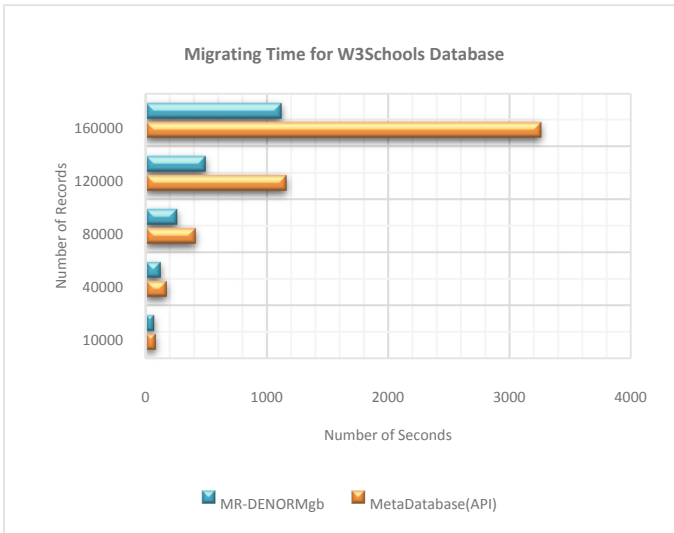


Fig. 1. MR-DNORM<sub>GB</sub> migrating time for Employees DB

Table 3 shows the comparative results of the data migration using MR-DNORM<sub>GB</sub> and MetaDatabase(API) techniques for the Tweets DB. It is found that, the graph-based denormalization technique made impact, if and only if there is the present of number of relationships among the entities.

Table 3. MR-DNORM<sub>GB</sub> migrating time for Tweets DB

Techniques	# of Rows				
	200000	400000	600000	800000	1000000
MetaDatabaseAPI	979	1900	3127	7052	9159
MR-DNORM <sub>GB</sub>	670	1080	1621	2959	3401

Figure 2 represents the graphical chart of the comparative results of the migrating time among the MR-DNORM<sub>GB</sub> and MetaDatabase (API) techniques. The X-axis refers to the number of seconds and Y-axis refers to the number of records taken for the data migration.

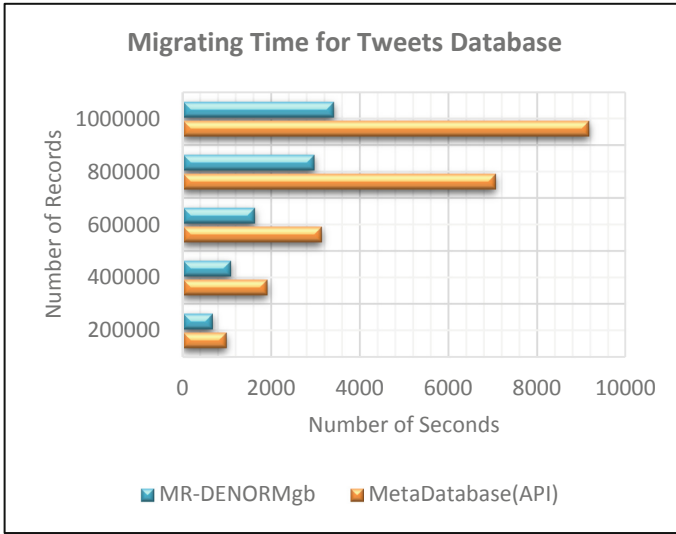


Fig. 2. MR-DNORM<sub>GB</sub> migrating time for Twitter DB

For evaluating the post-migration process, the comparative results are made between the normal SQL SELECT statement along with the JOIN query and NoSQL SELECT statement. Figure 3 depicts the graphical results of the SELECT statement used in the NoSQL database after the migration process of the Tweets DB. X-axis denotes the number of records and Y-axis denotes the number of seconds.

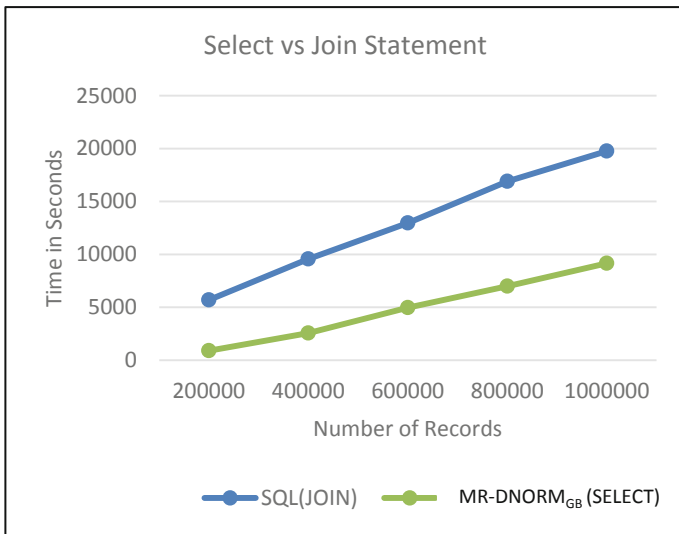


Fig. 3. Performance comparison over Twitter Database



The proposed MR-DNORM<sub>GB</sub> technique produced better results when compared to other techniques. It is shown, that the SELECT query performs 2.x time faster than other techniques.

Figure 4 depicts the graphical results of the SELECT statement used in the NoSQL database after the migration process of the Employees DB. X-axis denotes the number of records and Y-axis denotes the number of seconds. The proposed MR-DNORM<sub>GB</sub> technique produced better results when compared to other technique. It is shown, that the SELECT query performs 2.x time faster than other techniques.

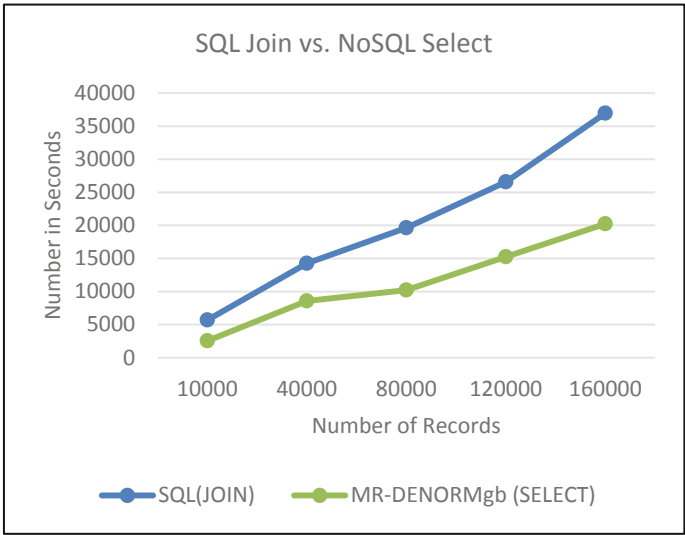


Fig. 4. Performance comparison over Employees Database

## 5 Conclusion

In this article, the graph-based denormalization method is proposed for an efficient schema conversion and post-migration process. The main advantage of the MR-DNORM<sub>GB</sub> technique is the efficient post-migration process. The ‘select’ query statement is considered as the post-migration process. Usually the join query statement is used for retrieving data from different entities. This will increase the execution time and reduce the overall query performance. In-order to solve this the depth first search based denormalization technique is used to reduce the data retrieval time. The proposed denormalization approach outperformed well when compared to the existing Meta-Database baseline method. It is also found that the proposed technique produced 2.x times faster in the data retrieval when compared to the existing techniques. Every method has its own disadvantages, where the denormalization method leads to the data redundancy. This will occupy more space in the disk, whereas the data retrieval is faster than the normalized database.

## References

1. Sanders, G.L., Shin, S.K.: Denormalization effects on performance of RDBMS. In: Proceedings of the HICSS Conference, January 2001
2. Shin, S.K., Sanders, G.L.: Denormalization strategies for data retrieval from data warehouses. *Decis. Support Syst.* **42**(1), 267–282 (2006)
3. Wei, Z., Dejun, J., Pierre, G., Chi, C.-H., van Steen, M.: Service-oriented data denormalization for scalable web applications. In: Proceedings of the International World-Wide Web Conference, April 2008
4. Lombardo, S., Di Nitto, E., Ardagna, D.: Issues in handling complex data structures with NoSQL databases. In: Proceedings of the 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), pp. 443–448, September 2012
5. Li, Y., Manoharan, S.: A performance comparison of SQL and NoSQL databases. In: Proceedings of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), pp. 15–19, August 2013
6. Boicea, A., Radulescu, F., Agapin, L.I.: MongoDB vs Oracle – database comparison. In: Proceedings of The 3rd International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), pp. 330–335, September 2012
7. Grolinger, K., Hayes, M., Higashino, W.A., L’Heureux, A., Allison, D.S., Capretz, M.A.M.: Challenges for MapReduce in big data. In: Proceedings of IEEE World Congress on Services (SERVICES), pp. 182–189, June 2014
8. Naheman, W., Wei, J.: Review of NoSQL databases and performance testing on HBase. In: Proceedings of International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), pp. 2304–2309, December 2013
9. Scavuzzo, M., Di Nitto, E., Ceri, S.: Interoperable data migration between NoSQL columnar databases. In: Proceedings of IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations (EDOCW), pp. 154–162, September 2014
10. Hsu, J.-C., Hsu, C.-H., Chen, S.-C., Chung, Y.-C.: Correlation aware technique for SQL to NoSQL transformation. In: Proceedings of the 7th International Conference on Ubi-Media Computing and Workshops (UMEDIA), pp. 43–46, July 2014
11. Zhao, G., Li, L., Li, Z., Lin, Q.: Multiple nested schema of HBase for migration from SQL. In: Proceedings of 9th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), pp. 338–343, November 2014
12. Zhao, G., Lin, Q., Li, L., Li, Z.: Schema conversion model of SQL database to NoSQL. In: Proceedings of 9th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), pp. 355–362, November 2014
13. Sellami, R., Bhiri, S., Defude, B.: ODBAPI: a unified REST API for relational and NoSQL data stores. In: Proceedings of IEEE International Congress on Big Data (BigData Congress), pp. 653–660, June 2014
14. Li, X., Ma, Z., Chen, H.: QODM: a query-oriented data modeling approach for NoSQL databases. In: Proceedings of IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA), pp. 338–345, September 2014
15. Gadkari, A., Nikam, V.B., Meshram, B.B.: Implementing joins over HBase on cloud platform. In: Proceedings of IEEE International Conference on Computer and Information Technology (CIT), pp. 547–554, September 2014

16. Wei, Z., Pierre, G., Chi, C.-H.: Scalable join queries in cloud data stores. In: Proceedings of the 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp. 547–555 May 2012
17. Lawrence, R.: Integration and virtualization of relational SQL and NoSQL systems including MySQL and MongoDB. In: Proceedings of International Conference on Computational Science and Computational Intelligence (CSCI), pp. 285–290, March 2014
18. Van Hieu, D., Smachat, S., Meesad, P.: MapReduce join strategies for key-value storage. In: Proceedings of the 11th International Joint Conference on Computer Science and Software Engineering (JCSSE), pp. 164–169, May 2014



# Quality Aware Data Aggregation Trees in Sensor Networks

Preeti Kale<sup>(✉)</sup> and Manisha J. Nene

Defence Institute of Advanced Technology, Pune, India  
{preeti\_pcse16,mjnene}@diat.ac.in

**Abstract.** Wireless Sensor Networks (WSNs) are key enablers for IoT and pervasive computing paradigm. While devices are being seamlessly enabled with connection and communication capabilities, exploring techniques to quantify and improve quality has gathered significance. This work explores quality of a Data Aggregation Tree (DAT) in sensor networks. DATs are building blocks for data collection in WSNs. In this work Quality of Experience (QoE) and Quality of Service (QoS) of DATs is evaluated using data aggregation ratio  $\alpha$  and generated data  $\delta$  respectively. An algorithm Quality Aware Data Aggregation Tree (QADAT) to construct a quality aware DAT is proposed. QADAT adapts the DAT to network and user expectation dynamics. Simulation results show the effectiveness of the proposed algorithm and demonstrates quality awareness through DAT adaptability.

**Keywords:** Quality of Service · Quality of Experience ·  
Data aggregation trees

## 1 Introduction

Wireless Sensor Networks are information and communication technology enablers for the Internet of Things (IoT) connecting everything in the smart world. IoT objects feature an IP address that allow connecting and communicating with other internet enabled objects extending internet connectivity to a diverse range of everyday things. Applications of IoT include smart cities, agriculture, home automation, healthcare, environmental monitoring, military surveillance and inventory tracking. While IoT supports interaction between everyday physical things, the paradigm of pervasive computing includes imperative technologies that cater to the anywhere anytime services of everyday things [6]. While devices are being seamlessly enabled with connection and communication capabilities, exploring techniques to quantify and improve quality have gathered significance. Quality can be measured in terms of Quality of Service (QoS), Quality of Experience (QoE) and Quality of Information (QoI) [2, 3, 8, 11] for sensor enabled devices. Sensor nodes are the building blocks for IoT and pervasive computing applications. A key target for the nodes is reduction in energy consumption for a sustainable smart world. This is facilitated by a WSN that

can adopt energy efficient techniques for routing and reduce number of packet transmissions [20, 24]. Transmission of packets between sensors consumes energy. In terms of power consumption, transmitting a single bit of data is equivalent to 800 instructions [16]. In such situations, employing data gathering mechanisms with prudent power utilization can address the objective of mitigating excessive energy consumption. Data Aggregation Tree (DAT) is one such technique that reduces packet transmissions by combining data [7, 19]. DAT in a sensor network efficiently collects data from the network. Efficiency is in terms of reducing the energy required for collecting data from all nodes in the network. Efficiency is also computed as improving the lifetime of a network. Many researchers have contributed towards minimizing energy consumption and maximizing network lifetime in sensor networks using DATs. DATs with minimum energy cost are described in [5, 12, 13, 15, 22, 25]. In these studies, it is assumed that all incoming data at a node is combined into one packet. DAT with maximum NL is discussed in several works [1, 9, 14, 21, 23]. In [10] DAT construction using path reestablishment is discussed. In [4, 17, 18] DATs are constructed with intermediate nodes aggregating incoming data into multiple packets. However, to the best of our knowledge, relating quality parameter to a DAT has not been explored.

This motivates us to investigate quality awareness of DATs. The following are the contributions.

1. Quality awareness of DATs is explored in terms of QoS and QoE. (Refer Sects. 2.1 and 2.2).
2. Proposed Quality Aware Data Aggregation Tree (QADAT) algorithm to construct a quality aware DAT. QADAT adapts the DAT to network and user expectation dynamics. (Refer Sect. 3)
3. Performance of QADAT is evaluated using simulations. Results show the efficacy of the proposed algorithm and demonstrate DAT adaptability. Refer (Sect. 4)

The remainder of this paper is organized as follows. Section 2 discusses QoS and QoE in a DAT. In Sect. 3, the problem is formulated and methodology for a quality aware DAT is proposed, devised and implemented. Section 4 describes the experimental setup and results. Finally Sect. 5 concludes the paper.

## 2 Quality of a DAT

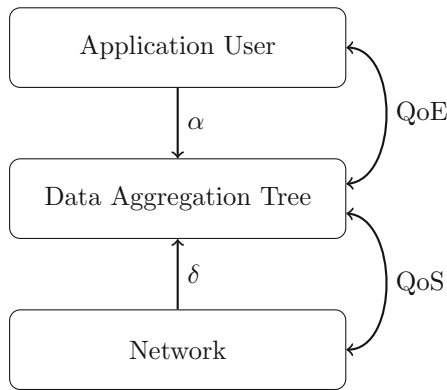
In this section QoS and QoE parameters for a DAT are identified and their suitability to applications is discussed.

Quality of a DAT is associated with its capacity to adapt to changing network and user needs. User requirements and expectations from a DAT depend on the underlying application. The application determines the data collection parameters of a DAT in the network. For example, in critical sensor applications like military surveillance, suspicious observations should be immediately reported. However in habitat monitoring applications, data is periodically reported.

In the proposed work, the DAT adaptability is facilitated by reevaluating and reestablishing multi-hop paths to suit the application dynamics. Paths in a DAT are influenced by several factors including environmental conditions, network transmission congestion, packet collisions and data collection parameters. This work reestablishes path in the DAT using data collection parameters given by

- data aggregation ratio  $\alpha$  and
- the amount of data  $\delta$  generated at each node.

Data aggregation ratio  $\alpha$  determines the number of data reports that can be combined into one packet. Amount of data  $\delta$  generated at each node decides the number of data packets each node transmits. Both of these parameters contribute towards DAT quality as shown in Fig. 1.



**Fig. 1.** Quality aware DAT in WSNs,  $\alpha$  is data aggregation ratio and  $\delta$  is amount of data generated

## 2.1 Quality of Service QoS

QoS objectively measures the performance parameters like packet loss, end to end delay, network lifetime for a given network. In the context of a DAT, the QoS provided by a DAT depends on the cost of a DAT. Higher DAT cost decreases network survivability and hampers QoS. In this work, DAT cost is determined by the energy consumed by all nodes in the network. Each node consumes energy in receiving data from child nodes and transmitting data to its parent node. Cost incurred can be reduced by employing techniques for balanced energy consumption to improve Network Lifetime (NL). NL is a QoS parameter for a DAT.

QoS is affected by  $\delta$  as shown in Fig. 1. If the nodes generate more (less) data, NL is reduced (improved).

## 2.2 Quality of Experience QoE for a DAT

QoE is the impact of the network behaviour on the end user that is not captured by network performance parameter measures. QoE in the context of a DAT measures the user expectations from attributes associated with collected data. Measuring user expectation requires awareness of the underlying application.

For example given a DAT

- Application: Habitat monitoring; Nodes sense and send temperature data
- User requirement: Collect and send temperature data periodically every  $t$  time units
- User expectation: Updated temperature values, every  $t$  time units.
- Attributes of collected data: In this case, attribute is be number of nodes from which data is collected.

In this example, the dynamics of user expectations and user requirements can be met by scanning the data attributes.

In the proposed work, the network captures user needs, controls the data collection parameters and modifies the underlying DAT. Application dependent data aggregation ratio  $\alpha$  decides user needs and QoE is provided by reestablishing communication paths in the DAT based on value of  $\alpha$ .

QoS and QoE together make the DAT aware of the user requirements and network limitations. With this information, a quality aware DAT adapts by refining path reestablishment decisions.

## 3 Quality Aware Data Aggregation Tree

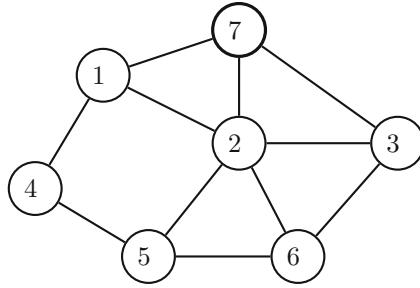
In this section, the problem of Quality Aware data aggregation Tree QAT is formulated and a methodology to construct a quality aware DAT is devised using examples. Finally an algorithm for Quality Aware Data Aggregation Tree (QADAT) is described.

### 3.1 Problem Formulation

This work considers random deployment of sensor nodes in the area of interest. The sensor network is represented as a graph  $G = (V, E)$ . The set of vertices  $V$  in the graph represent the sensor nodes and set of edges  $E$  represents communication links. For example, consider a randomly deployed sensor network of 6 nodes as shown in Fig. 2. The proposed technique constructs a DAT for  $G$  such that the DAT responds to changing user and network requirements given by  $\delta$  and  $\alpha$  (Refer Sects. 2.1 and 2.2). The problem is termed as Quality Aware data aggregation Tree (QAT) problem and stated as follows.

Given

- a sensor network represented as a graph  $G = (V, E)$
- the data aggregation ratio  $\alpha$  and
- data  $\delta_x$  generated by each node  $x$  in the network such that  $x \in V$

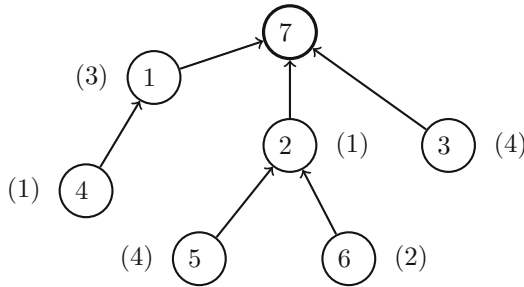


**Fig. 2.** A sensor network  $G = (V, E), V = \{1, 2, 3, 4, 5, 6, 7\}, E = \{(7, 1), (7, 2), (7, 3), (1, 4), (1, 2), (2, 5), (2, 6), (2, 3), (3, 6)\}$  node 7 is the sink node.

The objective of Quality Aware data aggregation Tree (QAT) problem is to construct a quality aware DAT  $D = (V_D, E_D)$  such that  $V_D = V, E_D \in E$  and the number of packet transmissions  $P_D$  required to collect data from all nodes is reduced.

### 3.2 Methodology

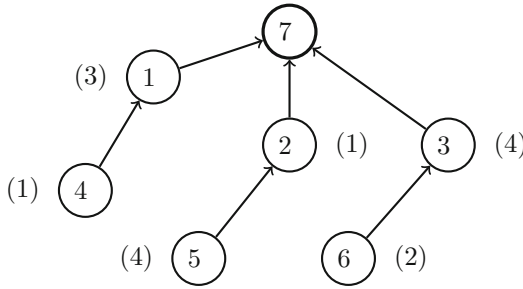
A key technique to construct a QA DAT is based on reducing the number of packet transmissions. This is effected by combining data at intermediate nodes using the values of  $\alpha$  and  $\delta$ . Consider the network shown in Fig. 2. Two possible DATs  $D_1$  and  $D_2$  for the network are given in Figs. 3 and 4 respectively.



**Fig. 3.** DAT  $D_1$  for  $\alpha = 3, P_{D_1} = 11$ .  $\delta_x$  is represented by values in brackets.

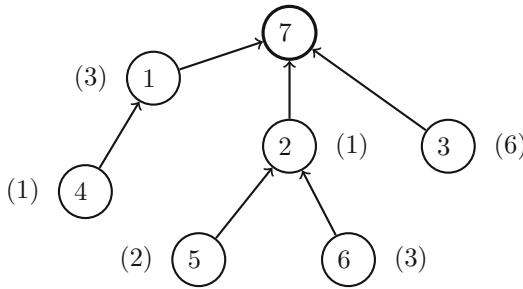
Let  $\alpha = 3$  signifying that at most 3 data reports can be combined into 1 packet. Consider path from node 4 to sink node 7 via intermediate node 1. In this case, node 4 transmits 1 packet and node 1 combines data reports to transmit 2 packets. Similarly paths (5, 2), (2, 6), (2, 7), (3, 7) transmit 2, 1, 3, 2 packets respectively. Total transmissions  $P_{D_1} = 11$ . For DAT  $D_2$ , total number of packet transmissions is given by  $P_{D_2} = 10$ . As more packet transmissions signify increased energy consumption and decreased QoS in the network,  $D_2$  is a quality aware DAT.



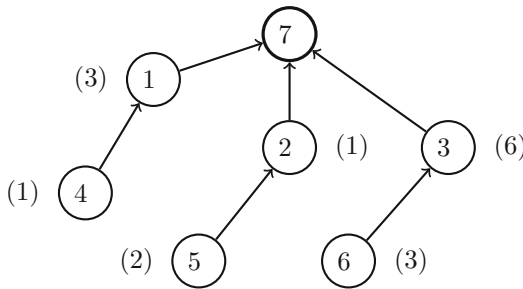


**Fig. 4.** DAT  $D_2$  for  $\alpha = 3, P_{D_2} = 10$ .  $\delta_x$  is represented by values in brackets.

To understand the effect of changing  $\alpha$  and  $\delta$  values on the DAT, it is assumed that  $\delta_3$  and  $\delta_6$  change to 6, 3 units respectively and  $\alpha$  changes to 2. The new values for DATs are represented in Figs. 5 and 6. For  $\alpha = 2, P_{D_1} = 12$  and  $P_{D_2} = 13$ , making  $D_1$  quality aware. This shows how changing  $\alpha, \delta$  values affect quality awareness of the DAT.



**Fig. 5.** DAT  $D_1$  for  $\alpha = 2, P_{D_1} = 12$ .  $\delta_x$  is represented by values in brackets.



**Fig. 6.** DAT  $D_2$  for  $\alpha = 2, P_{D_2} = 13$ .  $\delta_x$  is represented by values in brackets.

### 3.3 Algorithm QADAT

**Input** : A WSN represented by  $G = (V, E)$

**Output** : A quality aware DAT  $D$

**Steps**

1. Sink initiates DAT construction in the network.
2. Each node receives information about the nodes that lie in its communication range.
3. Each node selects a parent node and establishes a path to send data to the sink.
4. User requirements are captured using value of  $\alpha$ .
5. The network conditions are evaluated using value of  $\delta$ .
6. Each node reevaluates its path to the sink. If a path with less packet transmissions is identified then the path is reestablished.
7. Steps 4–6 are repeated as long as paths in DAT are successfully reestablished.

## 4 Simulation Results

In the simulation setup, WSNs are generated by deploying  $N$  sensor nodes in the area of interest. Deployment is in a  $10 \times 10$  sq.units field with transmission range at each node  $g = 2$ . The data units  $\delta$  generated by sensor nodes is randomly selected from the interval 1 to  $B$  where  $B = 5$  units. Data aggregation ratio  $\alpha$  is set between 1 to 100.

A randomly deployed sensor network of 30 nodes is shown in Fig. 7. Sink node 31 is randomly placed in the area of interest. Amount of data  $\delta$  generated by nodes 1 to 30 is 4, 5, 5, 1, 3, 5, 1, 2, 2, 1, 2, 1, 3, 4, 4, 5, 4, 2, 4, 1, 3, 3, 2, 1, 5, 3, 1, 3, 5, 5 data units respectively.

### 4.1 Observations for Quality Aware DAT When $\alpha = 1$

Figure 8 shows a quality aware DAT  $Q1$  when  $\alpha = 1$  for the network in Fig. 7. In this case, data generated at all nodes is individually transmitted. Quality awareness is controlled by the application criticality.

### 4.2 Observations for Quality Aware DAT When $\alpha = 25$

Figure 9 shows QA DAT for the network in Fig. 7 when  $\alpha = 25$ . In this case, maximum of 25 data units are combined into one packet at each intermediate node. The quality aware DAT  $Q2$  in this scenario differs from  $Q1$  as depicted by encircled nodes in Fig. 9. These nodes have reestablished their paths to the sink to suit QoE requirements given by  $\alpha = 25$ . For example, path  $(10 \rightarrow 22 \rightarrow 31)$  is reestablished as path  $(10 \rightarrow 19 \rightarrow 31)$

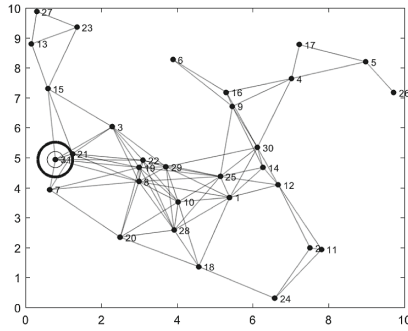


Fig. 7. An example connectivity graph  $G(V, E)$  representing initial random deployment of 30 nodes placed in a  $10 \times 10$  area with transmission range  $g = 2$ . Encircled node 31 is the sink node

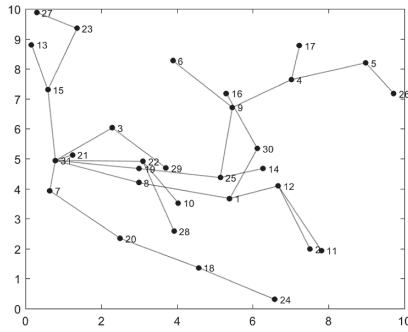


Fig. 8. Quality aware DAT  $Q1$  for  $\alpha = 1$

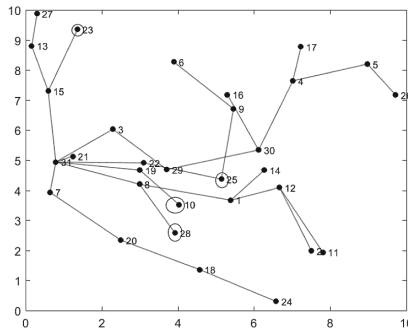


Fig. 9. Quality aware DAT  $Q2$  for  $\alpha = 25$

### 4.3 Observations for Quality Aware DAT When $\alpha = 100$

Figure 10 shows QA DAT for the network in Fig. 7 when  $\alpha = 100$ . In this case, maximum of 100 data units are combined into one packet at each intermediate node. The encircled nodes in Fig. 9 show nodes that have reestablished their paths to the sink to suit QoE requirements.

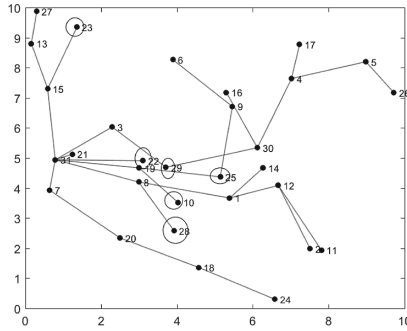


Fig. 10. Quality aware DAT Q3 for  $\alpha = 100$

## 5 Conclusion

WSNs are enablers for IoT and pervasive computing paradigm. Adopting energy efficient DAT for collecting data from the network is an essential requirement. Although efficient DAT construction techniques have been extensively studied, understanding quality of a DAT has not been sufficiently explored. In this paper, QoE and QoS parameters for a DAT are identified and discussed. The work proposes that data aggregation ratio  $\alpha$  and units of generated data  $\delta$  capture QoE and QoS parameters of a DAT respectively.

QADAT algorithm to construct a quality aware DAT is proposed and devised. QADAT allows the DAT to adapt to network and user expectation dynamics. Each node in a DAT evaluates and reestablishes communication paths to improve quality awareness of a DAT. Simulation results demonstrate the efficacy of the proposed algorithm. DAT for varying values of  $\alpha$  and  $\delta$  are simulated and demonstrate DAT adaptability.

Future work is formed by interesting challenges to maintain quality in dynamic environments where nodes fail or are unreachable.

## References

1. Al-Kiyumi, R.M., Foh, C.H., Vural, S., Chatzimisios, P., Tafazolli, R.: Fuzzy logic-based routing algorithm for lifetime enhancement in heterogeneous wireless sensor networks. *IEEE Trans. Green Commun. Network.* **2**(2), 517–532 (2018). <https://doi.org/10.1109/TGCN.2018.2799868>

2. Al-Turjman, F.M.: Information-centric sensor networks for cognitive IoT: an overview. *Ann. Telecommun.* **72**(1–2), 3–18 (2017)
3. Bisdikian, C., Kaplan, L.M., Srivastava, M.B.: On the quality and value of information in sensor networks. *ACM Trans. Sens. Netw. (TOSN)* **9**(4), 48 (2013)
4. Buragohain, C., Agrawal, D., Suri, S.: Power aware routing for sensor databases. In: *Proceedings of IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2005*, vol. 3, pp. 1747–1757. IEEE (2005)
5. Cristescu, R., Beferull-Lozano, B., Vetterli, M., Wattenhofer, R.: Network correlated data gathering with explicit communication: NP-completeness and algorithms. *IEEE/ACM Trans. Network.* **14**(1), 41–54 (2006)
6. Ebling, M.R.: Pervasive computing and the internet of things. *IEEE Pervasive Comput.* **15**(1), 2–4 (2016). <https://doi.org/10.1109/MPRV.2016.7>
7. Fasolo, E., Rossi, M., Widmer, J., Zorzi, M.: In-network aggregation techniques for wireless sensor networks: a survey. *Wirel. Commun.* **14**(2), 70–87 (2007)
8. Hassan, J., Das, S., Hassan, M., Bisdikian, C., Soldani, D.: Improving quality of experience for network services [guest editorial]. *IEEE Netw.* **24**(2), 4–6 (2010)
9. He, J., Ji, S., Pan, Y., Li, Y.: Constructing load-balanced data aggregation trees in probabilistic wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **25**(7), 1681–1690 (2014). <https://doi.org/10.1109/MWC.2007.358967>
10. Kale, P., Nene, M.J.: Path reestablishment in wireless sensor networks. In: *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 1659–1663, March 2017. <https://doi.org/10.1109/WiSPNET.2017.8300043>
11. Kilkki, K.: Quality of experience in communications ecosystem. *J. UCS* **14**(5), 615–624 (2008)
12. Krishnamachari, L., Estrin, D., Wicker, S.: The impact of data aggregation in wireless sensor networks. In: *22nd International Conference on Distributed Computing Systems Workshops, 2002 Proceedings*, pp. 575–578. IEEE (2002)
13. Kuo, T.W., Lin, K.C.J., Tsai, M.J.: On the construction of data aggregation tree with minimum energy cost in wireless sensor networks: NP-completeness and approximation algorithms. *IEEE Trans. Comput.* **65**(10), 3109–3121 (2016)
14. Lin, H.C., Chen, W.Y.: An approximation algorithm for the maximum-lifetime data aggregation tree problem in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **16**(6), 3787–3798 (2017). <https://doi.org/10.1109/TWC.2017.2688442>
15. Luo, H., Liu, Y., Das, S.K.: Routing correlated data in wireless sensor networks: a survey. *IEEE Netw.* **21**(6), 40–47 (2007)
16. Madden, S., Franklin, M.J., Hellerstein, J.M., Hong, W.: Tag: a tiny aggregation service for ad-hoc sensor networks. *SIGOPS Oper. Syst. Rev.* **36**(SI), 131–146 (2002). <https://doi.org/10.1145/844128.844142>
17. Matsuura, H.: Maximizing lifetime of multiple data aggregation trees in wireless sensor networks. In: *2016 IEEE/IFIP Network Operations and Management Symposium (NOMS)*, pp. 605–611. IEEE (2016)
18. Nguyen, N.T., Liu, B.H., Pham, V.T., Luo, Y.S.: On maximizing the lifetime for data aggregation in wireless sensor networks using virtual data aggregation trees. *Comput. Netw.* **105**(C), 99–110 (2016). <https://doi.org/10.1016/j.comnet.2016.05.022>
19. Rajagopalan, R., Varshney, P.K.: Data aggregation techniques in sensor networks: a survey (2006)
20. Shaikh, F.K., Zeadally, S., Exposito, E.: Enabling technologies for green internet of things. *IEEE Syst. J.* **11**(2), 983–994 (2017)

21. Shan, M., Chen, G., Luo, D., Zhu, X., Wu, X.: Building maximum lifetime shortest path data aggregation trees in wireless sensor networks. *ACM Trans. Sens. Netw. (TOSN)* **11**(1), 11 (2014)
22. Tan, H.Ö., Körpeovglu, I.: Power efficient data gathering and aggregation in wireless sensor networks. *ACM Sigmod Rec.* **32**(4), 66–71 (2003)
23. Wu, Y., Mao, Z., Fahmy, S., Shroff, N.B.: Constructing maximum-lifetime data-gathering forests in sensor networks. *IEEE/ACM Trans. Network.* **18**(5), 1571–1584 (2010)
24. Zhu, C., Leung, V.C.M., Shu, L., Ngai, E.C.H.: Green internet of things for smart world. *IEEE Access* **3**, 2151–2162 (2015). <https://doi.org/10.1109/ACCESS.2015.2497312>
25. Zhu, Y., Sundaresan, K., Sivakumar, R.: Practical limits on achievable energy improvements and useable delay tolerance in correlation aware data gathering in wireless sensor networks. In: 2005 Second Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE SECON 2005, pp. 328–339. IEEE (2005)



# Light Tracking Bot Endorsing Futuristic Underground Transportation

Ragul M. Gayathri, Bisati Sai Venkata Vikas, and J. Thomas<sup>(✉)</sup>

Department of Information Technology, Faculty of Engineering,  
CHRIST (Deemed to be University), Bengaluru, India  
ragul.m.gayathri@gmail.com, vikas.bisati@gmail.com,  
j.thomas@christuniversity.in

**Abstract.** Controlling a bot machine that uses non-conventional energy form, i.e. light is said to have an upper hand in pioneering transportation system. The expanding request of making the streets more secure has persuaded a ton of organizations to create finest autonomous vehicles. This paper will concentrate on the potential outcomes of utilizing just light-sensing gadgets alone for the light tracking bot using advanced color detection algorithm. The algorithm would help the bot in sensing the color of light and act accordingly, for instance green color to proceed, red color to stop. This particular requisition has high scope in real time application over the emergent underground transportation system; speculating on how the emerging innovative advances fit to the fiddle urban areas of the 21st century.

**Keywords:** Autonomous vehicles · Light-sensing · Color detection · Bot machine · Iot · Underground transportation

## 1 Introduction

Cities are the urbanised place of focus where many people live and work. Also there are some places for government trade and exchange and transportations with commercial associations. These days, there is a requirement for a superior transportation system which is necessary required to avoid this bulging clog. Elon Musk, CEO of Tesla Motors, has revealed a propelled vision of transportation including underground roadway structures underneath clamoring urban networks, for instance, Los Angeles. ‘The Boring Company’ is the undertaking that will impact everything to happen, also will rely upon a monstrous arrangement of entries (subsequently ‘debilitating’) and has been named “astonishing and impossible” by investigators. John McGuire, Chief Innovation Officer of Aurecon quotes “So also likewise with most extraordinary headways today, science fact was once science fiction. On the off chance that we will help structure the inevitable destiny of transport, we should have the ability to envision it”. A significant number of the world’s biggest urban communities have achieved their ability to retain new foundation ‘on the ground’. These urban communities are taking a gander at arrangements – both above and beneath the ground – to beat portability challenges. Exploring through since quite a while ago settled fabricated frame can be in fact and tastefully difficult, so making underneath the ground transport systems, for

example, underground rail and street burrows is high on numerous urban communities plans, and these undertakings are as of now changing urban areas around the globe. As far as energy is considered, it is a polymorphic quantitative conserved quantity. Being the only form of energy that can be directly seen, plays a vital role in locomoting path in circumstances of underground navigation through complex surroundings where electromagnetic radiation travels one path and not another.

Establishing a prepollency over a bot machine that has an ability to use the renewable resources namely light, wind, sound and so on is said to have an emphasized high ground in spearheading transportation framework system. The extending solicitation of making the avenues progressively secure has triggered a huge amount of associations to make best autonomous machines. An autonomous vehicle requires an unfathomable number of different sensors as lidars, gyros, radars, tachymeters, etc. and pushed programming as well. We might have, at any point, seen a feline seek after a laser pointer or a spotlight shaft. Imagine a scenario in which a robot doing the same. Light tracking bot machine, being a mobile robot which senses the light, follows the light on the locomoting path.

## 2 Details Experimental

### 2.1 Literature Survey

Nasrudin et al. [1] built a bot machine that has ability to pursue the white line put on a flat smooth surface lit by LED and the minimal effort light dependant resistor as the sensor. Thorough examination has been connected to decide the ideal design for the sensor on the versatile robot. The line following robot will distinguish the light force that is bounced back from the white shading way. Jia et al. [2] affirmed a model on averting impacts among cyclists and overwhelming products vehicles (HGVs). An impact shirking framework, which is intended to maintain a strategic distance from side-to-side crashes among HGVs and cyclists, is proposed. Manjur et al. [3] have exhibited a robot, which is minimized, self-sufficient and completely utilitarian. It is a proposed model which can be utilized in such a situation, which might be helpless and unsafe to individual. Kak et al. portrayed the model of the procedure of light examining for 3D robot vision by utilizing shot hypothesis [4]. Here the scanner adjusts by registering coefficient of lattice and a lot of lines are appeared. In this way picture pixels areas can be changed over into the world directions of protest focuses by utilizing grid. Kim et al. guaranteed that utilizing an attractive compass sensor, a cell phone controlled riding robot can be controlled by a rider to move with heading bearing of a cell phone [5]. Hasan et al. asserted in [6] that their robot which is a numerous source Multiple Destination Robot (MDR-1) could pursue exceptionally clogged bend getting constant information from the sensors and separate among different hues and pick an ideal line and its objective among various hued line as it could detect line. Likewise could recognize nearness of deterrent on its way having close circle control framework and revision framework.

Koren et al. expressed that the vector-field histogram is another constant snag shirking strategy for versatile techniques controlling the portable robot towards the



objective [7]. They created and tried effectively this technique on their bot machine. The calculation permits persistent and quick movement of portable robot ceaselessly for snag. The reaction of the vehicle is relied upon the probability for the presence of a snag. Johann et al. guaranteed another continuous deterrent evasion approach created and executed for portable robots [8]. To maintain a strategic distance from impacts and to progress towards the objective, this methodology permits recognizing obscure hindrances and guiding for keeping away from crashes and progressing forward. Arvin et al. depicted a system connected on an independent robot having two techniques in direction control in pivot and straight development which can keep up various speed in forward and turn around [9]. In [10], Uhler et al. portrayed a technique and a gadget having something like two close separation sensors introduced on a vehicle to identify objects. Ruler et al. asserted in [11] a portable robot having vision framework with the end goal that it includes something like one radiation projector where an organized light emission is anticipated.

## 2.2 Methodology

The substantiation has been made in premise of incorporating the capacity of light tracking. This is intended to be utilized in support of underground transportation framework where it very well may be traveled through client's chosen course by just utilizing light. In addition, the bot machine can recognize hindrance by utilizing sensor and move clockwise and anticlockwise which gets a reasonable course for itself. In the first place an investigation of the gear and the hypothesis behind their usefulness was made, to have the capacity to assess the correct use of the diverse segments. For the accompanying examination, a finish model is assembled based on Arduino programming and a bot machine equipment. Sensors and electric engine control are then added to the robot vehicle together with an additional power source fit as a fiddle of a battery bundle (Fig. 1).

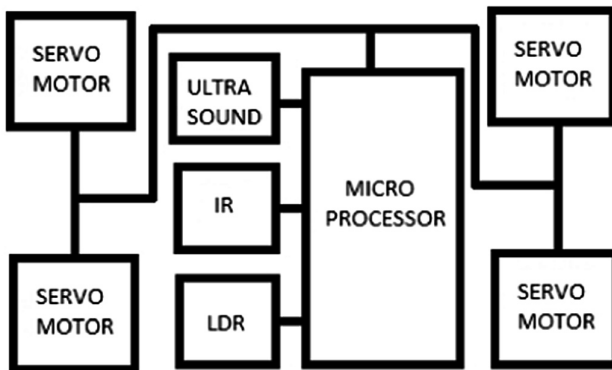


Fig. 1. System architecture of the light tracking bot machine

For the demonstration, a prototype of an underground system is made. The depiction of raised pavement markers are replaced by Light Emitting Diode strips, which assists the bot machine in moving by being the source of light. Light sensor is a gadget that recognizes the surrounding light dimension and sends a yield flag which differs with the light power. Light sensors retain light vitality and respond with a physical change in a range from infra-red to bright light and make power in type of electrons. Light dependent resistors (LDR) or photoresistors are light touchy gadgets frequently used to show the nearness or nonattendance of light, or to gauge the light force. In obscurity, their obstruction is high, here and there up to 1 M $\Omega$ , however when the LDR sensor is presented to light, the opposition drops significantly, even down to a couple of ohms, contingent upon the light power. LDRs have an affectability that differs with the wavelength of the light connected and are nonlinear gadgets. They are utilized in numerous applications however are in some cases made out of date by different gadgets, for example, photodiodes and phototransistors. A few nations have restricted LDRs made of lead or cadmium over ecological security concerns.

An infrared sensor emits in order to sense some aspects of the surroundings. It enables recognition of the color of LED strip. An ADC also provides an isolated measurement such as an electronic device that converts an input analog voltage or current to a digital number representing the magnitude of the voltage or current. Typically the digital output is a two's complement binary number that is proportional to the input, but there are other possibilities. The primary hardware for executing the work that our robot pursues the trail of light is LDR. Light Dependant Resistors are the resistors whose esteem changes relying upon the measure of encompassing light. Voltage levels are distinguished utilizing the simple pins which can gauge between 0–5 V. Obstruction esteems can be changed over into voltage changes by making a voltage divider.

A voltage divider takes in a voltage and after that yields a small amount of that voltage relative to the information voltage and the proportion of the two estimations of resistors utilized. The condition for which is: Yield Voltage = Input Voltage\*(RS2/(RS1 + RS2)) Here, RS1 is the main resistor estimation and RS2 is the esteem of the second. The less the measure of encompassing light is, the higher is the opposition, progressively encompassing light means a lower obstruction.

Algorithm 1 [Detecting the road lane via LDR (Double road instance)]:

---

```

If ((left_Lane_Bright=true) && (right_Lane_Bright=true))
Wheel=move(true)
Else
Brake()
End

```

---

The algorithm is proposed for double road instance. The value of light, emitted by the LED strip is going to decide the act of the bot whether to move or stop.

Algorithm 2 [Detecting the color of the light]:

---

```

If (color_Value=00ff00)
Wheel=move(true)
Else
Stop()
End

```

---

The algorithm proposed detects the color of the LED light. If value of “Green” color is encountered, then the bot machine follows the wavelength of the same and keeps a track of the LED strip alone.

### 3 Discussions and Conclusions

#### 3.1 Results

Name	Value range	Inference
OFFSET	$0.0 < x < \infty$	The maximum counteract between
VERTICAL_PORTION	$0.0 < x \leq 1.0$	Determines the percentage of rows (from a frame) that will be analyzed for signals
SIZE_OF_BUFFER	$1 < x < \infty$	Number of buffered frames during classification
RATE_OF_DETECTION	$0.0 < x \leq 1.0$	The (%) rate at which a value must be detected to be classified as a signal
THRESHOLD_GREEN	$0 < x < 255$	The minimum GREEN value of pixel
THRESHOLD_RED	$0 < x < 255$	The minimum RED value of pixel

#### 3.2 Discussion

The light tracking bot machine seems to have extensive military application in diverse fields such as healthcare, defense, education, industries and transportation. In field of healthcare, this bot machine is used for performing fragile surgeries, in defense for surveillance purpose, in education for academic researches, in industries for small scale manufacturing units, in transportation for underground systems, so on.

#### 3.3 Conclusion

From the demonstration, controlling a bot machine by usage of only light is considered be an inefficient way of operation. Though it is achievable, this application is still bounded by certain confinements. Additional sensors are required to achieve collision

avoidance in more precise way. Conclusion still could be strained with respect to the data thus determined even though it is not the best possible way to construct a tracking a bot machine. As a whole, the light sensing application is ease-to-use and cost effective. It requires a lot of advancement to attain a state of stand-alone methodology. For an underground transportation system, this application has an ample amount of scope to work on.

## References

1. Nasrudin, N., Ilis, N.M., Juin, T.P., Chun, T.T.K., Zhe, L.W., Rokhani, F.Z.: Analysis of the light dependent resistor configuration for line tracking robot application. In: 2011 IEEE 7th International Colloquium on Signal Processing and its Applications, Penang, pp. 500–502 (2011)
2. Jia, Y., Cebon, D.: Field testing of a cyclist collision avoidance system for heavy goods vehicles. *IEEE Trans. Veh. Technol.* **65**(6), 4359–4367 (2016)
3. Manjur, N., et al.: Light following & obstacle avoiding robot using autonomous & android based manual controller. In: 2015 18th International Conference on Computer and Information Technology (ICCIT), Dhaka, pp. 511–515 (2015)
4. Chen, C., Kak, A.: Modeling and calibration of a structured light scanner for 3-d robot vision. In: Proceedings of 1987 IEEE International Conference on Robotics and Automation, vol. 4. pp. 807–815. IEEE (1987)
5. Kim, Y., Hwang, S.G., Rhee, S.-Y., Kim, D.H.: Implementation of a personal riding robot with a magnetic compass sensor using a smartphone interface. In: 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on IEEE Advanced Intelligent Systems (ISIS), pp. 17–22 (2014)
6. Hasan, K.M., AI-Nahid, A., Reza, K.J., Khatun, S., Basar, M.: Sensor based autonomous color line follower robot with obstacle avoidance. In: 2013 IEEE Business Engineering and Industrial Applications Colloquium (BEIAC), pp. 598–603. IEEE (2013)
7. Borenstein, J., Koren, Y.: The vector field histogram-fast obstacle avoidance for mobile robots. *IEEE Trans. Robot. Autom.* **7**(3), 278–288 (1991)
8. Shafin, M., Kabir, K.L., Ridwan, I., Fuad, T.A., Bardhan, S., Raju, M.I.H., Tahira, A., Afrin, I., Mondal, S., Tumpa, S.N., et al.: Mongol barota: a next generation rover. In: 2014 8th International Conference on IEEE Software, Knowledge, Information Management and Applications (SKIMA), pp. 1–8 (2014)
9. Arvin, F., Samsudin, K., Nasseri, M.A.: Design of a differential-drive wheeled robot controller with pulse-width modulation. In: IEEE Innovative Technologies in Intelligent Systems and Industrial Applications, pp. 143–147. IEEE (2009)
10. Zimmermann, U., Pruksch, A., Uhler, W.: Method and device for detecting objects, April 2004
11. Evans Jr., J.M., Weiman, C.F., King, S.J.: Visual navigation and obstacle avoidance structured light system, August 1991



# A Survey of ECG Classification for Arrhythmia Diagnoses Using SVM

Doshi Ayushi<sup>1</sup>(✉), Bhatt Nikita<sup>1</sup>, and Shah Nitin<sup>2</sup>

<sup>1</sup> Department of Computer Engineering, CSPIT CHARUSAT, Changa, India  
ayushidoshi313@gmail.com,

nikitabhattach.ce@charusat.ac.in

<sup>2</sup> Department of Quality Assurance, Techsmith Solutions Pvt Ltd.,  
Thalaj, Ahmedabad, India

nitin@techsmith.co.in

**Abstract.** For Detecting Arrhythmia, the commonly used Medical test is an Electrocardiogram (ECG) which is widely used by medical practitioners to measure the electrical activity of heart. By Analysing ECG signal's each heart beat we can find the abnormalities present in heart rhythm. In this work we survey different methods used for classifying ECG arrhythmia using Support Vector Machine and also discussed about the challenges associated with the classification of ECG signal. For classification we require Pre-Processing of ECG signal, Preparation Method, Feature Extraction or Feature Selection Methods, Multi class classification strategy and kernel method for SVM classifier. Recently, for the classification we have several datasets available which have been clinically detected arrhythmia present in each ECG recordings. By initiating this research survey we aim to explore current methodology for diagnosing arrhythmia and classifying ECG signal using SVM.

**Keywords:** ECG · DWT · SVM · Arrhythmia · Denoising technique

## 1 Introduction

Arrhythmia is a critical disease that results in adverse effect on human heart. There are numerous types of arrhythmias and each type is related with a specific pattern, due to this reason the identification and classification of arrhythmia is made possible. Some effects will result in severe cardiac disease and the other do not have any symptoms. Generally, Arrhythmia results in irregular heart-beat which is the condition where heart beats: too fast (tachy-cardia), too slow (brady-cardia), too early (pre-mature contraction), too erratically (fibrillation) [1]. Arrhythmia is a common symptom of cardiovascular disease like heart attack or stroke so, that detection of this disease is more important. American Heart Association had reported that more than four million Americans suffer from different types of arrhythmia [2].

Abnormality in human heart is detected by ECG test. A specialist may prescribe ECG to the individual who may in risk of coronary artery disease by reason of high cholesterol, high blood sugar level, Family History and Hypertension. Tiny electrical impulse are produce by human heart which could be spread in heart muscles.

This impulse can be detected by an ECG machine [3]. Normal healthy heart's ECG have characteristic shape. An Electrical activity of heart being change because of any irregularity present in heart rhythm [4]. The process of identifying and classifying arrhythmia using ECG is very tedious task because some condition it is necessary to analyse each heart beat of every signal [5].

Support Vector Machine is commonly used machine learning algorithm which solves classification as well as regression problem for identifying heart arrhythmia because of its good classification and generalisation properties. It gave very successful result when working in this area [2]. Classification of ECG signal have 3 steps mainly, Pre-processing, Extracting Features, and classification.

This paper includes following sections. In Sect. 2 Basic introduction of ECG medical test and ECG processing techniques, Sect. 3 includes current challenges in ECG signal denoising, Sect. 4 includes survey of ECG classification, Sect. 5 includes Analysis of survey and finally Sect. 6 includes conclusion of this survey. This paper gives overview of existing studies for ECG signal processing and arrhythmia detection from it, also discussed challenges in classification of ECG. Different pre-processing and Feature extraction techniques as well as different types of kernels used in Support Vector Machine. This paper will help beginners to decide proper Dataset pre-processing technique, as well as proper feature extraction techniques for classification.

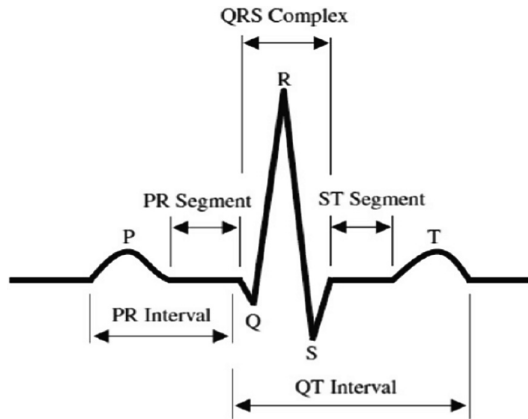
## 2 Background Knowledge

The main function of heart is pumping the blood to over-all body. For that myocardial muscles are contracting and expanding in that response Electrical current produces in the heart. This electrical current can be detected and measured by Electro-cardiogram (ECG) [7]. ECG signal is repetition of P-QRS-T waves which are having specific magnitude and intervals as shown in Fig. 1 [8].

The magnitude and amplitudes of ECG are depends on fundamental features of ECG which are describe in Table 1. In arrhythmia diagnoses feature extraction of signal is most important because of find set of relevant features that can be achieve better accuracy.

In feature extraction method magnitude and intervals between these waves are calculated to get abnormality in rhythm [4]. Feature extraction is based on time domain and frequency domain. As time domain method is not adequate for feature extraction so that we use frequency domain methods recently [8]. The main methods for feature extraction are Discrete wavelet Transform (DWT), Discrete Cosine Transform (DCT), Continuous Wavelet Transform (CWT). For better result of feature extraction technique signal pre-processing is done on ECG signal in which noise and missing values should be replace or remove [2].

Various recursive digital filters are used to remove noise which can be made from advance micro-controller and micro-processor. Commonly used filter is Finite Impulse Response (FIR) filter [4]. Recently, Wavelet based methods are used to remove the noise for that Discrete Wavelet Transform and Continuous Wavelet Transform methods are used which can be easily available in MATLAB Toolbox Function [5].



**Fig. 1.** Sample ECG signal [7]

**Table 1.** Feature extraction table

Feature	Description
P wave	ECG signal starts with P wave which will be smooth and rounded. It represents depolarization of left and right atrium Duration: 0.1 s Amplitude: 0.1–0.12 mV
QRS complex	QRS Complex have 3 continuous deflection for Q wave R wave and S wave. It represent ventricular depolarization Duration: 0.08 s
T wave	It represents ventricular re polarization. The peak of wave is slightly closer to its end compare to its beginning Duration: 0.27 s Amplitude: 0.3 mV
RR interval	It represent heart rate in beats per minute. Distance between 2 consecutive R wave Duration: 1 s
PR interval	It represent electrical signal generated by the sinus node (Natural pacemaker) is normal or not. Functionally it is PQ interval Duration: 0.2–0.3 s
QT interval	It represent ventricular systole. It also represent flow of blood and electrical impulse from atrial chambers to ventricles. It is directly related to heart rate Duration: 0.36 s
ST segment	It is flat section of ECG which represents ventricular repolarization of whole cardiac cycle. It begins with end of QRS complex to begin of T wave Duration: 0.32 s

Basically, Pre-processing techniques are highly dependent on the method we choose for feature extraction and classification. After, Features are derived from the ECG signal model should be built using Machine learning algorithm for arrhythmia beat classification [5]. For classification support vector machine is very efficient in signal processing. From the training dataset Support Vector Machine calculate hyper plane which divides original data into different classes which have maximum margin between hyper plane and adjacent sample. If the feature space is linearly not separable then kernel function is used. Kernel is mathematical function which transforms feature space in to higher Dimension. Different types of kernel are available like Linear, Non-Linear, Polynomial, Radial Basis Function and Sigmoid Function, among them most popular kernel is Radial Basis Function (RBF) because it has localize and finite response Kernels. Support vector machine is binary classifier but for classify more then two class we require strategy call one-against-one and one-against-all. The main sequential steps for Arrhythmia classification are pre-processing signal, feature extraction, and classification [10].

### **3 Challenges in ECG Signal Classification**

#### **3.1 ECG Signal Acquisition**

ECG is non-stationary signal, some time it also take unwanted noise like Electromyogram, Motion artefacts, and muscle contraction. Elimination of this noise from ECG signal lead to loss of information because noise and information lie in overlaid manner. This loss of information directly affect the classification accuracy [11].

#### **3.2 ECG Data-Set Challenges**

Furthermost large clinical studies still record ECG on paper printouts so for applying computational techniques we require some amount of digitization. In addition, most of studies in this paper is based on publicly available datasets of ECG signal like MIT-BIH were originally captured in analogue format but after some time it was converted in digital form. Moreover, database have less no of patients and require more amount of pre-processing techniques to denoise the signal and many ECG databases are not publicly available [12].

#### **3.3 Lack of Standardization of the ECG Features**

Features of ECG signal are based on chronological selection of wave boundaries in particular time and amplitude domain. ECG is analysed at different scale based on local maxima, minima and zero score of the signal. So that approximation of maxima or minima is not sufficient for clinical diagnoses of any disease. Because small change in localization may lead to misclassification [4, 13].



### 3.4 Variability of ECG Features

ECG is based on cardiac rhythm and heart rate. But rate of heart varies with individuals physical and mental condition like stress anxiety, exercise, excitement. So that, changes in the heart rate can subsequently change segments (features) Like RR interval, QT interval, as well as PR interval. This varying features may lead to miss-classification so varying heart rate should be discarded from the ECG signal [13].

### 3.5 Uniqueness of ECG Patterns

Uniqueness of ECG refers to interclass variability and intraclass similarity of testing patterns in target signal. To address the individuality of ECG methods should be tested on large dataset but currently it is tested at limited dataset [4].

### 3.6 Finding Out Appropriate Feature Selection and Pre-processing Method

Feature section and pre-processing technique directly affect the accuracy of classification. Feature extraction technique should be extremely accurate and should ensure fast extraction of features from the ECG signal [7].

## 4 Literature Survey of ECG Classification

There are many researchers who have worked on ECG classification for arrhythmia detection. They used different pre-processing methods, feature extraction and selection techniques as well as different classification techniques for diagnoses and classification of Arrhythmia. Many investigators uses MIT-BIH dataset for ECG classification.

Xu et al. [2] used PCA (Principal Component Analysis) and FDR (Fisher Discriminant Ratio) for feature reduction. They obtained 76.97% and 78.23% Accuracy respectively. They concluded that PCA is linear transformation method that's why its not suitable for non-linear manifold feature space so FDR is better transformation technique for non-linear manifold.

Nasiri et al. [29] proposed novel approach for Arrhythmia classification. They used combination of Genetic Algorithm and Support Vector machine for arrhythmia classification and obtain 93.46% overall classification accuracy. They used Genetic Algorithm for feature extraction. They also use Principal Component Analysis (PCA) only approach for feature extraction but GA provides better classification accuracy compare to PCA only method [29] (Table 2).

**Table 2.** Literature survey of ECG classification

Researchers	ECG features	Dimensionality reduction	SVM algorithm	Dataset	Performance measure	% (percent)
Seung Hwan Lee Hyun-ChulKo, Young-Ro Yoon	RR interval QRS Slope	ECG record sampled at different rate Feature Extraction: Morphological Information (QRS Complex)	Gaussian RBF kernel with One-Vs-All Strategy Classification: 4 types of Arrhythmia	MIT-BIH Database & Creighton University dataset	Sensitivity	93
Sean shensheng Man-WaiMak Chi-Chung Cheung	QRSTA, QRS Duration, Amplitude of T, Average width of R	For feature selection: Fisher Discriminant Ratio For feature Reduction: Principal Component Analysis (PCA)	K-class Kernel with One against rest Strategy Classification: 5 types of Arrhythmia	UCI Arrhythmia Dataset	Accuracy (using FDR) Accuracy (using PCA)	78.23 76.97
Halil İbrahim, BÜLBÜL Neşe, USTA Musa YILDIZ	P, Q, R, S, T waves	Feature extraction: Hybrid approach (Combination of DWT, DCT, CWT)	Kernel Adraton (KA) Support vector Machine Classification: 16 classes	MIT-BIH Arrhythmia Database		
Zhijian Chen, JiahuiLuo, Kaiwen Lin Jiaquan Wu, Taotao Zhu.	QRS Area ratio	Feature extraction: Principal Component Analysis (PCA) Sparse Matrix	They use weak linear classifier and Non linear Support Vector Machine classifier (Strong SVM)	MIT-BIH Arrhythmia Database	Accuracy (With linear classifier) Accuracy (Without Linear classifier)	98 41.7
N Jannah S. HadjiIoucas	R Peak, P wave, T wave	Feature Extraction: DFT	They used traditional SVM in complex space Classification: 4 classes	ST-T Database	Accuracy (MSVM) Accuracy (CSVM)	86 94

*(continued)*

Table 2. (continued)

Researchers	ECG features	Dimensionality reduction	SVM algorithm	Dataset	Performance measure	% (percent)
Najlaa Jannah Sillas Hadjioucas		Feature Extraction: Principal Component Analysis (PCA)	RBF SVM with one-against- one strategy and also Soft Independent Modelling of Class Analogy (SIMCA)	St Petersburg INCART 12-lead Arrhythmia Database	Accuracy (MSVM) Accuracy (SIMCA)	76.83 97.7
MonikaRani Ekta Reeta Devi	DWT	Feature Extraction: DWT	Linear SVM Classification:	MIT-BIH Arrhythmia Database	Accuracy Sensitivity Specificity	98 98 98
Czarina Isabelle M. Cruz Jastine P. Marasigan Anna Patricia G. Perez Joana Erika V. Pillejera Nikka P. Veron Angelo R. dela Cruz		Feature Extraction: DWT	They used One against One Support Vector Machine (OAO SVM) Classification: Accuracy	MIT-BIH Database	Accuracy	95
Usha Desai C. GurudasNayak G. Seshikala		Feature Dimensionality Reduction: Independent Component Analysis (ICA) Feature Extraction: DCT	They used Quadratic kernel Function. Classification: 5 Class	MIT-BIH Database	Accuracy	95.98
Udita Dev Roy SantanuGhorai Anirban Mukherjee		Feature Extraction: Kernel Canonical Co-relation Analysis (KCCA)	They used One against One Support Vector Machine (OAO SVM) Classification: 4 Class	MIT-BIH Database	Accuracy	93.25

(continued)

Table 2. (continued)

Researchers	ECG features	Dimensionality reduction	SVM algorithm	Dataset	Performance measure	% (percent)
Tahmida Tabassum Monira Islam	1. Heart rate 2. QRS Complex 3. PR Interval 4. ST Segments 5. ST Interval	Feature Extraction:	They used Multi class SVM Classification: 4 Class.		Accuracy	84.6
Prof. Alka S. Barhate Dr. Rajesh Ghongade Abhishhek S. Thakare	1. R Point Location 2. QRS Complex Detection	Feature Extraction: DWT	They used Multi-class SVM Classification: 4 Class	MIT-BIH Data base	Sensitivity Specificity	100 99.66
Usha Desai C. Gurudas Nayak G. Seshikala		Feature Extraction: DWT Feature Dimensionality Reduction: ICA	They used Quadratic polynomial and RBF kernel for SVM classification: 5 Class.	MIT-BIH Data base	Accuracy	98.49
Neenu Jacob Liza Annie Joseph		Feature Extraction: XWT (Cross Wavelet Transform)	They used RBF kernel for Classification	MIT-BIH Data base	Sensitivity (SVM) Sensitivity(2D SVM) Specificity (SVM) Specificity(2D SVM)	96.4 98.4 89.5 87.7

(continued)

Table 2. (continued)

Researchers	ECG features	Dimensionality reduction	SVM algorithm	Dataset	Performance measure	% (percent)
EllyMatullmah Faris Al Afif M. Ivan Fanany		Feature Reduction: Using Kernel-PCA (Gaussian, Polynomial, Linier) Feature Extraction: DWT		MIT-BIH Arrhythmia Database	Accuracy (Wavelet SVM + KPCA) Accuracy (Linier SVM + KPCA)	96.75  97.5
K. Amtul Salami G. SriLakshmi2	ST Segment QRS Complex T Wave	Feature Extraction: DWT		MIT-BIH Arrhythmia Database	Accuracy	98.65
DimitraAzariadi, VasileiosTsoutsouras, Sotirios, Xydis DimitriosSoudris		Feature Extraction: DWT	They used RBF kernel Classification: 2 Class	Own Data collect through sensors & MIT-BIH Arrhythmia dataset	Accuracy	98.9

Salam [14], perform QRS complex detection and ST segment detection and R peak detection using Discrete Wavelet Transform and Adaptive least square method and gain 98.67% accuracy which give better result compare to analysis using features like P wave, QRS Complex and T wave.

Halil et al. [5] used DWT, DCT, and CWT hybrid approach in signal wave transformation to improve overall classification performance. In this study we acquire better accuracy in hybrid approach compare to individual transformation method.

Subramanian and Lakshmi et al. [27] detect the QRS complex from ECG signal with 93% accuracy and 90% specificity for that he used three types of algorithms name Pan Tompkins's Algorithm, Derivative based and Wavelet Transform(DWT) based algorithm among them DWT based Multi-wavelet based algorithm provides better accuracy and specificity. According, to Lakshmi et al. (2011) Daubechi's signal for wavelet transform give better accuracy in wavelet transform because this wavelet pickup minute detail which can be lost by other wavelet methods like Haar wavelet algorithm. However, Daubechi's algorithm is conceptually more intricate, and has complex computations it gives efficient result. Eaurodo et al. also stated that Daubechies wavelet are most promising among all the wavelets for QRS detection. Among them Daubechies order 2 provide better accuracy.

Faziludeen and Sabiq [30] used Pan Tomkins algorithm for detecting QRS complex and Discrete wavelet Transform and Support Vector Machine for classification of ECG. They extracted 25 features from wavelet analysis like mean, variance, Standard Deviation, minimum and maximum of detail co-efficient and classify 3 classes of arrhythmia and obtain very high accuracy.

## 5 Analysis of Literature Survey

### 5.1 ECG Dataset Present

Recently, there are several datasets publicly available for Bio-medical signal processing. From that many are stored by Physio net and others are abandoned by their owners. AHA database was created by American Heart Association for diagnoses of arrhythmias. There are 2 versions of this dataset are available shorter version have five minutes unannotated ECG signal prior to 30 min of annotated segment of each recording. And longer version have 2.5 h of unannotated signal prior to each annotated signal. This data contains 154 recordings at 250 Hz frequency. It compose of 3 signals and it have 7 types of arrhythmia [7].

Another dataset is UCI cardiac dataset. Which have 245 samples. It contains total 16 classes of heart arrhythmia. This data contains 76 attributes [2]. CU database have 35 recordings and each have 8 min sampled at 250 Hz with 12bits resolution. This database have data about different types of ventricular arrhythmia. 3 files of this dataset are annotated [14].

Most widely used data-set for ECG is MIT-BIH Arrhythmia dataset which have 48 recordings of heartbeat at 360 Hz. Each recordings have 30 min and 47 different partition. Each record consists of 2 leads that are lead-A and lead-B. generally, Lead A is used for analysis of heart-beats and lead B is used for arrhythmic classification. Database contains 3 files that are signal file annotation file and header file [4].

## 5.2 Pre-processing of ECG Signal

ECG signal contains different types of noise in signal which degrade the performance of classification. To remove this type of noise from signal we require Pre-processing Technique. Which type of noise we remove from ECG signal is completely depends on method we choose for further processing for feature extraction and classification [5]. Major types of noise present in ECG signal are listed below

### 1. Powerline Interface

It is high frequency noise normally between 48 Hz to 50 Hz. This noise is because of sinusoidal alternating current which can be used as source by ECG acquisition equipment [7].

### 2. Baseline wander

It is low frequency noise normally below 1 Hz Which is caused by breathing movements of different organs on acquired signal [4].

### 3. Electromyographic Interface

It is high frequency and high amplitude noise. This noise is due to electrical impulse of another organs from human body rather than heart [5].

### 4. Lead Reversal

This type of noise is because of misplacement of electrode which cause reversing in amplitude of heart beat waveforms [9].

### 5. Electrode Movement

This is high frequency and high amplitude noise cause by changes of impedance in skin as well as movement of the subject of electrode [3].

## 5.3 ECG Signal Preparation

Before, Extract the features from pre-processed ECG signal one method is proposed to maximize the performance of feature extraction that is preparation method [3]. In this method we pre-prepare the signal for feature extraction phase by reducing variability and several inconsistency from the ECG signal [8].

### 1. Length inconsistency

If the ECG signal acquire from the middle of the heart beat then extent of the signal may vary. Which may cause wrong feature extraction from ECG signal [3].

## 2. Amplitude Variation

This variation is caused because of wrong placement of electrode at signal acquisition time. If the amplitude of the heart-beat are changed then we can not extract appropriate features [15].

## 3. Heart rate variability

At the time of ECG signal acquisition if the heart rate vary over time which cause the changing the shape of Different segments and waves [8].

To remove this type of variability steps require like Fiducial point Detection, Signal Normalization or outlier detection. Signal segmentation can segment the signal using fix the signal span [16]. In Fiducial point detection generally QRS Complex detection and R-peak detection for further feature extraction. For detecting QRS complex there are number of ways like using Pan-Tompkins Algorithm, Signal squaring method and Wavelet Transform method are used. In signal preparation method another method is normalization of amplitude and time of signal. For that we use z-score normalization and Min-Max Normalization method [14]. Outlier detection method is generally used for avoid unwanted wave from the ECG signal. For that certain methods like Gaussian Mixture Model and Normalized cross-correlation between candidate heart beats method are used.

## 5.4 Feature Extraction of ECG Signal

Any information extracted from the heart beat used to discriminate its type is called a feature of ECG. This stage is most important for better classification of heartbeat arrhythmia. For the feature there are two types of approach [20]. Feature selection and Feature extraction. In Feature selection features are selected from existing set of features [15]. That means selected features are subset of existing features in ECG signal. In feature extraction new features are extracted using different methodology where extracted features are not subset of original features [21].

### 1. Feature Extraction using Morphological features

In temporal analysis feature are extracted based on the time domain. This features are based on heart beat wave forms as well as their on set and offset points. This types of features are P, Q, R, S, and T waveforms. And also find its amplitude, duration, interval level and area measurement of fiducials. But this type of approach is not perform better when we used off-the-person ECG wavelet and seamless ECG wavelet [19]. Noise and variability presented in the heart beat can change the amplitude which can change the features of ECG signals. So that, this methods are less efficient [3].

### 2. Feature Extraction using Segments of the signal

In spectral analysis Features are extracted based on fixed size of segments of ECG. This features are QRS complex, ST segment QT segments which can be analysed using Fourier Transform and Wavelet Transform like Discrete Wavelet Transform and



Continuous Wavelet Transform [15]. After converting features in to Fourier transform the features are being very big so that analysis being very easy. However, spectral analysis (Fourier Transform) have certain limitation it can not capture certain abnormality which are based on time domain [21].

### 3. Feature Extraction using Hybrid approach

To overcome the abnormality based on time and frequency Domain this type of analysis comes in the picture. The features extracted in this type of analysis are QRS complex, QT complex, ST segment, RR interval. In this analysis wavelet transform is done for every features [8]. In the Wavelet Transform method original signal is convolve with wavelet. So, that we acquire 2 wavelet co-efficients. A Coefficient and D co-efficient [7]. A co-efficient is approximation output which contains low frequency signal of original input signal. D co-efficient is multi dimension output which gives high frequency components. This output Co-efficients can be represented in time domain as well as frequency domain [11]. So, that classification of the signal is being very good because we can not miss any parameter of ECG [8].

## 5.5 Classification of ECG Using SVM Algorithm

Support Vector Machine is classification algorithm which classify labelled input dataset by giving optimal hyper plane between different classes with maximum margin from the hyper plane. It have very good generalization capability. Suppose that we have training dataset (x, y). Where x is input and y is its corresponding output. So, that Hyper plane should be

$$w \cdot x_i + b \geq 0 \text{ where } y = v \tag{1}$$

$$w \cdot x_i + b \geq 0 \text{ where } y = -v \tag{2}$$

Here w is hyper plane’s co-efficient vector. Support Vector Machine’s Optimization problem stated that the margin between nearest point and hyperplane should be maximized. It can be represented the mathematical terms:

$$\text{Min } \frac{1}{2} (w \cdot w^t) \tag{3}$$

Where,  $D(w \cdot x_i + b) \geq 1$

Here,  $w^t$  and b are scaler of the SVM. The total margin should be  $\frac{2}{\|w\|}$ . Margin means difference between 2 Support Vectors. The main aim of the classifier is to maximize the margin and minimize the error rate. Using Lagrange multiplier  $\alpha \geq 0$  solution can be given by,

$$W = \sum D\alpha x \tag{4}$$

Here,  $\alpha$  coefficient's small factor should be nonzero. The boundary of the decision should be given by  $x_i$ . All other irrelevant input patterns corresponding to zero  $\alpha$  should be removed. Now input pattern vector  $x_i$  can be given as:

$$f(x) = \text{sgn}\left(\sum D\alpha(x_i x_i') + b\right) \tag{5}$$

By replacing the term  $(x_i x_i')$  with kernel function  $k(x, x_i)$  input pattern should be map in higher Dimension. The data which can not be linearly separable should be converted in to higher dimensional data then separate the data in higher dimension and convert back in to original feature space. This is called kernel function. There are many types of kernel available for Support Vector Machine Classifier like Polynomial kernel, Gaussian kernel, Gaussian Radial Basis Function (RBF) kernel Laplace RBF kernel, sigmoid kernel, Linear Spline Kernel. Among them, Radial basis functions are most commonly used with Support Vector Machine. Support Vector Machine mainly designed for solving binary classification problems but it can also solves the multi problem using different methods and also have multi class classification capability [21]. We implement different types of methods for multi-class classification of ECG using SVM.

1. Hierarchical Support Vector Machine

In this method certain binary SVM classifier are arranged in a binary tree structure. For training of each SVM classifier binary decision subtask's hierarchy should be design properly so that they can take decision appropriately. One binary classifier is present at each node of the tree which can be trained using 2 classes. This method provides high classification accuracy and computationally efficient [23].

2. One vs One Method

In this method we require  $n(n - 1)/2$  binary classifier for solve any n class problem. Every classifier is trained to separate the data from one class to all the another class. The conclusion is taken based on maximum number of votes for particular class. This method works bitterly then One vs All method (Fig. 2).

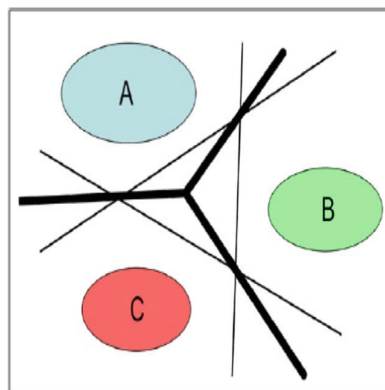


Fig. 2. One vs one method [12]

### 3. One vs All Method

One vs All method also require  $n(n - 1)/2$  binary classifier for  $n$  class problem but it is slightly different then One vs one method. This method states that only one SVM accept the decision and another class do not accept the decision (Fig. 3).

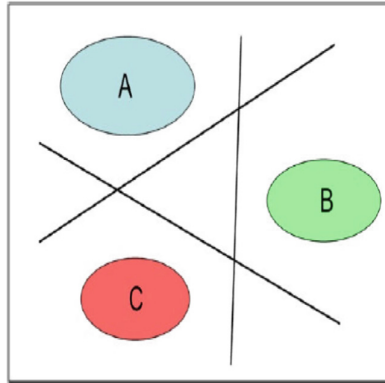


Fig. 3. One vs all method [12]

Some times training data are not linearly separable so or that data should be converted in higher dimensional feature space then classify the data and converted back into its original form. This procedure is done with the help of kernel. There are many types of kernel available for Support Vector Machine Classifier like Polynomial kernel, Gaussian kernel, Gaussian Radial Basis Function (RBF) kernel Laplace RBF kernel, sigmoid kernel, Linear Spline Kernel. Among them, Radial basis functions are most commonly used with Support Vector Machine.

## 6 Conclusion

In this survey, through detailed presentation and discussion of arrhythmia detection using ECG classification we concluded that Support Vector Machine using RBF kernel provides better accuracy compare to another Kernel.

## References

1. Hammad, M., et al.: Detection of abnormal heart conditions based on characteristics of ECG signals. *Measurement* **125**, 634–644 (2018)
2. Xu, S.S., Mak, M.-W., Cheung, C.-C.: Deep neural networks versus support vector machines for ECG arrhythmia classification. In: 2017 IEEE International Conference on Multimedia & Expo Workshops (ICMEW). IEEE (2017)

3. Cruz, C.I.M., et al.: A comparative study between DWT-ANFIS and DWT-SVM in ECG classification. In: 2016 IEEE Region 10 Conference (TENCON). IEEE (2016)
4. Jambukia, S.H., Dabhi, V.K., Prajapati, H.B.: Classification of ECG signals using machine learning techniques: a survey. In: 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA). IEEE (2015)
5. Luz, E.J.S., et al.: ECG-based heartbeat classification for arrhythmia detection: a survey. *Comput. Methods Programs Biomed.* **127**, 144–164 (2016)
6. Usta, N., Yildiz, M.: Classification of ECG arrhythmia with machine learning techniques. In: 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE (2017)
7. Pinto, J.R., Cardoso, J.S., Lourenço, A.: Evolution, current challenges, and future possibilities in ECG biometrics. *IEEE Access* **6**, 34746–34776 (2018)
8. Peshave, J.D., Shastri, R.: Feature extraction of ECG signal. In: 2014 International Conference on Communications and Signal Processing (ICCSP). IEEE (2014)
9. Joshi, S.L., Vatti, R.A., Tornekar, R.V.: A survey on ECG signal denoising techniques. In: 2013 International Conference on Communication Systems and Network Technologies (CSNT). IEEE (2013)
10. Jannah, N., Hadjiloucas, S.: A comparison between ECG beat classifiers using multiclass SVM and SIMCA with time domain PCA feature reduction. In: 2017 UKSim-AMSS 19th International Conference on Computer Modelling & Simulation (UKSim). IEEE (2017)
11. Haritha, C., Ganesan, M., Sumesh, E.P.: A survey on modern trends in ECG noise removal techniques. In: 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE (2016)
12. Lyon, A., et al.: Computational techniques for ECG analysis and interpretation in light of their contribution to medical advances. *J. R. Soc. Interface* **15**(138), 20170821 (2018)
13. Singh, Y.N., Singh, S.K., Ray, A.K.: Bioelectrical signals as emerging biometrics: issues and challenges. *ISRN Signal Process.* **2012**, 13 Pages (2012)
14. Salam, K.A., Srilakshmi, G.: An algorithm for ECG analysis of arrhythmia detection. In: 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). IEEE (2015)
15. Lee, S.H., Ko, H.-C., Yoon, Y.-R.: Classification of ventricular arrhythmia using a support vector machine based on morphological features. In: 2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). IEEE (2013)
16. Kallas, M., et al.: Multi-class SVM classification combined with kernel PCA feature extraction of ECG signals. In: 2012 19th International Conference on Telecommunications (ICT). IEEE (2012)
17. Chen, Z., et al.: An energy-efficient ECG processor with weak-strong hybrid classifier for arrhythmia detection. *IEEE Trans. Circuits Syst. II Express Briefs* **65**, 648–952 (2017)
18. Jannah, N., Hadjiloucas, S.: Detection of ECG arrhythmia conditions using CSVM and MSVM classifiers. In: 2015 IEEE Signal Processing in Medicine and Biology Symposium (SPMB). IEEE (2015)
19. Rani, M., Devi, R.: Arrhythmia discrimination using support vector machine. In: 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE (2017)
20. Desai, U., Nayak, C.G., Seshikala, G.: An efficient technique for automated diagnosis of cardiac rhythms using electrocardiogram. In: IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). IEEE (2016)

21. Roy, U.D., Ghorai, S., Mukherjee, A.: Kernel-based feature extraction for patient-adaptive ECG beat classification. In: 2016 International Conference on Systems in Medicine and Biology (ICSMB). IEEE (2016)
22. Barhatte, A.S., Ghongade, R., Thakare, A.S.: QRS complex detection and arrhythmia classification using SVM. In: 2015 Communication, Control and Intelligent Systems (CCIS). IEEE (2015)
23. Desai, U., et al.: Machine intelligent diagnosis of ECG for arrhythmia classification using DWT, ICA and SVM techniques. In: 2015 Annual IEEE India Conference (INDICON). IEEE (2015)
24. Jacob, N., Joseph, L.A.: Classification of ECG beats using cross wavelet transform and support vector machines. In: 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS). IEEE (2015)
25. Alonso-Atienza, F., et al.: Detection of life-threatening arrhythmias using feature selection and support vector machines. *IEEE Trans. Biomed. Eng.* **61**(3), 832–840 (2014)
26. Imah, E.M., et al.: A comparative study on daubechies wavelet transformation, kernel PCA and PCA as feature extractors for arrhythmia detection using SVM. In: 2011 IEEE Region 10 Conference TENCON 2011. IEEE (2011)
27. Subramanian, B.: ECG signal classification and parameter estimation using multiwavelet transform (2017)
28. Narayana, K.V.L., Rao, A.B.: Wavelet based QRS detection in ECG using MATLAB. *Innovative Syst. Des. Eng.* **2**(7), 60–69 (2011)
29. Nasiri, J.A., et al.: ECG arrhythmia classification with support vector machines and genetic algorithm. In: 2009 Third UKSim European Symposium on Computer Modeling and Simulation, EMS 2009. IEEE (2009)
30. Faziludeen, S., Sabiq, P.V.: ECG beat classification using wavelets and SVM. In: 2013 IEEE Conference on Information & Communication Technologies (ICT). IEEE (2013)



# An Efficient Trust and Energy Aware Protocol Using TAODV-ACO in MANETs

Ambidi Naveena<sup>(✉)</sup> and Katta Rama Linga Reddy

Electronics and Telematics Department,  
G.Narayanamma Institute of Technology and Science, Hyderabad, India  
ambidinaveena@yahoo.com, kattareddy2000@yahoo.com

**Abstract.** Mobile Ad-Hoc Network (MANET) is a relationship of the mobile nodes with constrained transmission range and asset with no fixed infrastructure. But, malicious attack of node reduce the trust-level nodes that lead to insecure in delivering data. The increments in attacks cause extreme energy consumption that tends to a decrease in network-lifetime. The security and routing issues are concentrated by introducing trust aware ad-hoc protocols. In this research proposal, Trust-Aware ad-hoc Routing (T2AR) with Ant Colony Optimization (ACO) is used for maximizing the trust level based on trust-rate, energy, mobility based malicious behavior prediction. Ad-hoc On-Demand Distance Vector (AODV) uses two processes to find and maintain routes: the route detection process and the route maintenance. Hence, the T2AR-AODV-ACO methodology precisely transmits data from source to destination (S-D) by executing better throughput, routing overhead, end-to-end delay and energy consumption in trust aware ad-hoc routing.

**Keywords:** Ad-hoc On Demand Distance Vector · Ant Colony Optimization · Mobile Ad-Hoc Network · Trust-Aware ad-hoc Routing

## 1 Introduction

Trust management for MANET has risen as dynamic research region, which is appeared by the expansion of trust protocol to help mobile gathering based applications lately [1]. The social trust came from the communication network to get a composite trust metrics as a reason for evaluating trust of mobile nodes in MANETs [2]. The interruption location and reaction on the reliability of a Cyber-Physical System (CPS) including sensors, actuators, control units and physical objects for controlling and securing a physical foundation are major drawbacks in Trust-based MANETs [3].

A dependable Routing Protocol (RP) for improved reliability, quality and security of communication in portable adhoc networks and sensor systems are utilized for level calculation for finding the best route between nodes [4]. The distributed mobile nodes incorporated with the ad-hoc mobile network in such a way it prevent and identify best route and misbehaving nodes while transmitting data packets to destination [5]. The Payload based mutual authentication (PAWN) performs on optimal percentage of cluster heads election, authentication and allows to communicate with nearby nodes using cluster head based tokens for limiting the energy consumption [6].

A Sybil attack recognizable scheme for a cluster based hierarchical network mainly organized to check and detect forest fires. However, if one or more identities of a Sybil node moves via. the detection procedure, they eventually detect the packet loss and malicious nodes in the networks [7]. A data gathering system called MAMS where Mobile Agents (MAs) and a Mobile Server (MS) agreeably assemble data. MAs gather information over the WSN and restore this to the MS [8]. A quick occasion distinguishing calculation named RENDEZVOUS quicken the on-screen character's discovery procedure while keeping the vitality utilization of sensor nodes to a base [9]. The advancement of trust instruments, gives a short summary of traditional trust procedures and underline the difficulties of trust scheme in WSNs. The trust esteem transmission and evaluation perform low in reducing the energy consumption [10].

To overcome this problem, T2AR-AODV-ACO energy-model based evaluation of trust scheme is presented in this paper. The AODV organize the sequential information for the neighbor log-collection. The lack of positional updates during the mobility of nodes is not effective, hence the optimization techniques is used in the paper. The curiosity shows in T2AR is in the usage of immediate and indirect trust observation schemes on neighbor-log results and trust affirmation by methods sequence ID planning. The execution of the proposed methodology evaluated in terms of end-to-end delay, energy consumption, routing overhead and throughput.

The remaining paper is presented as follows: Sect. 2, a brief description about related works. Section 3, presents a review on "Trust aware ad-hoc RP along with ACO" Methodology consists of neighbor estimation, trust update and distance calculation using RSSI techniques in MANETs. Section 4, demonstrated the simulation-parameters and Experimental results of the "Trust aware ad-hoc RP" and Sect. 5 designates the conclusion of this research work.

## 2 Related Work

Yan and Wang [11] proposed a structure for the Attribute based encryption (ABE) model to help information get to checking of the individual portable nodes. The worked of trust display dependent on the suggestion is the testing assignment due to attackers and packet loss in networks.

Saha and Mitra [12] implemented a new trust based on demand RP that can be modified to the individual energy surrounding of the nodes in a MANET. The selection of the secure and reliable node helps in detecting and reducing wormhole and rushing attack, which is different based on the packet drops. The working process of system model is complicated, and this increased the delay in the network.

Bijon et al. [13] presented a trust based packets sharing model in the MANET based on the existence of uncertainty. The multiple recommendations techniques reduce traffic, successfully reflect uncertainty, and adapts human-like behavior. The extra time required for the signal recommendation and also it is difficult to propagate recommendation in the opposite direction.

Shabut et al. [14] presented an energy aware and social trust inspired multidimensional trust management models, which was executed to accomplish Quality of Services (QoS) parameters by overcoming ad-hoc network challenges. The specific

routing method does not use the routing process in a network, hence it provided less throughput and increased the delay of the node.

Patel et al. [15] introduced the trust value based algorithm to identify and defense gray-hole attack by clustering technique. The trust management model computes the trust rate of the wireless nodes through peer-to-peer and link evaluation in Trust ad-hoc networks. The trust value calculation didn't achieve better efficiency in this work.

### 3 Ad-Hoc RP Based on Trust Aware Using AODV-ACO

In this research work, the T2AR protocol is implemented for improving the node's trust-level in an environment of MANETs. For the most part, the proposed method optimizes the functions of AODV route reply and request directing calculation with the limitations of trust-rate, energy, portability based false/malicious activities in network.

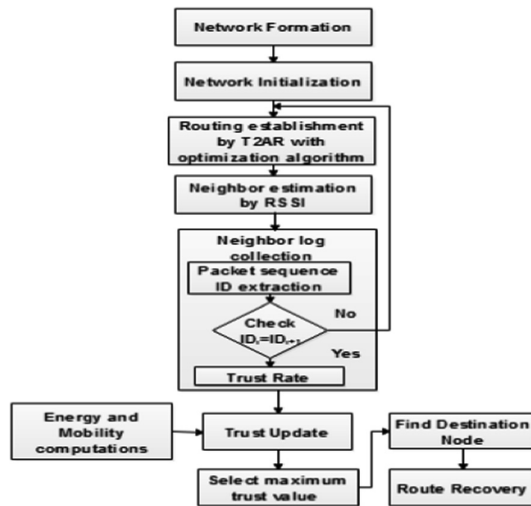


Fig. 1. Overview of the proposed work

The trust value is surveyed through the crossover estimations of the energy, mobility and achievement rate of the packet delivery. The over-all flow diagram of the proposed technique is presented in Fig. 1. The working principle of the T2AR-AODV-ACO methodology is described in the below five steps.

1. The neighbor detecting and route maintenance rely upon the log gathering from the nodes, which give the proper trust rate values. Further, the trust rate is every so often refreshed via the locational information to update the security-level of the nodes.
2. The routing establishment developed by using T2AR with ACO optimization algorithms.
3. The use of immediate or indirect perception procedures followed by the grouping ID coordinating to expand the trust-level.



### 3.1 Trust Model in the Networks

In this section, T2AR-AODV-ACO trust model is explained briefly. The fundamental objective of the model is to give joined solutions for determining the best routing path and energy of packets sent. The trust display how to figure the trust of the routing path by utilizing the trust estimation of each and every nodes. The trust display makes the communication among trust calculation and network statistics. The primary commitment is to determine solutions to the uniform energy consumption for every one of the nodes to build and arrange its lifetime. The trust architecture comprises of two phases: trust advancement and trust calculation for routing process. In trust arrangement of action arrange, each node gathers the network measurements like packet sent, and data packet dropped, etc., in light of which trust of a node is resolved. The requested routing-path comprises the node as an intermediary node, though the gathering of statistics is calculated continuously. Once the route/way from S-D is demanded, all the intermediate nodes determine their trust rated values [17].

### 3.2 Trust Based AODV RP in Ad-Hoc Networks

The incorporation of trust model show with AODV calculation is done so as to prevent the malignant characteristics and uniform use of system resources. The AODV routing is changed dependent on the followings:

- RREP packet is send by AODV-RP for every RREQ data to make the destination sends various RREP packet for RREQ.
- The improvement of RREP packet structure is increased in the path to have trust value.
- The storing of the trust-esteem for every section of S-D is suitable for the routing table.
- AODV sends demand to instruct the directing way at consistent time period. Henceforth, at normal interval, source node will have different ways each with its trust an incentive from which one with the most extreme trust is chosen.

### 3.3 Trust Based Route Optimization Using ACO Algorithm

ACO algorithm takes fascination based on the qualities of ants in nature and from the related field of ACO to determine the issues of routing in sensor networks. The important source of inspiration is found in the limit of particular sorts of ants to look through the base way between their nest and a nourishment sources utilizing Pheromone (Impulsive Chemical Substance). Insects leave clues of pheromone as they migrate between sources to destination. Ants astoundingly go over the range of high pheromone powers searching for sustenance. The larger amount of pheromone is received, when the minimum path is done quicker. The positive establishment process allows the colony to reach the shortest path.

## 4 Result and Discussion

The T2AR-AODV-ACO method is processed in NS2 to improve better energy model and routing for transmission of data using AODV RP with ACO optimization algorithm. The ACO calculation is utilized to get the upgraded way and transmit information packets to the destination. This area gives a definite perspective on the outcome that are obtained utilizing T2AR-AODV-ACO. The T2AR-AODV-ACO procedure is utilized for giving trust estimation in the nodes of the message packets. The experimental results is calculated by taking the parameters as Through-put, routing-overhead, delay and energy-consumption compared with TERP methodology, which is implemented. The execution is determined by estimating the throughput, routing overhead, delay and energy consumption parameters.

Comparison analysis of T2AR-AODV-ACO is evaluated by varying the number of malicious nodes 1, 2, 3, 4 and 5. The Figs. 2, 3, 4 and 5 shows the comparison of the Throughput, Routing Overhead, delay and energy Consumption between existing methods. Throughput increased 7% in T2AR-AODV-ACO than TERP Methodology.

Delay decreased 6% in T2AR-AODV-ACO compared to TERP Methodology. The routing overhead decreased 8% in T2AR-AODV-ACO compared to TERP methodology. Energy Consumption decreased 7% in T2AR-AODV-ACO than TERP methodology [16]. Therefore, the QoS parameter values such as Throughput, routing overhead, delay and energy consumption of TERP implemented and theoretically referred in below cited paper [16].

Comparative analysis of T2AR-AODV-ACO evaluated by varying the nodes 20, 40, 60, 80 and 100. The Figs. 2, 3, 4 and 5 shows the comparison of the throughput, routing overhead, delay and energy Consumption between TERP existing methods.

The comparison of nodes vs. throughput between T2AR-AODV-ACO and TERP is plotted in Fig. 2. The throughput value increased in T2AR-AODV-ACO method, when compared with the TERP method with different malicious nodes 1, 2, 3, 4 and 5.

The comparison of nodes vs. routing overhead between T2AR-AODV-ACO and TERP is plotted in Fig. 3. The routing overhead decreased in T2AR-AODV-ACO method, when compared with the TERP method by varying different 20, 40, 60 80 and 100 Nodes.

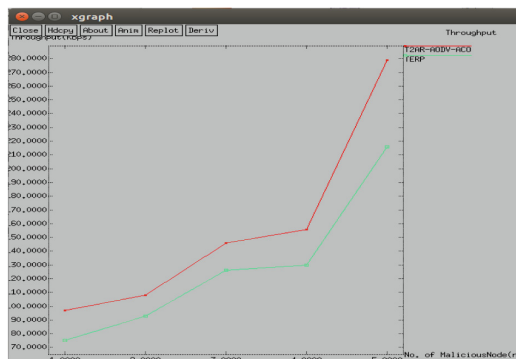


Fig. 2. Malicious node vs. Throughput

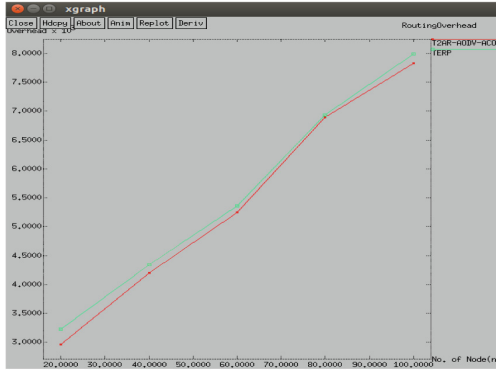


Fig. 3. Node vs. routing overhead

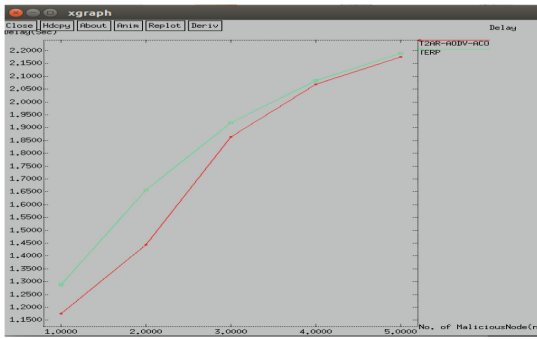


Fig. 4. Malicious node vs. delay

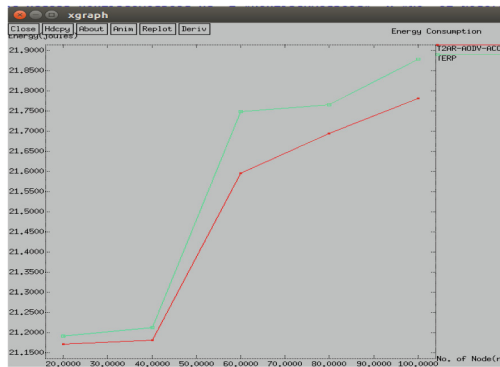


Fig. 5. Node vs. Energy consumption

The comparison of nodes vs. delay between T2AR-AODV-ACO and TERP is plotted in Fig. 4. The delay decreased in T2AR-AODV-ACO method, when compared with the TERP method by varying different 20, 40, 60 80 and 100 Nodes.

The comparison of nodes vs. energy between T2AR-AODV-ACO and TERP is plotted in Fig. 5. The energy consumption decreased in T2AR-AODV-ACO method, when compared with the TERP method by varying different malicious nodes 1, 2, 3, 4 and 5.

Thus, T2AR-AODV-ACO techniques effectively used for transferring trusted data packet from S-D in sensor networks with increase in throughput by decreasing routing overhead, delay and energy consumption. The simulation parameters of T2AR-TERP Methodology is explained as follows, the simulation start time and ending time is 0.0–5.0. The fixed nodes such as 20, 40, 60, 80 and 100 nodes are randomly distributed in the area. Here, each data packet starts its journey from a random location to a random destination with randomly selected speed. In traffic model, the Constant-bit rate (CBR) traffic sources are used with 802\_11 MAC Type. Antenna model used is Omni Antenna with 28 ms minimum speed and Initial transmit and receive power is 0.660 and 0.395 W.

## 5 Conclusion

The “T2AR-AODV-ACO” methodology used for Trust based secured route path between the source node and the destination node. The Trust based AODV RP with ACO optimization is used for maintaining energy and secured trust based routing in ad-hoc networks. Thus, overall methodology provides better results in term of throughput, routing overhead, end-to-end delay and energy consumption in trust aware ad-hoc routing compared to TERP methodology by varying the no. of fixed nodes and malicious nodes. The hybrid trust based security can be further enhanced by using optimization and also by detecting the malicious nodes in the trust based ad-hoc networks.

## References

1. Chen, R., Guo, J., Bao, F., Cho, J.H.: Trust management in mobile ad hoc networks for bias minimization and application performance maximization. *Ad Hoc Netw.* **19**, 59–74 (2014)
2. Chen, R., Guo, J., Bao, F., Cho, J.H.: Integrated social and quality of service trust management of mobile groups in ad hoc networks. In: *Proceedings of IEEE 9th International Conference on Information, Communications & Signal Processing*, pp. 1–5 (2013)
3. Mitchell, R., Chen, I.R.: Effect of intrusion detection and response on reliability of cyber physical systems. *IEEE Trans. Reliab.* **62**, 199–210 (2013)
4. Jawhar, I., Trabelsi, Z., Al-Jaroodi, J.: Towards more reliable and secure source routing in mobile ad hoc and sensor networks. *Telecommun. Syst.* **55**, 81–91 (2014)
5. Wen, D., Huai-Min, W., Yan, J., Peng, Z.O.U.: A recommendation-based peer-to-peer trust model. *J. Softw.* **15**, 571–583 (2004)
6. Jan, M., Nanda, P., Usman, M., He, X.: PAWN: a payload-based mutual authentication scheme for wireless sensor networks. *Concurr. Comput. Pract. Exp.* **29**, e3986 (2017)
7. Jan, M.A., Nanda, P., He, X., Liu, R.P.: A Sybil attack detection scheme for a forest wildfire monitoring application. *Future Gener. Comput. Syst.* **80**, 613–626 (2018)

8. Dong, M., Ota, K., Yang, L.T., Chang, S., Zhu, H., Zhou, Z.: Mobile agent-based energy-aware and user-centric data collection in wireless sensor networks. *Comput. Netw.* **74**, 58–70 (2014)
9. Paul, B., Marcombes, S., David, A., Struijk, L.N.A., Le Moullec, Y.: A context-aware user interface for wireless personal-area network assistive environments. *Wireless Pers. Commun.* **69**, 427–447 (2013)
10. Yu, Y., Li, K., Zhou, W., Li, P.: Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. *J. Netw. Comput. Appl.* **35**, 867–880 (2012)
11. Yan, Z., Wang, M.: Protect pervasive social networking based on two-dimensional trust levels. *IEEE Syst. J.* **11**, 207–218 (2017)
12. Saha, H.N., Mitra, P.: Intelligent energy aware fidelity based on-demand secure RP for MANET. *Int. J. Comput. Netw. Inf. Secur.* **10**, 48–64 (2018)
13. Bijon, K.Z., Haque, M.M., Hasan, R.: A trust based Information sharing model (TRUISM) in MANET in the presence of uncertainty. In: *Proceedings of IEEE Twelfth Annual International Conference on Privacy, Security and Trust (PST)*, pp. 347–354 (2014)
14. Shabut, A.M., Kaiser, M.S., Dahal, K.P., Chen, W.: A multidimensional trust evaluation model for MANETs. *J. Netw. Comput. Appl.* **123**, 32–41 (2018)
15. Patel, N.J.K., Tripathi, K.: Trust value based algorithm to identify and defense gray-hole and black-hole attack present in MANET using clustering method. *Int. J. Sci. Res. Sci. Eng. Technol.* **4**, 281–287 (2018)
16. Sivakumara, D., Jeganb, J., Selvakumarc, K.: Cuckoo search based Reliable Energy and Trust aware Routing Protocol (CRETRP) for wireless sensor network. *Int. J. Control Theory Appl.* **10**, 121–134 (2017)
17. Patel, V.H., Zaveri, M.A., Rath, H.K.: Trust based routing in mobile ad-hoc networks. *Lect. Notes Softw. Eng.* **3**(4), 318 (2015)



# An Octagonal Shaped MIMO UWB Antenna with Dual Band Notched Characteristics

V. N. Koteswara Rao Devana<sup>1(✉)</sup> and A. Maheswara Rao<sup>2</sup>

<sup>1</sup> Department of ECE, JNTUA, Anathapuramu, A.P., India  
dvnk Rao@gmail.com

<sup>2</sup> ECE Department, PBRVITS, Kavali, A.P., India

**Abstract.** A MIMO–UWB microstrip feed monopole antenna with C band and lower WLAN notch band characteristics is proposed. UWB frequency range is obtained by two octagonal shaped monopole radiating patches etched on FR-4 dielectric and with a partial ground plane. A T-shaped stub is used to decouple energy between the two radiating patches. Two Notched bands, one at 3.7 to 4.2 GHz, and the other at 5.15–5.35 GHz are achieved with two U-shaped slots etched out on two radiating patches. The dimension of antenna is  $60 \times 35 \times 1.6 \text{ mm}^3$ , that covers  $-10 \text{ dB}$  bandwidth of 7.5 GHz,  $<-15 \text{ dB}$  mutual coupling, and  $<0.01$  envelope correlation coefficient over 3.1 to 10.6 GHz frequency range except the two notch bands, makes it a suitable for portable UWB applications.

**Keywords:** MIMO · Band notched · Ultra-wideband antenna · Micro strip line feed

## 1 Introduction

To enhance the channel capacity and performance of data transmission Multiple-Input-Multiple-Output (MIMO) technology is used in Communication Systems [1]. MIMO technology is recently adapted in mobile phones, that can be used in communication technologies like WiMAX, WCDMA, WLAN and UWB [2], to realize high speed data transmission. In 2002, frequency band of 3.1 to 10.6 GHz is authorized for applications with low power emission [3] by Federal Communication Commission (FCC). Ultra wide band (UWB) antennas can be designed with different shapes of patch and ground [4, 5]. MIMO technology improves the performance of radio communication systems [6].

Various types of methods are proposed for MIMO-UWB technology, to reduce mutual coupling between radiators [7–9]. Moreover, UWB systems transmits only  $-41 \text{ dBm}$  of power, relatively small to the power transmitted by narrow band technologies like C and WLAN bands within the UWB spectrum. Thus, electromagnetic interference takes place between UWB and C, WLAN band systems. To mitigate such interference with C and WLAN band, UWB systems need notch filters. Inverted U-shaped [10], L-shaped [11], U-shaped [12] structures can be introduced in ground or patch to obtain notch bands. Further, MIMO antenna performance depends on the measurement of  $S_{12}$  and ECC reported in [13–16].

The work focussed on designing a UWB MIMO antenna with C and Lower WLAN notch band characteristics. Two octagonal shaped radiators with modified ground is used to achieve UWB frequency range and reduction of coupling between patches is suppressed with a T-shaped ground-stub. By introducing two inverted U-shaped slits band notch functionalities are achieved.

## 2 Antenna Design

The geometry of the proposed MIMO UWB antenna is shown in Fig. 1. Two identical octagonal shaped monopoles close to each other are etched on top of FR-4 with a dielectric constant 4.3, and dimensions of  $60 \times 35 \times 1.6 \text{ mm}^3$ . The radiators are excited by microstrip feed line with dimensions  $W_f \times L_f \text{ mm}^2$ .

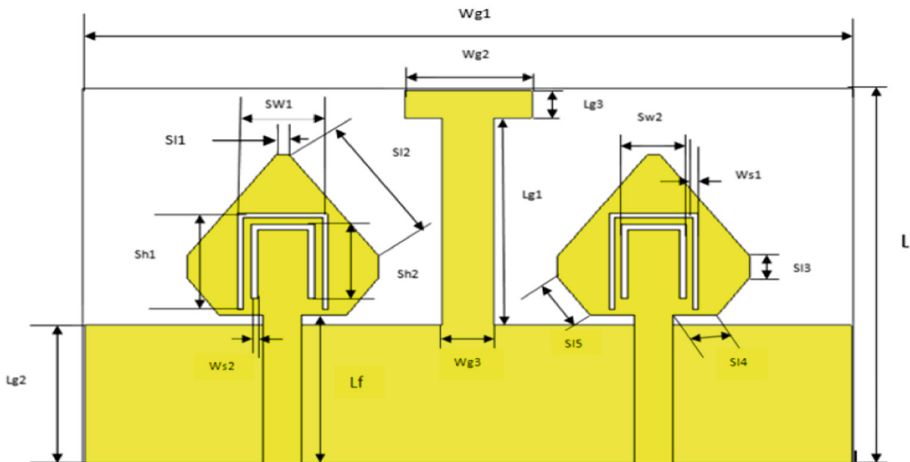


Fig. 1. Proposed UWB MIMO antenna.

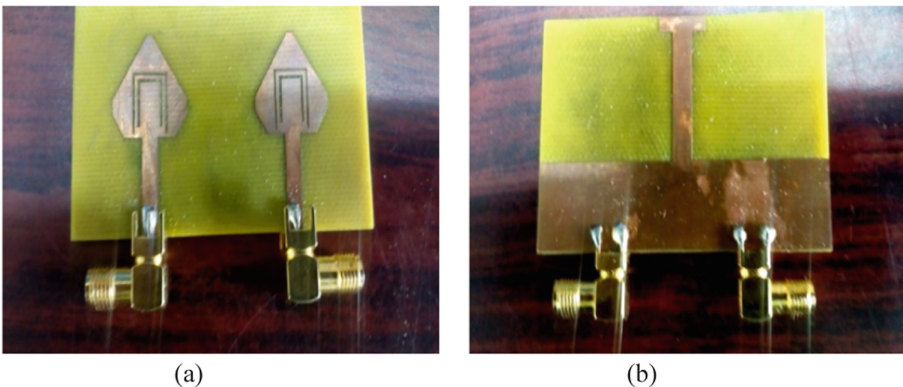


Fig. 2. Prototype of the proposed antenna (a) Front view (b) Back view.

The defected ground is used to achieve the required UWB bandwidth and a T-shaped stub is used to minimize  $S_{21}$  between two radiating patches. For each radiating element, two inverted U-shaped slots are introduced, whose function is to generate a notch at 3.7–4.2 GHz for C-band applications with upper inverted U-shaped slot, and other at 5.15–5.35 GHz for lower WLAN applications with lower inverted U-shaped slot. In Fig. 2, the fabricated antenna is shown.

The optimized dimensions of proposed antenna are shown in Table 1.

**Table 1.** Dimensions of proposed antenna.

Parameter	Value (mm)	Parameter	Value (mm)	Parameter	Value (mm)
$W_{g1}$	60	$L_{s1}$	9	$W_f$	3
$L_{s2}$	7	$W_{g2}$	4	$SI_1$	1
$W_{g3}$	10	$SI_2$	11.8	$W_{s1}$	0.4
$SI_3$	0.5	$W_{s2}$	0.5	$SI_4$	4.3
$L$	35	$SI_5$	3.5	$L_f$	14
$S_{h1}$	9	$L_{g1}$	13	$S_{h2}$	7
$L_{g2}$	19.5	$S_{w1}$	7	$L_{g3}$	2.5
$S_{w2}$	5	–	–	–	–

### 3 Simulation Results and Discussion

The proposed antenna is simulated by CST ver. 2017 and the results are measured by Anritsu MS2037C/2 network analyzer. Various electrical characteristics such as return loss ( $S_{11}$ ), VSWR, surface current distribution, mutual coupling ( $S_{12}$ ), 2-D radiation pattern, ECC and diversity gain are discussed in the following sections.

#### 3.1 Return Loss and Mutual Coupling

The return loss plot ( $S_{11}$ ) of a single element octagonal shaped monopole antenna is shown in Fig. 3, that covers frequency range of 3.59–9.31 GHz. But, to achieve UWB bandwidth ranging from 3.1–10.6 GHz, two closely spaced identical octagonal shaped patches are used. The  $S_{11}$  plot of two element MIMO antenna covers 3.29–11.95 GHz as shown in Fig. 4. For the better performance of MIMO, the value of mutual coupling ( $S_{12}$  or  $S_{21}$ )  $< -15$  dB. The return loss ( $S_{11}$ ) and mutual coupling parameter ( $S_{12}$ ) of the two element MIMO- UWB antenna with and without T-shaped stub are shown in Fig. 5. From Fig. 5, by introducing the T-shaped stub the mutual coupling is reduced to  $< -15$  dB over UWB frequency range.



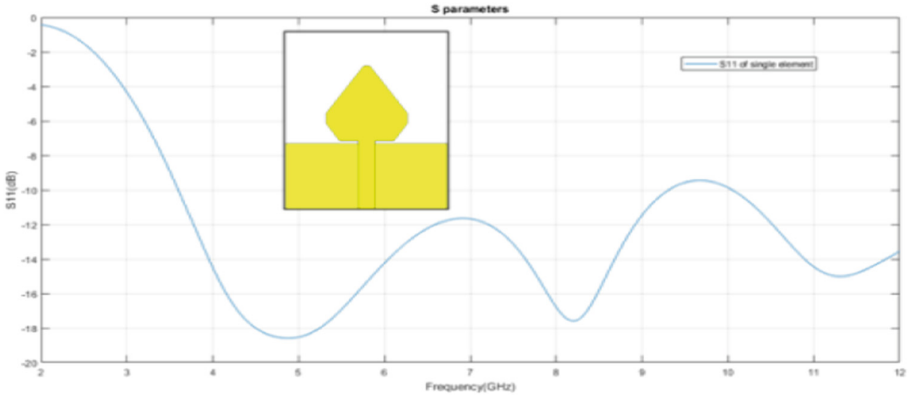


Fig. 3.  $S_{11}$  plot for single element.

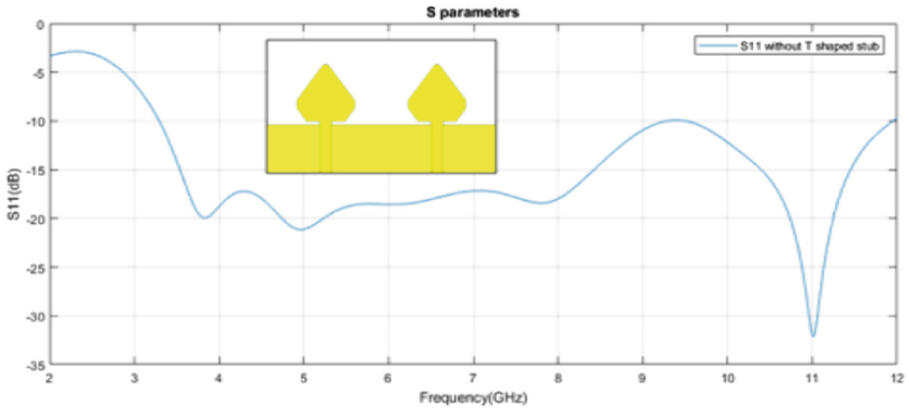


Fig. 4.  $S_{11}$  plot for two element.

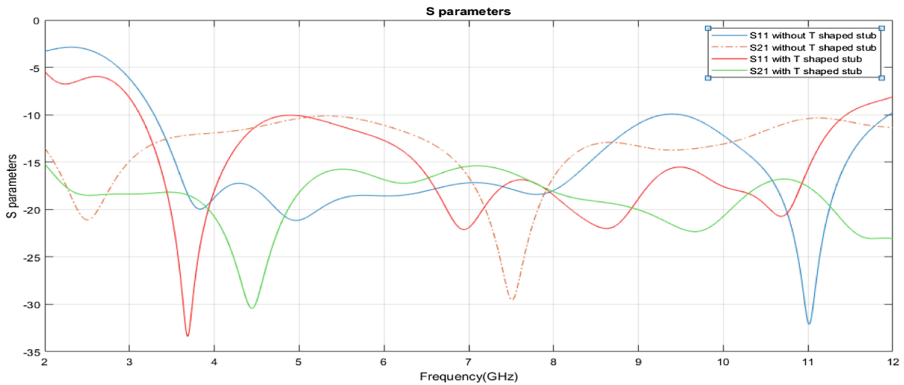
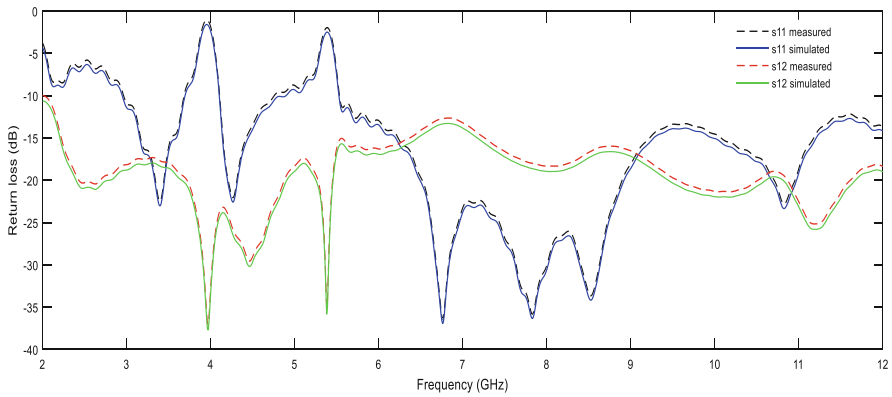


Fig. 5.  $S_{11}$  and Mutual coupling ( $S_{21}$ ) plots without and with T-Shaped ground stub.

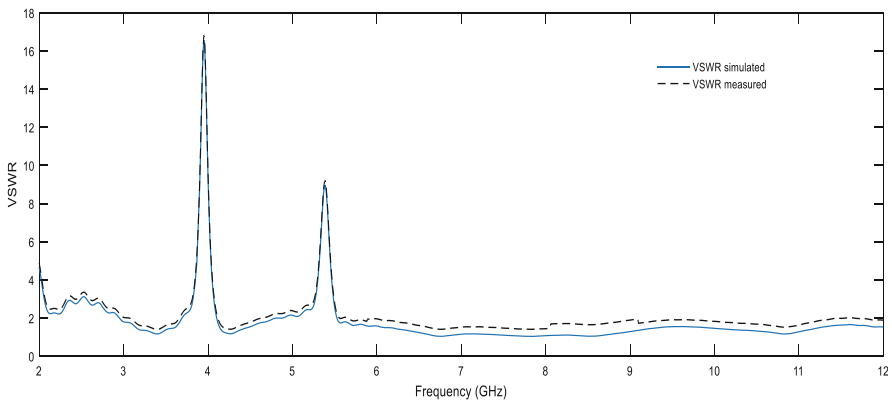
To suppress these interferences, band rejection functionality is introduced in MIMO UWB element by introducing U-shaped slots into the patch. The simulated and measured return loss ( $S_{11}$ ) and Mutual Coupling parameter ( $S_{12}$ ) of proposed antenna with notched band characteristics at C and Lower WLAN applications are shown in Fig. 6.

### 3.2 Voltage Standing Wave Ratio (VSWR)

The simulated and measured values of VSWR of the antenna lies between 1 and 2 over entire UWB frequency except the two notched frequency bands. The VSWR is approximately 14.61 at 3.92 GHz and 8.5 at 5.34 GHz indicating that the proposed MIMO-UWB antenna rejects C and Lower WLAN bands as shown in Fig. 7.



**Fig. 6.** Return loss ( $S_{11}$ ) and mutual coupling ( $S_{21}$ ) of proposed MIMO-UWB



**Fig. 7.** VSWR of proposed MIMO-UWB antenna.

### 3.3 Radiation Pattern

In Fig. 8, the 2-D radiation patterns at two notch frequencies 3.92, 5.34 GHz and resonant frequencies at 3.33, 6.74 GHz are shown. From the radiation pattern plots, it is observed that at resonant frequencies the 2-D pattern is nearly Omni directional in H-plane and dipole like pattern in E-Plane.

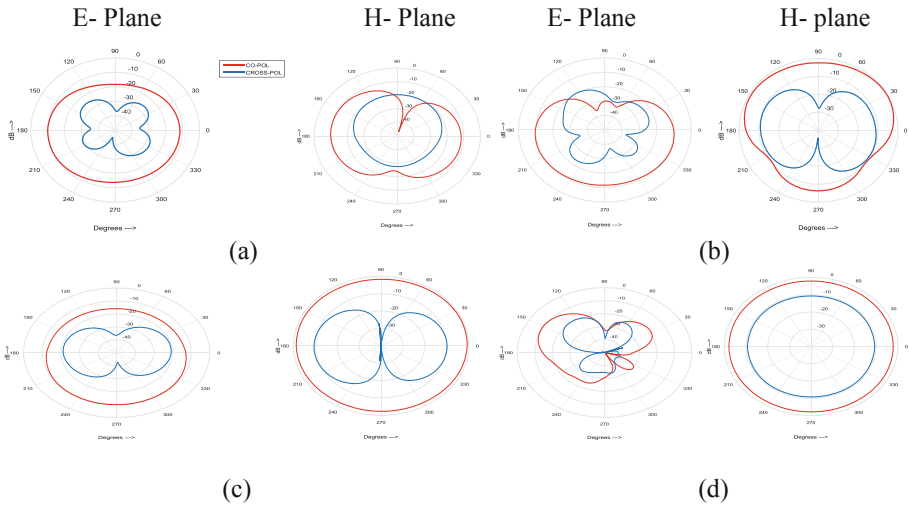


Fig. 8. 2-D radiation patterns at (a) 3.92 GHz (b) 5.34 GHz (c) 3.33 GHz (d) 6.74 GHz.

### 3.4 Surface Current Distribution

In Fig. 9(a)–(b), the surface currents at the two resonant frequencies 3.33 GHz, 6.74 GHz and at the two notch frequencies 3.92 GHz, 5.34 GHz are shown. At two resonant frequencies 3.33 and 6.74 GHz, the surface current distributions are minimized and at two notch frequencies 3.92 GHz and 5.34 GHz, the surface currents are concentrated highly around U-shaped slots shown by red areas in Fig. 9(b). Thus, the overall radiation at 3.92 and 5.34 GHz is very limited, creates notch bands at C and Lower WLAN bands.

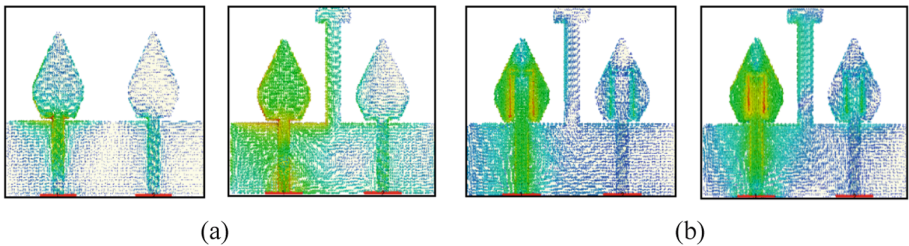
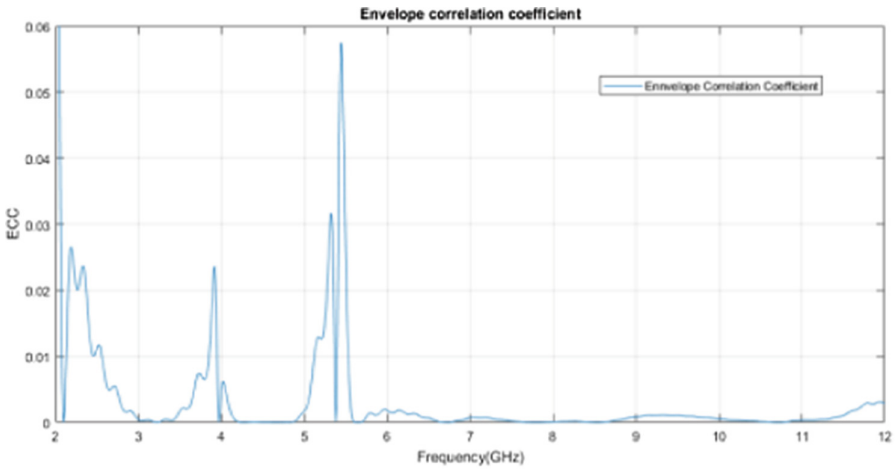


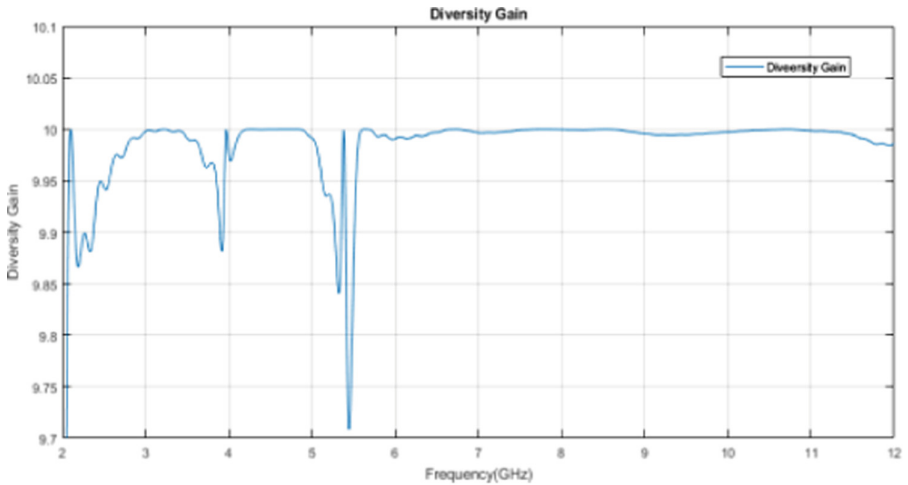
Fig. 9. Current distribution at (a) 3.33, 6.74 GHz (b) 3.92, 5.34 GHz.

### 3.5 Envelope Correlation Coefficient and Diversity Gain

In Fig. 10, the envelope correlation coefficient of proposed antenna is shown. From Fig. 11, the diversity gain of the proposed antenna is very flat around 10 db over 3.1 to 10.6 GHz except at the two notch frequency bands.



**Fig. 10.** Envelope Correlation Coefficient of proposed antenna.



**Fig. 11.** Diversity gain of proposed antenna.

## 4 Conclusion

An octagonal shaped two element MIMO-UWB with two band notch characteristics is presented. The mutual coupling between the two radiating patches is reduced by using T-shaped stub. The MIMO-UWB covers frequency range from 3.29–11.95 GHz. Two band notches at C from 3.7–4.2 GHz and Lower WLAN from 5.15 to 5.35 GHz are achieved by introducing two U-shaped slots into the patch. Thus, the proposed antenna is suitable candidate for MIMO-UWB applications.

## References

1. Foschini, G.J.: On limits of wireless communications in a fading environment when using multiple antennas. *Wirel. Pers. Commun.* **6**(3), 311–335 (1998)
2. Lee, J.M., Kim, K.B., Ryu, H.K., Woo, J.M.: A compact ultrawide band MIMO antenna with WLAN band-rejected operation for mobile devices. *IEEE Antennas Wirel. Propag. Lett.* **11**, 990–993 (2012)
3. FCC, Ultra-Wideband Operation FCC Report and Order, Technical rep. US47 CFR Part 15 (2002)
4. Shakib, M.N., Moghavvemi, M., Mahadi, W.N.: A low profile patch antenna for ultrawideband application. *IEEE Antennas Wirel. Propag. Lett.* **14**, 1790–1793 (2015)
5. Ojaroudi, N., Ojaroudi, M., Ebazadeh, Y.: UWB/Omni Directional Microstrip Monopole Antenna for Microwave Imaging Applications (2014)
6. Zheng, L., Tse, N.C.: Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels. *IEEE Trans. Inf. Theory* **49**, 1073–1096 (2003)
7. Yang, F., Wang, Z.M.: Reducing mutual coupling of closely spaced microstrip MIMO antennas for WLAN application. *IEEE Antennas Wirel. Propag. Lett.* **10**, 310–313 (2011)
8. Malekpour, N., Amin Honarvar, M., Dadgarpur, A., Virdee, B.S., Denidni, T.A.: Compact UWB MIMO antenna with band-notched characteristic. *Microwave Opt. Technol. Lett.* **59**(5), 1037–1041 (2017)
9. Liu, L., Cheung, S.W., Yuk, T.I.: Compact MIMO antenna for portable devices in UWB applications. *IEEE Trans. Antenna Propag.* **61**, 4257–4264 (2013)
10. Sharma, A., Sharma, M.M.: An UWB Antenna Design with Dual Band Notched Characteristic Using U-Shaped Slots (2016)
11. Emadian, S.R., Ghobadi, C., Nourinia, J.: *Microwave Opt. Technol. Lett.* **54**(6), June 2012
12. Shen, J., Wang, J., Li, C.: Progress in Electromagnetic Research Symposium (PIERS), Shanghai, China, 8–11 August 2016
13. Liu, L., Cheung, S.W., Yuk, T.I.: Compact MIMO antenna for portable UWB applications with band-notched characteristic. *IEEE Trans. Antenna Propag.* **63**, 1917–1924 (2015)
14. Blanch, S., Romeu, J., Corbella, I.: Exact representation of antenna system diversity performance from input parameter description. *Electron. Lett.* **39**, 705–707 (2003)
15. Li, J.F., Chu, Q.X., Li, Z.H., Xia, X.: Compact dual band notched UWB MIMO antenna with high isolation. *IEEE Trans. Antennas Propag.* **61**, 4759–4766 (2013)
16. Tang, T., Lin, K.: An ultrawideband MIMO antenna with dual band-notched function. *IEEE Trans. Antennas Propag.* **61**, 4759–4766 (2014)



# On the Construction of Impacts of Mobility in Multicast Routing Protocol in Mobile Ad Hoc Networks

K. Muthulakshmi<sup>(✉)</sup>, S. Nithya Devi, and N. Archana

Electronics and Communication Engineering, Dr NGP Institute of Technology,  
Coimbatore, Tamil Nadu, India

{muthulakshmi, nithyadevi, archana}@drngpit.ac.in

**Abstract.** The Mobile Ad-hoc Network (MANET) is defined as the grouping of different wireless mobility nodes that tends to create provisional networks without having any wired network connections. There are no static topology in the network because of the nodes mobility. Here the topology of the network has the ability to change their connection at any time and more often too, which can't be guessable. This paper focused for evaluates the various mobility models impacts [3] in Mobile Ad-Hoc Network. Here we present about the independent metrics of multicast routing protocol for capturing the characteristics of mobility which includes the resolution of temporal and spatial dependence, restrictions, geographic resolution, Pause time and hybrid networks.

## 1 Introduction

A Mobile Ad-hoc networks (MANET) are used to enable wireless communication between mobile nodes without making use of any infrastructure. The research of Mobile Ad-Hoc Network is emerging its gain because of small ubiquity, inexpensive wireless communicating devices. Most of the MANETS has not yet deployed. Research of MANET mostly based on simulation. In this manuscript, we target the mobility impact models which based on MANET performance in routing multicast protocols. Here traffic pattern is used for randomly selects the terminous pairs with extended session times. Many existing works depends on the pattern of Node Mobility which predicted to be a Random way point. In the simulator distribution of the current network simulator distribution, the model of mobility implementation [12] is as follows:

### A. Random Walk Model (RWK)

At every timeslot, a node changes their speed and direction, randomly selects the moves & terminous point, which acts towards it with a random direction  $[0, 2\pi]$  and new speed chosen from a uniform distribution. Where  $2\pi$  is the direction of maximum of permissible direction for all mobility nodes.

### B. Random Waypoint Model (RWP)

Every time, the nodes uses the randomly chosen velocity  $[0, V_{\max}]$  and reaches the random destination anywhere in the network field. After the node reaches it terminous point, then it released the “pause time”-  $T_{\text{pause}}$  parameters by the meaning of node stops

for the duration. Where  $V_{max}$  is maximum velocity within the network.  $T_{pause}$  is small, network becomes highly dynamic and  $T_{pause}$  is long, network becomes stable.

**C. Reference Point Group Mobility**

At every instant, the nodes are classified in to certain clusters, Every cluster has a head which act as a leader, the leaders mobility follows the random way point. Each node of the group follows the leader’s mobility closely with some deviation. Each and Every Node contains specific direction & speed which should be ordered by the leader node. (i.e.) the head node. It has the 2 types single and multi-groups. In the below Eqs. 1 and 2 describes the speed and direction of the nodes.

$$V_{speed}(t) = V_{leaders\ speed}(t) + V_{max}(t) \tag{1}$$

$$\Theta_{direction}(t) = \Theta_{leaderdirection} + \Theta_{max}(t) \tag{2}$$

**D. Smooth Random Mobility Model (SRMM)**

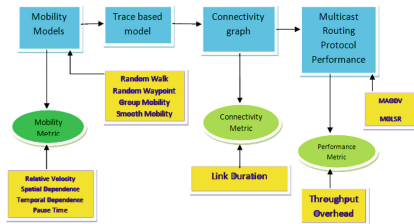
At every instant node the node’s direction & speed of its mobility increases smoothly as moving manner. Speed chosen randomly from  $[0, 0.5 V_{max}, V_{max}]$ . The speed frequency is predicted by the approach of Poisson technique. Thus the mobile node’s speed is varying highly from the present speed of the node which is noted as  $V(t')$  to the target new speed  $V(t)$  by acceleration speed  $[0, a_{max}]$  or deceleration speed  $[a_{min}, 0]$  respectively. Then the upcoming speed is evaluated by using the below formula.

$$V(t) = V(t - \Delta t) + a(t) \Delta t \tag{3}$$

Where  $V(t)$  is target new speed,  $a(t)$  is acceleration speed,  $\Delta t$  is difference in speed. In Eq. 3 describes the new target speed.

Mobility characteristics are spatial dependence, temporal dependence, relative velocity, geographic restriction and pause time. Mobility characteristics are listed below:

- (1) **Pause time:** The node suspends an action temporarily after reaching destination.
- (2) **Hybrid Resolution Structure:** We consider the survivability of multicast routing protocol.



**Fig. 1.** Frame work for proposed work

As shown in Fig. 1. Our proposed model concentrates following aspects, the model of mobility, mobility metrics, traces based model, connectivity graph, the metrics for connectivity, the connection between multicast routing protocol & mobility and also the performance for analyzing of impacts in node mobility [1].

## 2 Related Work

### A. Mobility Model

We review several mobility models, among these we choose few stochastic mobility models. The examples shown in this segment are often met with several changes in the reality studio.

#### I. Random Movement Based

##### 1. Random Way Point Mobility Model (RWP)

The RWP is demonstrated in the Fig. 2. We accept a varying number nodes in a fixed size rectangular group. [Sufficiently large] The simulation takes up with the mobility of nodes consistently disturbed in rectangle clusters. Each and Every client selects a arbitrary terminus point and selects a arbitrary terminus point and chooses a random speed distributed consistently in interval (Fig. 3).

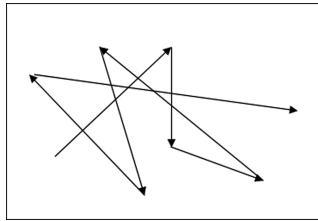


Fig. 2. RWP node mobility

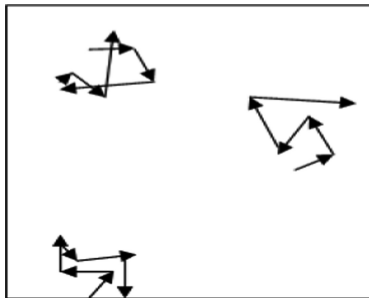


Fig. 3. RWM node mobility



## II. Spatial Resolution Dependency

### A. Random Direction Mobility Model (RPGM)

See Fig. 4.

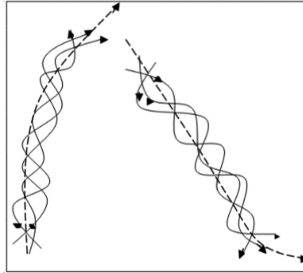


Fig. 4. Group mobility

### B. Metrics for Connectivity

The connectivity graph metrics aim to examine this issue. These metrics might also assist in relating mobility metrics with protocol performance. The connectivity metrics are considered as link duration. Link Duration is a touchstone of stability of the liaison between these guests. The connectivity metric is to plug in the mobility model with trace analysis is likewise related to multicasting protocol through connectivity metrics.

### C. Trace Based Models

The realistic traces can then be studied and relevant statistics can be taken out. Subsequently from the real trees can be utilized in the mobility model that can also accept the supplementary inputs from operator of the model the size of the scenario, the size of the hotspot, speed and pause time distribution & so on (Fig. 5).

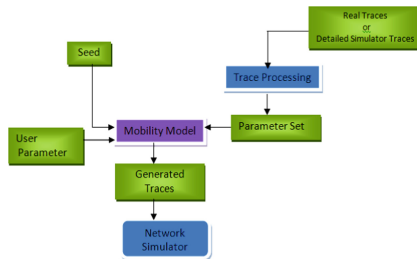


Fig. 5. SM Node mobility

### D. Multicast Routing Protocol Performance

There are more innovative research are processing in the field of multicasting in Ad hoc Networks [6]. They suggest a tree construction scheme which reduces data overhead and increases throughput [2] by getting to maximum use of the broadcast nature of the wireless medium. We compare different approaches to reliable reactive multicast routing protocols, namely MAODV and MOLSR [8] (Fig. 6).

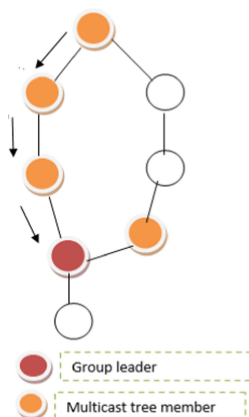


Fig. 6. MAODV multicast tree building

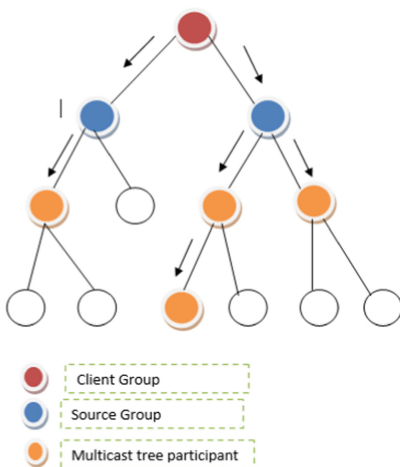


Fig. 7. MOLSR multicast tree building

In Fig. 7 shows the molding of a tree with hop by hop movements. The comparison between multicast routing protocol MAODV and MOLSR described in the below Table 1.

**Table 1.** Characteristics between MAODV and MOLSR

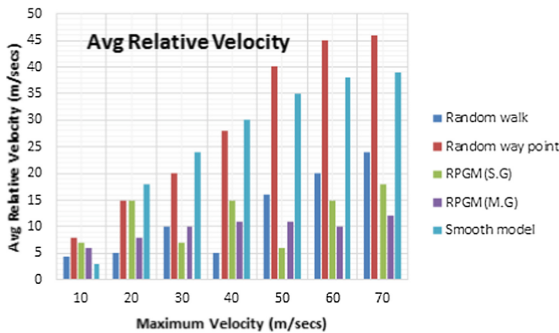
Characteristics	MAODV	MOLSR
Design structure	Tree based (core tree)	Tree based (source tree)
Loop free	Yes	Yes
Scalability	Fair	Fair
Control packet flooding	Flat	Flat
Periodic message requirement	Yes	Yes

### 3 Simulation and Results

**Relative Velocity:** The standard value of relative velocity is taken. i.e. Difference in velocity between node pairs [shown in Eq. 4]. It also symbolized as a “Relative Speed”.

$$RV_{i,j}(t) = |V_i(t) - V_j(t)| \tag{4}$$

**Average Relative Velocity:** The figure shows the graph between average relative speed and maximum velocity, through experimentation, we obtain the maximum average velocity is obtained in random waypoint model with the precondition of this that relative speed is equal dimension of mobility space. Variation in Relative velocity with increasing mobility for the Random waypoint model shown in Fig. 8.



**Fig. 8.** Variation in relative velocity with mobility models

**The Average Level of Spatial Resolution Dependence:** It is the value of average spatial dependence over the time instants & node pairs have must satisfy the certain condition. In the figure the graph is plotted between the degree of spatial defense, and maximum speeds in m/Sec. Through the experimenting random waypoint mobility pattern have a higher value of spatial dependency in the dimension of the mobility distance. Variation in Spatial dependence with the increasing mobility of the Random waypoint model shown in Fig. 9.

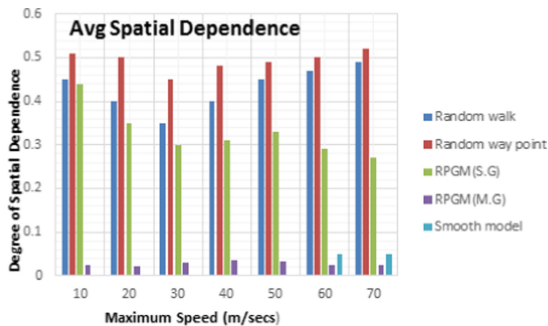


Fig. 9. Variation in spatial dependence with mobility models

**Temporal Resolution Dependence:** It is the quantity of similar velocity of each node of two times slots( $t, t'$ ).

In figure, the graph is drawn between degree of temporal dependence and maximum speeds in m/sec's, Through our experimentation random walk have the smallest value. Variation in Temporal dependence with increasing mobility for Group mobility (M.G) model shown in Fig. 10.

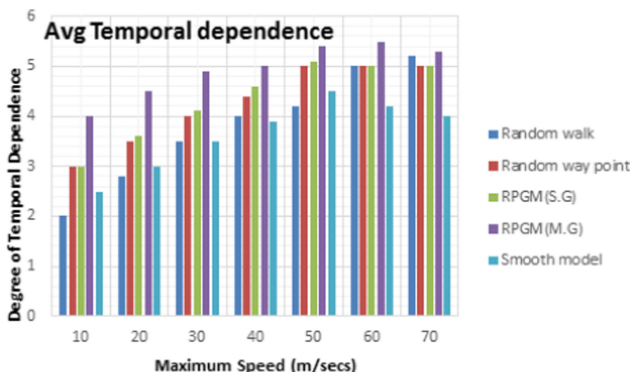


Fig. 10. Variation in temporal dependence with mobility models

**Pause Time:** It is the measure of ‘stop an action’ released by nodes temporarily after reaching destination node.

**Average Pause Time:** it the value of averages pause time released by every require nodes. In this fig, the graph is plotted between the point of interruption time and maximum speed in m/sec's. Variation in Pause time with increasing mobility for Group mobility (M.G) model shown in Fig. 11.

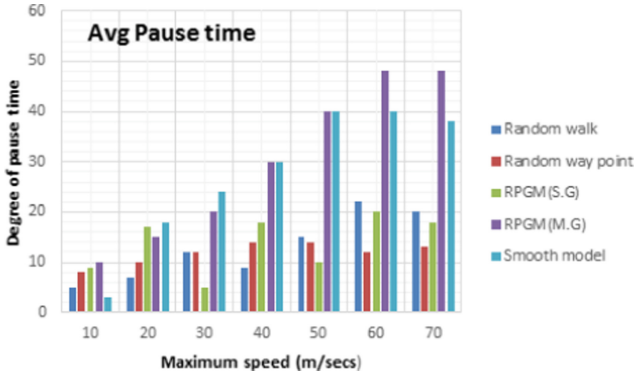


Fig. 11. Variation in pause time with mobility model

**Average Link Duration:** Generally, the graph between the degree of link duration and maximum speeds in m/Sec. Through the graph we obtained average link duration in group mobility. Variation in Link duration with increasing mobility for Group mobility (S.G) model shown in Fig. 12.

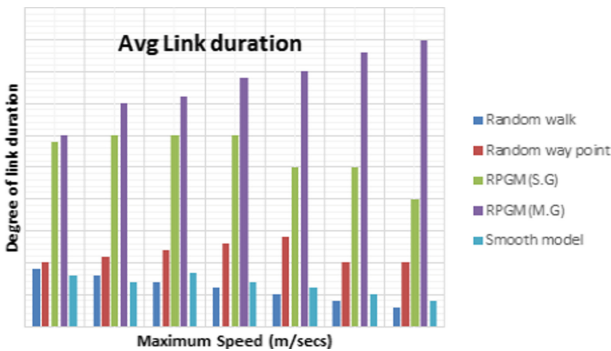


Fig. 12. Variation in link duration with mobility models

Performance of MOLSR & MAODV for fluctuating throughput on different mobility models.

Variation in throughput with the increasing mobility of Group mobility (S.G) model in shown in Figs. 13 and 14.

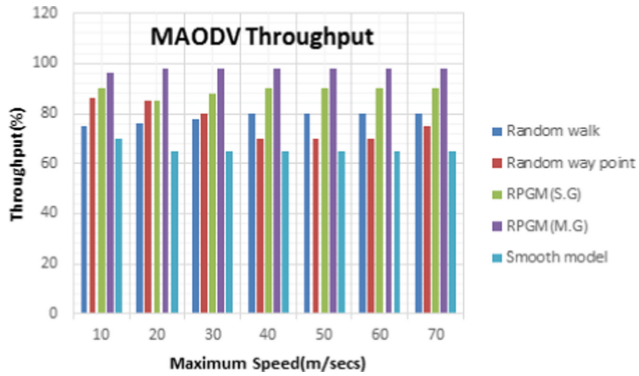


Fig. 13. Throughput variation for MAODV

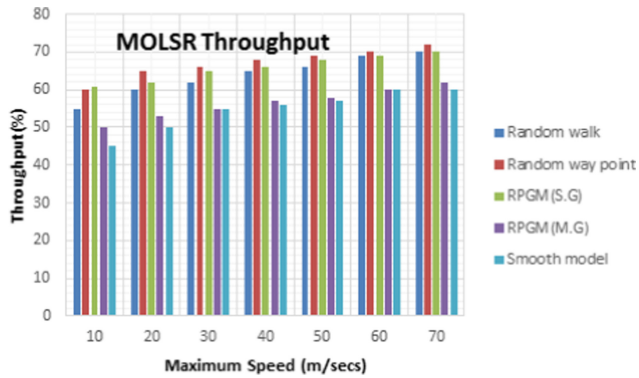


Fig. 14. Throughput variation for MOLSR

Performance of MOLSR & MAODV for fluctuating Overheads:

From the graph we can attend that performance of MAODV much better than MOLSR even after the maximizes the node numbers. Overhead Variation with decreasing for group mobility in MAODV shown in Fig. 15. Variation in Overhead with increasing mobility for Group mobility (M.G) model in MOLSR shown in Fig. 16.

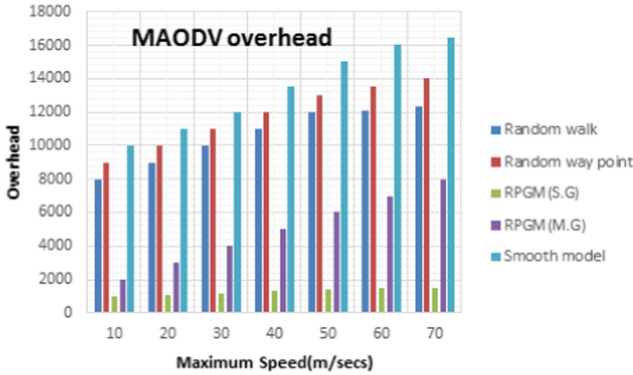


Fig. 15. Overhead variation for MAODV

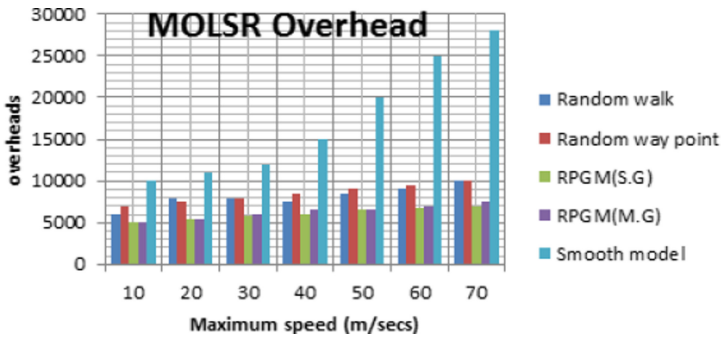


Fig. 16. Overhead variation in MOLSR

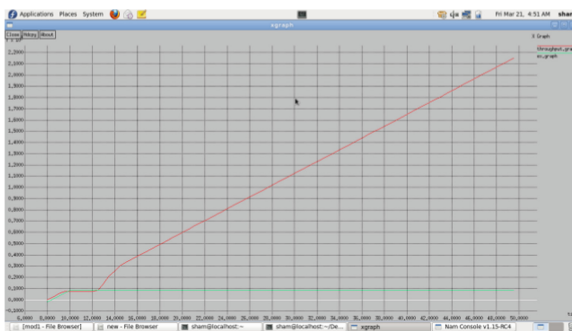


Fig. 17. Throughput between Existing [MOLSR] and proposed [MAODV] protocols

In Fig. 17 Shows the throughput graph between the two methods wherein the throughput observed when using the MAODV has higher than of that in the case of MOLSR models with mobility models.

## 4 Conclusions and Future Work

The simulation results shows about the multicast routing protocol performance which differs differently across various node mobility. Then the outcome of the study shows that a perspective of one model can't suits different model. So the application of the node mobility has been presented for route selection model. Here, while compare to the MOLSR, MAODV gives a good performance in high network mobility. For identifying the new path for finding the terminous point, MAODV is much faster. The previous model for finding the path splits as it appeals for the approach of route repair whereas MOLSR has no route repair approach. Also, MAODV has no route repair approach for finding its terminous point, Hence the packets are dropped.

## References

1. Al Hanbali, A., Kherani, A.A., Groenevelt, R., Nain, P., Altman, E.: Impact of mobility on the performance of relaying in ad hoc networks. In: Proceedings of INFOCOM 2006, Bracelona, Spain (2006)
2. El Gamal, A., Mammen, J., Prabhakar, B., Shah, D.: Throughput-delay trade-off in wireless networks. In: Proceedings of INFOCOM 2004, Hong Kong (2004)
3. Timcenko, V., Stojanovic, M., Rakas, S.B.: Manet routing protocols vs. mobility models performance analysis and comparison. In: Proceedings of the 9th WSEAS International Conference on Applied Informatics and Communications (AIC 2009) (2009)
4. Helmy, A.: Important: a framework to systematically analyze the impact of mobility on performance of routing protocols for ad hoc networks A. In: IEEE INFOCOM (2003)
5. Gossain, H., Cordeiro, C.D.M., Agrawal, D.P.: Multicast over wireless mobile ad hoc networks: present and future directions. *IEEE Netw.* **17**(1), 52–59 (2003)
6. Murthy, C.S.R., Manoj, B.S.: *Ad Hoc Wireless Networks: Architectures and Protocols*. Prentice Hall, New Jersey (2004)
7. Jacquet, P., Minet, P., Laouiti, A., Viennot, L., Clausen, T., Adjih, C.: Multicast optimized link state routing. IETF manet draft-ietf-manet-olsr-molsr-01.txt (2002)
8. Joang, M., Lu, L.T.: A peer-to-peer zone based two-level link state routing for mobile ad hoc networks. *IEEE J. Sel. Areas Commun.* **17**, 1415–1425 (1999). Special issue on wireless ad hoc networks
9. Johansson, P., Larsson, T., Hedman, N., Mielczarek, B., Degermark, M.: Scenario-based performance analysis of routing protocols for mobile ad-hoc networks. In: Proceedings of IEEE/ACM MOBICOM 1999 (1999)
10. Tsumochi, J., et al.: Impact of mobility metric on routing protocols for mobile ad hoc networks. In: PACRIM Communications, Computers and Signal Processing (2003)
11. Zheng, Q., et al.: Recent advances in mobility modeling for mobile ad hoc network research. In: ACMSE (2004)
12. Essays, UK.: *Implementation Of Mobility Models For Manet S Using Glomosim Simulator Computer*, November 2013
13. Singh, S.K.: Performance evaluation of proactive, reactive and hybrid routing protocols with mobility model in mantes. *IJRET: Int. J. Res. Eng. Technol.* **2**, 254–259 (2013)
14. Kumar, S., Sharma, S.C., Suman, B.: Mobility metrics based classification & analysis of mobility model for tactical network. *Int. J. Next Gener. Netw. (IJNGN)* **2**(3), 2565–2573 (2010)





# Dynamic Trust Based Secure Multipath Routing for Mobile Ad-Hoc Networks

V. Sathiyavathi<sup>1</sup>, R. Reshma<sup>1</sup>, S. B. Saleema Parvin<sup>1</sup>,  
L. SaiRamesh<sup>2(✉)</sup>, and A. Ayyasamy<sup>3</sup>

<sup>1</sup> Department of Computer Science,  
Justice Basheer Ahmed Sayeed College for Women, Chennai, India  
sathya.mca2006@gmail.com, saleemasaffiaahil@gmail.com,  
reshmakumar2000@yahoo.com

<sup>2</sup> Department of Information Science and Technology, CEG, Anna University,  
Chennai, India  
sairamesh.ist@gmail.com

<sup>3</sup> Department of Computer Engineering, Government Polytechnic College,  
Nagercoil, India  
samy7771@yahoo.co.in

**Abstract.** In this paper, we propose a new secure routing protocol for mobile Ad-hoc networks. The proposed new secure routing protocol works by evaluating the trustworthiness of each node to reduce the hazards from malicious mode and enhance the security of network. A new trust computation model is used to calculate the trustworthiness of a node based on the historical behavior. The trust value is evaluated by including the intruder node using Intrusion Detection System (IDS). In this paper, intruder nodes are detected based on the packet delivery mode during the communication. The Ad-hoc on demand multipath distance vector routing protocol is used in this paper which is based on the trust model that computes the trust of nodes and makes decision accordingly. A new dynamic and trust-based routing protocol named Ad-hoc on demand Dynamic Trusted Multipath Distance Vector (AODTMDV) has been proposed for performing effective and secured multi-path routing in MANETs.

**Keywords:** Trust prediction model · Intrusion detection system · Multipath

## 1 Introduction

Nowadays, there is a rapid increase in the interest to deploy the new mobile technologies in everyday world. People are able to communicate from anywhere and at any time to request services from various locations. A Mobile Ad-hoc Network (MANET) is a connectionless network that allows mobile nodes to join and leave at any time due to the attackers. Trusted routing is carried out after the fault tolerant routing is to reduce the complexity by avoiding the error node using error reporting protocol in fault tolerant routing. In some existing systems, initially the trust of the nodes is calculated and routing is carried based on that. After that, sometimes the trusted nodes energy may reduce or that node is considered for routing because of not in communication path.

So, in the proposed system the fault tolerant routing may provide the nodes involved in the routing phase. From that, the trust of the nodes is calculated and routing will be reconstructed as secure multipath routing. The reliability of hub is assessed in this model, which is utilized with an attacking prevention system to agreeably distinguish and disconnect the vindictive hubs from the system. At long last, a trusted way is acquired in view of the trust esteem. So, there is no guarantee that some trusted nodes are permanent members of the network to improve the reliability [1].

Trust is used to measure the degree of belief by an individual or node regarding the transaction behavior of any other individual or node. In computer network, it is necessary to know the trust values of other nodes in order to provide secure communication. A trusted node in a computer network is different from a malicious node. A trusted node sends all the packets to the neighbors. On the other hand, a malicious node will drop the packets which are of important to the communication. Moreover, a trusted node is helpful in nature and helps to enhance the security and performance whereas a malicious node will try to destruct the communication by either carrying out active attacks or passive types of attacks. Therefore, isolation of malicious nodes using trust measure will reduce the risk in computer communication.

#### Nomenclature

IDS	Intrusion Detection System
AODTMDV	Ad-hoc on demand Dynamic Trusted Multipath Distance Vector
MANETs	Mobile Ad-hoc Networks
AOMDV	Ad-hoc On-demand Multi-path Distance vector routing protocol
AODV	Ad-hoc On-demand Distance Vector Routing Protocol

The trust mechanism makes decision based on some trust related information [1]. Generally, intrusion detection systems are classified into two methods such as detecting misbehavior and anomaly detection system. Misuse detection systems detect attacks based on the known attack signatures. The main advantage of developing intrusion detection system is that they can reduce false positives [2]. In this work, trust prediction model and recommendation model for path formation is implemented using the base of AODV. Some of the related work also discussed in Sect. 2 which helps to understand the problem defined here. And finally, the experiments are carried out and performance analysis is done using the bench mark parameters in Sect. 4.

## 2 Related Work

There are many works which are present in literature and explain about the techniques for intrusion detection. Among them, Sun et al. [3] have proposed a new information theory based framework to estimate trust and to model it in ad hoc networks. In their framework, trust is considered as a measure of belief about nodes in the environment. Liang and Shi [4] proposed two kinds of measures to handle uncertainty in trust modeling for this purpose; they have proposed a new algorithm which can estimate the trust effectively.

Trust model can be build based on the requirements given by the user's in the group. In [5], the cluster based trust model is implemented by which within the certain

cluster, the nodes are evaluated with their trust using the cluster head. In this work, the cluster head is considered as overall administrator for maintaining the trust level of the individual node. If sometimes, node maybe in two different clusters then each cluster has to given the trust value for that node separately. This will reduce the computational complexity for the individual nodes.

The intelligent energy aware approach for wireless sensor networks is given in [6] which use the intelligent rules with standard classification to make a efficient decision for routing. In [7], fuzzy clustering method is used for energy efficient routing with intelligent rules. This system really makes the communication in a secure way with energy efficiency. Quality of services is the main theme while the routing between the nodes in MANET as discussed in [8]. This work uses the context aware approach with fuzzy based technique to make routing in MANET.

The performance evaluation of routing mechanism in MANET is examined by implementing reusability in path formation. It also includes load balanced process by analyzing the proper channel [9]. Another work discussed in [10] describes the trust based routing mechanism in MANET. Hierarchical based fuzzy approach is applied here too implement trust routing.

Based on the literature survey, it comes to know that trust based routing is needed for network communications. And also, the available techniques for trust based routing are efficient in some manner but not satisfied on all QoS parameters. This proposed work implements the trust based routing using the basic AODV protocol and enhance by applying intelligent rules. With these trust mechanism, intrusion detection system is also introduced which makes the system secure.

### 3 System Architecture

The architecture of the system proposed in this work consist of four major components namely trust evaluation module, Intrusion Detection System module, trust path formation module and trust based secure routing strategy as shown in Fig. 1.

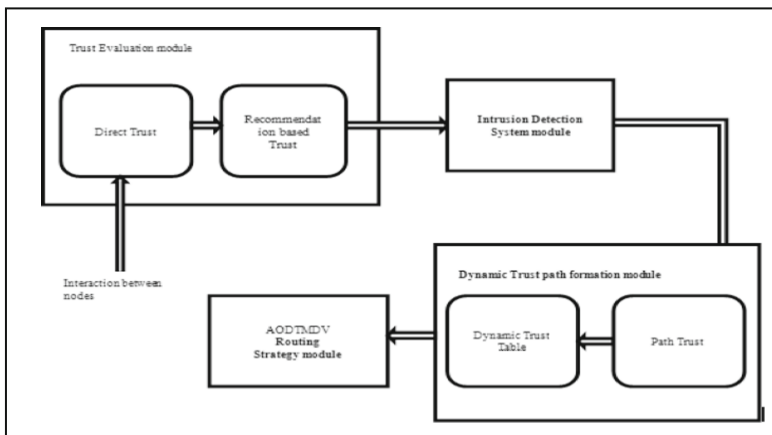


Fig. 1. System architecture

This architecture explains the trust based routing system and the new trust prediction model used to identify a secure path with the help of intrusion detection system.

### 3.1 Trust Prediction Model

In this work, trust is evaluated based on knowledge from neighbours called historical trust and also by the direct trust obtained from the transactions. However, temporal constraints are additionally considered in this work to improve the accuracy of the trust values.

Direct trust of the node is calculated by using the information retrieved from the neighbour nodes is computed using equation via utilizing two neighbour entities' historical interaction information.  $Stn(i, j)$  means node  $i$  make a satisfactory mode of node  $j$  and the value must be between 0 and 1. It also includes the past score  $P_{ij}$ .

$$DT_{ij}^{tn} = \frac{\sum_{m=0}^{tn} S_m(i, j)}{N} + P_{ij} \tag{1}$$

$DT_{ij}$  is the direct trust evaluated by node  $i$  for node  $j$ .  $N$  is the number of interaction between node  $i$  and node  $j$  and  $tn$  is the  $n^{th}$  time interval.

The recommended trust value  $RT$  is evaluate using the recommendation value of each node in the path  $RC$  and direct trust value of the node  $DT$ . For example,  $j$  is the neighbouring node for node  $i$ , then the trust value for  $j$  is evaluated by applying the recommendation given by  $i$ .

$$RT_{irj} = RC_{ir} + DT_{rj} \tag{2}$$

$RC_{it}$  is represented as the recommending path as given in Eq. (3) by applying the direct value of all nodes  $DT$ .

$$RC_{it} = DT_{i1} \times DT_{12} \times DT_{23} \times \dots \dots \times DT_{(r-1)r} \tag{3}$$

Assuming there are  $n$  recommending nodes. Using these trust attenuation rules, it is possible to get  $n$  recommendation trust values:  $RT_{iP1j}, RT_{iP2j}, \dots, RT_{iPnj}$ . Then node  $i$  can computes the recommendation trust  $RT_{ij}$  for node  $j$  using Eq. (4).

$$RT_{ij} = \sum_{k=1}^n RT_{ipkj} \tag{4}$$

Finally, node  $i$  make a synthesis of the evaluated node  $j$ 's historical trust value via Eq. (5) for the time  $t$  in the time interval  $[t_1, t_2]$

$$HTV_{ij} = \alpha DT_{ij}(t) + \beta RJ_{ij}(t) \quad t_1 \leq t \leq t_2 \tag{5}$$

From Eq. (5), it is observed that the historical trust value  $HTV$  is evaluated using direct trust between the source and destination node. In this  $\alpha$  and  $\beta$  are the co-efficient which combined and considered as 1. The weights  $\alpha$  and  $\beta$  are assigned to  $DT_{ij}$  and  $RT_{ij}$  respectively.

The trust score is evaluated for individual node based on the following two constraints. First one evaluates the nodes which perfectly send their acknowledgement to neighbors whenever they receive the packets. Second one is evaluating the Nodes which are dropped the packets more.

$$ITV_i = (ACK/RP) \tag{6}$$

where

- ITV<sub>i</sub> = Trust value of node i
- ACK = No. of acknowledgements sent to the neighbours
- RP = No. of packets received from neighbours

Finally, the overall trust score of the particular node is calculated by using the equation.

$$TV_{ij} = (ITV_i + HTV_{ij} * 2)/2 \tag{7}$$

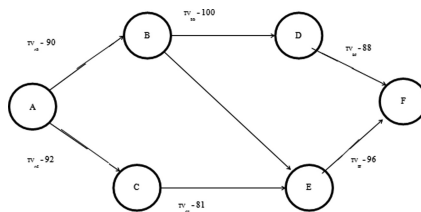
The threshold value is calculated using equation based on the mean value of the overall trust score for all the nodes which is present in the network scenario.

$$TM = \sum TV_i/n \tag{8}$$

**Table 1.** Trust table of node *i*

Node_id	Trust value	Backlist
I	93	0
J	73	0
K	23	1
....	....	....

The threshold value TM is evaluated for the network nodes and also malicious nodes are included in the black list in the trust table as given in Table 1. The node trust value which is lower than the threshold value TM is considered as malicious nodes. Based on the trust value of all nodes, the threshold value TM evaluated as 23 for TV<sub>jk</sub>. Then the node K is thought as malicious node to the node J and it is included as malicious node in trust table. The flag is raised as 1 once the node is included in black list.



**Fig. 2.** Path trust computation

### 3.2 Trust Path Formation

Once the trust value is evaluated based on recommendation of neighbor nodes the path using that trust value is formed as given in Eq. (9).

$$Path\ Trust\ Value: Path\ TV_{sd} = \min \left\{ \begin{array}{c} TV_{nk} \\ s \leq n \leq d - 1 \\ k = n + 1 \end{array} \right\} \quad (9)$$

From the Eq. (9), the trust value for the specific path is calculated between the source node  $s$  and destination node  $d$ . Adjacent node for the path is taken as  $m$  and  $k$ . The graph given in Fig. 2 represents the directed path communication between the node A and B where there is the directed edge is mentioned with the trust value ( $TV(AB) = 90$ ).

And also the overall trust value for  $PathTV(AF) = \min\{TV(AB), TV(BD), TV(DF)\} = \min\{90, 100, 88\} = 88$ ). From Fig. 2, it can be seen that there are different paths are available from A to F. The route trust value is calculated and most trustworthy path is considered for communication (i.e.  $Path\ TV(AF) = 90$ ). The trust value of all intermediate nodes within the path is taken into account for calculating path trust value.

Routing with path trust value is given as procedure as follows.

- Step 1: Prepare route request packet.
- Step 2: Obtain historical trust values.
- Step 3: Perform route discovery
- Step 4: Find the best five routes based on distance and trust values
- Step 5: Check the application.
- Step 6: If it is TCP based use route1 and route2 else use route 3, route 4 and route 5.

## 4 Result and Discussion

The experiments are carried out the set up the simulation environment using NS2. The topology is build by mentioning the mobility of the node and its speed with pause time. The standard AODV is modified by incorporating trust based mechanism and it called as Ad-hoc on demand Trust based Distance Vector (AOTDV) protocol. It also identifies the malicious nodes in the network using this approach.

**Table 2.** Packet delivery ratio analysis

No. of malicious node	Packet delivery ratio (%)	
	AOTDV	AOTMDV
0	100	100
5	85	89
10	60	66
15	58	62
20	56	59

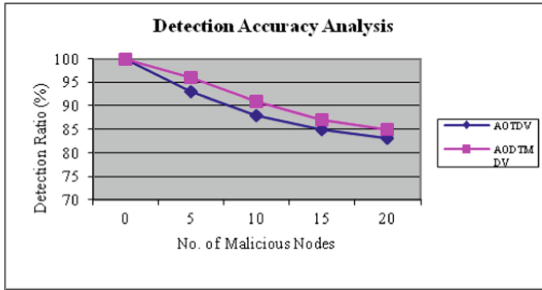


Fig. 3. Detection accuracy analysis

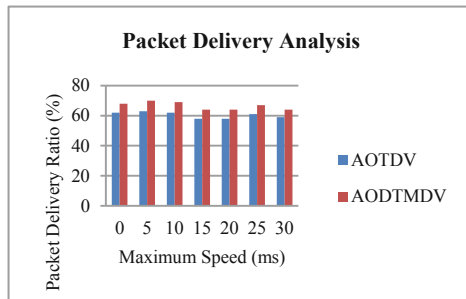


Fig. 4. Packet delivery analysis based on speed

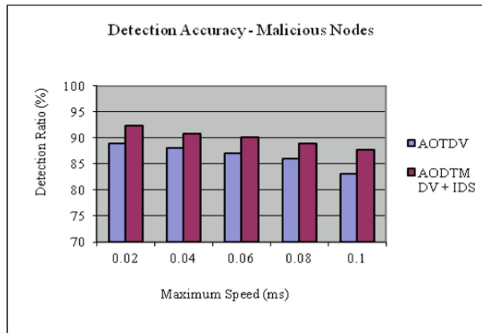


Fig. 5. Performance analysis of AODTV and AODTMDV + IDS

Table 2 shows the performance analysis of proposed AODTMV using packet delivery ratio. The results are shown that proposed approach is far better than existing AODV routing protocol which also explained in chart representation as shown in Fig. 4. And, Fig. 3 shows the pictorial representation of the detection accuracy of proposed AODTMV by comparing with AODTV. The detection accuracy is not only based on the detection of malicious nodes but it also detects the intrusion in the network. Figure 5

shows the overall processing speed of the system in detecting the malicious nodes. It is also observed the proposed AODTMV is performs better than AODTV.

## 5 Conclusion

In this paper, a trust expectation model in view of fleeting requirements has been proposed for MANETs for secure element steering. Trust has been ascertained in view of hubs authentic practices. This model is more steady, versatile and vigorous, and thus improves system's security and execution. Joined with the dynamic trust forecast model, interruption location framework is likewise executed. With these techniques a novel multi-way responsive directing convention Ad-hoc On-interest Dynamic Trusted Multipath Distance Vector Routing (AODTMDV) is utilized to find dependable forward ways and ease the assaults from pernicious hubs in different circumstances. In this convention, a source builds up various dependable ways as possibility to a destination in a solitary course revelation for the specific time. This convention gives an adaptable and plausible way to deal with pick a most limited way in all way competitors. The reproduction results break down the viability of this trust model and the novel trusted directing convention.

## References

1. Li, X., Jia, Z., Zhang, P., Zhang, R., Wang, H.: Trust-based on-demand multipath routing in mobile Ad Hoc networks. *IET Inf. Sec.* **4**(4), 212–232 (2010)
2. Shakshuki, E.M., Kang, N., Sheltami, T.R.: EAACK—a secure intrusion-detection system for MANETs. *IEEE Trans. Ind. Elect.* **60**(3), 1089–1098 (2013)
3. Sun, Y.L., Addada, V.G., Setia, S., Jajodia, S.: Securing MAODV: attacks and countermeasure: In: 2005 Proceedings of IEEE SECON, pp. 521–532 (2005)
4. Liang, Z., Shi, W.: Analysis of ratings on trust inference in open environments. *Els B.V* **65**(2), 99–128 (2007)
5. Chen, A., Xu, G., Yang, Y.: A cluster-based trust model for mobile Ad Hoc networks. In: 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–1 (2008)
6. Selvakumar, K., Sairamesh, L., Kannan, A.: An intelligent energy aware secured algorithm for routing in wireless sensor networks. *Wirel. Pers. Commun.* **96**(3), 4781–4798 (2017)
7. Kamalanathan, S., Lakshmanan, S.R., Arputharaj, K.: Fuzzy-clustering-based intelligent and secured energy-aware routing. In: Handbook of Research on Fuzzy and Rough Set Theory in Organizational Decision Making, pp. 24–37. IGI Global (2017)
8. Ayyasamy, A., Venkatachalapathy, K.: Context aware adaptive fuzzy based QoS routing scheme for streaming services over MANETs. *Wirel. Netw.* **21**(2), 421–430 (2015)
9. Ayyasamy, A., Venkatachalapathy, K.: Performance evaluation of load based channel aware routing in MANETs with reusable path. *Int. J. Eng. Adv. Technol. (IJEAT)* **3**(1), 183–186 (2013)
10. Xia, H., Jia, Z., Ju, L., Zhu, Y.: Trust management model for mobile Ad Hoc network based on analytic hierarchy process and fuzzy theory. *IET Wirel. Sens. Syst.* **1**(4), 248–266 (2011)
11. Xia, H., Jia, Z., Ju, L., Li, X., Sha, E.H.-M.: Impact of trust model on on-demand multi-path routing in mobile Ad Hoc networks. *Els. Comput. Commun.* **36**(9), 1078–1093 (2013)





# A Review on Various Approaches in Video Steganography

S. Raja Ratna<sup>1</sup>(✉), J. B. Shajilin Loret<sup>1</sup>, D. Merlin Gethsy<sup>1</sup>,  
P. Ponnuru Krishnan<sup>2</sup>, and P. Anand Prabu<sup>3</sup>

<sup>1</sup> Department of CSE, V V College of Engineering, Tirunelveli, India  
{rajaratna, shajilin, merlin}@vvcoe.org

<sup>2</sup> Dr. Sivanthi Aditanar College of Engineering, Tirunelveli, India

<sup>3</sup> V V College of Engineering, Tirunelveli, India

**Abstract.** Steganography is the technique in which the secret messages are hidden within the data. It keeps both the data and their existence in a secure manner. It is used in various real time applications and also it enables a secure communication. Text files, images, audios, and videos are used in steganography to conceal the communication. The main objective of this paper is to provide a general analysis on various approaches in video steganography. It covers related works, the strength of steganography, types of steganography and different techniques of video steganography. The absolute study of various techniques of video steganography is also highlighted.

**Keywords:** Communication · Secret · Steganography · Video

## 1 Introduction

Secure communication is useful in many cases to develop an efficient new communication approaches. Plenty of techniques are used for the guaranteed communication of data. Cryptography and steganography are some of the methods used for secure communication.

Cryptography is used to securely transfer sensitive message from intruders. Other than the source and destination nobody can identify the data. By enabling secure communication schemes, intruders cannot read or understand the sensitive messages. Similarly, by using steganography techniques the secret messages are secured and transmitted by hiding it within the data.

Depending on the cover object, data hiding in steganography can be classified into text, image, audio and video steganography respectively.

This paper focuses on video steganography. The paper proceeds as follows. Section 2 describes the types of steganography and Sect. 3 describes the comparative analysis of video steganography techniques. Finally Sect. 4 concludes the paper.

## 2 Types of Steganography

Steganography is the method of covering the secret message into a cover object and prevent that message from intruders. Steganography can be classified as, Text, Image, Audio and Video steganography on the basis of the cover medium.

### 2.1 Text Steganography

In text steganography, inside the text messages, the data to be securely transmitted are hidden and the text is used as a cover medium. The embedded message is recovered by the receiver by applying the previously shared key. Text steganography is one of the techniques, where the sharing of information is through letters and writings. Line-shift coding, word-shift coding, feature coding are some of the text steganography techniques. In text steganography, the meaning of the text is changed by using semantic methods.

### 2.2 Image Steganography

Images are one the most popular cover media for hiding data. The secret message is embedded into the image using pixel intensities. The cover medium in the image steganography is called as vessel or containers. The image after getting the embedded process is called as stegno-image. The data hiding in an image is done by using embedding algorithm. In the transmission channel, the secret message is not predicted by the intruders. Least significant bit, masking, filtering and transformations in the image are the commonly used image steganography techniques for hiding the secret message.

### 2.3 Audio Steganography

Audios are used as a cover object to hide the message in audio steganography. In audio steganography during embedding, the analog audio signal is changed into binary signals and some bits are used to protect the secret message. LSB replacement technique is the most extensively used audio steganography technique for the hiding secret message. It is also called as LSB coding. Another technique for hiding secret message using audio steganography is the spread spectrum technique, where the secret messages are spread across the frequency spectrum of audio signals. The fact used in the audio steganography is that the human ear cannot identify the little changes in the audio signal.

### 2.4 Video Steganography

Video is a cover medium to hide the secret data. The benefit of video steganography is the capacity to hide a large amount of data and the changes in the contiguous flow of data cannot be easily identified. The method of video steganography merges both audio and video strategies. The video is the accumulation of frames [4], and the frame selection is done in the embedding process [12]. The various video steganography

techniques are spatial domain technique [13, 14], transform domain technique [23, 24], cryptography based technique [28, 29] and format based technique.

### 3 Comparative Analysis of Video Steganography Techniques

Videos are the most important media for secure communication of the secret message. The existing video steganography techniques are spatial domain technique, cryptography based technique, and format based technique.

#### 3.1 Spatial Domain Technique

In spatial domain technique, data hiding is directly based on pixel values. The various spatial domain techniques are, Least Significant Bit [4, 5], and Pixel Value Differencing [11–13].

##### 3.1.1 Least Significant Bit (LSB)

LSB is one of the basic techniques for data hiding. It is also an easier technique for secret communication of data in the spatial Domain. LSB plays an important role in the secure transmission. In this technique, image's least significant bit is exchanged by the data bit. Different LSB techniques are listed in Table 1.

##### 3.1.2 Pixel Value Differencing

In pixel value differencing, the numbers of embedding bits are calculated based on the variation between the chosen pixels and its neighbor. This technique provides high embedding capacity. Different pixel value differencing techniques are listed in Table 2.

**Table 1.** Least significant bit

Technique	Description	Advantages	Disadvantages
Tri-way pixel value differencing [11]	All processes are executed in the compressed domain. Some information is embedded into the macro blocks	For good quality video, optimal results are obtained and degradation is reduced	Used only in compressed videos
Enhanced Pixel value differencing (EPVD) [12]	The luminance components are used to enclose the data bits. No modification is done in critical side information	Achieves good video quality	Low bit rate compression because of bandwidth limitation
Pixel Value Differencing [13]	The data hiding technique is based on pixel value differencing and modulus function. Optimal solution is used to revise pixels	Time complexity is reduced High embedding efficiency	Less video quality

**Table 2.** Pixel value differencing

Technique	Description	Advantages	Disadvantages
Frames Decomposition Technique [4]	The additional security is provided for video using password encryption	Achieves high security	This technique does not work if the frame count is less than 255
Back-propagation Neural Network Method [5]	The neural network is trained to perform the XOR operation	The receiver receives the secret message without any modification	AVI format videos are only used to perform the operations

### 3.2 Cryptography Based Techniques

Cryptography based techniques are used to provide added security to the entrenched data. The secret key is used for both encryption and decryption processes [25–28]. Different cryptography techniques are listed in Table 3.

**Table 3.** Cryptography based techniques

Technique	Description	Advantages	Disadvantages
Randomization and parallelization [25]	Feedback shift register is used to embed secret information	Performance is higher	Used only for embedding larger data
Pixel mapping [26]	Information mapped on video file is done very efficiently. Private key provides security	Simple and easy	Information security is low
AES algorithm [27]	The LSB and cryptography are combined to provide secure data transmission	Increases security and provides secure communication	Video quality is poor
Frame selection logic [28]	It is used to embed the secret data in frames	Robust and achieves less computational time	Data hiding capacity is low

### 3.3 Format Based Techniques

Different video formats can be used as a cover object. This technique is used to perform the operations of specific video formats. H.264/AVC, MPEG, and FLV are the different formats [30–32]. Multivariate regression-flexible macro block ordering, Video steganography scheme and Context adaptive variable length coding are some of the format based techniques used for hiding data. Different format based techniques are listed in Table 4.

**Table 4.** Format based techniques

Technique	Description	Advantages	Disadvantages
Multivariate regression flexible macro block [30]	Macro level features are associated using second-order multivariate regression	Embedding capacity is high	Poor robustness
Video steganography scheme [31]	Additional data are stored in FLV file structure. 100% lossless extraction is achieved	Simple and there is no loss in data extraction	Ability to hide one file at a time
Context adaptive variable length coding [32]	The operations are done in $4 \times 4$ residual data blocks	High capacity to store data. Operation speed is high	Used only for flash video formats

## 4 Conclusion

Steganography is one of the most constructive system for secure data communication. It is the technique of covering the data within the data. The paper presents a review of the strength of steganography and various types of steganography. Different video steganography techniques are surveyed and its methodology, advantages, and disadvantages are also discussed.

**Acknowledgement.** This work was supported in part by Anna University recognized research center lab at V V College of Engineering, Tisaiyanvilai, Tamil Nadu, India.

## References

1. Abbass, A., Soleit, E., Ghoniemy, S.: Blind video data hiding using integer wavelet transforms. *J. Ubiquitous Comput. Commun.* **2**, 11–25 (2007)
2. Bansod, S., Mane, V., Raha, R.: Modified BPCS steganography using hybrid cryptography for improving data embedding capacity. In: *IEEE International Conference on Communication, Information & Computing Technology*, pp. 1–6 (2012)
3. Bhattacharyya, S., Sanyal, G.: A novel approach of video steganography using PMM. In: *International Conference on Information Processing*, pp. 644–653. Springer (2012)
4. Bhattacharyya, S., Khan, A., Nandi, A., Dasmalakar, A., Roy, S., Sanyal, G.: Pixel mapping method based bit plane complexity segmentation steganography. In: *IEEE World Congress on Information and Communication Technologies (WICT)*, pp. 36–41 (2011)
5. Chang, P., Chung, K., Chen, J., Lin, C.: A DCT/DST-based error propagation-free data hiding algorithm for HEV intra-coded frames. *J. Vis. Commun. Image Represent.* **25**, 239–253 (2014)
6. Dasgupta, K., Mondal, J.K., Dutta, P.: Optimized video steganography using genetic algorithm. *Int. Conf. Comput. Intell.: Model. Tech. Appl.* **10**, 131–137 (2013)
7. Hu, S.D., Tak, U.K.: A novel video steganography based on non-uniform rectangular partition. In: *IEEE International Conference on Computational Science and Engineering*, pp. 57–61 (2011)

8. Idbeaa, T., Samad, S., Husain, H.: An adaptive compressed video steganography based on pixel-value differencing schemes. In: IEEE International Conference on Advanced Technologies for Communication, pp. 50–55 (2015)
9. Jalab, H., Zaidan, A., Zaidan, B.: Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation. *J. Comput.* **1**, 108–113 (2009)
10. Kapotas, S., Skodras, A.: A new data hiding scheme for scene change detection in H.264 encoded video sequences. In: IEEE International Conference on Multimedia and Expo, pp. 277–280 (2008)
11. Khare, R., Mishra, R., Arya, I.: Video steganography using LSB technique by neural network. In: IEEE International Conference on Computational Intelligence and Communication Network, pp. 898–902 (2014)
12. Kolakalur, A., Kagalidis, I., Vuksanovic, B.: Wavelet based color video steganography. *IACSIT Int. J. Eng. Technol.* **8**, 165–169 (2016)
13. Kumar, S., Yadav, A.K., Gupta, A., Kumar, P.: RGB image steganography on multiple frame video using LSB technique. In: IEEE International Conference on Computer and Computational Sciences, pp. 226–231 (2015)
14. Li, Z., Jiang, J., Xiao, G., Fang, H.: An effective and fast scene change detection algorithm for MPEG compressed videos. In: International Conference on Image Analysis and Recognition, pp. 206–214. Springer (2006)
15. Lin, T., Chung, K., Chang, P., Huang, Y.: An improved DCT-based perturbation scheme for high capacity data hiding in H.264/AVC intra frames. *J. Syst. Softw.* **86**, 604–614 (2013)
16. Ma, X., Li, L., Tu, H., Zhang, B.: A data hiding algorithm for H.264/AVC video streams without intra-frame distortion drift. *IEEE Trans. Circuits Syst. Video Technol.* **20**, 1320–1330 (2010)
17. Mozo, A., Obien, M., Rigor, C., Rayel, D., Chua, K., Tangonan, G.: Video steganography using Flash Video (FLV). In: IEEE Conference on International Instrumentation and Measurement Technology, pp. 822–827 (2009)
18. Mstafa, R., Elleithy, K.: A DCT-based robust video steganographic method using BCH error correcting codes. In: IEEE Conference on Long Island Systems, Applications and Technology, pp. 1–6 (2016)
19. Mstafa, R., Elleithy, K.: A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11). In: IEEE Wireless Telecommunications Symposium (WTS), pp. 1–8 (2015)
20. Mstafa, R., Elleithy, K.: A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes. In: IEEE Conference on Systems, Applications and Technology, pp. 1–7 (2015)
21. Lemos, N., Sonawane, K., Roy, B.: Secure data transmission using video. In: IEEE International Conference on Contemporary Computing, pp. 231–243 (2015)
22. Noda, H., Furuta, T., Niimi, M., Kawaguchi, E.: Application of BPCS steganography to wavelet compressed video. In: IEEE International Conference on Image Processing, vol. 4, pp. 2147–2150 (2004)
23. Reddy, M., Kumar, A.: Secured data transmission using wavelet based steganography and cryptography by using AES algorithm. In: International Conference on Computational Modeling and Security, vol. 85, pp. 62–69. Elsevier (2016)
24. Reddy, M., Kumar, V., Reddy, K.: A practical approach for secured data transmission using wavelet based steganography and cryptography. *Int. J. Comput. Appl.* **67**, 18–23 (2013)
25. Shanableh, T.: Data hiding in MPEG video files using multivariate regression and flexible macro block ordering. *IEEE Trans. Inf. Forensics Secur.* **7**, 455–464 (2012)
26. Sherlyand, A., Amritha, P.: A compressed video steganography using TPVD. *Int. J. Database Manag. Syst.* **2**, 67–80 (2010)

27. Singh, S., Agarwal, G.: Hiding image to video: a new approach of LSB replacement. *Int. J. Eng. Sci. Technol.* **2**, 6999–7003 (2010)
28. Sudeepa, K., Raju, K., Kumar, H., Aithal, G.: A new approach for video steganography based on randomization and parallelization. In: *International Conference on Information Security & Privacy*, vol. 78, pp. 483–490. Elsevier (2015)
29. Tamboli, M., Gulve, A.: Improving security in tri pixel difference value method. *Int. J. Inf. Electron. Eng.* **2**, 505–508 (2012)
30. Thakur, V., Saikia, M.: Hiding secret image in video. In: *IEEE International Conference on Intelligent Systems and Signal Processing*, pp. 150–153 (2013)
31. Zhao, W., Jie, Z., Xin, L., Qiaoyan, W.: Data embedding based on pixel value differencing and modulus function using indeterminate equation. *J. China Univ. Posts Telecommun.* **22**, 95–100 (2015)
32. Thakur, A., Singh, H., Sharda, S.: Secure video steganography based on discrete wavelet transform and arnold transform. *Int. J. Comput. Appl.* **123**, 25–29 (2015)
33. Viral, G., Jain, D., Ravin, S.: A real time approach for secure text transmission using video cryptography. In: *IEEE International Conference on Communication Systems and Network Technologies*, pp. 635–638 (2014)
34. Zhang, Y., Zhang, M., Niu, K., Liu, J.: Video steganography algorithm based on trailing coefficients. In: *IEEE International Conference on Intelligent Networking and Collaborative Systems*, pp. 360–364 (2015)



# Detection of DOM-Based XSS Attack on Web Application

Shubhangi Ninawe<sup>(✉)</sup> and Rakhi Wajgi

Department of Computer Technology,  
Yashwantrao Chavan College of Engineering, Nagpur, Maharashtra, India  
Shubhangininawe@gmail.com

**Abstract.** Cross-Site Scripting (XSS) is one of the huge issues of any Web-based or Online applications. In this attack, the attacker uses malicious code to intercept the information through users web application and sends it to the corresponding web server. This is possible because web browsers are capable of executing the instructions stored in Web pages. This enables the attackers to make use of this feature, so as to execute the malicious code in a user's Web browsing application. This attack if happened, may result in very slow and poor web surfing. It is also capable of stealing the cookies, passwords and other personal information of the user. These kind of attacks are very easy in terms of implementation but the prevention or detection of this attack is a challenging task. In this paper firstly the existing research on the prevention of XSS is presented. Then a framework is proposed to detect the XSS, which can provide a legitimate solution for the mitigation of the attack.

**Keywords:** Cross-Site Scripting · Web application attack · Injection attacks · Network security · Web application protection

## 1 Introduction

The Internet or say World Wide Web (WWW), is global and huge interconnected framework alluding millions of servers, networks, users and administrators. In the initial days of internet, there were only websites developed by static webpages, which was used to display and communicate static information. With the rapid growth in technology, the internet and website also developed promisingly. The website which were used to static one, now turned into the dynamic, progressive and responsive. Now the webpages not only displays the static data but can also communicate the data stored in the remotely situated database and webservers. Today, the dynamic web pages are used for developing web based applications. It helps in actualizing and giving access to online benefits. It is used for winding up genuinely inescapable in a wide range of plans of action and associations. Today, most frameworks, for example, Social Networks, medicinal services, sites, managing an account, or even crisis reaction, are depending on web based applications. Clients can utilize web applications for speaking with different clients by means of texting, for perusing email and for dealing with their photos and different records, for altering and review video or notwithstanding making spreadsheets, introductions, and content archives. Subsequently, the Internet is turning



into an indispensable part our day by day life. So there must incorporate, an expansion instrument to guarantee security for web clients.

The main focus of this study is on the specific type of attack called as Cross-Site Scripting. Because of the advancement to help requests of the developing web, HTML and other web dialects do not have the principled instrument to isolate untrusted information (client substance) from confided in information. the need of a powerful security mechanism on those web applications is an essential concern. Subsequently, there are cross-webpage scripting assaults on web applications. To relieve issue of XSS assaults, XSS barrier is required. There are different XSS resistances classified as appeared in Fig. 1.

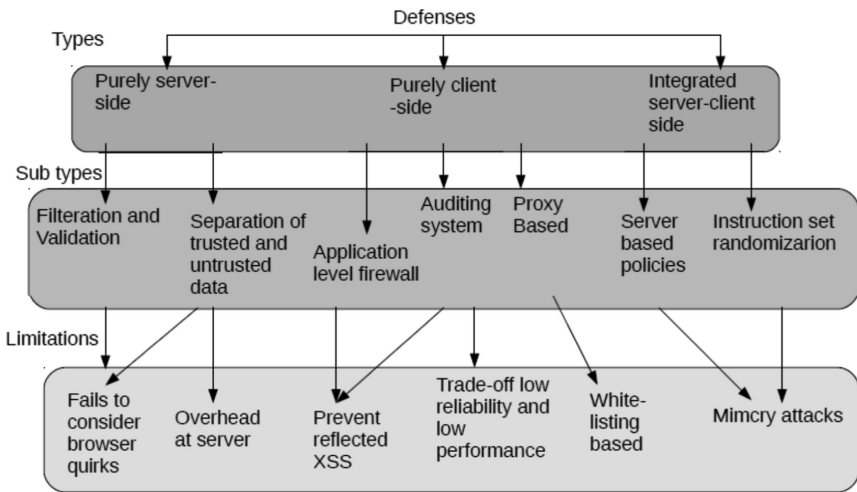


Fig. 1. Types of existing defenses

## 2 Cross-Site Scripting Attack

There are various ways the attacker can attack the website or web application. One of the serious threat is Cross Site Scripting(XSS). Generally, XSS is a technique, where the attacker tries to exploits the loopholes and vulnerabilities present in the source code of the web page. These loopholes allows the attacker to inject the malicious codes or scripts in the source through end-user. The injected codes can collect or hijack the critical, personal or business data of the user. Formally, the XSS can be stated as illegal use of technology for attacking the user. The injected code can be of any scripting language like JavaScript, VBScript, ActiveX, HTML, or Flash. Such scripts can be implemented on webpages with weak security measures for aggregating the confidential information. The XSS attack can lead to compromised security, loss of control over the data. It can make user confused with those of a substantial client, or execute vindictive code on the end-client frameworks. Here the attacker the inserts the malicious code as a normal hyperlink which is communicated over any conceivable

methods on the web. The Cross Site Scripting attack can be categorise in three types as Persistent, Non-Persistent and Document Object Module (DOM) Based Cross Site Scripting.

### 2.1 Persistent XSS Attack

Web Applications with weak approval components for information related to message sheets are generally prone to Persistent XSS Attacks. The chances of this attack are more when the payload is really put away in the site. as in the precedent gave before at whatever point an attacker will enter a remark that it contains a noxious content [4] and it dwells on the web application. Figure 2 shows the sequence of this type of attacks.

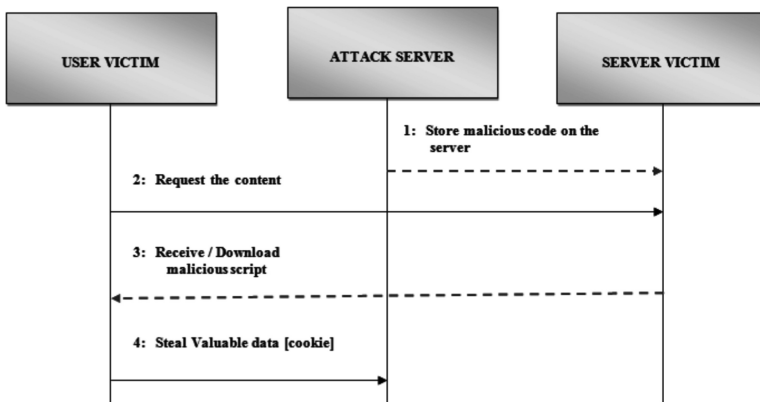


Fig. 2. Persistent cross site scripting attack

The content of the page and malicious code will be executed by the script that heaps the page containing the remark. There is a different event when such a lethal attack is directed by the attackers. For instance, a persistent XSS attack against Hotmail was directed in October 2001. Here the remote attacker was permitted to take .NET Passport identifiers of Hotmail’s clients by gathering their related program’s treats. Also, on October 2005, an outstanding persistent XSS attack which influenced the online informal organization MySpace was used by the worm Samy to engender itself over MySpace’s client profiles.

### 2.2 Non-persistent XSS Attack

The non-persistent XSS attack additionally called as reflected XSS attack, misuses the escape clauses existed in a web application when it uses data given by the client so as to create an active page for that client. The sequence of this type of attack is shown in Fig. 3. As such, and as opposed to putting away the vindictive code installed into a message by the attacker, here the malevolent code itself is specifically reflected back to the client by methods for an outsider instrument. By utilizing a ridiculed email,

for example, the attacker can trap the unfortunate casualty to click a connection which contains the vindictive code. At the point when the injured individual’s program executes the URL [6], the focused on site echoes or reflects back to the client’s program, for the most part, appearing with a blunder message thus.

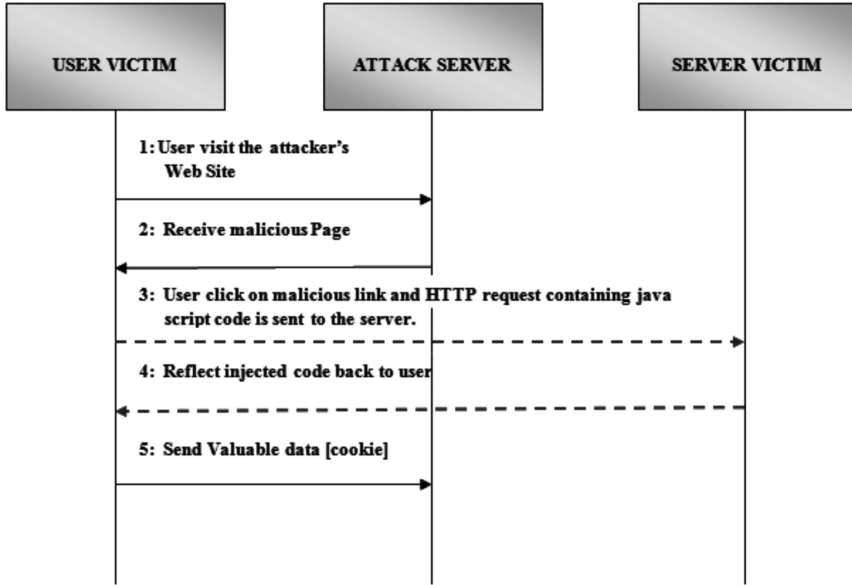


Fig. 3. Non-persistent XSS attacks

Non-persistent XSS attacks are by a wide margin the most well-known kind of XSS attacks against current web applications, and is ordinarily consolidated together with different procedures, for example, phishing and social designing, so as to accomplish its destinations (e.g., take client’s delicate data, for example, charge card numbers). On account of the idea of this variation, i.e., the way that the code isn’t persistently put away into the application’s site and the need of outsider systems, non-persistent XSS attacks are regularly performed by gifted attackers and related to misrepresentation attacks.

### 2.3 Document Object Module(DOM)-Based XSS Attack

To implement this type of attack, the attacker adjust the “condition” for DOM over the side of customer. It is contrary to sending the infected code to the server. The web applications gain the advanced website specialists that can be moved increasingly more of the handling apparatus to the client’s program. At the point when a client associated with a web application, it will be normal for their program to produce a portion of the code that it will be executed and show to the client. In this type of attacks [5], the cyber attackers debase a program’s information or condition so that the created code is vindictive. A program’s informational index or condition, usually considered as a

DOM (Document Object Module). It contains the information that has been given as contribution by the client (for example name, address, secret key, remark field) [4]. The program utilizes the information inside the DOM to create the code and execute in the injured individual’s program. Figure 4 speaks to the grouping of DOM-based attack.

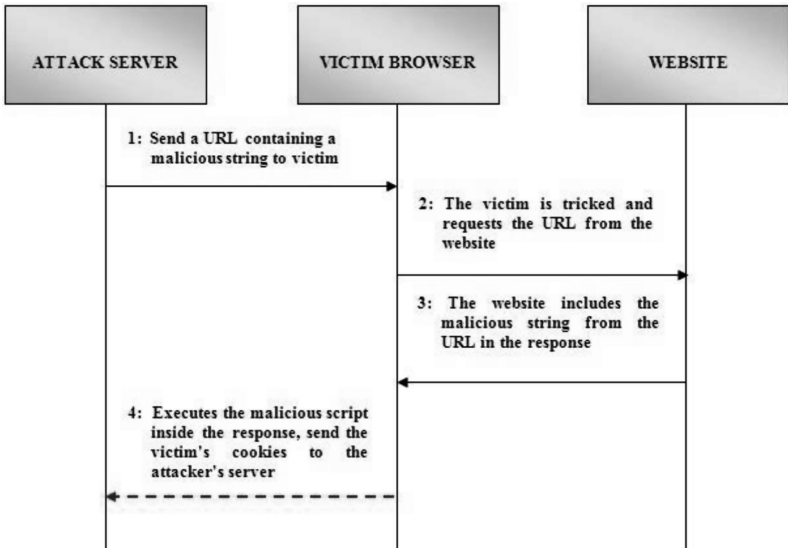


Fig. 4. Document object module based attack

This type of attack, allows the attacker to modify the HTML or XML record. It is possible through the alteration in programmer’s original source script. Thus, the XSS is worked out by utilizing the helplessness of the DOM. The reflected or put away XSS attack is not expected to show such kind of weakness. It does not allow the malignant code to be infused into the page. Similarly, the unreliable DOM object is an issue, which can be deployed by the customer side in the website page or application.

### 3 Related Work

Thought it been long time that XSS attacks are in existence. Still it is one of the most serious threats to web application security [6]. The severity of the thing can be understood by the fact that OWASP [3], which is a famous index of web application vulnerabilities, has listed the XSS attacks in top 10 critical attacks on Web Application Security. According to the Report Statistics of White Hat security 2016 on Web Application Security, nearly half of all web-based exploits are done through XSS attacks. It is unfortunate that we can not get rid of such attack as it is very easy to deploy by the attackers. It is executed by the user’s web browser and many websites are still vulnerable to such attacks. According to the research conducted by Acunetix [12],

more than 33% web applications are still vulnerable to XSS and are easy target to attack. As per the report of Synk [3], which is a provider of vulnerability scanning products, the number is even higher. They report that around 50% of the existing Web Application are prone to XSS.

A solution was designed that uses a genetic algorithm approach to detect and remove the XSS vulnerabilities from the web application [7]. The first component involves in this solution was to convert the source code entered by attacker in the application, to the control flow graph. The second component focuses on detecting the XSS from the user's browser. The third component concentrates on removing the XSS from the URL. This approach combines user experience modeling and user behavior simulation as black-box testing [6, 8–10]. The approach was unable to provide instant web application protection, and they cannot guarantee the detection of all flaws as well.

In another paper [2], SQL and XSS architectures were proposed. They developed an SQL injection and XSS detection method [3] that looks for attack signature by using a filter for the HTTP request sent by the user. In paper [6] fuzzy logic was used for detection of web security and phishing website detection using a rule-based security assurance system. It relies on extracting the exploitation paths of the XSS vulnerabilities of the web application. The works was done to access risks due to different types of code injections vulnerabilities.

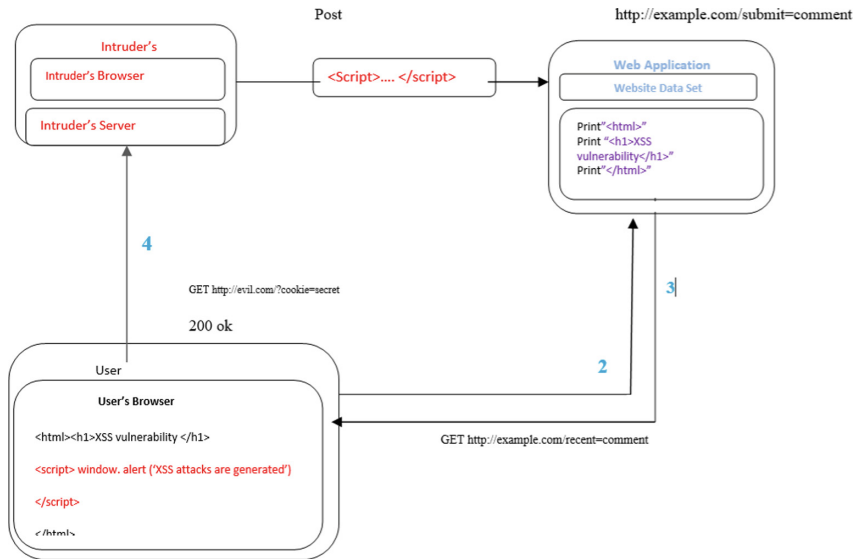
In a paper presented in [2], solution of the learning algorithm that can select a set of attributes from a given data set based on weight by the SVM technique and classify into fuzzy rule based on the processing of the Apriori algorithm was proposed.

## 4 Proposed Model

As it is seen in XSS attack that when an intruder attacks the server side, it brings about corrupting the execution of web application as an outcome, the customer side feels poor web perusing knowledge. XSS is one of the most abused shortcomings in web application and of the most concentrated ones. In this paper, a methodology is proposed for attacking and distinguishing XSS in the web application.

### 4.1 Exploiting XSS Attacks

The misuse of XSS attacks run noxious JavaScript code in the unfortunate casualty's program, an attacker first figures out how to infuse a payload into the internet browser that the injured individual can visit the infused payload [11]. Obviously, an attacker could utilize social designing systems to persuade a client for visiting a helpless page with an infused JavaScript payload in the unfortunate casualty program. An XSS attack happens a defenseless site needs to specifically incorporate client contribution to its pages. At that point, an attacker can embed a string in the URL interface that will be utilized inside the page and treated as code in the injured individual's program.



**Steps of Generating XSS attacks:**

The site database gets infected by the malicious JavaScript code deployed by the attacker.

The web page from the web application where the malicious code is injected receives the requested by victim.

The web page having the malicious code as the part of the HTML body was accessed by the victim's browser.

The victim's individual's program will execute the malicious content inside the HTML body. The attacker currently just need to separate the unfortunate casualty's treat when the Http ask for lands at the server, after which the attacker can utilize the injured individual's stolen treat for infiltrating the internet browser.

**4.2 Detecting the XSS Attacks**

Xenotix framework was used to detect any XSS attack or redirection vulnerabilities that use a maliciously crafted URL link to introduce mischievous data into Web Pages (both statically and dynamically generated). When the data (or a manipulated form of them) passed to one of the subsequent application programming interface (API), the application may be vulnerable to the XSS attacks. We identify all uses of the APIs which may be used to access DOM-based XSS data can be controlled through uniform resource locators (URLs).

**Algorithm 1:** XSS Attack Generation And Detection

- Step1: Create the Web Application For Organization
- Step2: Write the JavaScript on Search Box
- Step3: To Generate The XSS Attack On The Web Browser
- Step4: Configure the server 127.0.0.1 in Xenotix Framework
- Step5: Running the DOM XSS Analyzer
- Step 6: Detection of DOM-Based XSS Attack

Thus, a general approach for detecting XSS vulnerabilities is discussed above and Xenotix Framework is used for attacking and detecting the XSS vulnerability for the web application designed for an organization.

## 5 Conclusion

In this paper, we presented DOM-based XSS attack for detecting the XSS vulnerability in the web application. XSS is a versatile attack which is open for the ethics and Client-side attack. It could be used to steal sensitive information, such as session tokens, user credential or commercially valuable data, as well as to perform the sensitive operation. This method can also be used in websites of net banking, legal official site, online shopping, etc. Here we are focused on penetration test reports, it is a good time to ignore the traditional proof of concept alert box payload as it will be misleading for security stakeholders.

## References

1. Thopate, P., Bamm, P., Kamble, A.: Cross site scripting attack detection & prevention system. *Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET)* **3** (2014)
2. Ayeni, B.K., Sahalu, J.B., Adeyanju, K.R.: Detecting cross-site scripting in web application using fuzzy inference system. *J. Comput. Netw. Commun.* **2018** (2018). Article ID 815948. <https://doi.org/10.1155/2018/8159548>
3. Kaur, D., Kaur, P.: Cross-site scripting attack and their prevention during development. *Int. J. Eng. Dev. Res.* **5**(3) (2017). ISSN 2321-9939
4. Kaur, G.: Study of cross-site scripting attack and their countermeasure. *Int. J. Comput. Appl. Technol. Res.* **3**(10) (2014). ISSN 2319-8656
5. Singh, A., Sthappan, S.: A survey on XSS web-attack and defence mechanism. *Int. J. Adv. Res. Comput. Sci. Softw. Eng. (IJARCSSE)* **4**(3) (2014). ISSN 277-128X
6. Shalini, S., Usha, S.: Prevention of cross-site scripting attacks(XSS) on web application in the client side. *Int. J. Comput. Sci. Issues* **8**(4), 650 (2011)
7. Hydera, I., Sultan, A.B.M., Zulzalil, H., Admodisastro, N.: Cross-site scripting detection based on an enhanced genetic algorithm. *Indian J. Sci. Technol.* **8**(30), 1–7 (2015). <https://doi.org/10.17485/ijst/2015/68130/86055>
8. Avancini, A., Ceccato, M.: Towards security testing with taint analysis and genetic algorithm. In: *Proceedings of the 2010 ICSE Workshops on Software Engineering for secure Systems*, pp. 65–71. ACM, Cape Town (2010)

9. Shar, L.K., Tan, H.B.K.: Automated removal of cross site scripting vulnerabilities in web application. *Inf. Softw. Technol.* **54**(5), 467-478 (2012). <http://linkinghub.elsevier.com/retrieve/pii/S0950584911002503>
10. Shuai, B., Li, M., Li, H., Zhang, Q., Tang, C.: Software vulnerability detection using genetic algorithm and dynamic taint analysis. In: 3rd International Conference on Consumer Electronics, Communication and Network (CECNet), pp. 589–593. IEEE, November 2013. <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6703400>
11. Gupta, S., Sharma, L.: Exploitation of cross-site scripting (XSS) vulnerability on real world web application and its defense. *Int. J. Comput. Appl.* **60**(14), 28–93 (2012)
12. Acunetix vulnerability Scanner. [http://www.acunetix.com/vulnerability\\_scanner](http://www.acunetix.com/vulnerability_scanner)
13. OpenWeb application Security Project. [https://www.owasp.org/index.php/Top\\_10](https://www.owasp.org/index.php/Top_10)
14. Tang, Z., Zhu, H., Cao, Z., Zhao, S.: L-WMxD: lexical based webmail XSS discover. In: IEEE Conference on Computer Communication Workshops (INFOCOM WKSHPs), pp. 976–981 (2011)





# A Review on Clustering Algorithms in Wireless Sensor Networks for Optimal Energy Utilisation

Bhagyashri Julme<sup>(✉)</sup> and Pragati Patil

Department of Computer Science and Engineering,  
Abha-Gaikwad Patil College of Engineering, Nagpur, Maharashtra, India  
bhagyashrijulme70@gmail.com

**Abstract.** Wireless sensor networks (WSNs) is a structure whose construction and design typically consist of the distributed sensor nodes. This type of networks is applicable to variety of domains. The application of WSN consists of Military and security forces, disaster management, health monitoring, agriculture and irrigation sector, etc. The biggest hurdle that comes across in WSN is its intrinsic nature of limited power. It is the most challenging thing which affects the lifetime of the sensor network. That is the main reason due to which there is a need to develop the systems for saving the power utilization in WSN. For optimal use of the power in WSN so as to improvise the network lifetime data transfer path are selected in such a way that the total energy requirement for transferring the data along the path is minimized. Cluster-Based data aggregation in WSN is one such way that plays a vital role in minimizing energy consumption. In the clustering, the cluster heads are selected that gathers data from sensor nodes. This process is called as data aggregation. The aggregated data is then transferred to the base station. Using this way the sensor nodes overhead of transferring the data to BS will be reduced, thus reducing the energy consumption of the network. In this paper, we present the various existing researches conducted for minimum energy utilization and improvising network lifetime. Wireless sensor networks (WSNs) is a structure whose construction and design consist of the distributed sensor nodes. This type of networks is applicable to a variety of domain. The application of WSN consists of Military and security forces, disaster management, health monitoring, agriculture and irrigation sector, etc. The biggest hurdle that comes across in WSN is its intrinsic nature of limited power. It is the most challenging thing which affects the lifetime of the sensor network. That is the main reason due to which there is a need to develop the systems for saving the power utilization in WSN. For optimal use of the power in WSN so as to improvise the network lifetime data transfer path are selected in such a way that the total energy requirement for transferring the data along the path is minimized. Cluster-Based data aggregation in WSN is one such way that plays a vital role in minimizing energy consumption. In the clustering, the cluster heads are selected that gathers data from sensor nodes. This process is called as data aggregation. The aggregated data is then transferred to the base station. Using this way the sensor nodes overhead of transferring the data to BS will be reduced, thus reducing the energy consumption of the network. In this paper, we present the various existing researches conducted for minimum energy utilization and improvising network lifetime.

**Keywords:** Data aggregation · Clustering · Energy consumption · Network lifetime · Wireless Sensor Network

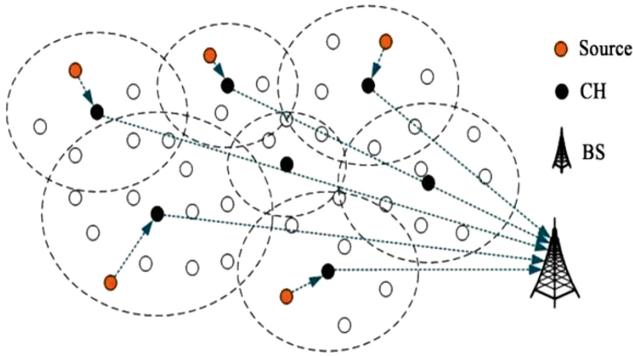
## 1 Introduction

Recently, the Wireless Sensor Network (WSN) technologies have been evolved tremendously. It brought the promising chances of implementing this technology for various application. WSN can have various application in commercial as well as non-commercial sectors such as health care monitoring, agriculture, smart home automation, military and security. A WSN is distributed structure designed by number of sensors. This sensor can have variety of task like collecting the data, transmitting the data, real-time data monitoring or resource monitoring. It can also be used for environmental condition monitoring. WSN is an organized structure of sensor nodes which senses the data and transmitted it to Base Station. In the implementation of such networks, sometimes the sensors needs to be deployed in a far distant and inaccessible area due to which the power source for such sensor have to be a portable batteries. This batteries have a very limited power capacity and once it is deployed it cannot be charged again. While processing, transmitting and receiving the data, these sensor nodes consume energy. Now due to the low capacity of the power source and high utilization of the energy by the sensor nodes the biggest challenge in WSN is the optimal and efficient utilization of the energy so as to improvise the lifetime of the network.

Lack of optimal energy utilization is one of the greatest limitations of the wireless sensor nodes. Numerous analysts are working in energy effective sensor nodes, advancement of energy proficient system convention and topology. Power is devoured by a sensor hub to detect preparing and to transmit information. Information transmission is the most energy expending activities. Presentation of clustering approach in the WSN information transmission will diminish the energy utilization.

There are various techniques for data routing in which the most energy efficient routing algorithm is cluster routing. In this, the entire network of sensor nodes is divided into the number of group of sensors called as clusters. In each cluster, one sensor node is elected as the cluster head. This cluster head is a simple sensor node just like other nodes of the cluster but it has a special responsibility of gathering the data from all the other nodes of the cluster. This process of collection of data from the nodes is called a data aggregation. The cluster head aggregates the data and transmit it to the base station. If only the cluster head is communicating the data to the base station, it is obvious that the overheads on the sensor nodes that can occur if all the nodes in the cluster needs to communicate with the base station would be reduced.

It is very much true that use of cluster based routing can reduce the energy consumption of the network, but there are many issues related to the clustering. The main issue is that the entire burden of transmission is on CH only. The implementation of cluster-based routing is energy efficient only if the selection of cluster head is proper. Thus the proper selection of cluster head becomes the most important aspect of cluster based routing. Usually the CH are elected from one of the sensor nodes deployed where this network is homogenous in nature [1, 2] (Fig. 1).



**Fig. 1.** Basic architecture for wireless sensor network

The distance from base station and region of communication are also among the major concerns that plays crucial role while implementing the clustering in WSN. Another important aspect of clustering is the transmission of data between the CH and the BS. If the transmission is not direct between BS and CH than multihop routing is required. This generates the importance of inter-cluster head connectivity. And also the cluster head should not be exhausted unnecessarily which may otherwise lead to unnecessary loss of energy of cluster head nodes [3, 4].

In this paper the review on various research conducted by the research community for minimizing the energy utilisation of the system is presented. We discuss about the most promising and widely used approaches for the formation of cluster-based routing. In the end we present our conclusion from the study.

## 2 Literature Survey

Here in this paper [5] the authors presents a protocol for cluster-based WSN which is a Low Energy Adaptive Clustering Hierarchy or LEACH. In this clustering algorithm the cluster heads are selected in rounds. It is an energy efficient adaptive algorithm where the clustering nodes are grouped on the basis signal quality and the local cluster heads are used as routers to the SINK. In this scheme all the sensor nodes in the cluster takes part in the data transmission in turns by rotating the cluster head. This is because the transmission of data from head to base station utilises the maximum energy. This type of balanced arrangement leads to the proper and equal energy utilization of all nodes. This eventually leads to the extended lifetime of the network.

Hybrid Energy Efficient and Distributed proposed in [6] is a conveyed cluster convention. A vital element of HEED convention is it to misuse the accessibility of different transmission control levels at sensor nodes. The HEED ends in a consistent number of cycles that is autonomous of networks distance across. It just accepts the sensor nodes can control their transmission control level and not think about the dispersion of nodes or about hub capacities. There are four basic goals as pursues: (1) expanding system life expectancy, (2) unflinching number of emphasis, (3) diminishing control overhead, (4) creating all around dispersed CHs and smaller clusters. Notice pick a CHs based on a cross breed of two clustering parameters. The essential

parameter is utilized to pick an underlying arrangement of CHs while the auxiliary parameter is utilized for breaking ties CHs.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS) [2] is a close ideal chain-based convention. It is utilized to build the system lifetime of every hub by utilizing communitarian methods. This permits just neighborhood coordination among nodes and the data transmission expended in correspondence is decreased. In PEGASIS, every hub discusses just with a neighbor and alternates transmitting to the BS. In sensor networks, is utilized to diminish the measure of information transmitted between sensor nodes and the BS. Information union consolidates at least one information bundles from various sensor estimations to deliver a solitary parcel. The thought in PEGASIS is to shape a chain among the sensor nodes with the goal that every hub will get from and transmit to a nearby neighbor. Assembled information moves from hub to hub, get combined, and in the long run, an assigned hub transmits to the BS.

In [7], two different parameters are contemplated in the clustering model and are considered amid the clustering venture notwithstanding the energy utilization and the separation to the BS. These parameters, named reachability and Link Quality Indicator (LQI) are utilized to play out the CHs determination. The principal parameter speaks to the reachability of the hub, with  $N$  is the number of neighbors of the hub  $I$  and  $d_{ij}$  is the separation between hub  $I$  and hub  $j$ . The second parameter is LQI which describes the quality gathering of a bundle at a hub.

In [8] and [9] the proposed calculations partition the surface into districts of the equivalent region that will be considered as clusters. Nodes arranged in a similar zone are allocated to a similar cluster and will take as CH the closest hub arranged at the focal point of the zone. For this situation, the number of individuals in the clusters can show an extensive variety.

Stanislava Soro et al. [10] propose an Unequal Clustering Size (UCS) display for two-layer sensor arrange which the BS is situated in the focal point of the watched zone, UCS can prompt progressively uniform energy dissemination among the cluster head nodes, in this way expanding system lifetime.

The creators in [11] propose an energy proficient uneven clustering calculation for system topology association, in which speculative cluster heads utilize uneven challenge reaches to construct clusters of uneven sizes. The calculation proposed in this paper is like EECS.

In [12], a separation based cluster arrangement technique is proposed to create clusters of unequal size in single-hop networks. A weighted capacity is acquainted with let clusters more distant far from the BS have littler sizes, in this way some energy could be protected for long-separate information transmission to the BS. In this paper, we have broken down nodes energy utilization to acquire the ideal correspondences sweep of nodes and ideal cluster measure.

### 3 Conclusion

As we discussed reduction in energy utilisation is the most crucial factor in improving the network lifetime. Clustering is a method which truly helps in reducing the power consumption. Various systems based on location, residual energy, average energy,

density, etc are also presented recently. Designing a routing protocol which should be effective, scalable and reliable for WSNs is the most challenging task. Thus there is a significant study on the development of the energy efficient system for WSNs. In this paper we presented the survey of some of the reliable clustering algorithms in wireless sensor networks. The LEACH and other important protocols for WSNs reported till date are presented.

## References

1. Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H.: Application specific protocol architecture for wireless microsensor networks. *IEEE Trans. Wirel. Commun.* **1**(4), 660–670 (2002)
2. Lindsey, S., Raghavendra, C.S.: PEGASIS: power efficient gathering in sensor information system. In: *Proceedings of IEEE Aerospace Conference*, vol.3, pp. 1125–1130, March 2002
3. Banerjee, S., Khuller, S.: A clustering scheme for hierarchical control in multihop wireless networks. In: *Proceedings of 20th Annual Joint Conference of the IEEE Computer & Communications Societies (INFOCOM 2001)*, vol.2, pp. 1028–1037, April 2001
4. Bandyopadhyay, S., Coyle, E.J.: An energy efficient hierarchical clustering algorithm for wireless sensor networks. In: *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications IEEE Societies (INFOCOM 2003)*, vol.3, pp. 1713–1723, April 2003
5. Singh, A., Rathkanthiwar, S., Kakde, S.: LEACH based-energy efficient routing protocol for wireless sensor networks. In: *Proceeding of International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT-2016)* (2016)
6. Younis, O., Fahmy, S.: HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Trans. Mob. Comput.* **3**(4), 366–379 (2004)
7. Pah Pahwa, P., Virmani, D., Kumar, A., Rathi, V., Swami, S.: Dynamic cluster head selection using fuzzy logic on cloud in wireless sensor networks. *arXiv preprint arXiv:1601.03810* (2015)
8. Banerjee, B.I., Datta, B., Kumari, A., Mandal, S.: Compact clustering based geometric tour planning for mobile data gathering mechanism in wireless sensor network. In: *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 2098–2104. IEEE, September 2014
9. Zhou, Z., Du, C., Shu, L., Hancke, G., Niu, J., Ning, H.: An energy-balanced heuristic for mobile sink scheduling in hybrid WSNs. *IEEE Trans. Ind. Inform.* **12**(1), 28–40 (2016)
10. Soro, S., Heinzelman, W.B.: Prolonging the lifetime of wireless sensor networks via unequal clustering. In: *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, pp. 236–240 (2005)
11. Li, C.F., Ye, M., Chen, G.H., Li, C.F., Ye, M., Chen, G.H., et al.: An uneven cluster-based routing protocol for wireless sensor networks. *Chin. J. Comput.* **30**(1), 27–36 (2007). (in Chinese)
12. Ye, M., Li, C.F., Chen, G.H., Wu, J.: EECS: an energy efficient clustering scheme in wireless sensor networks. In: *Proceedings of IEEE International Performance Computing and Communications Conference (IPCCC)*, pp. 535–540 (2005)



# Error Performance Analysis of RF Subcarrier Adjusted FSO Communication Framework over Robust Environmental Disturbance

Bobby Barua<sup>1</sup>(✉) and Satya Prasad Majumder<sup>2</sup>

<sup>1</sup> Ahsanullah University of Science and Technology, Dhaka, Bangladesh  
bobby@aust.com

<sup>2</sup> Bangladesh University of Engineering and Technology, Dhaka, Bangladesh  
spmajumder@eee.buet.ac.bd

**Abstract.** RF subcarrier tweak in FSO correspondence framework end up well known step by step because of the enhancement in the framework execution, which are for the most part affected by the robust environmental disturbance due to turbulence. In this paper, we infer error execution limits for RF subcarrier adjusted FSO correspondence frameworks with synchronous RF demodulator working over solid environmental disturbance channel which is demonstrated by gamma-gamma. Execution results are assessed as far as normal CNR, BER and penalty of power endured by the framework because of turbulence impacts.

**Keywords:** Amplitude shift keying (ASK) modulation · Atmospheric turbulence channel · Error performance analysis · Free-space optical communication · Gamma-gamma model

## 1 Introduction

Remote optical correspondences, also called free space optical (FSO) interchanges the media transmission innovation that utilization light wave to pass data in between the two ends. FSO is the costeffective and high transmission capacity get to system, which is getting developing consideration with late commercialization victories [1]. With a possible high data rate limit, with minimal effort in unnecessary spectrum and especially broad band width the FSO correspondence is an alluring answer to the “last mile” problem to overcome any problems between the last client and fiber optics infrastructures [2]. Its extraordinary features suppress additional features for various applications, including expanding metropolitan territory systems, undertaking/neighborhood connectivity, fiber backup, back-haul for remote cell systems, excess connection and catastrophe recuperation [3]. Then again this regularly developing interest of increment in information and interactive media administrations has prompted blockage in routinely utilized radio recurrence (RF) range and emerges a need to move from RF bearer to optical transporter [4–7].

As it may be, the actual disability of the FSO correspondence is due to air disturbances, due to the diversity of the overwhelming file due to temperature and weight fluctuation due to abnormalities. As a result of the Flu Options in Flash Blanching,

the climate problem is known as flash blurring, otherwise the optical letter is called freelancing [9], highly polluting the connection performance, especially on the distance of 1 km or more links. In some articles of high hypothesis [4, 10, 11], Andrews et.al demonstrates modified Ryotov Hypothesis and gamma-gamma pdf is proposed as a tractable numerical model for barometric disruption. The gamma-gamma PDF can be easily identified with a barometric condition and provides a suitable financing for the test results. Again various disturbance relief strategies for FSO systems have been proposed, for example, vigorous adjustment procedures, decent variety methods, versatile optical innovation and so forth [5–10]. Notwithstanding all, subcarrier regulation ended up well known step by step. Analyses are now focused to create subcarrier adjusted FSO correspondence framework for the enhancement of FSO framework. So it is extremely hard to comprehend the viability of every parameter of the FSO connect from the PC reproduction work. So inquire about work is started to discover execution results scientifically.

In this article, we will examine error performance execution of optical link through air joins working over robust environmental turbulent paths, where the disturbance incited blurring is depicted by the gamma-gamma dispersion with ASK adjustment design. What’s more, the execution results are assessed in terms of CNR, BER and power penalty suffered by the choppiness impact.

## 2 System Model

Figure 1 demonstrates the block graph of the RF subcarrier adjusted FSO correspondence framework with intelligible beneficiary. Each info information originally adjusted in ASK adjuster. The yields of the adjusters are joined utilizing RF mixer. The RF regulated flag at that point are forwarded to the optical signal adjuster where electro optic balance happens with the yield of the laser. At that point the EOIM flag transmitted through air tempestuous channel. At the less than desirable end the optical flag is gotten by a photodetector and the yield photograph finder current is intensified by pre-amplifying device. The yield of the pre-amplifying device is the joined RF flag that is distributed by a RF pass band channel to decrease the impact of the commotion due to preamplifier and photo identifier. The ideal RF subcarrier is then demodulated by a synchronous RF demodulator to get the information data.

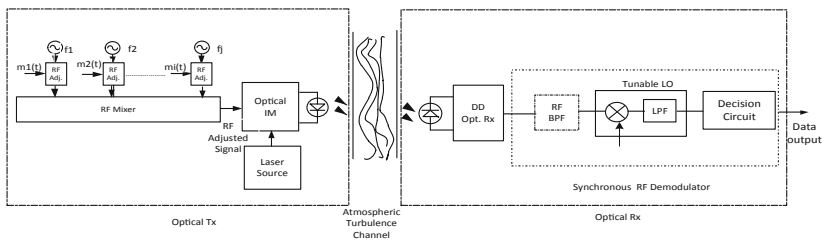


Fig. 1. Structure of RF subcarrier

The unwavering quality of the correspondence connection can be resolved in the event that we utilize a decent probabilistic model for the choppiness. Notwithstanding the way that log-normal movement is the most for the most part used model for the probability density function (pdf) of the irradiance in view of its straightforwardness, this pdf show is only applicable to delicate unsettling influence conditions [9].

### 3 Atmospheric Turbulence Model

As the quality of choppiness builds, various dissipating impacts must be considered. In such cases, log-ordinary insights display substantial deviations contrasted with test information [4]. Furthermore, it has been seen that log-normal pdf thinks little of the conduct in the tails as contrasted and estimation results. Since location and blur probabilities are essentially founded on the pdf tails, disparaging the district sufficiently great influences the accuracy of execution investigation. Because of the confinements of log-normal model, numerous measurable models have been proposed. Al-Habash et al. [11] has proposed a measurable model that affects the immunity of gamma-gamma PDF every spontaneous deliberate methods. The PDF of the force variance is given by [11]:

$$p(i) = \frac{2(ab)^{(a+b)/2}}{\gamma(a)\gamma(b)} i^{\frac{(a+b)}{2}-1} K_{(a-b)}(2\sqrt{abi}), i > 0 \tag{1}$$

$i$  is the flag force,  $\Gamma(\cdot)$  is the gamma function and  $K_{(a-b)}$  is the second order modified Bessel function of  $\mathbf{ab}$  where  $\mathbf{a}$  and  $\mathbf{b}$  are the PDF elements experienced shine illustration through plane ripples and on account of zero-inward plane are given by [11]:

$$a = \frac{1}{\exp\left[\frac{0.49 n_r^2}{(1 + 1.11 n_r^{12/5})^{7/6}}\right] - 1} \tag{2}$$

$$b = \frac{1}{\exp\left[\frac{0.51 n_r^2}{(1 + 0.69 n_r^{12/5})^{5/6}}\right] - 1} \tag{3}$$

and

$$n_r^2 = 1.23 C_n^2 n^{7/6} L^{11/6} \tag{4}$$

where  $n_r^2$  where Ryotov Change  $C_n^2$  is the Refractive list structure Parameter,  $\mathbf{n}$  speaks the number of the wave which is  $2\pi/\lambda$  and  $\lambda$  represents the working wave length and  $\mathbf{L}$  speaks to the Proliferation separate.



### 4 Theoretical Analysis of the System

Let  $d_i(t)$  is the info flag that will be forwarded utilizing  $j$  subcarrier, where  $m_i(t)$  is given by:

$$d_i(t) = \sum_k^{\infty} a_k^i p(t - kT_b) \tag{5}$$

Where  $T_b$  is the bit time frame,  $p(t)$  beat state of a bit,  $a_k$  is the  $k$ -th bit adequacy.  $f_j$  is the  $j$ -th subcarrier recurrence tweaked by an information series  $d_i(t)$  and combined. The yield in electrical field is given by:

$$e_{sc}^i(t) = \sum_{i=1}^l \sum_k^{\infty} a_k^i p(t - kT_b) . A_{sc_i} \cos \omega_{sc}^i t \tag{6}$$

The yield of the optical adjuster is given by:

$$e_{opt}(t) = \sqrt{2P_T} [1 + m_a . A_{sc}(t)] e^{j\omega_c t} \tag{7}$$

where  $P_T$  speaks to the forwarded power of the laser and  $m_a$  is the force adjustment list. Presently the adjusted flag is then forwarded through the optical wireless channel. The got flag at the beneficiary can be expressed as:

$$e_r(t) = \sqrt{2P(t)} [1 + k_a . A_{sc}(t)] e^{j\omega_c t} + n_b(t) \tag{8}$$

In the equation  $P = P_R i(t)$ ,  $P_R$  is the gotten power equivalent to  $P_T e^{g_L}$ ,  $g$  is the constriction coefficient of the climatic channel  $L$  speaks to the connection remove,  $n_b$  is the foundation commotion and  $i$  speaks to the choppiness prompted blurring. The photo detector current,  $i_D$  is given by:

$$\begin{aligned} i_D(t) &= R_D |e_r(t)|^2 \\ &= 2R_D P(t) + 2R_D P(t) \times m_a . A_{sc}(t) + 2R_D P(t) \times (m_a . A_{sc}(t))^2 \end{aligned} \tag{9}$$

where  $R_D$  is the photodetector responsivity. Considering the given estimation of  $i(t) = i$ , the RF transporter control at the yield of the BPF is given by:

$$C(i) = \frac{(2 R_D P_R i m_a A_{sc})^2}{2} \tag{10}$$

The commotion control at the yield of the band cruise channel is given by:

$$\begin{aligned} \sigma_n^2 &= \sigma_{sh}^2 + \sigma_{th}^2 \\ &= 2qB [R_d P_R i \times m_a . A_{sc}(t)] + \frac{4kT}{R_L} B \end{aligned} \tag{11}$$

where the band width of the BPF is given by  $\mathbf{B}$ ,  $\sigma_{sh}^2$  is the shot commotion difference,  $\sigma_{ih}^2$  is the warm clamor change. Presently the Bearer to Commotion Power Proportion adapted on a given choppiness actuated blurring  $i$  can be communicated as:

$$CNR(i) = \frac{\frac{(2R_D P_{Rim_a} e_{sc}(t))^2}{2}}{2qB[R_D P(t) \times m_a \cdot e_{sc}(t)] + \frac{4kT}{R_L} B} \tag{12}$$

So, the BER conditioned can be expressed as:

$$BER(i) = \frac{1}{2} \operatorname{erfc} \left[ \frac{\sqrt{CNR(i)}}{2\sqrt{2}} \right] \tag{13}$$

Finally, the average value of BER is given by:

$$BER = \int BER(i) \cdot p(i) di \tag{14}$$

where  $p(i)$  represents PDF of disturbance due to turbulence.

### 5 Results and Discussion

This part the unmistakable execution evaluation impacts that have been acquired with the guide of numerically studying the legitimate verbalizations affirmed in Fragments III and IV, we analyze the bit botch value execution final product the use of Matlab. The parameters details are provided in table below.

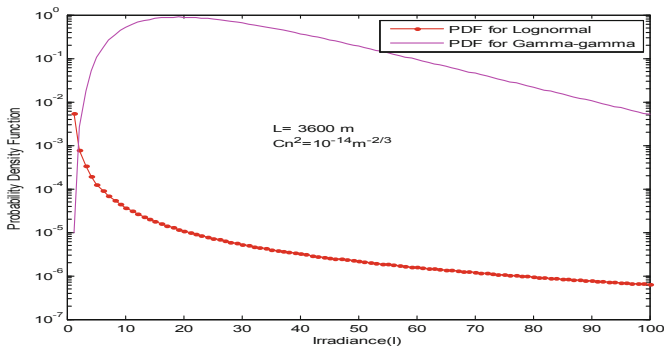
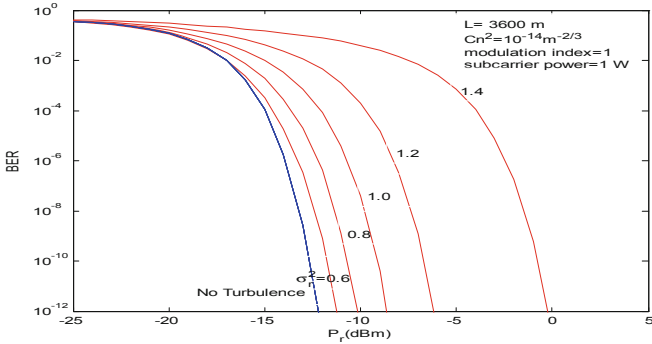


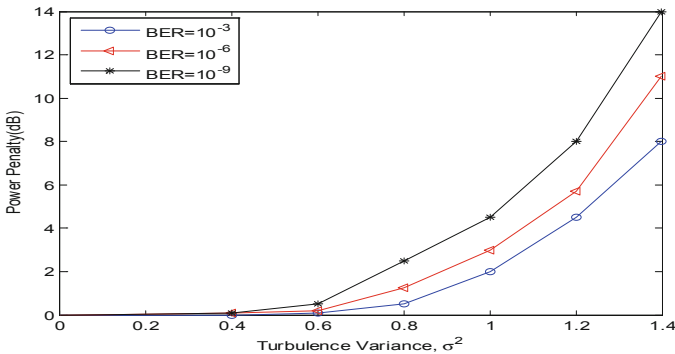
Fig. 2. Graphical representations of PDF for both lognormal and gamma-gamma representation.

The plots of the likelihood thickness work under lognormal and gamma-gamma display with common estimation of sparkle file and disturbance quality is appeared in Fig. 2.



**Fig. 3.** BER performance evaluation with respect to the received optical power under the influence of environmental turbulence strength.

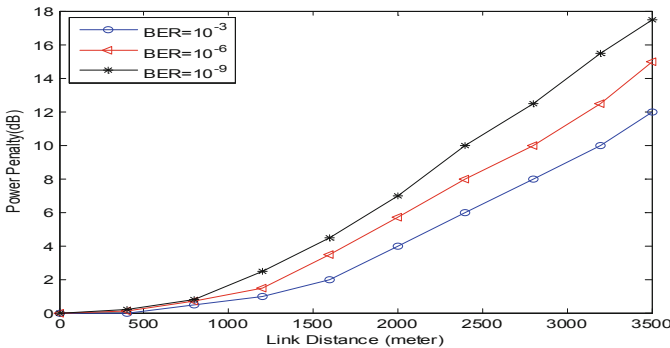
Figure 3 demonstrates the graphical representation of BER versus optical got control with disturbance fluctuation as parameter. It is seen that the framework execution debase because of the impact of air choppiness. At higher fluctuation, the required optical power is more at a given information rate.



**Fig. 4.** Power penalty versus turbulence variance under different BER conditions.

Presently the impact of disturbance can be gotten by plotting the blurring difference against the power penalty and the graphical representations are appeared in Fig. 4. The penalty in power speaks to the addition in got capacity to accomplish an ideal error performance in a choppiness channel contrasted with the perfect path. It is additionally seen that for same choppiness level the blurring punishment is higher for lower BER.

For instance, when the disturbance change is 1.2 the blurring punishments are  $\sim 8.6$  dB, 5.8 dB and 5.1 dB for BER of  $10^{-9}$ ,  $10^{-6}$  and  $10^{-3}$  separately. Of course, the execution of error weakens as distance increments from 1000 m to 3600 m. Similarly, it's far apparent that a ramification in distance from 2500 m to 3600 m consequences in a more extreme execution weakening than for the scenario where distance increments from 1000 m to 2500 m.



**Fig. 5.** Power penalty observation with respect to the link distance for different condition of BER.

The impact of disturbance is found by presenting the FSO connect separate with respect to the penalty of power are appeared in Fig. 5. The penalty graph speaks to the augmentation in got capacity to accomplish an ideal BER in a disturbance channel. It is additionally seen that for the similar form of connection separate the penalty in power is maximum at lowest BER condition. For instance, when the connection remove is 2000 m the penalty in power are  $\sim 6.3$  dB, 4.9 dB and 3.7 dB for BER of  $10^{-9}$ ,  $10^{-6}$  and  $10^{-3}$  separately.

## 6 Conclusion

We have examined error rate execution of RF subcarrier adjusted optical frameworks based on free space working over environmental disturbance path, which are displayed through gamma-gamma distribution. Not at all like the customarily used log-normal doubt that is correct for showing slight unsettling influence, the gamma-gamma distribution demonstrate works for a grouping of tempestuous conditions. The parameters that are used in this distribution are effectively identified with viable framework parameters, for example, the working recurrence; connect separate, focal point opening giving profitable bits of knowledge into FSO framework execution. Considering this as of late presented channel display, we inferred a BER articulation for RF subcarrier

tweaked FSO joins with Inquire. The outcomes demonstrate that framework endures huge power punishment because of environmental choppiness which is increasingly conspicuous at lower RF adjustment and lower interface separate. Taking the BER at  $10^{-9}$  is a viable execution focus for an optical communication framework through free space where intelligent results may fill in as an essential as well as stable procedure to assess error rate execution without falling back on long reenactments.

## References

1. Sadiku, M.N.O., Musa, S.M.: Free space optical communications: an overview. *Eur. Sci. J.* **12**(9), 55–68 (2016)
2. Khalighi, M.A., Uysal, M.: Survey on free space optical communication: a communication theory perspective. *IEEE Commun. Surv. Tutor.* **16**(4), 2231–2258 (2014)
3. Hranilovic, S.: *Wireless Optical Communication Systems*. Springer, Heidelberg (2005)
4. Samimi, H., Azmi, P.: Performance analysis of adaptive subcarrier intensity-modulated free-space optical systems. *IET Optoelectron.* **5**, 168–174 (2011)
5. Tang, X., Rajbhandari, S., Popoola, W.O., Ghassemlooy, Z., Leitgeb, E., Muhammad, S.S., Kandus, G.: Performance of BPSK subcarrier intensity modulation free-space optical communications using a lognormal atmospheric turbulence model. In: *IEEE Conference*, pp. 17–20 (2010)
6. Popoola, W.O., Ghassemlooy, Z.: BPSK subcarrier intensity modulated free-space optical communications in atmospheric turbulence. *J. Lightwave Technol.* **27**, 967–973 (2009)
7. Popoola, W.O., Ghassemlooy, Z., Allen, J.I.H., Leitgeb, E., Gao, S.: Free-space optical communication employing subcarrier modulation and spatial diversity in atmospheric turbulence channel. *Optoelectron. IET* **2**, 16–23 (2008)
8. Henniger, H., Wilfert, O.: An introduction to free-space optical communications. *J. Radio Eng.* **19**(2), 16–23 (2010)
9. Andrews, L.C., Phillips, R.L., Hopen, C.Y.: *Laser Beam Scintillation with Applications*. SPIE Press (2001)
10. Andrews, L.C., Phillips, R.L., Hopen, C.Y., Al-Habash, M.A.: Theory of optical scintillation. *J. Opt. Soc. Am. A* **16**(6), 1417–1429 (1999)
11. Al-Habash, M.A., Andrews, L.C., Phillips, R.L.: Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media. *Opt. Eng.* **40**(8), 1554–1562 (2001)



# A Method for Identifying Human by Using Gait Cycle

Snehal N. Kathale<sup>1</sup>(✉) and Supriya Solaskar<sup>2</sup>

<sup>1</sup> Computer Engineering, St. Francis Institute of Technology,  
Borivali (W), Mumbai, India  
snehalathale@sfitengg.org

<sup>2</sup> Information Technology, St. Francis Institute of Technology,  
Borivali (W), Mumbai, India  
supriyasolaskar@sfitengg.org

**Abstract.** Biometrics is a term which is used to identify the person by using their body characteristics. This paper describes a method to recognize and identify the persons by their gait cycle. This paper focuses on identifying a human by using neural network which is used to train the dataset. In order to identify an individual, various algorithms are used like background subtraction, frame differencing etc. Human identification is an increasing approach for a security reason and promising technology for military services, banks and colleges. Gait is the new biometric authorization system which does not need to contact any device for authentication. This is the promising research area because it is difficult to hide.

**Keywords:** Gait cycle · Biometrics · Human identification · Neural network

## 1 Introduction

In the era of technology and internet, the need to authenticate and identify individuals is growing at a higher pace. Biometrics method refers to authentication techniques that depend on physical characteristics that can be automatically checked and measurable. Humans have used different body characteristics to recognize each other. Several types of biometric identification schemes are Face, fingerprint, hand, geometry, retina, iris, signature, vein, voice. In this paper gait is the area which is used to identify the person. Generally there are two recognition based techniques namely Model based and appearance based. Approached appearances can affect from appearance changes which can gives the outcome into the change of the walking or viewing directions [1]. Whereas, model-based approach select the moves of the human body from captured frames and fitting their models to the input images [1–4]. Stance phase and swing phase are the two important components of gait.

## 2 Related Work

The given literature review is based on several research papers which includes appearance based & model based methods for gait recognition. Static and dynamic characteristics of a moving person are described using model based approach [19]. Description and analysis of the research is described below:

Modified Independent Component Analysis (MICA) is a capable self-correlational based gait recognition system used for human identification. First, the background technique is completed from a video sequence. Then by using background subtraction algorithm, the moving foreground things from the single image frame are segmented. Subsequently, the morphological skeleton operator of human body is used to track the moving silhouettes frames of a walking figure. After that MICA based on Eigen space transform vectors is trained using the sequence of silhouette images. Lastly, the MICA placed system distinguishes the countenance of gait & there by human beings when a video sequence is fed [1]. An efficient approach to gait recognition is, Identification of a human body depends on principal component analysis (PCA). After that, Eigen space conversion which is based on PCA is applied to time-varying distance vectors. And then Mahalanobis distances-based supervised classifications are performed in the lower dimensional Eigen space for human identification [2] (Fig. 1).

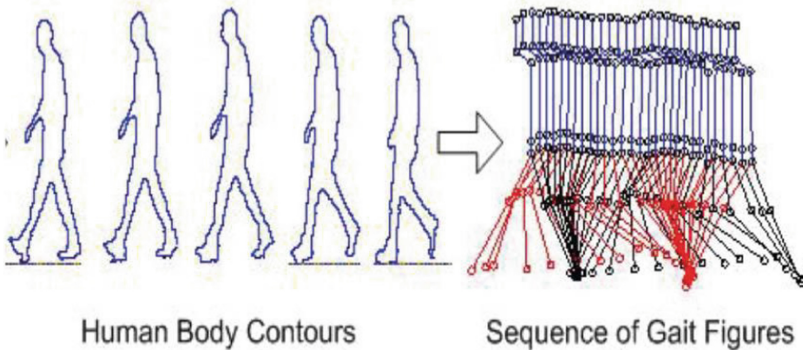


Fig. 1. Gait signature [5]

Kale et al. [17] proposed a view-based approach for identifying persons from their walking style. They have considered two non-identical features: the width of the outer outline of the binary configuration and entire binary shape of a walking person. Direct approach is the second method which is used to train the Hidden Markov Model (HMM) and it works with the extracted values feature vector directly. HMM is basically used for identifying and recognizing the patterns like iris, thumb, handwriting, gesture, speech [7–9].

### 3 Implementation

The following gait recognition system specifies gait in terms of a gait patterns computed directly from the series of silhouettes [10]. The proposed system contains the 3 modules particularly,

- (1) Human Detection (identification) & tracking [10]
- (2) Feature Extraction
- (3) Training & recognition (Fig. 2).

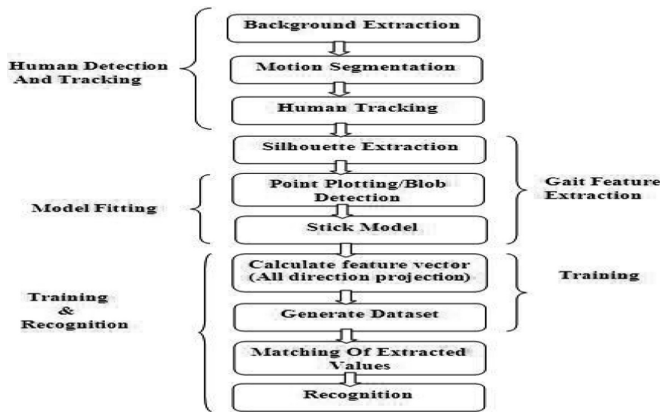


Fig. 2. Block diagram for proposed human gait recognition system

#### 3.1 Human Detection and Tracking

Detecting and tracking a human from video sequence is the initial step for recognition of gait. Here an assumption is that the video sequence is catches by a camera, and the only moving object in video sequence is the subject [10, 21] (Human) for the propose system. Here we put it the box on subject and detect the only human from video. This technique detects and tracks the moving silhouettes of the person. Human detection and tracking process has two sub modules: (1) Foreground Modeling and (2) Human tracking [1].

##### 3.1.1 Background Modeling

In Background subtraction technique, an image’s forepart is extracted for next processing. The objects can be humans, cars, trees, flowers, text etc. in its front. The extensively used idea for identifying moving objects or things from video is Background subtraction algorithm. Background subtraction is usually done for the images where most of the question is a part of a video stream [1, 2, 5].

In visual surveillance the critical task is to extract dynamic things and video sequence objects recorded by utilizing the camera. Background modeling is an approach to this critical task [3, 5].



- (1) **Changes in Light:** The model should adapt to moving changes in light effects as it affects the result.
- (2) **Moving substances in background:** The background model should be vigorous to moving background [3] like rain, trees, waving leaves, waving trees & snow etc.
- (3) **Shadows:** For more accurate detection of rotating and dynamic objects, the model, the shape should comprises the shadow, casting by the moving objects [10, 21].
- (4) **Camouflage:** Revolving & dynamic objects should be noticed even though their vibrant features are alike as of the background model [7, 10, 21].

### 3.1.1.1 Foreground Extraction

After the first module of background subtraction, dynamic objects from the videos must be segmented for next procedures. For modeling background from the captured video a easier motion detection technique which denotes on the values of the median which is used [10]. Let  $A$  denotes a video having  $N$  number of image frame. The background  $A(x, y)$  can be calculated by using the median formula as shown below: [10]

$$A(x, y) = \text{median}[A1(x, y), A2(x, y) \cdots \cdots \cdots A3(x, y)] \quad (1)$$

Where,  $A(x, y)$  represents the framework brightness which calculated in the pixel location  $(x, y)$  whereas median means its median value. Where  $A$  denotes the video sequences with  $N$  number of the frames [10], the original image, extracted background frames are provided for the foreground modeling [1, 7]. In order to effects on changes of clothing and lighting it is acceptable to consider the binary silhouette of the model which can be obtained by the difference in image with a proper threshold value  $T$  [1–3].

The primary assumption made is that, the only dynamic objects in video is the movable and camera is fixed and static [7]. In the next step walking figure is tracked from the extracted binary forepart of image. The stick model function for human tracking is adopted. Skeletization is nothing but the connectivity and degree of the original part of image after removing the unwanted foreground images.

### 3.1.1.2 Frame Differencing

Frame differencing is defined as a difference between two video frames. When the pixels have changed t apparently something was changing in the values or appearance of the image. One of the advantage of frame differencing is the advanced computational load and another is that the background model is mostly robust. The background is based entirely on the staring frame; it can take changes in the background faster than any other method. Its takes the single frame per second [1, 5]. The method used for the observing the different frames in single videos is frame differencing. It is used for calculating the difference from two frames which helps in generating the dataset for training module. All the generated frames calculate their values as compared to previous one. It is easier to remove useless data or images from selected videos by using frame differencing [1, 5, 7].

### 3.1.2 Feature Extraction

Before this process, the binary silhouette to calculate the gait cycle is taken and then the total frames number in single gait is considered [10]. The total time period between two identical frames during the walking is considered as a single gait and is computed from heel stroke to foot stroke of one leg. Gait cycle has two main stages namely, stance phase and swing phase. In stance phase, the leg is on the ground, on the other hand in moving stage that same foot is not in contact with the ground & the leg is moving for the next foot strike [1, 3, 7].

#### 3.1.2.1 Silhouette Extraction

The Silhouette image is generated from an order sequence of binary configured images. A complete gait cycle means “A foot from rest (standing) position to-right-leg-forward-to-rest-to left- leg- forward-to-rest position [3]. That’s why, gait cycle calculation mandatory for gait identification. Temporal components like Stride length, Step length represent movement of the body over time.

#### 3.1.2.2 Model Fitting

Model fitting is the procedure which is one of the pictorial representations that draws from their predicted values. Stick model n point/blob detection are the two parts which consist in fitting the model. For model fitting background subtracted images are necessary of. The block diagram Fig. 3 show the step by step procedure up to model fitting.



Fig. 3. Block diagram for model fitting

For producing a model more exact for biometric applications, the training set of values is divided into several clusters attending to the different positions the person images. To take silhouette of a human diagram from a frontal interpretation is fairly difficult from a lateral view [1–3].

##### 3.1.2.2.1 Blob Detection

The detection of Blob is the more difficult stage of fitting of the human model. Here we have recognized distorted & split blobs related to a single person. Model fitting is applied to recover the blob segmentation and to obtain a roughly form. For plotting the points or blob the different sigma values are calculated. This procedure is continuously to convergence to find more consistent silhouette. The process generates the sigma values for blob detection. This sigma values plots the blob on different frames. All the plotted values stored in matrix form generate the dataset of different frames within a single video [4]. The below figure shows the blob detection after their background subtraction (Figs. 4 and 5).

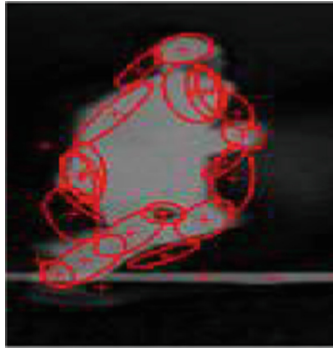


Fig. 4. Blob plotting

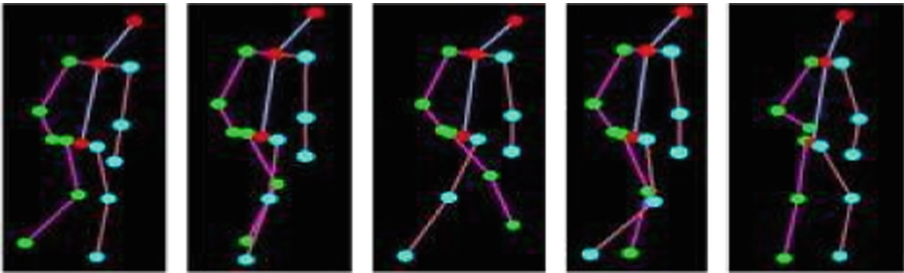


Fig. 5. Stick model [18]

Stick model is drawn with the help of blobs. All the generated blobs have their center points which show the exact sigma values. The stick model is generated by connecting all the entire center points. After joining all the co-ordinates we get the extracted stick model for calculating all the data set values.

$$b_i = \begin{cases} 1, & \text{if } x_{2i-1} = 0 \text{ and } (x_{2i} = 1 \text{ or } x_{2i+1} = 1) \\ 0, & \text{otherwise} \end{cases}$$

The eight values  $x_1, x_2 \dots x_8$  are the values neighbors of  $p$ , beginning with the east neighbor and numbered in counter-clockwise order [10]. This is the morphological function which connects the number of co-ordinates for creating the stick model.

The human gait cycle is divided into four stages: (i) right foot stop & left foot moving behindhand (ii) right foot moving forward & left foot halt (iii) left moving behindhand & right foot halt (iv) left moving forward & right foot halt. We have measured the 6 various points for the skeleton consistent to the knees, hips, & ankles. All the coordinates are found from their detected blobs and after joining this co-ordinate have detected the stick model. We basically considered 9–10 coordinates for storing that dataset values.

### 3.1.3 Training and Recognition

A biometric system used for verification as well as identification system. The submitted claim for authentication is either rejected or accepted by the system. Identification is a process where an individual recognizes by searching the template [20] or stored database for a match [10, 21].

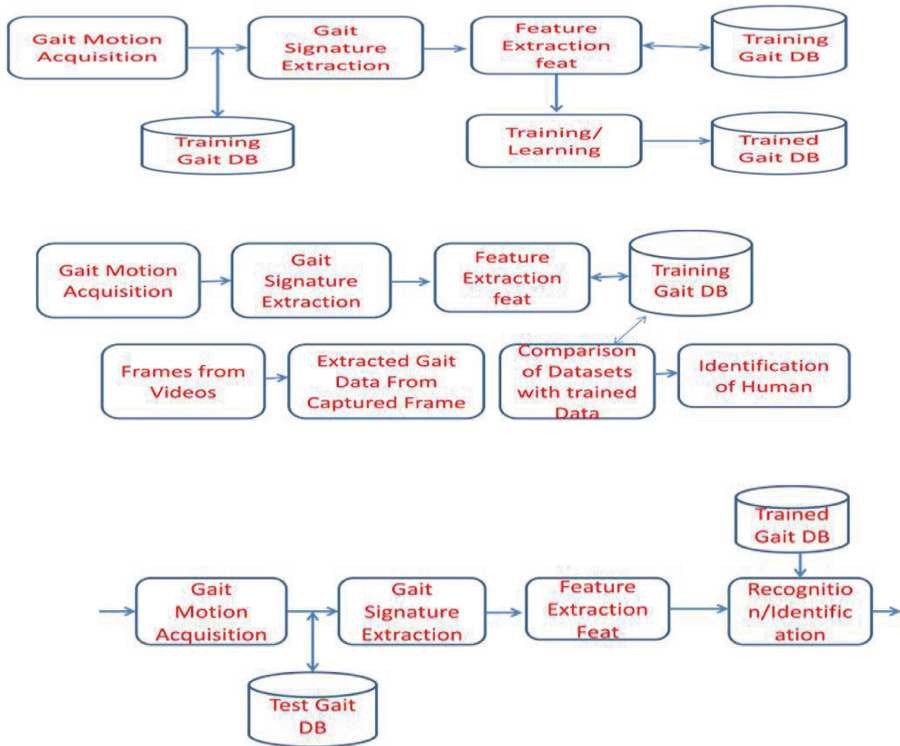


Fig. 6. (a) Training phase [4] (b) Recognition phase [4] (c) Identification phase

Figure 6 shows the training and recognition, identification module schematically. A typical human identification by their gait cycle was separated into recognition & training modules. Then after background subtraction and silhouette representation we skeletonize the image after frame differencing for receiving a digital description of the representative. The feature vectors for each person after scheming the skeletization then trained by a pattern recognition algorithm by using neural network toolbox in MATLAB, and the trained outcome will be stowed in a gait recognition database system person wise [3]. In addition, the recognition module identifies the person. After the trained database in the recognition stage, the video camera archives the gait human movements to be recognized, and it handovers it into the similar kind of feature vector as in training [2, 3].

Figure 6(c) demonstrates of the gait identification system block diagram. It uses the neural network of multi-layered for training and recognizing the gait. The typical biometric system also working on the same principles and components which mentioned above [3, 5]. In the Identification module the stored datasets is compared with new frame which is captured by camera. A comparison is done between the stored values and captured values. If dataset is similar between the two images it gives the result of comparing their vector values.

To be more particular, Distance measure is calculated as  $d = \|PR - PN\|_2$  where  $\| \cdot \|_2$  Shows the  $l_2$  -norm,  $PR$  the reference pattern &  $PN$  the video sequence new pattern [1, 3].

### 3.2 Gait Identification by Using Neural Network

Back propagation algorithm is used for training the network. The nodes of external layer divided into two groups. One is to for information of maximum output nodes [20] and another for to decode the output of gait identification Code [13].

## 4 Experimental Results

The effectiveness of the proposed system and discussions of the results are presented in this section. When the project is executed a screen appears where the option is available to play the video.

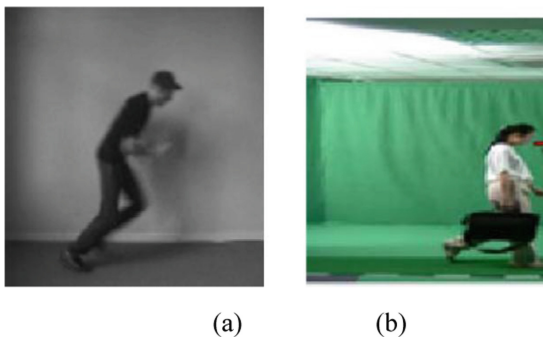
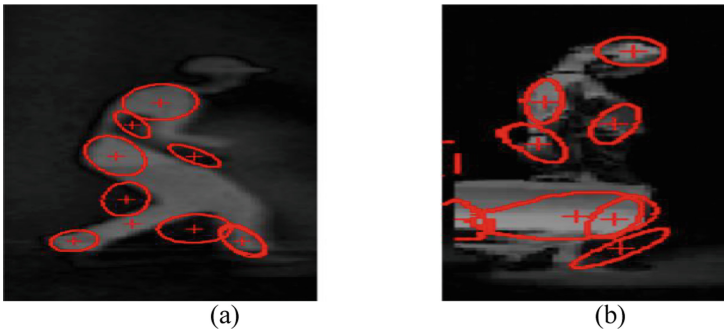


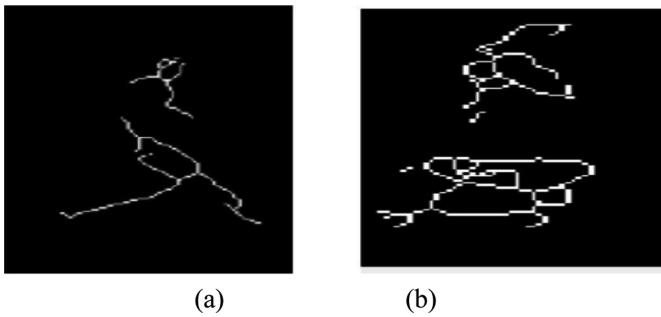
Fig. 7. Frames taken from images



**Fig. 8.** Silhouetted images (background subtracted images)



**Fig. 9.** Blob images



**Fig. 10.** Stick model after connecting the center points of blob.

After selecting a video Background subtraction algorithm gives the foreground image as shown in Fig. 7. The Kalman filter for filtering the unwanted and noisy frames is used.

$$[P, xp, PP, K] = Kalman Filter(CX, CY, handles);$$

Here Kalman filter is used for removing the unwanted noise.

After getting the silhouetted images as shown in Fig. 8. We put the blobs with their median values. Once we get the blobs we attached all the center points so we get the stick model with their vector values and it's stored in dataset. This is represented in Figs. 9 and 10.

After getting the stick model we trained the all frames by using neural network toolbox as shown in Fig. 11.

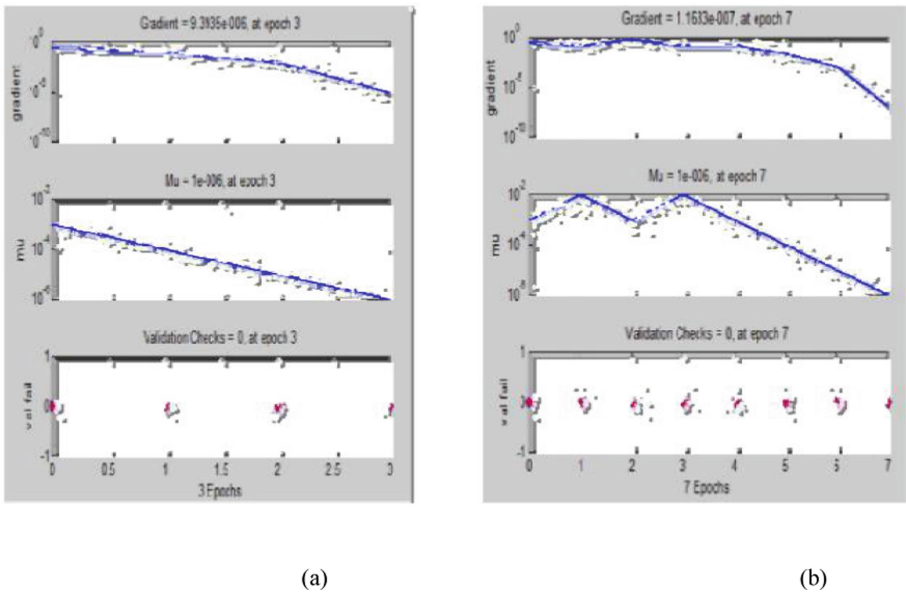


Fig. 11. Trained plot set

This process is similar for all phases like training phases, recognize phase and identification phase. In identification phase after recognizing the gait we compared this gait vectors with captured images. If these values are similar then it shows the exact name of a person whose gait matches with the stored gait. As depicted in Fig. 12 persons named XYZ and ABC are recognized from Gait.



**Fig. 12.** Identified individuals after matching the dataset

## 5 Conclusion and Future Scope

Gait is considered as an important behavioral as well as a valuable biometric characteristic for human identification and recognition. In this paper, the method has been tried on the gait features databases. An Extensive outcome on image exterior orders shows that these systems have a satisfying recognition result. The proposed recognition comes near to achieve highly competitive result with regards to the most of published recognition and identification approaches. To enhance the result of the model we have developed a human gait analysis to take into vectors temporal charismatic to track human body. The combination of temporal constraints on the system increase accuracy reliability, sureness, reliability and soundness. By using this approach we developed a recognition approach accurate up to 75–80%. The proposed method identifies the person more accurately than the other approaches which were developed earlier. This is one of the approach which is used for security purpose in any surveillance are military areas, banks and parks etc.

## References

1. Pushpa Rani, M., Arumugam, G.: An efficient gait recognition system for human identification using modified ICA. *Int. J. Comput. Sci. Inf.* **2**(1), 55–67 (2010)
2. Ekinci, M.: Human identification using gait. *Turk. J. Elec. Engin.* **14**(2), 267–291 (2006)
3. Yoo, J.-H., Hwang, D., Moon, K.-Y., Nixon, M.S.: Automated human recognition by gait using neural network. In: *Image Processing Theory, Tools & Applications*. IEEE (2008)
4. Kordjazi, N., Rahati, S.: Gait recognition for human identification using ensemble of LVQ neural networks. In: *International Conference on Biomedical Engineering (ICoBE)* (2012)
5. Orrite-Uruñuela, C., del Rincón, J.M., Elías Herrero-Jaraba, J., Rogez, G.: 2D silhouette and 3D skeletal models for human detection and tracking. In: *Proceedings of the 17th International Conference on Pattern Recognition, ICPR 2004* (2004)
6. Wang, C., Zhang, J., Wang, L., Pu, J., Yuan, X.: Human identification using temporal information preserving gait template. *IEEE Trans. Pattern Anal. Mach. Intell.* **34**(11), 2164–2176 (2011)



7. Rustagi, L., Kumar, L., Pillai, G.N.: Human gait recognition based on dynamic and static features using generalized regression neural network. In: Second International Conference on Machine Vision (2009)
8. Kim, D., Paik, J.: Gait recognition using active shape model and motion prediction. *IET Comput. Vision* **4**(1), 25–36 (2010)
9. Xu, D., Huang, Y., Zeng, Z., Xu, X.: Human gait recognition using patch distribution feature and locality-constrained group sparse representation. *IEEE Trans. Image Process.* **21**(1) (2012)
10. Sudha, L.R., Bhavani, R.: Biometric authorization system by video analysis of human gait in controlled environments. In: IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 (2011)
11. Kewatkar, S., Kathale, S., Pande, Y.: Gait recognition by modified counter propagation method. *IJPRET* **1**(8), 193–200 (2013)
12. Kathale, S., Gulhane, V.: Comparative study of various approaches for human identification and gait recognition. *Int. J. Adv. Res. Comput. Sci.* **4**(3) (2013)
13. Lien, C.-C., Tien, C.-C., Shih, J.-M.: Human gait recognition for arbitrary view angle. In: International Conference on Innovative Computing, Information and Control, ICICIC 2007 (2007)
14. Huang, D.-Y., Hu, W.-C., Chuang, C.-W., Chen, M.-S., Ko, C.-C.: Gait recognition of different people groups based on Fourier descriptor and support vector machine. In: IEEE International Conference on Control System, Computing and Engineering (2011)
15. Sun, B., Yan, J., Liu, Y.: Human gait recognition by integrating motion feature and shape feature. In: IEEE Conference on Multimedia Technology (ICMT) (2010)
16. Agostini, V., Balestra, G., Knaflitz, M.: Segmentation and classification of gait cycles. *IEEE Trans. Neural Syst. Rehabil. Eng.* **22**(5) (2014)
17. Kale, A., Sundaresan, A., Rajagopalan, A.N., Cuntoor, N.P., Roy-Chowdhury, A.K., Krüger, V., Chellappa, R.: Identification of humans using gait. *IEEE Trans. Image Process.* **13**(9), 1163–1173 (2004)
18. Stick Model for Gait Cycle. <http://www.google.co.in/images>
19. Yang, Q., Qiu, K.: Gait recognition based on active energy image and parameter-adaptive kernel PCA. In: 6th IEEE Joint International Conference, September 2011
20. Walzak, T., Grabski, J.K., Grajewska, M., Michalowska, M.: Application of artificial neural network in man's gait recognition. In: ICCM, September 2015
21. Kanwar, A., Upadhyay, P.: An appearance based approach for gait identification using infrared imaging. In: ICICT 2014 (2014)

# Author Index

## A

Adwani, Kakan, 421  
Aeishel, Georgy, 387  
Aggarwal, Gaurav, 460  
Alqahtani, Abdulrahman Saad, 252  
Amardeep, Rashmi, 431  
Anand Prabu, P., 626  
Anandha Banu, E., 301  
Anbarasa Kumar, A., 103  
Anna Palagan, C., 157  
Archana, N., 607  
Asanambigai, V., 453  
Ashok Kumar, K., 145  
Aswin, A. V., 412  
Ayushi, Doshi, 574  
Ayyasamy, A., 453, 618

## B

Balaji, S., 336  
Barua, Bobby, 647  
Basavaraju, N. M., 477  
Beslin Pajila, P. J., 438  
Bhagyashree, S. R., 363  
Biradar Sangam, M., 116  
Biswas, Indira N., 226  
Bittal, Vijaylaxmi, 64  
Brundha, 395

## C

Chaudhary, Jayesh, 127

## D

Desai, Urmi, 94  
Desale, Poonam, 42

Deshmukh, Pranali, 226  
Devana, V. N. Koteswara Rao, 599  
Dharshana Shahini, R., 311  
Dinesh Kumar, A., 252  
Dongre, Nilima, 64

## E

Elangovan, Uma, 494

## G

Garg, Sheetal, 363  
Germanus Alex, M., 30  
Golden Julie, E., 438  
Gomathi, S., 470  
Gomes, Francisco S., 226  
Gopala Krishnan, C., 504  
Gopalakrishnan, Mahalakshmi, 494  
Gothwal, Mayuri S., 42  
Gupta, Rajiv Kumar, 1

## H

Hara Gopal Mani, P., 145  
Hari Priya, S., 311  
Hatti, Daneshwari I., 84

## I

Indira, K., 353  
Indira Priyadarshini, B., 145

## J

Janani, M., 380  
Jayapandian, N., 387  
Jevin, J. A., 504  
John Peter, S., 30

Jose, Deepa, 190  
 Joy Winnie Wise, D. C., 518  
 Julme, Bhagyashri, 642

**K**

Kadhiwala, Bintu, 199  
 Kalaivani, S., 212  
 Kale, Preeti, 557  
 Kallimani, Rakhee, 404  
 Kathale, Snehal N., 655  
 Krishnan, Mukesk, 336  
 Kudale, Bharti, 226  
 Kulalvaizmozhi, V. P., 30  
 Kumar, Arvind, 282  
 Kumari, Parveen, 460  
 Kuriakose, Bineeth, 412

**L**

Lamani, Dharmanna, 48  
 Lata, Ragha, 169

**M**

M. Gayathri, Ragul, 568  
 Mahajan, J. R., 74  
 Maheswara Rao, A., 599  
 Majumder, Satya Prasad, 647  
 Manjunath, T. C., 48  
 Manohar, E., 301  
 Manoj, P., 380  
 Manuel, Shibu, 344  
 Marikani, T., 294  
 Meenalochini, M., 380  
 Meghana, M. S., 511  
 Merlin Gethsy, D., 626  
 Moholkar, Kavita, 487  
 Monica Rachel, K., 518  
 More, Neha J., 226  
 More, Priyanka, 42, 226  
 Mubarakali, Azath, 252  
 Muthulakshmi, I., 328  
 Muthulakshmi, K., 607

**N**

Naveena, Ambidi, 591  
 Nene, Manisha J., 557  
 Nikita, Bhatt, 574  
 Ninawe, Shubhangi, 633  
 Nisha, M. Sharon, 470  
 Nithya Devi, S., 607  
 Nitin, Shah, 574  
 Nivethan, 231

**P**

Pacharaney, Utkarsha Sumedh, 1  
 Pajila, Beslin, 395

Panimalar, S., 271  
 Panimozhi, K., 511  
 Parasuraman, Kumar, 103  
 Parveen, Shama, 538  
 Parveen, Suraiya, 538  
 Patel, Ami, 127  
 Patel, Marmik, 179  
 Patil, Nita, 238  
 Patil, Pragati, 642  
 Pavithra, G., 48  
 Pavithra, K., 511  
 Ponnu Krishnan, P., 626  
 Prakash Rao, R., 145  
 Prem Jacob, T., 271

**R**

Rahman, Nafisur, 538  
 Rai, Shashwat, 487  
 Raja Priya, N., 518  
 Raja Ratna, S., 626  
 Raja Sundari, K., 518  
 Rajalingam, S., 19  
 Rajan, Anitha Amaiti, 395  
 Rakesh, N., 317, 421  
 Rami, Devangi, 179  
 Rasane, Krupa, 404  
 Rathika, V., 546  
 Rathod, Krishna, 487  
 Rathod, Krupa, 487  
 Ravi, R., 207  
 Rawat, C. S., 74  
 Reddy, Katta Rama Linga, 591  
 Reddy, Pranayanath, 116  
 Reji Kumar, K., 344  
 Reshma, R., 618  
 Rethishkumar, S., 527

**S**

Sahajrao, Pradnya S., 42  
 Sahana, S., 511  
 SaiRamesh, L., 618  
 Saleema Parvin, S. B., 618  
 Sankar, Sriram, 231  
 Santhiya, C., 353  
 Sarbhukan, Vaishali V., 169  
 Sathiyavathi, V., 618  
 Sawarkar, Sudhir, 238  
 Selva Nidhyananthan, S., 311  
 Selvi, V. Perathu, 470  
 Senthilkumar, T. K., 19  
 SenthurSelvi, V., 470  
 Shaikh, Aarzo A., 42  
 Shajilin Loret, J. B., 626  
 ShakulHameed, A., 380

Sharma, Chhavi, 282  
Shekhar, R., 116  
Shreekanth, T., 477  
Shubha, N., 511  
Shyamala, K., 212, 294  
Singh, Sugandha, 460  
Singhal, Prachi, 373  
Sinha, Pranit, 387  
Sivakumar, K., 504  
Solanki, Urvashi, 199  
Solaskar, Supriya, 655  
Soni, Mukesh, 179  
Soundara Rajan, K., 157  
Srinivasan, Karthik, 252  
Surya, S., 207  
Sutagundar, Ashok V., 84  
Swaminathan, Aravind, 395  
Swetha, K., 353

**T**

Tandel, Bhavini N., 94  
Thanga Selvi, R., 328

ThippeSwamy, K., 431  
Thomas, J., 568  
Tomar, Mritunjay, 487  
Tomar, S. K., 282

**U**

Uma Maheswari, R., 19

**V**

Vadivu, G., 373  
Vedavathi, L., 477  
Velu, S. Ganesh, 504  
Venkat Tejas, R., 317  
Verma, Pankaj, 64  
Vijayakumar, R., 527  
Vikas, Bisati Sai Venkata, 568  
Vinotha, P., 190

**W**

Wajgi, Rakhi, 633

**Y**

Yamuna Bee, J., 336