Studies in Computational Intelligence 1007

Rajeev Agrawal
Jing He
Emmanuel Shubhakar Pilli
Sanjeev Kumar *Editors*

Cyber Security in Intelligent Computing and Communications

Springer

Studies in Computational Intelligence

Volume 1007

Series Editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland

The series "Studies in Computational Intelligence" (SCI) publishes new developments and advances in the various areas of computational intelligence—quickly and with a high quality. The intent is to cover the theory, applications, and design methods of computational intelligence, as embedded in the fields of engineering, computer science, physics and life sciences, as well as the methodologies behind them. The series contains monographs, lecture notes and edited volumes in computational intelligence spanning the areas of neural networks, connectionist systems, genetic algorithms, evolutionary computation, artificial intelligence, cellular automata, self-organizing systems, soft computing, fuzzy systems, and hybrid intelligent systems. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution, which enable both wide and rapid dissemination of research output.

Indexed by SCOPUS, DBLP, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at https://link.springer.com/bookseries/7092

Rajeev Agrawal · Jing He ·
Emmanuel Shubhakar Pilli · Sanjeev Kumar
Editors

Cyber Security in Intelligent Computing and Communications

Springer

Editors

Rajeev Agrawal
GL Bajaj Institute of Technology
and Management
Greater Noida, Uttar Pradesh, India

Emmanuel Shubhakar Pilli
Malaviya National Institute of Technology
(MNIT)
Jaipur, India

Jing He
Kennesaw State University
Kennesaw, GA, USA

Sanjeev Kumar
Department of Master of Computer
Applications
GL Bajaj Institute of Technology
and Management
Greater Noida, Uttar Pradesh, India

ISSN 1860-949X ISSN 1860-9503 (electronic)
Studies in Computational Intelligence
ISBN 978-981-16-8011-3 ISBN 978-981-16-8012-0 (eBook)
https://doi.org/10.1007/978-981-16-8012-0

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

In the present age of intelligent computing and communication, a need for digital transformation was realized greatly with the emerging technology interventions increasing in all the domains including business, education, healthcare, household, etc. This intensified growth of online and remote applications or service integration with traditional system raising cyber security challenges. The aim of this research book is to provide immersed cyber security growing challenges with topical advancements in the computational intelligence and communication technologies. To derive the potential future directions for intelligent and smart computing solutions in cyber communication environment, this book includes invited peer-reviewed chapters on the emerging intelligent computing and communication technological research advancements, experimental outcomes and cyber security practices, threats and attacks with challenges.

All the chapters in the book are organised thematically into three comprehensive areas:

- cyber security practices, recent trends and challenges,
- intelligent computing and communication security and
- security resilient smart applications

The book begins with state-of-the-art survey and reviews of cyber security trends and issues, covers recent developments in intelligent computing and communication and finally presents smart healthcare, agriculture, virtualized infrastructures, block chain technology, vehicle online education and many other real-life applications using IoT, Big data, cloud computing, artificial intelligence and machine learning.

This book will be of interest to graduate and postgraduate students, research scholars and professors. This research book can also be a valuable resource for practitioners and professionals working in the field of smart city visualization through secure and intelligent application design, development and deployment to foster digital revolution and reliable integration of advanced computing and communication technologies with local and global significance.

Greater Noida, India	Dr. Rajeev Agrawal
Georgia, US	Dr. Jing He
Jaipur, India	Dr. Emmanuel Shubhakar Pilli
Greater Noida, India	Dr. Sanjeev Kumar
September 2021	

Acknowledgements

Thought of publishing a research book with recent trends, practices and future directions in the field of Cyber Security, Intelligent Computing and Communications would never have become true without the contribution of many who directly indirectly extended their cooperation to complete this book.

First and foremost, we give our special thanks to all the authors and team of peer reviewers, who contributed to present a focused and thematically organized content in this book, and truly made this volume possible.

We would also like to express our heartfelt gratitude to Springer editorial and publishing team for their consistent guidance and efforts. It is an honor and privilege to work with one of the leading research publication organization; Springer and converting our dream into reality in the form of this book.

We are highly grateful to Shri Pankaj Agarwal, Vice Chairman, GL Bajaj Institute of Technology and Management, Greater Noida for his consistent encouragement and facilitation. At last but not the least we are very thankful to Prof. (Dr.) Madhu Sharma Gaur, Head MCA, and her enthusiastic team who unconditionally cooperation throughout the process.

Contents

Cyber Security Practices, Trends and Challenges

Intelligent Computing and Communication Security

Security Resilient Smart Applications

Editors and Contributors

About the Editors

Rajeev Agarwal is a professor at G.L. Bajaj Institute of Technology and Management, Greater Noida, India. He has an illustrated experience of more than 27years in teaching and research, holds a B.E. degree in electronics engineering, and M.Tech. degree in system engineering. He received a Ph.D. degree in wireless communication channels from the School of Computer & System Sciences, JNU, New Delhi. He was a visiting professor at Kennesaw State University, Georgia, the USA, under a joint research project in remote patient monitoring & medical imaging. His research areas include planning and performance analysis of wireless networks and medical image analysis for automated diagnosis, performance analysis of fog, and edge networks. He has more than 70 publications in international journals and proceedings. He has been awarded by various state and national agencies for his contributions to research and academics. He is also serving as a reviewer for several reputed international journals and a member of the editorial board for two international journals.

Jing He is an associate professor from the Department of Computer Science, College of Computing and Software Engineering (CCSE) at Kennesaw State University (KSU), USA. His current research interests mainly include a robust future learning environment using intelligent sensing, big data analytics, cloud computing, machine learning, and artificial intelligence security technologies. He has published over 90 papers. In addition, she has edited/authored 7 book chapters/books. Her work has been cited more than 1,570 times based on Google Scholar, and her current h-index is 22. Moreover, she successfully led a Google IgniteCS sponsored Women Summer Camp titled "Girls Mentor Girls" at Girls Inc. Atlanta in Summer 2016. She earned the KSU Outstanding Early Career Faculty Award KSU in August 2017

Emmanuel Shubhakar Pilli is an associate professor in the Department of Computer Science and Engineering, Malaviya National Institute of Technology, Jaipur. He has over 24 years of academic, research, and administrative experience. Dr. Pilli is also an honorary dean (Network & Hardware), Rajasthan ILD Skill University, Jaipur. He received his M.Tech. (Computer Science) from Birla Institute of Technology, Ranchi, in 2001 and a Ph.D. (Computer Science) from the Indian Institute of Technology Roorkee in 2012. Dr. Pilli guided 5 Ph.D., 38 M.Tech., and 37 B.Tech. projects. His research areas are security, forensics, cloud computing, big data, IoT, blockchain, and quantum computing. He has 82 publications in international journals and conferences.

Sanjeev Kumar has over 12 years of academic and 05 years of research experience. Dr. Kumar is an assistant professor in the Department of Computer Applications, G.L. Bajaj Institute of Technology and Management, Greater Noida. He received his MCA degree from Uttar Pradesh Technical University, Lucknow, and a Ph.D. (Computer Science) degree from Gurukula Kangri University, Haridwar. He has supervised 2 M.Tech. and 25 MCA projects and has published over 14 research papers in the international journal and conferences of repute. His research interests are soft computing, computer networks, wireless communication, 5G, and security.

Contributors

Nidhi Agarwal Integrated School of Education, Ghaziabad, India

Naveen Aggarwal CSE, UIET, Panjab University, Chandigarh, India

Zahoor Alam IME Department, Indian Institute of Technology Kanpur, Kanpur, India

Rigzin Angmo CSE, UIET, Panjab University, Chandigarh, India

Anjali Department of Electrical Electronics and Communication Engineering, SET, Sharda University, Greater Noida, India

Shashank Awasthi G.L Bajaj Institute of Technology & Management, Greater Noida, India

A. B. Bavani Sankar Indian Institute of Information Technology Allahabad, Prayagraj, India

Prashant Bhat Garden City University, Bengaluru, India

Karamjit Bhatia Gurukula Kangri Vishwavidyalaya, Haridwar, India

Sansar Singh Chauhan G.L. Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India

Pushpa Choudhary Department of Information Technology, G. L. Bajaj Institute of Technology and Management, Greater Noida, India

Shilpa Choudhary Department of Electronics & Communication Engineering, G.L. Bajaj Institute of Technology and Management, Greater Noida, India

Archana Das Department of Computer Science & Engineering, Accurate Institute of Management & Technology, Greater Noida, U.P., India

Saswat Kumar Das Department of Mechanical Engineering, IIMT College of Engineering, Greater Noida, U.P., India

Shiv Ashish Dhondiyal Graphic Era Deemed to be University, Dehradun, Uttarakhand, India

P. M. Diaz Department of Mechanical Engineering, Sreyas Institute of Engineering and Technology, Hyderabad, Telangana, India

Sushil Chandra Dimri Graphic Era Deemed to be University, Dehradun, Uttarakhand, India

Soumya Garg Indian Institute of Information Technology Allahabad, Prayagraj, India

Urvashi Garg CSE Department, Chandigarh University, Mohali, India

Ruchika Gupta Amity University Uttar Pradesh, Greater Noida, India

Shiv Narain Gupta Department of Electronics and Communication Engineering, Greater Noida Institute of Technology, Greater Noida, India

Shradha Gupta Department of Applied Science and Humanities, G. L. Bajaj Institute of Technology and Management, Greater Noida, UP, India

Vivek Gupta Department of Electronics and Communication Engineering, Greater Noida Institute of Technology, Greater Noida, India

Ajay Indian Central University of Rajasthan, Ajmer, India

Mayank Jain Galgotias University, Greater Noida, Uttar Pradesh, India

Shiva Pujan Jaiswal Department of Electrical Electronics and Communication Engineering, SET, Sharda University, Greater Noida, India

Saurav Jha Department of Electronics and Communication Engineering, Greater Noida Institute of Technology, Greater Noida, India

M. Julie Emerald Jiju Department of MCA, CSI Institute of Technology, Thovalai, Kanyakumari, Tamil Nadu, India

Jasleen Kaur CSE Department, Chandigarh University, Mohali, India

Rijwan Khan ABES Institute of Technology, Ghaziabad, India

Aizad Khursheed EEE Department, Amity University, Greater Noida, India

Priya Kohli Graphic Era Hill University, Dehradun, Uttarakhand, India

Bhavika Kulkarni MIT School of Engineering, Pune, India

Indrajeet Kumar Graphic Era Hill University, Dehradun, Uttarakhand, India

Krishan Kumar Gurukula Kangri Vishwavidyalaya, Haridwar, India

Pankaj Kumar Ministry of Electronics and Information Technology, Government of India, New Delhi, India

Puneet Kumar Kalinga University, Chhattisgarh, India

Surjeet Kumar Department of Computer Applications, VBS Purvanchal University, Jaunpur, UP, India

Anil Kumar kurra VFSTR (Deemed To Be University), Vadlamudi, India

Soumyadev Maity Indian Institute of Information Technology Allahabad, Prayagraj, India

Pradnya Malaganve Garden City University, Bengaluru, India

Arpana Mishra Department of Electronics and Communication Engineering, IIMT, Greater Noida, India

C. Mohan Department of Electrical Electronics and Communication Engineering, SET, Sharda University, Greater Noida, India

Jatin Manav Mutharasu MIT School of Engineering, Pune, India

Swagat Nayak Indian Institute of Information Technology Allahabad, Prayagraj, India

Usha Rani Nelakuditi VFSTR (Deemed To Be University), Vadlamudi, India

Ganesh Prasad Pal Department of Computer Science & Engineering, G.L. Bajaj Institute of Technology & Management, Greater Noida, U.P., India

Anand Bhushan Pandey Department of Information Technology, G. L. Bajaj Institute of Technology and Management, Greater Noida, India

Harikesh Pandey Department of Information Technology, GL Bajaj Institute of Technology and Management, Greater Noida, India

Utshav Pandey MIT School of Engineering, Pune, India

Prof. Mohandas Pawar MIT School of Engineering, Pune, India

Sanjeev Kumar Pippal G.L. Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India

K. Praveen TIFAC-CORE in Cyber Security, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Mayank Raj Department of Mechanical Engineering, IIMT College of Engineering, Greater Noida, U.P., India

Ajay Rana Amity University, Noida, India

Deepak Singh Rana Graphic Era Deemed to be University, Dehradun, Uttarakhand, India

B. Rethick MIT School of Engineering, Pune, India

Aritro Sengupta Ministry of Electronics and Information Technology, Government of India, New Delhi, India

Vidit Shukla Department of Electronics & Communication Engineering, G.L. Bajaj Institute of Technology and Management, Greater Noida, India

Abhay Pratap Singh Department of Computer Science, Haridwar, India

Amit Singh Ministry of Electronics and Information Technology, Government of India, New Delhi, India

Arjun Singh Department of Information Technology, GL Bajaj Institute of Technology and Management, Greater Noida, India

Arun Kumar Singh Department of Information Technology, G. L. Bajaj Institute of Technology and Management, Greater Noida, India

Jay Singh G. L. Bajaj Institute of Technology and Management, Greater Noida, India

Mahendra Singh Department of Computer Science, Haridwar, India

S. Vikram Singh EEE Department, Amity University, Greater Noida, India

Taranjeet Singh Mangalmay Institute of Engineering and Technology, Greater Noida, India

Vijay Paul Singh CSE, UIET, Panjab University, Chandigarh, India

Sonal CSE, UIET, Panjab University, Chandigarh, India

Sonam Department of Computer Applications, VBS Purvanchal University, Jaunpur, UP, India

Sandeep Srivastava GL Bajaj Institute of Technology & Management, Greater Noida, India

Ikul Kamanda Steve Department of Electrical Electronics and Communication Engineering, SET, Sharda University, Greater Noida, India

Priyesh Tiwari Department of Electronics and Communication Engineering, Greater Noida Institute of Technology, Greater Noida, India

Ashish Tripathi Department of Information Technology, G. L. Bajaj Institute of Technology and Management, Greater Noida, India

Tushita CSE, UIET, Panjab University, Chandigarh, India

Lalit Kumar Tyagi G.L Bajaj Institute of Technology & Management, Greater Noida, India

Neha Tyagi G.L Bajaj Institute of Technology & Management, Greater Noida, India

Purneshwari Varshney Department of Electronics & Communication Engineering, MBM Engineering College, Jodhpur, India

Prem Chand Vashist Department of Information Technology, G. L. Bajaj Institute of Technology and Management, Greater Noida, India

Tulika Vijay CSE, UIET, Panjab University, Chandigarh, India

Vrince Vimal Graphic Era Hill University, Dehradun, Uttarakhand, India

V. Vishnu TIFAC-CORE in Cyber Security, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Cyber Security Practices, Trends and Challenges

State-of-the-Art Survey on Web Vulnerabilities, Threat Vectors, and Countermeasures

Jasleen Kaur and Urvashi Garg

1 Introduction

The primary reason behind any web attack is insufficient security or design flaws in the web application, thereby, allowing hackers to enter into the system and steal confidential data such as username, passwords, transaction details, session Ids/token, and database-related information. According to a survey, PHP (78.5%) and JavaScript (94.7%) are the most commonly used server-side and client-side programming languages, respectively [1].

A cyber-criminal would first analyse the website for a vulnerability using online tools such as vulnerability scanners or botnets. Vulnerabilities such as virus-infected administrator's system, weak password, out of date security patches, browser plugins, and permissive coding practices may give a chance to the hacker to enter the system and steal the data. Moreover, a recent survey was conducted on the usage of worldwide web in which the authors depicted that most common vulnerabilities are found at application level, which is layer 7 according to the OSI network model [2], and 93% of data breaches occur due to human error while designing and developing the web application [3]. For an instance, neglect of data validation could give a clear path to attacker to deceive the web server into running unsafe commands [4]. In 2019, an EDGESCAN organisation generated a vulnerability statistics report in which it claimed that 19% of all vulnerabilities were associated with layer 7, and the rest 81% of vulnerabilities were linked with network layer. SQL injection was significant at 5.55%, XSS at 14.69%, and other injection attacks such as OS, CRLF, and JavaScript were significant at 8.18%. According to 2020 Cyber security report, approximately 93% of the files, which were shared through web in India, were found to be malicious [5], and 64% of the organisations in India are believed to be impacted by the information disclosure vulnerability. Despite the extensive research

J. Kaur (✉) · U. Garg
CSE Department, Chandigarh University, Mohali, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_1

Table 1 Top 10 common vulnerabilities and exploits (CVE)

CVE Number	Vulnerability name
CVE1	Injection
CVE2	Broken authentication
CVE3	Sensitive data exposure
CVE4	XML external entities (XXE)
CVE5	Broken access control
CVE6	Security misconfigurations
CVE7	Cross site scripting (XSS)
CVE8	Insecure deserialisation
CVE9	Using components with known vulnerabilities
CVE10	Insufficient logging and monitoring

being done in developing new tools and protocols to detect, prevent, and mitigate the web attacks, still numerous websites are non-immune to the web attacks. This clearly depicts the need to detect the software-related vulnerability in order to prevent web security exploitation by the hacker. Following are the top 10 vulnerabilities in 2020 [6] according to OWASP (Open Web Application Security Project) [7] (Table 1).

Figure 1 demonstrates an attacker interrupting normal communication between client and server, getting successful in bypassing the system, and modifying the crucial data. The attack is viable due to the nature of HTTP and HTTPS protocol. In case of HTTPS, two connections are built up: one SSL connection is created between the client and the hacker, second SSL connection is created between the hacker and web server where the cybercriminal splits the TCP connection between the client and web server. In 2019, SSL labs claimed that 1.2% of HTTPS servers are still vulnerable to attack. For example, DROWN attack vulnerability can be easily carried out on websites using HTTPS and SSL/TLS services [8]. The misconfiguration and

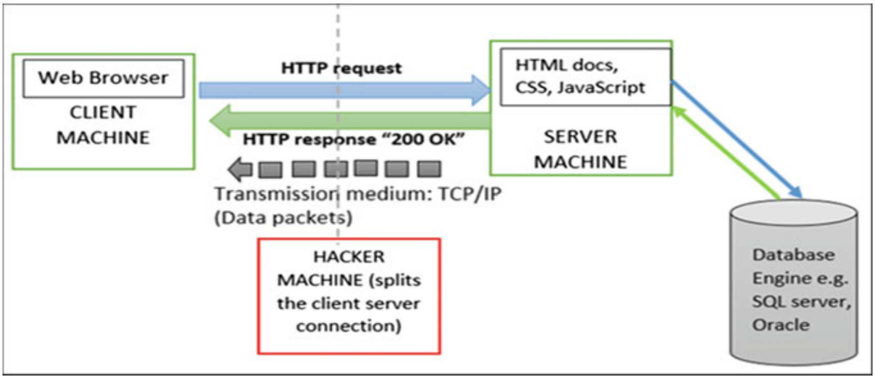

Web Browser
CLIENT MACHINE
HTTP request
HTTP response "200 OK"
Transmission medium: TCP/IP
(Data packets)
HTML docs, CSS, JavaScript
SERVER MACHINE
HACKER MACHINE (splits the client server connection)
Database Engine e.g. SQL server, Oracle

Fig. 1 Scenario of attack on a web application

inappropriate default setting allow the attacker to decrypt TLS connection between client and server.

2 Literature Survey

2.1 SQL Injection Vulnerability Attack and Prevention

This web attack was first discovered in 1998 by a security researcher, Jeff Forristal, and is still at the top list since 2003. Antivirus programs are ineffective at handling SQLI attack. Any company that operates its website on SQL database is prone to this attack if it does not have sufficient input validations in its web forms. As a result, anyone can insert malicious SQL commands into the input string of a web form, web cookie, or a page request (browser), and can retrieve, modify, and delete the data present in the database putting data integrity, authentication, authorisation, and confidentiality at risk. In 2012, a researcher claimed that 97% of data breaches occur due to SQLi. Surprisingly, health industry is the most attacked industry and with maximum number of data breaches due to SQLi attack. The attack is done on data-driven applications as the behaviour of these applications generally depends upon the data input. Therefore, this attack is quite easy to execute. However, lack of awareness and implementation of security protocols by the organisations leads to data leaks resulting from SQLI attack. The attack could be carried out with one of the following objectives [9]:

- to identify injectable parameters
- to extract/retrieve data
- to add/modify data
- to perform DOS
- to evade detection
- to bypass authentication
- to execute remote commands
- to perform privilege escalation.

SQL injection attack has two stages [10]:

i. Injection attack stage 1
ii. Injection attack stage 2.

Stage 1 is known as reconnaissance. At this stage, the attacker passes random unexpected values to the arguments and observes how application responds. Stage 2 is known as actual attack. At this stage, the attacker provides carefully-crafted input values that will be interpreted as part of SQL commands rather than merely data. The database then executes the SQL commands as altered by the attacker. SQLi can be categorised into the following four types as illustrated in Fig. 2:

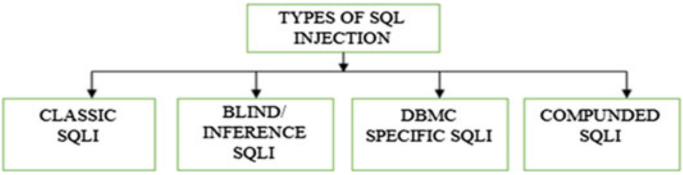


Fig. 2 Types of SQL injection vulnerability attacks [9]

2.1.1 CLASSIC SQL Injection Attack

It occurs generally when the user input is not filtered and escaped correctly in the web form. Owing to this, attacker sends batch commands to the database server, and in return receives specific output based on the input statements [11]. As a result, he can control application's entire database as illegitimate admin user. The input may include SELECT commands, which can download entire database including users' personal information such as unique identification, phone number or credit/debit card numbers. The attacker could also use INCLUDE or UPDATE commands to create new user accounts or alter the existing ones.

For instance, following Fig. 3, integer value '1' is passed to the web submission form (DVWA), where the security level was set as low, which returned the first name and surname for user id '1'. Similarly, it will return the values for user id 2 or 3. This means that website is vulnerable to SQLI attack. Moreover, the URL also depicts the id number. The URL is:

http://localhost/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#

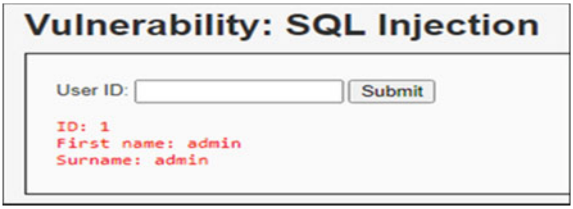
If the id number is changed in URL itself, the results will be displayed for that particular id. For example, if we change the id from 1 to 2 and press enter, the database will return the first name and surname for id 2.

We can also extract all first names and surnames by passing the string %' or '0'='0 in the input form. This will return the information for all five records present in the database (Fig. 4).

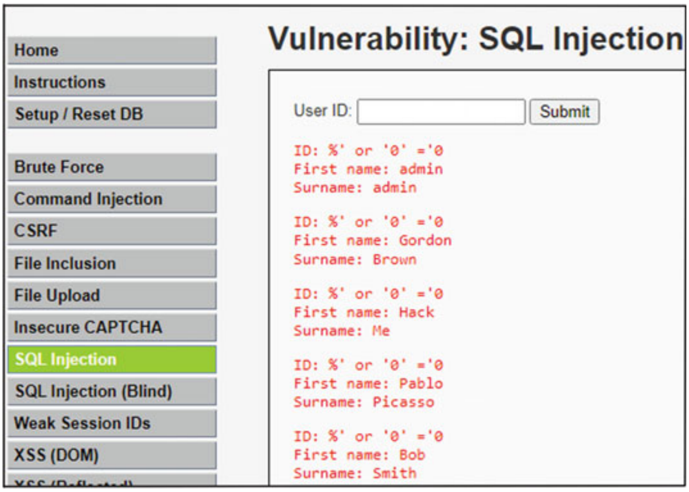
Classic SQLI can be implemented by one of the following techniques [1, 9, 12]:

i. Tautologies
ii. UNION SQL Queries
iii. Piggy-backed SQL queries
iv. Alternate encoding

Fig. 3 Extracting the values of argument 'id'


Vulnerability: SQL Injection

```
ID: 1
First name: admin
Surname: admin
```



Vulnerability: SQL Injection

```
ID: %' or '0' ='0
First name: admin
Surname: admin

ID: %' or '0' ='0
First name: Gordon
Surname: Brown

ID: %' or '0' ='0
First name: Hack
Surname: Me

ID: %' or '0' ='0
First name: Pablo
Surname: Picasso

ID: %' or '0' ='0
First name: Bob
Surname: Smith
```

Fig. 4 Extracting the values for all records

v. Illogical Queries
vi. Stored Procedures.

USING TAUTOLOGY

Tautology means an expression or a logical statement, which is always true. This means that attacker can use such SQL statements, which will always be true, and hence results in executing the queries at the database server. The attack is carried with one of the following objectives:

- to extract/retrieve data
- to bypass authentication
- to identify injectable arguments.

The attack is implemented by using conditional expressions using OR operator.

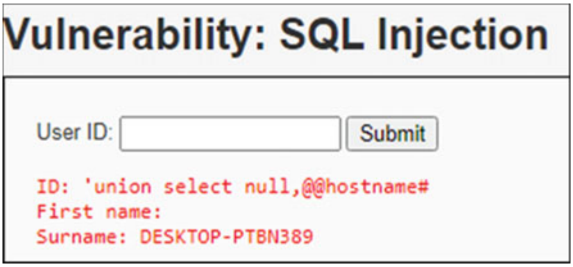
USING UNION COMMAND

UNION SQL attack is operated especially to determine the database version or the information about the number of rows and columns. Just like the former uses OR operator, this attack uses UNION operator where UNION is used to merge two SELECT statements.

The attack is carried out with one of the following objectives:

- to extract/retrieve data
- to bypass authentication.

By default, most of the databases such as MySQL stores the database-related information like name with version, number of tuples, etc. and can display the database



Vulnerability: SQL Injection

```
ID: 'union select null,@@hostname#
First name:
Surname: DESKTOP-PTBN389
```

Fig. 5 Using union query to retrieve the hostname

version while generating error messages for incorrect queries [13]. Such misconfiguration could allow attackers to compromise database for future attacks. For example, the following UNION SQL query will end up in extracting the information of all records with database version as the last one.

%' or 0=0 union select null, version() #

Attacker could also use the union statement to extract the hostname (Fig. 5) using the following command:

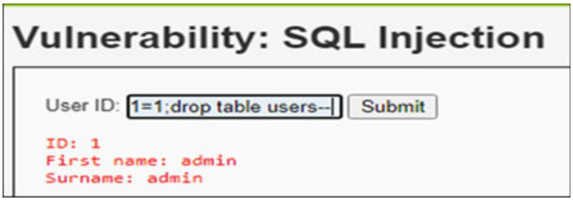
'union select null, @@hostname#

The attacker could also pass union queries to extract the details of information schema, location of database files, and even read files located on the remote system. Therefore, in order to avoid such type of attacks, it is always recommended to use prepared statements in conjunction with GET statement.

USING PIGGY-BACKED STATEMENTS

As the name implies, piggy-backed statement means to add one statement at the end of another statement to make it a single command by using semicolon. The database that would be vulnerable to such attack could allow multiple statements to be treated as a single statement if and only if the former statement comes out to be valid and true. For example, following Fig. 6 demonstrates inserting second query using semicolon after the first true query.

This vulnerability can be misused by the attacker to execute remote commands such as dropping the tables or to shut-down the entire system using command SHUTDOWN;–. As a result, he can effortlessly implement 'Denial of service (DoS)' attack.



Vulnerability: SQL Injection

User ID: 1=1;drop table users--

```
ID: 1
First name: admin
Surname: admin
```

Fig. 6 Sample example of piggybacked SQLI attack

USING ALTERNATE ENCODINGS

An attacker may use special encoding techniques in order to prevent detection of malicious code by the software [14]. For instance, he may use ghost characters to bypass the filters as Web or FTP server fails to detect the extra characters. These characters are the extra characters, which do not have any effect on the API layer, hence, will automatically get stripped off from input string. Following is the list of ‘improper handling of encoding’ vulnerabilities [15] that could allow attacker to do further damage:

i. Using char() of ASCII [1]
ii. Using ghost characters
iii. Passing special characters using % in the URL (URL encoding due to insufficient filtering on the URL)
iv. Repetition of encoding or Double encoding
v. Encoding IP/web address
vi. Adding NULL bytes in the input
vii. Using Unicode/UTF-8 encoding technique
viii. Using NULL terminator by post-fixing the data to avoid filter.

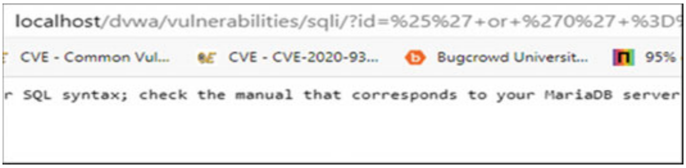
This type of attack is difficult to implement as the developer needs to check the validation and proper sanitisation for all of the above-mentioned encodings including URLs, IP address, and input.

USING ILLOGICAL QUERIES

As the name suggests, a threat actor can pass incorrect SQL statements in order to collect critical information about the database just from the error or log messages, which could display errors related to syntax of code, logical error, or type mismatch error. This could lead to exposure of injectable arguments/parameters to the attacker. Due to this reason, this type of attack is also sometimes referred to as error-based injection [1]. For example, in the following Fig. 7, after inserting incorrect query, server return name of database in the error message.

USING STORED PROCEDURES

Stored procedures are the compound statements that contain a set of multiple SQL statements as a group, which further gets saved in a data dictionary of RDBMS [16]. This group is given a specific unique name. This provides flexibility to call these set of statements from multiple programs using a single name (just like we



```
localhost/dvwa/vulnerabilities/sqli/?id=%25%27+or+%270%27+%3D
```

```
r SQL syntax; check the manual that corresponds to your MariaDB server
```

Fig. 7 Sample example of error-based SQLI attack

call functions). As a result, they provide various benefits such as handling runtime errors, data validation, provide mechanism for access control, etc. There is a common myth among most of the developers that stored procedures are always safe. However, they are completely not, if dynamic SQL inside the stored procedure is not handled properly. What I mean to say is, if the dynamic query used inside the stored procedures is created by concatenating the user input values instead of formal parameters, then it is at high risk. For example, the following first statement illustrates the bad example of dynamic SQL.

sb.command.Append("Name="+inputName.value+, ",");

Good example:

sb.command.Append("Name=@Name");

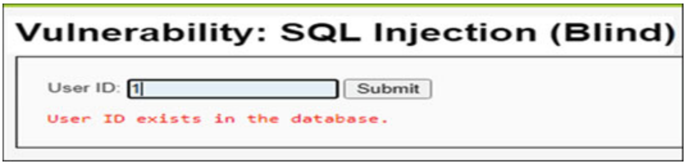
2.1.2 BLIND SQL Injection Attack

As the name suggests, in this type of attack, the results of SQL injection are hidden from the attacker, therefore, it becomes quite difficult for the attacker to extract data in one attempt [9, 11]. The attacker performs number of attempts before reaching to final successful request. It is also known as inference injection attack. For example, let us take the same example that we took in CLASSIC SQL injection attack. If we pass a true value, i.e. 1, then instead of getting the actual results such as value for first name and last name, we will get out mentioned in Fig. 8.

Blind SQLI attack has two types:

i. Time-based blind SQL injection attack
ii. Content-based SQL injection attack.

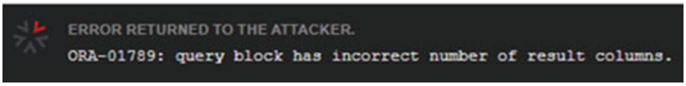
Sometimes, it is also referred to as conditional response as the attacker sends a malicious code with some conditions to the server and checks the response. In most cases, the queries are crafted as Boolean values, i.e. true or false. If the response happens to be true, the injectable parameters can be detected, else attacker can try another malicious set. It could also be the response rate of HTTP request [17]. In the first type, the attacker sets a time limit in the code and analyses the response received from the web server. Whereas, in the content-type, it is done depending upon the content generated by the query. In order to check whether the website is vulnerable to BLIND SQLI attack (stage 1: reconnaissance), attacker could use


Vulnerability: SQL Injection (Blind)

User ID: 1

User ID exists in the database.

Fig. 8 Sample example of SQL blind injection attack



```
ERROR RETURNED TO THE ATTACKER.
ORA-01789: query block has incorrect number of result columns.
```

Fig. 9 Sample error message

online vulnerability tool such as SQLMap (could be even used by researchers for teaching and learning process).

2.1.3 DBMS Specific SQL Injection Attack

This type of attack is done using two techniques: DB fingerprinting and DB mapping. DB fingerprinting means executing illogical queries in order to extract database-related information such as analysing error messages, inserting query to know DB version, ascertaining table names, information schema, and number of rows and columns, etc.. The type of error message generated by the database will vary depending upon the type of back-end database used. For example, the following error messages tell about the incorrect number of columns, so attacker can easily modify the input to obtain the correct result (Fig. 9).

The attacker could also construct a query to retrieve the exact version of database using inference testing as discussed earlier. By mapping the database using online tools, hackers can easily access the application's data layer.

2.1.4 COMPOUNDED SQL İnjection Attack

Compounded SQLI attack means that the attacker can use another attack in conjunction with SQLI attack. For instance, the following attacks can be executed by the attacker after performing SQLI attack.

i. XSS attack,
ii. insufficient authentication attack,
iii. DDoS attack, and
iv. DNS hijacking attack.

Finally, SQLI attack can be prevented only by considering the above-mentioned vulnerabilities while developing a website as firewalls, antivirus programs, and SSL are ineffective in preventing such attacks. Therefore, developer must consider the following points in order to avoid SQL injection attack on web application:

i. Using prepare() function (prepared statements)
ii. Including user input validation statements such as removing the extra special character or string such as –,;, ‘, SHUTDOWN, DROP, or DELETE (from web URL, web form or cookie) while receiving input from the user as such characters could be used to bypass the web filters.

iii. Treating received input from the user as a string instead of a command.
iv. Always keep in check of permission scheme of database, and doing regular checks of all system files for any modification to the system.
v. Configuring the database error messages so that critical information do not get exposed to someone who do not have access rights.

2.2 Broken Authentıcatıon and Sessıon Management Vulnerabılıty Attack and Preventıon

Since HTTP is a stateless protocol, some kind of protocol is required that can keep track of the activities of a particular user using the website and is passed as an argument in the GET or POST query. This is achieved by providing session ID or token to a user when he visits any website [18]. This session id is used to identify that user during the information exchange (HTTP request and HTTP response). The time span of the sessions is kept as short as possible for security purposes. If sessions are not handled properly during the website development, the attacker could use or steal any logged-in user's session id and can obtain the potential privileges. Session ID is usually generated as a random long string so that it becomes difficult for the user to guess the next one [18].

Generally, sessions can be maintained either on server side or on client side depending upon the web application's requirements. While storing session on server is a highly complex process and may result in an increase in latency time, the users' credentials are generally claimed to be much safer as the users' data are not exposed, and the cookie size is kept small. On the other hand, due to the complex nature of server-side session management, most developers prefer storing the session inside the authentication cookie on the client side. However, this common technique generally poses higher risks if the data integrity, authenticity, and confidentiality are not guaranteed.

The website could be vulnerable to session fixation attacks if the sessions and authentication are not handled properly while designing or developing the website. The following Fig. 10 demonstrates the session fixation attack.

Any website is vulnerable to broken authentication and session fixation attack if the following points are not considered:

i. Permits the use of weak password
ii. Permits the multiple failed login attempts
iii. Session ID is visible in the URL
iv. Multi-factor authentication is missing
v. Session ID is not refreshed during the activity
vi. Session id still persists in memory even when the user has logged out, especially when user sign-in using SSO (Single Sign ON that means signing-in by trusting the third party such as login through Google or Facebook)
vii. Using unencrypted communication channel for sending password or session ids/tokens.

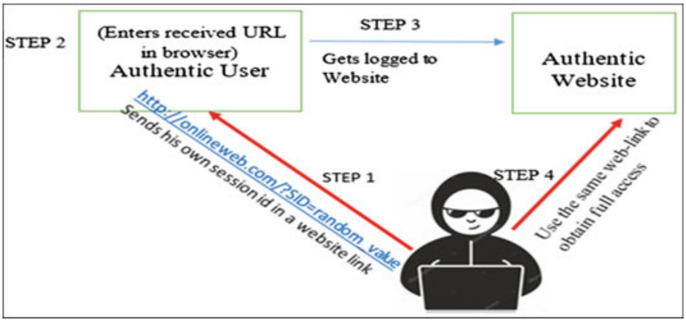

STEP 2
(Enters received URL in browser)
Authentic User
STEP 3
Gets logged to Website
Authentic Website
http://onlineweb.com/?SID=random_value
Sends his own session id in a website link
STEP 1
STEP 4
Use the same web-link to obtain full access

Fig. 10 Sample scenario of session fixation attack

viii. Using weak account recovery algorithms.

Md. Maruf Hassan et al. [15] executed a case study on weak authentication and session management vulnerability in Bangladesh and found out that a total of 267 public (72%) and private (28%) organisations were vulnerable to this attack, i.e. approximately 56% websites among their sample. The intruder can obtain the session id of targeted user using online tools such as Google dork, eat my cookie, or cookie manager.

Following points must be considered to prevent this type of attack:

i. Ensure strong password by adding validation checks.
ii. Limit the failed login attempts and alert the concerned user and the admin regarding the brute-force attempt.
iii. Ensure the shortest life span of each session ID.
iv. Sessions must be shared over the encrypted channels.
v. Use strong hashing and salting algorithm to store passwords in the database such as SHA256 [19].
vi. Better use POST method instead of GET method as it is more secure because it never expose the user's data either through web URL or server logs.
vii. Use strong hashing function to encrypt password.
viii. It is necessary to test all the platforms (such as Google or Facebook) used where sessions are being shared through URL.
ix. Include the option of asking old password while the processing request of changing the password.
x. Ensure the data are not cached in the browser, i.e. back button must not show the previous result in case of banking websites.
xi. Web application firewalls can be used to validate the sessions.
xii. Use SSL certificate.

2.3 Cross-Site Scripting Attack and Prevention

Two-third of all web apps are found to be vulnerable to cross-site scripting attack, also known as XSS attack. The term was first introduced in November 1999 when a group of security researchers heard about the injection of malicious scripts and image tags into the HTML pages of some dynamic websites. After 2 months, in February 2000, they published a report demonstrating the XSS vulnerability. For your knowledge, it was named XSS instead of its short form CSS only to avoid name ambiguity for Cascading Style sheets (CSS). The malicious script is executed on the client side, usually on user's browser. As a result, the communication between the user and vulnerable website is compromised. If a dynamic website is vulnerable to SQLI attack or broken authentication and session management attack, then there is a higher risk that the website will be vulnerable to XSS attack as well. Just like SQLI attack is targeted for SQL-based applications by passing SQL queries, XSS attack is targeted to HTML pages where the intruder injects the malicious code into HTML web pages. It is the most popular technique used by cyber-criminals to steal sessions or to attack a company's entire social network. According to Wikipedia, the most prominent websites such as Facebook, Twitter, and YouTube had also suffered from this attack in the past. The following steps explain the general scenario of attack:

Step 1: Attacker finds a vulnerable website, which allows the injection of untrusted malicious code into its webpage. For example, inserting false advertisements on the web page, displaying false content on the website.

Step 2: Attacker inserts malicious client-side JavaScript/ActiveX/VBScript/HTML code on the web application. This code is either sent to the victim's web browser or the web server depending upon the type of XSS attack.

Step 3: User clicks on the malicious link either while visiting the website or accessing service from the web server.

Step 4: Attacker has access to private credentials or details of the victim through a vulnerable website by bypassing the SOP (Same Origin Policy).

M. Liu et al. [18] conducted a survey on XSS attacks on their local vulnerable test website. The paper illustrated the various risks associated with XSS vulnerability. The risks include phishing attacks, exploitation of user's session id or token id, DoS and DDoS attacks, stealing client's web browser screenshot, and risk of XSS worms on click malicious link.

Germán E. Rodríguez et al. [16] conducted a survey on mitigation of XSS attacks and discovered that 40% of attacks are implemented using XSS technique. The following table illustrates the use of most common attacks with their percentage according to [16] (Table 2).

XSS attacks can be categorised into the following types [18]:

i. Server-side vulnerability

- Persistent XSS
- Non-Persistent XSS

ii. Client-side vulnerability

Table 2 Percentage of occurrence of attacks

Vulnerability attack	Percentage of occurrence (%)
XSS attack	40
SQLI attack	24
Inclusion of local files	4
DDoS attack	3

- DOM-based XSS

Persistent XSS is also known as Stored XSS. In this attack, the malicious script is added directly on the website (especially forms, blogs or comment sections), therefore, it is also known as direct/second-order/type-1/stored XSS attack as the script gets stored on the web server. So, whenever user visits that website, the malicious code gets executed, and hence, it is said to be more harmful than other two types.

If website is vulnerable to this attack, then attacker can execute phishing attack and key-logger attack. In former attack, the credentials of the user are compromised. In later, attacker is able to capture the keystrokes of the user for the vulnerable web page. Attacker can also construct a script to take screenshot of the web page by injecting that script on the website. As a result, personal data or bank balance of victim can be easily exploited. Bind-XSS is one of the types of Persistent XSS attacks. The following steps explain the scenario of stored XSS attack:

Step 1: Attacker posts a message containing malicious script on a form/blog.

Step 2: The script gets stored in the server's database.

Step 3: Victim visits the webpage with malicious content and requests a service.

Step 4: The website displays the content containing the malicious code.

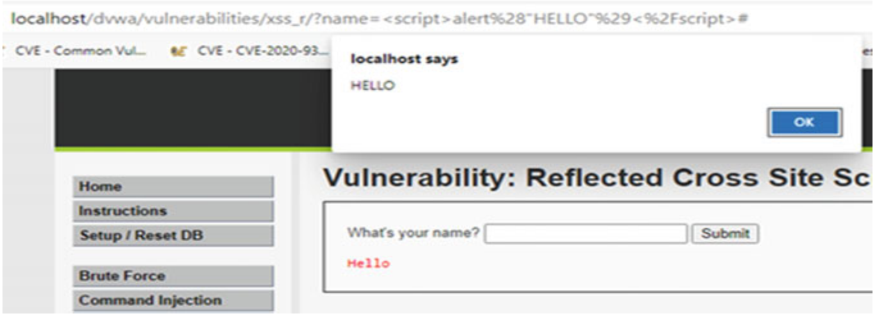
Step 5: Attacker gets complete control over the victim's system.

Non-Persistent XSS attack is also referred as type-II or reflected XSS attack where reflected means that the results of malicious query are visible to the attacker. The attacker crafts the malicious link in such a way that it appears to be from a trusted source. When the victim clicks on the malicious link, web server sends a response including the malicious script to the user. For example, the following figure demonstrates reflected XSS attack when a script query: <script> alert("HELLO") </script> is entered in the name box, it is reflected in the URL (Fig. 11).

DOM-based/type-0 XSS attack is a client-side vulnerability attack where DOM is abbreviated as Document Object Model. DOM is an object model for every HTML webpage. It includes the properties of the HTML page, which allows it to change its' content. So, when DOM-based XSS attack is executed, the JavaScript code is embedded in the client-side program, which allows it to modify the content of DOM and can also change the values of objects' properties, while the user visits the page without malicious link. Since the malicious code executes on victim's computer, server-side detection algorithm would fail to detect this type of attack.

Following points should be considered to prevent XSS attacks:

i. Execution of JavaScript code can be prevented by setting the cookie to HTTPOnly flag.



localhost/dvwa/vulnerabilities/xss_r/?name=<script>alert%28"HELLO"%29<%2Fscript>#

localhost says

HELLO

Vulnerability: Reflected Cross Site Sc

What's your name?

Hello

Fig. 11 Example of reflected XSS vulnerability

ii. Invalid requests can be redirected.
iii. Simultaneous multiple logins to the same account must be detected and session must be declared invalid.
iv. Escaping schemes could be used.
v. Appropriate response header must be used.
vi. Detection should be done at both client side and server side.

3 Conclusıon and Future Scope

In conclusion, with the rise of internet technology, it has become crucial to protect one's data and privacy, where the hackers could use numerous online tools to catch just one vulnerability in website, and if found can put the users' integrity, confidentiality, and authenticity at risk. SQL injection, XSS attack, and broke authentication attacks could put users' privacy at risk. It is suggested to use the artificial intelligence-based detection method to detect a web vulnerability.

Since it has become extremely crucial to protect online resources from being exposed to hackers as new attacks are being carried out every day by hackers, web attacks could be defeated by integrating the detection and prevention techniques using machine learning algorithms.

References

1. Ami, P.V., and Malav S.C., Top five dangerous security risks over web application. Int. J. Emerg. Trends Technol. Comput. Sci. **2**(1), 41–43 (2013)
2. A.M. Shabut, K.T. Lwin, M.A. Hossain, Cyber attacks, countermeasures, and protection schemes—a state of the art survey, in *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*, Chengdu (2016), pp. 37–44
3. K. Nirmal, B. Janet, R. Kumar, Web application vulnerabilities—the hacker's treasure, in *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore (2018), pp. 58–62

4. Hackers target 1 Indian firm over 1,500 times a week, January (2020), https://www.livemint.com/technology/tech-news/hackers-target-1-indian-firm-over-1-500-times-a-week-11580011583037.html
5. 95% of HTTPS servers vulnerable to trivial MITM attacks, March (2016), https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-mitm-attacks.html
6. OSWAP top ten security risks and vulnerabilities (2020), https://sucuri.net/guides/owasp-top-10-security-vulnerabilities
7. Y. Wang, D. Wang, W. Zhao, Y. Liu, Detecting SQL vulnerability attack based on the dynamic and static analysis technology, in *2015 IEEE 39th Annual Computer Software and Applications Conference, Taichung* (2015), pp. 604–607
8. SQL injection, March (2020), https://en.wikipedia.org/wiki/SQL_injection
9. S.A. Faker, M.A. Muslim, H.S. Dachlan, A systematic literature review on sql injection attacks techniques and common exploited vulnerabilities. Int. J. Comput. Eng. Inf. Technol. **9**, 284–291 (2017)
10. L. Ma, D. Zhao, Y. Gao, C. Zhao, Research on SQL ınjection attack and prevention technology based on web, in *2019 International Conference on Computer Network, Electronic and Automation (ICCNEA)*, Xi'an, China (2019), pp. 176–179
11. CWE: common weakness enumeration, https://cwe.mitre.org/data/definitions/173.html
12. J. Ombagi, Time-based blind SQL ınjection via HTTP headers: fuzzing and exploitation, in *Conference: 2017 Strathmore Research Symposium*, At Nairobi, Kenya (2017)
13. A.K. Dalai, S.K. Jena, Neutralizing SQL ınjection attack using server side code modification in web applications. Secur. Commun. Netw. Hindawi **2017**, 12 pages (2017)
14. O.B. Al-Khurafi, M.A. Al-Ahmad, Survey of web application vulnerability attacks, in *2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, Kuala Lumpur (2015), pp. 154–158
15. M.M. Hassan, S. Nipa, M. Akter, R. Haque, F. Deepa, M.M. Rahman, M.A. Siddiqui, M.H. Sharif, Broken authentication and session management vulnerability: a case study of web application. Int. J. Simul. Syst. Sci. Technol. **19**, 6.1–6.11 (2018)
16. G.E. Rodríguez, J.G. Torres, P. Flores, D.E. Benavides, Cross-site scripting (XSS) attacks and mitigation: a survey. Comput. Netw. J. Elsevier **166**, 22 pages (2020)
17. A. Shrivastava, S. Choudhary, A. Kumar, XSS vulnerability assessment and prevention in web application, in *2016 2nd International Conference on Next Generation Computing Technologies (NGCT)*, Dehradun (2016), pp. 850–853
18. M. Liu, B. Zhang, W. Chen, X. Zhang, A survey of exploitation and detection methods of XSS vulnerabilities. IEEE Access **7**, 182004–182016 (2019)
19. Sunardi, I. Riadi, P.A. Raharja, Vulnerability analysis of E-voting application using open web appli-cation security project (OWASP) framework. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **10**(11) (2019)

A Survey of Cyber Security Trends, Emerging Technologies and Threats

Anand Bhushan Pandey, Ashish Tripathi, and Prem Chand Vashist

1 Introduction

The information technology infrastructure, computer networks and digital devices have become the backbone of a society, a country and the world. The deployment of Internet in almost all walks of life has eased every task we do in our daily life but risked the security and privacy of those tasks and the information belonging to those tasks. Internet has changed the lifestyle so much that one wakes up with the start of sharing information on the Internet and goes to bed only after clicking on some links, browsing some information on the web or posting something on social media without any knowledge of how secure his shared information is? The very first thing that clicks into one's mind while discussing cyber world is cyber-crimes and cyber-attacks. The attacks have become so disastrous and frequent today that it costs billions of rupees to safeguard the cyber space from attackers [1].

For a criminal to attack someone's confidential data is much more easy and less risky than physically attacking him, and attacks can be done from anywhere in the world. The malwares that include spywares, viruses, Trojan horses and worms attack a system, and the system is compromised without any clue to the actual owner and the adversary gets the complete access to the confidential information of the legitimate owner [2].

One of the many ways in which a malware attacks the system is, whenever a USB drive is inserted into an infected system, the drive gets infected and every other device in which this infected drive is inserted subsequently gets infected. The malwares can attack any system from servers, end user systems to networking devices. The malware attacks the most vulnerable point of a system including software and hardware, and it's too difficult and expensive task to prevent a large volume of applications and

A. B. Pandey · A. Tripathi (✉) · P. C. Vashist
Department of Information Technology, G. L. Bajaj Institute of Technology and Management, Greater Noida, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_2

data and every point of large network [2]. The easier approach to protect the network and data is to guard the network at its perimeter and using firewalls, which enquires every access to the internal network, and if the access is malicious, the firewall and the antivirus installed reject the access. In spite of emerging technologies, the advancements and sophistications in malwares enable it to exploit the flaws of the technologies and avoid detection.

As the world is heading toward a new decade, the cyber criminals may come up with new techniques and approaches, identifying and neutralizing them will be the new challenge for organizations. What may be the attack vector? Will the criminals try new technologies like Biometrics and Artificial Intelligence or rely on those old conventional methods? The answers to such questions will be of utmost importance. If they are shifting to the biometrics, the security of the information gathered and that of the network authentication token is a serious problem needing a proper solution. If the token is compromised in any circumstances, the cyber criminals may get administrative access to the network creating damage beyond imagination. The drones that are information gatherers may be used for espionage as they can perform physical damage as well as data breaches. As per a recent prediction by Goldman Sachs, more than 17 billion dollars will be spent on drone functionality itself by the businesses in the next 5 years [3].

2 Cyber Security Trends

In spite of organizations' awareness and dedicated efforts toward cyber security, the security breaches and data compromises in many organizations as well as common people's cyber space had created news headlines in 2019. The cyber security trends [4–6] that will be the area of focus in 2020 are:

- "Data breach" remains to be the biggest concern for the organizations as the organizations are very conscious about their image after the data breach is in news. The records show that the flaws in the web applications are mostly responsible for the data breaches making web application security the top priority for organizations.
- "Skill gaps" in the cyber security staff appointed by the organizations along with the shortage of staff makes two out of three organizations' cyber space vulnerable to threats. Therefore, the organizations are relying on security tools like online vulnerability management solutions that make the organization secure even with a small team of security staff.
- "Cloud security" is another very vital issue to resolve as the data are being moved to the clouds; innovative approaches are required to protect that data and the critical infrastructure.
- "Cyber security automation with integration" is required as the cyber security professionals have to do a lot with less staff. Using agile processes, the organizations are easily managing security issues.

- "Awareness of cyber security's importance" is growing speedily, and organizations have realized that maintaining cyber-hygiene is mandatory and vital.
- "Mobile devices" are at risk making the complete supply chain of the organization vulnerable to indirect attacks. Secure web infrastructures and real-time management of vulnerabilities can reduce the risk.
- "State-sponsored cyber-attacks" such as attacks of distributed denial-of-service (DDoS) are sponsored by different countries to steal political and defense secrets; spread misinformation etc. in other countries.
- "IoT devices" are booming today to create automated infrastructure but at the same time, the chances of blunders in the field of cyber security have also increased. Examples are the vulnerable web platforms, insecure wireless networks, unverified updates etc. Any IoT device if compromised will serve as the weak link of the chain and entry point for fatal attacks to the system.
- "Artificial Intelligence", on one side, is helping the cyber experts in dealing with attacks by using machine learning and deep learning technologies to detect threats, on the other side, it is being used by cyber criminals to create sophisticated attack methods and malwares.
- "Phishing threat" can be said to be evergreen threat, as it remains to be the cause of many fraudulent payments, malware spreads and credential compromises.
- "5G Technology" is the future of the cyber word. With the enhance bandwidth provided by 5G technology, the number of devices, the number of sensors and the volume of data are going the explode. The preparations and the performances of the researchers and the organizations are going to decide whether it is a boon or a bane for the society, for the country and for the world.
- "Smart devices" such as smart TV, smart speakers, smartwatches etc. are increasing at the pace more than the pace they can be provided security from cyber threats.
- "Real-time operating system vulnerabilities" were discovered and exposed to the world's cyber research community in 2019 by Armis Labs, which they named "Urgent/11" [6].
- "Butterfly effect of ransomware" may be witnessed as a consequence of the constant bombardment by the attackers. Only the first 9 months of 2019 had seen 600–700 attacks on government agencies through ransomware [3].
- "Cyber Insurance" has become very popular in spite of constant warnings by the governments. However, the effect of such cyber protection cover is contrary to its objective because the attackers are targeting the ensured organizations more frequently as the chances of getting paid are more. Insurance companies generally opt to pay the ransom if the amount of ransom is less than the cost needed to rebuild the network [3]. There are estimates that the cyber insurance market is projected to be 7 billion dollars in the USA alone [3].
- "Certified Threat Intelligence Analyst (CTIA)" program is being used by the security threat analysts to learn the skills of identifying and combating the threats. CTIA is a method-driven program, which covers every aspect from planning to create effective threat reports.

3 Emerging Technologies

The emerging technologies include smartphones, social media, cloud computing, critical infrastructure etc.

3.1 Social Media

The social networking sites that provide its users a platform to connect to people and make friend, share their views, news and events also create the cyber-attack-prone points in the same proportion. The attacker finds out the careless people from the social network and uses them to attack and send spams to the people on his friends list.

3.2 Cloud Computing

The cloud computing concept provides the users' chance to use the services of various resources without spending money and requiring any management skills for the complex infrastructure. The service of account recovery provided by Google to its Gmail users was a compromised denial of service attack [7].

3.3 Smartphone Technology

With the exponential growth in the number of smartphone users, the number of mobile malwares is also growing. The case of cyber threats to the infrastructure of electricity grids to healthcare system, communication system to banking system are also being witnessed in very high proportion.

3.4 Critical Infrastructure

The infrastructure is the backbone of all the secure operations of modern-day society and is vital to national security, business and financial activities. This infrastructure is the lifeline for security of the cyber space of the country.

3.5 Internet of Things (IoT)

The Internet of Things (IoT) is one of the growing technologies that use the Internet or Internet like network to establish a connection among various intelligent IoT devices. IoT devices include the devices for a remote dashboard, for control, for servers, for routing or bridge device, and sensors [8]. These smart IoT devices are equipped with advanced functions and features to communicate over the Internet via some wireless protocols. In recent studies, the rapid growth of IoT technology has been encountered in different domains especially in the field of smart automation and Robotics.

3.6 Embedded Systems

These are the systems used to automate mechanical and electrical machines from Mp3 players, DVD players, refrigerators to ATMs, bar code readers, power grids, railways, airways etc. most of these machines need hard real-time or soft real-time constraints to meet their target outputs and any deviation may lead to devastation results.

4 Malwares

The malwares today are used to steal the confidential information of government organizations, corporate world and that of an individual but initially, malwares were used to check and enquire the security feature and loopholes in the protection layer of an application [2]. Another area in which the malwares are frequently being used is to get control of victim’s computer and display some unauthorized advertisement. For most of the attackers in cyber world, Trojans are the favorite malwares of the cyber criminals. The studies show that more than 75% of the cyber-attacks to steal information and network intrusion to take control of the network are through Trojan malwares. The malwares are spread using the following activities as vehicles for transportation.

4.1 Spams

The victim receives unwanted and inappropriate messages in his inbox without his consent, and the attacker does it all anonymously that too without any expense. The most common spams today are the email spams in which the inbox of the victim is flooded with unsolicited messages [9].

4.2 Phishing

It is a masquerading attack performed to acquire confidential information by deceiving the users into visiting malicious web pages claiming to be legitimate. The private information shared by an unsuspecting user is then used for criminal activities [10]. The phishers are using innovative techniques as the user is becoming knowledgeable and smart. The phishers send emails containing links to some fake malicious websites claiming to be legitimate organizations or use misspelled URLs to deceive the users to acquire their private information [11].

4.3 Web Downloads

The attackers use it as a speedy spread method for malwares. When user visits a website and clicks on some pop-up window, or as hidden downloads from some very popular websites, the malwares are injected into user's computer system. In most of the situations, the attacker sends spam messages to the user having links to malicious web pages and lures him to visit his malicious website, as soon as the user opens the website, the malware is automatically downloaded and installed on his machine without any clue to the user [12].

5 Emerging Threats

The emergence of new technologies has provided the cybercriminal variety of vulnerable points to attack, i.e., the emerging technologies have paved the way of emerging threats. Here, we discuss the emerging technologies and the threats to those technologies.

5.1 Social Media and Threats

Today, different social media platforms have mushroomed on the Internet, and each platform is flooded with millions of users of it. Twitter and Facebook are the most popular social media platforms with billions of active user accounts around the globe and have become the new communication platforms for new generation. The cyber attackers are using this platform to inject threats to the user's machines and as the users submit a lot of their confidential as well as personal details to these platforms, once the machine is compromised, all this information is revealed.

As per a report of Sophos, an IT security organization, most of the companies are worried that their employees share lots of their personal information with social media platforms, and there is an alarming increase in attacks on social media websites [13]. Koobface worm [14] was the worst case of social site attack by malwares, which used its Zombie arsenal to create new fake social media accounts to be friend with unaware users. Thomos and Nicol [14] discovered the inefficiencies of the social media websites in blacklisting the malicious websites using their blacklisting services. The other malware attack is on unused accounts of Facebook and Twitter and most of the time spread malwares by clicking and following the account of clueless users. In some cases, the malwares spread when the user clicks on "trending" topic contents [15]. Social sites are new and easy targets today for a number of organizations to seek user data, some firms use these data with legitimate intentions and some for malicious purposes.

5.2 Cloud Computing and Threats

If we talk about recent times, the cloud computing is the greatest technological paradigm shift [7]. The companies whether small or large are using the IT services provided by the cloud instead of using their own IT infrastructure and resources. The cloud computing possesses different characteristics like on-demand service, location-independent resource pooling, measured service, ubiquitous network access and rapid elasticity [7]. The users can assign themselves more resources through on-demand service without any human intervention. Resource pooling means every resource is shared between multiple users needing that resource. The measured service is the characteristic of cloud computing, which facilitates the users to pay according to their consumption of different services. Rapid elasticity means the capability of locating and releasing the resources as rapidly as needed.

The services offered by cloud computing may be grouped into the following categories: Platform as a Service (PaaS), Software as a service (SaaS) and Infrastructure as a Service (IaaS) [16]. IaaS provides virtual infrastructure components like storage, operating systems and virtual machines to run applications [16]. Programming environments access additional building blocks through PaaS category of services. Application software are enabled and provided through SaaS. Through multi-tenancy feature, a query rewriter is employed by salesforce.com at database level whereas at hardware level, hypervisors are used by Amazon. As the clients use the services provided by different service providers, the most important issue is to ensure that these services are secure and well protected. The active research area in cloud computing is policy integration and trust management where cloud providers control and manage the data and services of the users. The policy integration addresses the issues of secure interoperability, policy-evolution management and semantic heterogeneity.

5.3 Smartphones and Threats

As the smartphones are carried by an individual throughout the day, its computational capability and mobility can be used to organize work and lifestyle. The exponentially growing number of smartphone users indicates the critical requirement of smartphone security measures. As people store a lot of their personal but sensitive as well as confidential information in smartphones, it has become source of risk and the smartphones have become new targets of attack for cyber criminals [17]. The design-related flaws in the infrastructure for mobile communication and management are exploited by the cyber criminals to attack and peep into the encryptions of smartphones. In most of the cases, the criminals attack the system through Wi-Fi networks to steal the personal information of the users. A worm known as Cabir spreads through Bluetooth network and is another point of concern that needs to be addressed. The mobile software is also having some flows that are exploited by criminals to spread malwares, one example is the web browser.

There are reports that special malwares have been created in last couple of years to attack the the smartphones [18]. To address this all, a centralized market place is offered by companies, which helps remove any malicious application before it is installed, for example Apple offers App Store to install application to iPhone devices, Android too offers a market place to install applications for android users and removes malicious applications from the smartphones and marketplace based on user complaints [19] Sandboxing is another approach used by companies to prevent the processes from interaction avoiding the damages done by interactions.

5.4 Critical Infrastructure and Threats

The infrastructure is the backbone for all the communications, processes and activities. The complexity of interconnection of the infrastructure makes it very hard to protect it from attacks. The nature of the infrastructure is the recent area of research, which includes self-diagnostic techniques and self-healing system that automatically responds and recovers from any attack [20]. The communication, transport, public health, finance, oil and gas etc. are the areas that are part of critical infrastructure and nowadays are facing maximum threats.

In case of wars between countries, these are the very first targets of enemies. Cyber war is the attack by a nation on other nation's cyber space, networks or computer systems to harm them or only to create disruptions. This is the most fatal attack for a county as it can damage its security and security infrastructure [21]. A country must test and update its critical infrastructure and cyber defense system for possible threats to find the loop holes and eliminate them periodically. Advanced mitigation threats are the recent fatal threats to the critical in restructure, a multi-stage Bayesian [22] concept has been proposed that uses the incompleteness of the information of the advanced mitigation threats to counter such attacks by learning the nature of attacks and planning defensive strategies.

5.5 IoT and Threats

The attacks on sensors and embedded systems are the most fatal and sophisticated cyber threats today. Today Google, Apple and Cisco, the major ICT players take significant business decisions so as to make their position in IoT landscape [23]. The core business focus for telecom operators is machine to machine communication, and hence, the Internet of Things has shown a significant growth in the number of connected devices. The future of IoT is with other technologies like cloud computing, Big Data, Semantic technologies and Robotics. In future, the web platform of smart environments and connected devices would be integrated with the Internet of things today to make smart web of everything to support the changes in the society and the growth in economy.

Cyber security will pose a major challenge to IoT technology as with the passage of time number of IoT devices will grow to trillions. In the development of smart cities, many projects have been initiated worldwide. Likewise, the same effort has been seen in home automation. Diverse facilities and services are provided by automated homes to homeowners [24]. These services include less energy consumption, optimization of water consumption, home security service, effective use of home appliances etc. This is only possible because the smart devices are controlled by a smartphone or any other device on the network.

Recent research shows that a very high percentage of consumers have no confidence on the security mechanisms of IoT devices. The heterogeneous nature of the data as well as the devices in any IoT infrastructure is the challenge that makes it tough to provide a common security solution for any IoT deployment [25]. As the devices in IoT are connected through Internet, hence any malware threat to Internet creates a fatal threat to the devices related to healthcare, home security, business, finance and military. The solution to IoT threats includes mutual authentications and the use of new artificially intelligent machine learning tools that will detect security breaches and respond accordingly to recover [24].

5.6 Embedded Systems and Threats

Today, most of the embedded system-driven machines are on some network or on Internet itself so recent challenges to researchers include the security of the electronic devices having embedded integration circuits [26]. If the chip of such electronic devices is attacked with malicious intentions, the function of the system monitored by these devices may be affected to give fatal outcomes [27]. The Trojan malwares that are used to attack such electronic devices to alter their goals are hardware Trojans and hence are very tough to detect and eliminate. The embedded systems are the lifeline for most of the automated mechanical and electrical machines but if the security of such systems is compromised, the damages may be beyond imagination.

Cyber security experts are of the opinion that the year 2020 is going to invite the most complex and sophisticated threats that the cyber world has ever seen. Some of the threat types that the researchers have to face in the times to come are described and compared in terms of spread methods and target systems or environments. Table 1 shows the different kinds of emerging threats.

6 Current Scenario

The research shows that today most of the organizations are capable of direct attack prevention and are focusing on the new battleground created by the indirect attacks such as the attacks on the third parties and those on the vendors in the supply chain. The cyber resilience that uses cyber security and enterprise resilience in tandem offers the capability of quick response to the posed threats, which increases customer trust.

The Accenture Third Annual State of Cyber Resilience Report, 2020 [30] says that two types of organizations are there, the first group covers 17% of the organizations that are in elite group, and they have achieved a very high level of security innovations and the cyber resilience. The other group that covers 74% of the organizations, is a group of average performing organizations. The remaining 9% are bad performers as for as their security infrastructure and security budget are concerned. While the elite group is working on the improvements, the second group is following the path shown by the leaders of elite group. Some of the observations [30] of this report are:

- In the last 3 years, the number of organizations that allocate 20% of their IT budget in technology advancements has doubled.
- A decline of 27% in security breaches and 11% in direct attacks is reported in the last 3 years of time span.
- Out of the security breaches during the last 3 years, 40% were indirect attacks that too on some weak link of the supply chain.
- Sixty-nine percent believe that an unsustainable cost is being paid for staying a step ahead of the attackers in the battle going on between the organization and the attackers.

7 Conclusions and Directions for Future Research

Analyzing every aspect of the current cyber security trends, evolutions of cyber security techniques and technological assistance to it, the past, the present and the future of the threats, the conclusions can be presented under the following points:

Table 1 Emerging threats

Serial number	Threats/Malwares	Descriptions	Target systems/Environments
1	Cloud network vulnerability [28, 29]	Cyber criminals may target public clouds and any untrained employee may trigger any number of such vulnerabilities in the network	The organizations that lack tiered security programs of access
2	Ransomware and micro ransomware [3, 29]	It is the fastest-growing attack and aims at vulnerabilities, which are different from general malwares and easy to attack The emails are the biggest vehicle for ransomware spread	It can attack the industries that use the consumer data as an asset. Ex: Healthcare, POS Systems etc.
3	IoT Botnets [6]	The legion of bots was already created in leaked Merai Code 2016 are going to expand with the expansion of IoT technology	Even the systems with machine learning capabilities can be a victim of this attack
4	Polymorphism and PowerShell [30]	PowerShell manipulation is being included in malware tool kits by APT groups. The polymorphic malwares like Qbot can change its signatures	Most of the small companies
5	Third party breach [6]	Hackers use third parties, i.e., indirect attacks to attack the target and sanitize their trail after the attack making it difficult to follow	The organizations that are doing business by sharing their digital space and security features
6	AI tools [28, 29]	AI tools may be employed by hackers to consistently scan and attack the targeted system	The companies not having the staff and security technology to ward off the attacks that change their form consistently
7	Network security risk [29]	The hackers wait for the digital and cyber space expansions by the organizations to exploit	The organizations expanding their digital ecosystem and cyber space

(continued)

Table 1 (continued)

Serial number	Threats/Malwares	Descriptions	Target systems/Environments
8	Email network security risk [29]	The organizations do not take the vulnerabilities created by wireless networks, seriously making the email vulnerability fatal	The organizations having untrained employee who clicks on phishing mail
9	Attacks on Windows subsystem for Linux (WSL) [30]	WSL is the latest technology shipped out with windows 10 and is going to be the favorite target of the attacks in 2021	Environments going for updates to Windows 10
10	Search result Hijack [5]	The search engines personalize the searching behavior of an organization and the hackers may try to hack the behavioral patterns of the organization's search results Search result tempering may lead to showing malicious site and directing to that site. Once the site is opened any security compromise may result in	Any organization big or small
11	Malwares in mobile devices [5]	These are the malwares specially developed for mobile devices to access confidential information of the user such as passwords of banking apps etc. Studies show that out of all smartphone phone users about 35% use it for financial activities	Online payment Apps Ex: Banking Apps etc

(continued)

- The reason for the flooding in cyber threats is that the attacker connected to the cyber world can be anywhere in the world geographically, while attacking the target.
- With the revolutionary developments in technology and security algorithms, the nature and techniques of the threats have also changed with same or more pace.

Table 1 (continued)

Serial number	Threats/Malwares	Descriptions	Target systems/Environments
12	Remote Code Execution (RCE) attacks[6]	It is estimated that about 20 billion IoT devices on the Internet or other similar networks are prone to remote code execution (RCE) attacks	IoT devices
13	Smishing [5, 29]	The increase in online communications and interactions, the favorite target point of the attackers may shift from e-mails to online interaction platforms	WhatsApp, LinkedIn etc
14	Latest threats [5, 29]	Generally, the organizations respond to the attacks but the industry security systems should be proactive in facing the latest threats	Any organization big or small

- The introduction of the latest technologies such as Cloud Computing, IoT, Embedded systems, Social media and many more has created new battle grounds for the researchers and the criminals.
- The new technologies like Artificial Intelligence, Machine Learning and Deep Learning are very effectively and efficiently being used by cyber criminals too.
- Going through the history of the attacks and threats, it can be concluded that the cyber criminals have focused more and more on the technologies of transportation and distribution of the malwares as compared to the malware itself.
- Safety and security of the critical infrastructure is the focus of the researchers today as it is going to be the territory for a new war, i.e., the cyber war.

Thus, the conventional security measures are not going to work in future, as the Internet and Internet-connected devices are exponentially growing. The number of IoT smart devices is going cross 75 billion as per an estimate, creating an explosive situation in terms of the number and frequency of attacks [6]. This speedy growth of the Internet requires smart and innovative approaches to curb the threats. The scale of the infrastructure and the innovations in the security attacks are the major areas of concern for future research. The introduction of 5G technology will bring the newer scopes of threats, and hence, the researchers need to focus on this aspect of the technological development as well.

The reports show that most of the reputed organizations are capable enough to prevent and safeguard their cyber space from direct attacks, i.e., the attacks made on their digital space or web space directly, so the cyber-criminals are now trying to reach their digital space though weaker links in the supply chain of which they are part of. The researchers must try to address such indirect attacks and treat the cyber space of all the organizations, i.e., third parties in the supply chain as a cyber-village.

References

1. V. Benjamin, H. Chen, Securing cyberspace: identifying key actors in hacker communities, in *IEEE International Conference on Intelligence and Security Informatics* (2012), pp. 24–29
2. G. Cluley, Sizing up the malware threat–key malware trends for 2010. Netw. Secur. **2010**(4), 8–10 (2010)
3. Source. https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020
4. Innovate for Cyber Resilience
5. Cybersecurity Trends,
6. Cybersecurity Threats
7. D. Zissis, D. Lekkas, Addressing cloud computing security issues. Futur. Gener. Comput. Syst. **28**(3), 583–592 (2012)
8. S. Madakam, V. Lake, V. Lake, V. Lake, Internet of Things (IoT): a literature review. J. Comput. Commun. **3**(05), 164 (2015)
9. Y.Y. Chen, S.P. Yong, A. Ishak, Email hoax detection system using Levenshtein distance method. JCP **9**(2), 441–446 (2014)
10. M. Khonji, Y. Iraqi, A. Jones, Phishing detection: a literature survey. IEEE Commun. Surv. Tutor. **15**(4), 2091–2121 (2013)
11. I. Qabajeh, F. Thabtah, F. Chiclana, A recent review of conventional vs. automated cybersecurity anti-phishing techniques. Comput. Sci. Rev. **29**, 44–55 (2018)
12. L. Xu, Z. Zhan, S. Xu, K. Ye, Cross-layer detection of malicious websites, in *Proceedings of the Third ACM Conference on Data and Application Security and Privacy* (2013), pp. 141–152
13. C. Oehri, S. Teufel, Social media security culture, in *2012 Information Security for South Africa* (IEEE, 2012), pp. 1–5
14. K. Thomas, D.M. Nicol, The Koobface botnet and the rise of social malware, in *2010 5th International Conference on Malicious and Unwanted Software* (IEEE, 2010), pp. 63–70
15. Y. Altshuler, Y. Elovici, A.B. Cremers, N. Aharony, A. Pentland (eds.), *Security and Privacy in Social Networks* (Springer Science & Business Media, 2012)
16. Q. Zhang, L. Cheng, R. Boutaba, Cloud computing: state-of-the-art and research challenges. J. Internet Serv. Appl. **1**(1), 7–18 (2010)
17. C. Kasmi, J.L. Esteves, IEMI threats for information security: remote command injection on modern smartphones. IEEE Trans. Electromagn. Compat. **57**(6), 1752–1755 (2015)
18. D. He, S. Chan, M. Guizani, Mobile application security: malware threats and defenses. IEEE Wirel. Commun. **22**(1), 138–144 (2014)
19. Z. Fang, W. Han, Y. Li, Permission based Android security: issues and countermeasures. Comput. Secur. **43**, 205–218 (2014)
20. A. Zimba, Z. Wang, H. Chen, Multi-stage crypto ransomware attacks: a new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express **4**(1), 14–18 (2018)
21. C.J. Finlay, Just war, cyber war, and the concept of violence. Philos. Technol. **31**(3), 357–377 (2018)
22. L. Huang, Q. Zhu, Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks. ACM SIGMETRICS Perform. Eval. Rev. **46**(2), 52–56 (2019)
23. S. Sezer, T1C: IoT security: threats, security challenges and IoT security research and technology trends, in *31st IEEE International System-on-Chip Conference (SOCC)* (IEEE, 2018), pp. 1–2

24. F. Meneghello, M. Calore, D. Zucchetto, M. Polese, A. Zanella, IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. **6**(5), 8182–8201 (2019)
25. W. Zhou, Y. Jia, A. Peng, Y. Zhang, P. Liu, The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J. **6**(2), 1606–1616 (2018)
26. B. Yuce, P. Schaumont, M. Witteman, Fault attacks on secure embedded software: threats, design, and evaluation. J. Hardw. Syst. Secur. **2**(2), 111–130 (2018)
27. C. Paar, Hardware trojans and other threats against embedded systems, in *Proceedings of the ACM on Asia Conference on Computer and Communications Security* (2017), p. 1
28. Source. https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf
29. Source. https://securityintelligence.com/articles/these-cybersecurity-trends-could-get-a-boost-in-2020/
30. Source. https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET_Trends_Report_2019.pdf

Identifying Key Strategies for Reconnaissance in Cybersecurity

V. Vishnu and K. Praveen

1 Introduction

The Internet creates an opportunity for offenders to carry out different types of attacks. Public service transparency and anonymous internet connectivity are improving those attacks. Cyber-attacks cost US$ 114 billion per year, according to the Symantec cybercrime study released in April 2012. If indeed the time lost by companies attempting to recover from cyber-attacks is counted, the overall cost of cyber-attacks will exceed US$385 billion [1]. Cyber-attack victims are also rising significantly. Symantec's study, in which 20,000 people in 24 countries were interviewed, revealed that 69% were the victim of a cyber-attack in their lives. Symantec also estimated that 14 people are the targets of cyber-attacks every second [1]. How do cyber threats thrive? It's because cyber-attacks are less costly, easier and involve lesser risk than physical attacks. Cyber attackers only need a few resources besides a computer and an Internet connection. They are unaffected by geography and space. They are difficult to track and prosecute because of the open and anonymous nature of the Internet. Considering that attacks on IT infrastructure are very enticing, it is expected that the number and severity of cyber-attacks will continue to increase.

Cybersecurity is built to protect the digital assets of the company from ever-growing cyber-attacks. Cybersecurity can be achieved by the introduction of adequate security controls that include many security features, such as cybercrime deterrence, prevention and identification. Cybersecurity's primary purpose is to provide data and

V. Vishnu (✉) · K. Praveen
TIFAC-CORE in Cyber Security, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India
e-mail: cb.en.p2cys18029@cb.students.amrita.edu

K. Praveen
e-mail: k_praveen@cb.amrita.edu

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_3

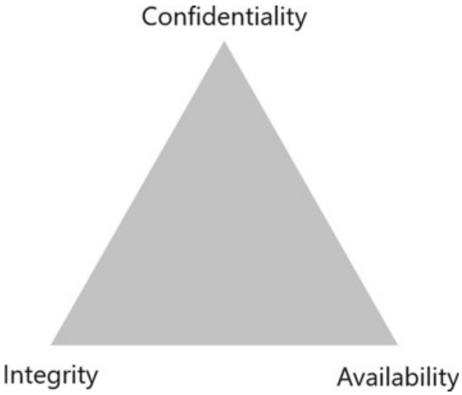


Fig. 1 The CIA triad

services with confidentiality, integrity and availability (CIA), sometimes referred to as the CIA triad (Fig. 1).

Attackers begin by gathering all types of data for a successful attack. Reconnaissance is one of the very first steps that attackers use to obtain information. Advanced port scanning techniques are accessible via free open-source software that provides a wealth of network information. This useful information includes port status, device types and variants, operating systems and service packages. Attackers are likely to succeed in combining information about vulnerable facilities with reconnaissance data. Social engineering is a technique of deception that uses human error to gain sensitive information, access or useful Intel. These "human hackers" scams in cybercrimes appear to attract unsuspecting users to reveal data, to spread malware or to give them access to restricted systems. Attacks can occur online, in-person and through other interactions. Social engineering schemes are based on how people think and behave. Once an attacker knows what motivates a user's actions, it can successfully trick and exploit the user. Unpatched software is terminology for defining a computer code with known vulnerabilities. Once security bugs occur in the computer code, software developers write add-ons to the code known as "patches" to fix the security gaps in the code. Running unpatched software is dangerous because hackers are well aware of vulnerabilities until they appear. Advanced Persistent Threats (APT's) typically involve multiple stages, including network hacking, the avoidance of tracking, the development of a strategy to target and monitor company data, the collections and exfiltration of confidential company data, to decide when the required information is most available. Advanced persistent threats have resulted in many massive, expensive privacy violations and are proven to be unnoticeable by traditional security assessments. Advanced persistent attacks are now becoming more and more common as cybercriminals try advanced techniques to accomplish their objectives. There have been a number of qualitative efforts to model a cyber-attack. As highlighted in Fig. 2, the most prominent of them is Lockheed Martin Model, which introduces the notion of a cyber-attack kill chain, describing sophisticated attacks, such as Advanced Persistent Threats (APTs), in seven steps: reconnaissance, weaponization, delivery,

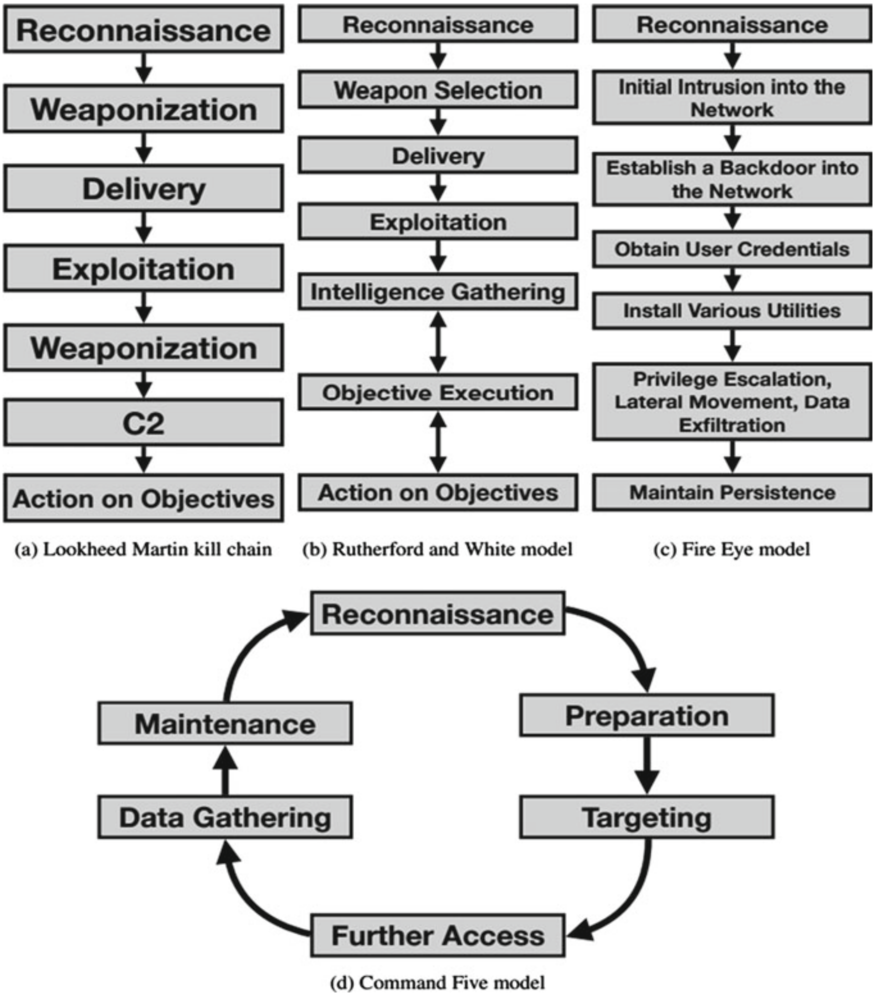


Fig. 2 Models for describing cyber-attacks: **a** Lockheed Martin cyber kill chain; **b** the Rutherford and White variant of the cyber kill chain model; **c** Fire Eye model; and **d** the Command Five Pty Ltd attack model [2]

exploitation, installation, command and control and act on the objective. Rutherford and White improved the model by adding intelligence gathering. Researchers at FireEye and Command Five introduced their own models to describe and model a cyber-attack.

2 Background

Confidentiality is securing resources from unwanted or illegal access, integrity is ensuring that data remain unchanged, availability ensures that data are available without any drop in access, non-repudiation ensures no one can deny another person any service and authentication ensures people with proper access is only allowed access. These features are the cornerstone of any security system and are better known as the five pillars of information security. We can consider a cyber-attack as an assault that breaches any of the pillars. The attacker, thus, tries to breach one or more of the pillars or to attack a targeted system as successfully as possible. The objective might be a host, a network or a major infrastructure of information systems [3].

2.1 Anatomy of a Typical Cyber-Attack

Reconnaissance. The first step where the attacker begins by learning and understanding the details of an organization and network and to identify online behavior of key people of the organization, typically the system architect and network administrator.

Information Enumeration. Enumeration is characterized as the process of listing of usernames, hostnames and IP addresses, network resources and devices used, the operating systems and network topology. The attacker creates an active connection and conducts guided queries to get to know the target and collect more information. These collected data will contain all the security vulnerabilities or weaknesses present in network and attempts to exploit them during the exploitation point.

Network and System Penetration. The attacker is now trying to penetrate the network and the infrastructures once they have access to the network. This can occur in several ways. The attacker can record keystrokes using a malware called keylogger to capture important information entered by a user like a password, or the attacker can plant a worm and leave. The worm will be able to spot vulnerable systems and start spreading across the entire network. They expect the attack to continue as long as the attacker wants to until detected. It could be months or years. A modern vector for attackers is cloud-based data storage. With large-scale adoption of this technology, there has been an increased lack of security features [4]. Basic Role-Based-Encryption schemes have not been implemented. This gives an attacker more data to play with.

Data Exfiltration. Once the attacker has penetrated the system, he has to transfer the data to his system. Any unauthorized transition of data is data exfiltration. Whether data are stolen from a printer or a thumb drive, it's a rather real threat to corporations. Attacks can be performed manually by an authorized person who has access to enterprise systems or by malicious external actors who have access to them. Exfiltration of data can be a big business for cybercriminals and a big problem for any organization that is attacked.

Attack Sanitation. This is the last process of an attack where an attacker cleans up. All evidence of the attackers' presence is removed from the network and host systems to look like nothing has happened.

2.2 Cyber Kill Chain

Lockheed Martin, an American defense company initially authored the Cyber Kill-Chain Framework for Cyber Intrusion Identification and Prevention as part of its information and intelligence-driven defense and security model. The model defines what adversaries need to accomplish in pursuit of that goal by targeting the network, exfiltration of data and maintaining persistence within the organization. This model essentially implies that stopping adversaries at any step in the kill chain breaks the sequence of attack. Attackers must make full headway through all steps of the kill chain to complete a successful attack. The outcome is an inescapable phase where all attacks last, and thus stopping them at this stage massively improves the potential of busting any cyber-attack. When stopped in the early stages of the chain, the speed of success will be enhanced. Moreover, any threat, and therefore its traces, could be an opportunity to learn more about the attackers, their methodology and use their resistance to improve security systems. A far more realistic configuration of defenses results in a greater understanding of enemies and their directions [5]. The Cyber-Kill Chain proposes that the attackers will take six specific steps to try their attacks: Reconnaissance: This stage may where attacker employs the process of target selection, the classification of organizational information, organizational rules and laws, information on the organization's technological preference and topography, social network behavior of the employees or mailing lists available on a public repository. Weaponization and Packaging: In this stage, the attacker employs several forms: internet-facing application and thin client penetration, licensed and publicly available resources or modified software (licensed by the organization or modified to suit their purpose), enterprise software bugs like an XML parser or a word processor spreadsheets and presentation software which makes use of macros, target the most common sites used by the employees and set up phishing sites. Usually, they are equipped with information on duplicitous or accurate objectives. Delivery: The payload is supplied either by the victim (for example the browsing of a malicious site that leads to a malware deployment). The supply of ransom software, or the opening of fake PDF documents, or an intrusion (SQL or network access exploit) is triggered. Delivery: After delivery to the user, computer or device, the malicious payload will compromise the targeted asset and therefore the environment will become an initial foothold. This will be generally achieved by exploiting a security flaw that already has a patch. Although zero-days are exploited, in most cases, adversaries do not need to perform them as most of the targets will already be affected.

3 Tool Selection

The goal of this research is to assess the features of free/open source reconnaissance tools developed by independent researchers. Open-source software is a type of computer software in which source code is released under a license in which the copyright holder grants users the rights to use, study, change, and distribute the software to anyone and for any purpose [3]. The following research process was adopted for the assessment:

- The selection of the most used reconnaissance tools.
- The assessment and evaluation criteria are defined solely based on the ease of use, availability of a graphical interface and the number of features it provides.
- The execution of the tool.
- The analysis of the output generated by each tool.

3.1 Reconnaissance Frameworks: A Comparison and Study of Open-Source Automated Recon Tools

We searched the GitHub repository, one of the biggest sources for open source projects, with the goal of selecting the five most common free/open source tools to be evaluated. We used keywords such as "Automated", "Reconnaissance" and "Cyber". We further filtered the search results using the following filters:

- The last update or commit is after 2016.
- OS independent, i.e. compatible with both Windows and Linux
- Makes use of OSINT for data collection.

In total, there were 264 public repositories on GitHub matching the above keywords. Using the inclusion filters and sorting by the most downloaded, we shortlisted the following five tools:

- Osmedeus
- AutoRecon
- AutoReconR
- InstaRecon
- InstaRecon.

For the assessment, only key functionalities of each framework are addressed, and no additional plug-ins are considered.

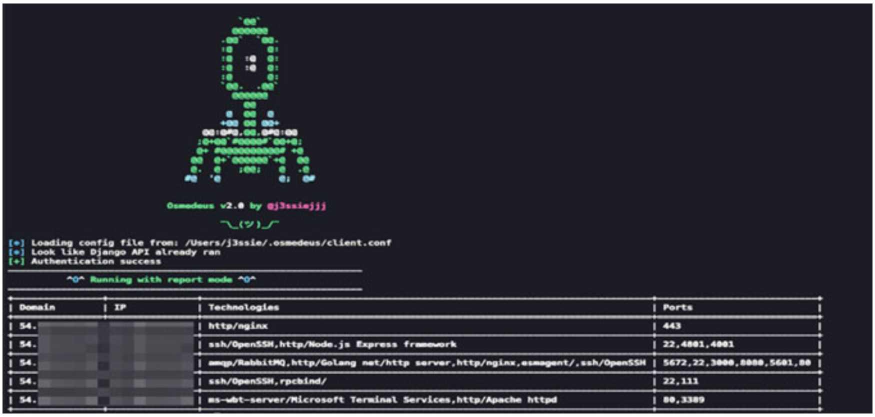
3.2 Evaluation Criteria

To evaluate the tools, we consider the following features.

- IP Recon: These tools are used to perform reconnaissance and gather information about the network the host is connected to.
- Social Engineering: This technique involves looking for reasoning to gain sensitive information or text by stimulating an individual mind or sense of social norms.
- Threat Intel: Cyber threat intelligence is information about risks and threat actors helping to prevent dangerous cyberspace incidents. Information outlets for cyber threats include open source information, social networking intelligence, human intelligence, digital intelligence, or deep and dark web intelligence.
- Forensic Tools: Tools used to investigate and gather evidence from various sources like an image file, audio file or even a sound file.

3.3 Evaluation Results

- Osmedeus is an open-source tool developed by a security researcher called @j3ssie. It is developed using a python client and Django API server. It can be used to scan the vulnerabilities of the target network and server. It features an impressive collection of tools such as web technology detection, IP discovery, and machine discovery. You can split the workspace to store all the scan data and logging information. Finally, it facilitates continuous scanning and allows you to access the scan report from the command line [6]. It is also loaded with web-based technology tracking, IP discovery, and system discovery backtrack features. The framework will split the workspace to store all scan data and log information. Eventually, it can support continuous scanning and allow you to view the scan report from the command line (Fig. 3).
- AutoRecon, developed by Tib3rius is an automated recon tool, which is capable of running multiple threads. This means that it can perform simultaneous network

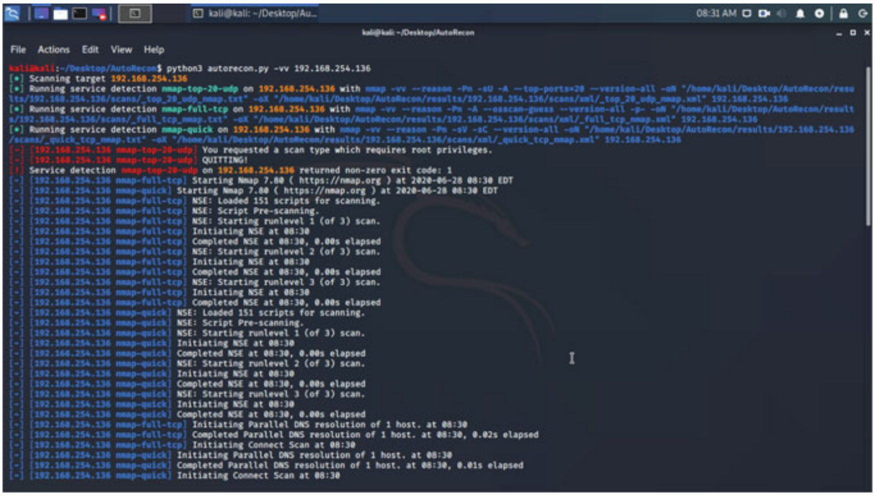


```
                    Osmedeus v2.0 by @j3ssiejjj

                             ¯\_(ツ)_/¯

[*] Loading config file from: /Users/j3ssie/.osmedeus/client.conf
[*] Look like Django API already ran
[+] Authentication success
-----------------------------------------------------------------------
         ^O^ Running with report mode ^O^
-----------------------------------------------------------------------
+-------------------+-------------------+------------------------------------------------------------------+-----------------------------------+
| Domain            | IP                | Technologies                                                     | Ports                             |
+-------------------+-------------------+------------------------------------------------------------------+-----------------------------------+
| 54.[redacted]     | [redacted]        | http/nginx                                                       | 443                               |
+-------------------+-------------------+------------------------------------------------------------------+-----------------------------------+
| 54.[redacted]     | [redacted]        | ssh/OpenSSH,http/Node.js Express framework                       | 22,4001,4001                      |
+-------------------+-------------------+------------------------------------------------------------------+-----------------------------------+
| 54.[redacted]     | [redacted]        | amqp/RabbitMQ,http/Golang net/http server,http/nginx,esmagent/,ssh/OpenSSH | 5672,22,3000,8080,5601,80 |
+-------------------+-------------------+------------------------------------------------------------------+-----------------------------------+
| 54.[redacted]     | [redacted]        | ssh/OpenSSH,rpcbind/                                             | 22,111                            |
+-------------------+-------------------+------------------------------------------------------------------+-----------------------------------+
| 54.[redacted]     | [redacted]        | ms-wbt-server/Microsoft Terminal Services,http/Apache httpd      | 80,3389                           |
+-------------------+-------------------+------------------------------------------------------------------+-----------------------------------+
```

Fig. 3 Osemedus [7]


kali@kali: ~/Desktop/Au...
08:31 AM
kali@kali: ~/Desktop/AutoRecon
File Actions Edit View Help

```
kali@kali:~/Desktop/AutoRecon$ python3 autorecon.py -vv 192.168.254.136
[*] Scanning target 192.168.254.136
[*] Running service detection nmap-top-20-udp on 192.168.254.136 with nmap -vv --reason -Pn -sU -A --top-ports=20 --version-all -oN "/home/kali/Desktop/AutoRecon/resu
lts/192.168.254.136/scans/_top_20_udp_nmap.txt" -oX "/home/kali/Desktop/AutoRecon/results/192.168.254.136/scans/xml/_top_20_udp_nmap.xml" 192.168.254.136
[*] Running service detection nmap-full-tcp on 192.168.254.136 with nmap -vv --reason -Pn -A --osscan-guess --version-all -p- -oN "/home/kali/Desktop/AutoRecon/result
s/192.168.254.136/scans/_full_tcp_nmap.txt" -oX "/home/kali/Desktop/AutoRecon/results/192.168.254.136/scans/xml/_full_tcp_nmap.xml" 192.168.254.136
[*] Running service detection nmap-quick on 192.168.254.136 with nmap -vv --reason -Pn -sV -sC --version-all -oN "/home/kali/Desktop/AutoRecon/results/192.168.254.136
/scans/_quick_tcp_nmap.txt" -oX "/home/kali/Desktop/AutoRecon/results/192.168.254.136/scans/xml/_quick_tcp_nmap.xml" 192.168.254.136
[-] [192.168.254.136 nmap-top-20-udp] You requested a scan type which requires root privileges.
[-] [192.168.254.136 nmap-top-20-udp] QUITTING!
[!] Service detection nmap-top-20-udp on 192.168.254.136 returned non-zero exit code: 1
[-] [192.168.254.136 nmap-full-tcp] Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-28 08:30 EDT
[-] [192.168.254.136 nmap-quick] Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-28 08:30 EDT
[-] [192.168.254.136 nmap-full-tcp] NSE: Loaded 151 scripts for scanning.
[-] [192.168.254.136 nmap-full-tcp] NSE: Script Pre-scanning.
[-] [192.168.254.136 nmap-full-tcp] NSE: Starting runlevel 1 (of 3) scan.
[-] [192.168.254.136 nmap-full-tcp] Initiating NSE at 08:30
[-] [192.168.254.136 nmap-full-tcp] Completed NSE at 08:30, 0.00s elapsed
[-] [192.168.254.136 nmap-full-tcp] NSE: Starting runlevel 2 (of 3) scan.
[-] [192.168.254.136 nmap-full-tcp] Initiating NSE at 08:30
[-] [192.168.254.136 nmap-full-tcp] Completed NSE at 08:30, 0.00s elapsed
[-] [192.168.254.136 nmap-full-tcp] NSE: Starting runlevel 3 (of 3) scan.
[-] [192.168.254.136 nmap-full-tcp] Initiating NSE at 08:30
[-] [192.168.254.136 nmap-full-tcp] Completed NSE at 08:30, 0.00s elapsed
[-] [192.168.254.136 nmap-quick] NSE: Loaded 151 scripts for scanning.
[-] [192.168.254.136 nmap-quick] NSE: Script Pre-scanning.
[-] [192.168.254.136 nmap-quick] NSE: Starting runlevel 1 (of 3) scan.
[-] [192.168.254.136 nmap-quick] Initiating NSE at 08:30
[-] [192.168.254.136 nmap-quick] Completed NSE at 08:30, 0.00s elapsed
[-] [192.168.254.136 nmap-quick] NSE: Starting runlevel 2 (of 3) scan.
[-] [192.168.254.136 nmap-quick] Initiating NSE at 08:30
[-] [192.168.254.136 nmap-quick] Completed NSE at 08:30, 0.00s elapsed
[-] [192.168.254.136 nmap-quick] NSE: Starting runlevel 3 (of 3) scan.
[-] [192.168.254.136 nmap-quick] Initiating NSE at 08:30
[-] [192.168.254.136 nmap-quick] Completed NSE at 08:30, 0.00s elapsed
[-] [192.168.254.136 nmap-full-tcp] Initiating Parallel DNS resolution of 1 host. at 08:30
[-] [192.168.254.136 nmap-full-tcp] Completed Parallel DNS resolution of 1 host. at 08:30, 0.02s elapsed
[-] [192.168.254.136 nmap-full-tcp] Initiating Connect Scan at 08:30
[-] [192.168.254.136 nmap-quick] Initiating Parallel DNS resolution of 1 host. at 08:30
[-] [192.168.254.136 nmap-quick] Completed Parallel DNS resolution of 1 host. at 08:30, 0.01s elapsed
[-] [192.168.254.136 nmap-quick] Initiating Connect Scan at 08:30
```

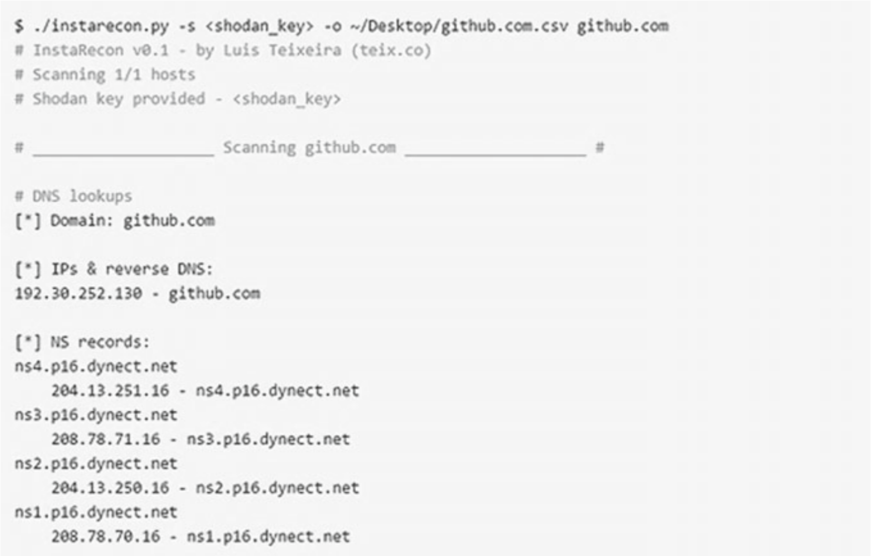
Fig. 4 AutoRecon [8]

scan at a time. The tool is highly flexible and is written in python. It uses modules from standalone recon apps [7]. The initial vector for the tool is a network scan which includes both port scan as well. The results from these scans are used for performing further enumeration of the network. The IP addresses of the targets can be provided as a list. Since multi-threading is enabled, multiple hosts can be scanned simultaneously. Port scanning can be customized to perform scans on well-known ports, top 1000 ports or all ports, suggests recommended commands to be performed after the initial scan. Proper directories are maintained. Logs and scan results are saved in a structural format. Vulnerable components are highlighted to help the user to target the system (Fig. 4).

- AutoReconR developed by Stefan Voemel is an improvement on AutoRecon with various added features. It attempts to automate parts of the identification and listing process of the network. Respective findings are described and summarized in an automatic report. As such, AutoReconR can make it easier to identify potential weaknesses in target systems more quickly and to find an entry point [8]. The tool is designed to run in the background while the tester can focus on other tasks in parallel. For example, in the laboratory environments provided by Offensive Security or during security tests such as OSCP, the tester can start writing exploits while AutoReconR scans the remaining targets and performs automatic service listings. Some of the features are: the possibility of specifying targets either via a command line or an input file. Define scanning and service listing profiles in custom configuration files. Automatically store scan results in a folder structure defined by service name. Launch additional actions based on identified services and service patterns. Summarize the results in a corresponding (at present very basic) PDF study combine software runtime and scan depth with the aid of complexity levels.

- InstaRecon developed by Luis Teixeira is an automated digital reconnaissance used to get the initial footprint of the system. It helps the attacker to obtain information about the target device or the network. This knowledge can be used to strike the device. That is why it can be called a Pre-Attack because all the information is checked to ensure a complete and effective resolution of the attack [9]. The features of InstaRecon are IP information and domain name information using whois and dig, Obtain IP address of domain name by using whatsmyip, Search engine lookup using Shodan, Domain Name Lookup using MX records, subdomain enumeration by using Google website reverse lookup (Fig. 5).

From Table 1, it is evident that there is a significant gap in the current open source tools. With the ever-changing threat landscape, the need for integrating social engineering and forensic tools along with a threat intelligence model has become paramount.



```
$ ./instarecon.py -s <shodan_key> -o ~/Desktop/github.com.csv github.com
# InstaRecon v0.1 - by Luis Teixeira (teix.co)
# Scanning 1/1 hosts
# Shodan key provided - <shodan_key>

# ____________________ Scanning github.com ____________________ #

# DNS lookups
[*] Domain: github.com

[*] IPs & reverse DNS:
192.30.252.130 - github.com

[*] NS records:
ns4.p16.dynect.net
    204.13.251.16 - ns4.p16.dynect.net
ns3.p16.dynect.net
    208.78.71.16 - ns3.p16.dynect.net
ns2.p16.dynect.net
    204.13.250.16 - ns2.p16.dynect.net
ns1.p16.dynect.net
    208.78.70.16 - ns1.p16.dynect.net
```

Fig. 5 InstaRecon [9]

Table 1 Comparison between the tools

Tool	IP Recon	Social engineering tool	Threat Intel	Automated workflow	Forensic tool
Osmedeus	Yes	No	No	Yes	No
AutoRecon	Yes	No	No	Yes	No
AutoreconR	Yes	No	No	Yes	No
Instarecon	Yes	No	No	Yes	No

4 Literature Survey/Related Work

To develop a reconnaissance tool, we need to analyze and characterize the relationship between an attacker and a victim. To systematically understand and characterize the behavior of cyber-attack reconnaissance behavior, Richard B. Garcia-LeBron (2018) proposes a systematic framework to study an attacker's behavior [10]. The system is composed of three abstraction levels: macroscopic, mesoscopic and microscopic as seen in Fig. 6.

On the macroscopic level, the graph of the time series of attacks in victim relations of the perception and understanding of cyber-attacker activities is studied. This graph-theoretical abstraction allows various information to be obtained by the use of a set of existing capabilities. To define the graphs of the attacker/victim relationship, the features that display these graphs were used which implements the comparisons that match different times windows between these graphs [12]. Additionally, the notions of efficient characteristics (i.e. features that may or may not characterize the creation of bipartite attacker-victim graphs) and robust characteristics (i.e. characteristics that are efficient in time resolutions) are described [13]. Finally, a dataset that was collected from a honeypot and used to conduct a case study to investigate the time resolutions that need to be considered to characterize as comprehensive as possible the evolution of the attacker-victim bipartite graphs [11]. Therefore to represent the behavior, only a small number of time resolutions have to be considered. At the mesoscopic level, the study of clustering cyber attackers using their identification behaviors, modeled as time series of reconnaissance activities is initiated [14]. A two-resolution methodology is used to characterize cyber-attack reconnaissance behaviors. At the microscopic level, a system to classify and organize temporal-spatial behaviors is proposed. The system provides a novel concept for the identification actions of the attackers dubbed: attacker identification trajectories. It also provides the cluster of attacker reconnaissance trajectories called a visual representation: Attacker reconnaissance trajectory hierarchy trees. A target reconnaissance model was proposed by Hung T. Nguyen et al. (2016) using probabilistic

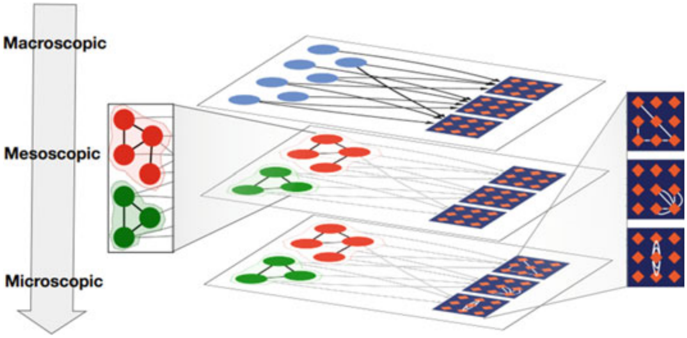


Fig. 6 The three levels of abstraction proposed by Richard B. Garcia-Lebron [11]

graphs on Facebook. Michael Glassman et al. (2012) present the idea of OSINT as an essential component in understanding the resolution of human problems in the twenty-first century. OSINT is a result of the emerging ties of human intelligence, which occur off the emergence of the Internet and World Wide Web expansionism of everyday life in various ways. Abel Yeboah-Ofori et al. (2016) propose a framework to thoroughly analyze and review existing study results on cyber intelligence and open-source information analysis and recognize all the risks and weaknesses of social networks online for mitigating purposes.

5 Design Considerations for a New Open Source Tool

Reconnaissance can take place vertically and horizontally. First, an intruder needs to obtain all possible subnet information from hosts and ports. This allows for the development of a targeted network map. Second, the attacker tries to evaluate the possible vulnerabilities of particular services. Cyber Reconnaissance is critical in today's world due to an increase in cyber warfare involving actions by a political entity or nation-states to attack and attempt to damage other nations' computers or information networks through, for example, computer viruses or denial of service attacks. Cyber reconnaissance is designed to level the playing field by providing organizations with a high-resolution picture of their cyber landscape from an adversary's perspective. While cybersecurity uses the implementation of technical means to protect the critical infrastructure or assets of an organization, it is also important that data collected during the reconnaissance phase is converted into intelligence, also known as cyber threat intelligence (CTI). The CTI is based on the collection of intelligence using open-source intelligence (OSINT), social media intelligence (SOCMINT), human intelligence (HUMINT), or insight from the deep and dark web.

5.1 Techniques Involved

Network scanning and port scanning. Processes to learn about a network's structure and actions—not hostile intrinsically, but often used by malicious individuals to conduct recon before trying to penetrate a network. Network Scan detects and maps all active hosts to their IP addresses within a network. Port Scan scanning refers to the process of sending packets to various host ports and analyzing responses to gain information about their operating system and running services. The first step in aggressive network scanning is often the host discovery process of deciding which devices on a network are down and up. For host discovery, two protocols are used most regularly: Address Resolution Protocol (ARP) scan and various forms of ICMP (Internet Control Message Protocol) scan. Because all individual ARP requests are required to map IP addresses to MAC addresses on a local subnet, ARP requests can be forwarded to multiple IP addresses on a local area network (LAN) based on the ARP response. Port scanning may be used to identify service uses in particular ports once the hosts that are available on the network have been scanned by network scanning. Typically, port scanning attempts to classify port as one of three names, Open: the destination answers with a packet that indicates the port that listens to it, meaning that any service used (usually TCP or UDP) for scanning is also in use. Closed: The request packet has received the destination but replies that there is no port listening service. Filtered: the port may be open, but the packet was filtered out of the firewall and excluded, so no response was received.

OS Fingerprinting. To detect OS, networks, utilities, and program names and numbers, attackers can send custom packets to the target. These packets will receive the victim's response in the form of a digital signature. This signature is one of the keys to recognize which applications, protocols and OS is running the target system. If the attackers have the right details, they will know your scenario and will be able to build a complete infrastructure map of all your services and potential network topology to fine-tune their digital assault. OS Fingerprinting is a method for determining which operating system the remote computer is running. OS Fingerprinting is often used for cyber reconnaissance because most exploitable bugs are unique to the operating system.

6 Conclusion and Future Work

The importance of reconnaissance has been discussed in-depth in the paper. Global cyber threat landscape mandates organizations to perform penetration test exercises often to secure their systems from the ever-evolving attacker landscape. From the cyber-kill chain, it is obvious that reconnaissance is the first step in any attack. Therefore, the need for an automated tool is necessary to streamline the process. The tools mentioned in the paper are the first step toward that and are not the finished product. We can further improve this software by including the following modules: Forensic Module: To obtain metadata from video and audio files, documents, etc. Automated Workflows: To directly provide input for reverse DNS lookup from the Nmap scan result page. CVE details: To obtain public vulnerabilities of the technology used Since OSINT is an ocean of data, there have to be two key components to any software, Fluidity and Rigor. Therefore, the new proposed system would be designed based on the experimental results of the attacker victim relationship. This helps us to model our software on current attacker trends. Along with this, a study on alert correlation systems will help us in reducing the number of alerts generated by an IDS or IPS when obtaining dataset to generate an attacker model [15]. A major issue when taking datasets generated from these systems is the false positive. Negating this will help us better in identifying actual threats. This will help in timely insight, which will enable to organize a better defense from this ever-changing threat.

References

1. Internet Security Threats Report. https://www.symantec.com/threatreport/
2. J.R. Rutherford, G.B. White, Using an improved cybersecurity kill chain to develop an improved honey community, in *Hawaii International Conference on System Sciences (HICSS)* (2016), pp. 2624–2632
3. E. Alata, M. Dacier, Y. Deswarte, M. Kaaniche, K. Kortchinsky, V. Nicomette, V.-H. Pham, F. Pouget, Collection and analysis of attack data based on honeypots deployed on the internet, in *Quality of Protection* (2006), pp. 79–91
4. D. Nidhin, I. Praveen, K. Praveen, Role-based access control for encrypted data using vector decomposition, in *Proceedings of the International Conference on Soft Computing Systems* (2016), pp. 123–131
5. D. Kiwia, A. Dehghantanha, K.-K. Choo, J. Slaughter, A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. J. Comput. Sci. **2**(5), 394–409 (2018)
6. Osemedeus, https://github.com/j3ssie/Osmedeus.git
7. AutoRecon, https://github.com/Tib3rius/AutoRecon.git
8. AutoReconR, https://github.com/svo80/AutoReconR.git
9. InstaRecon, https://github.com/vergl4s/instarecon.git
10. R.B. Garcia-Lebron, K.M. Schweitzer, R.M. Bateman, S. Xu, A framework for characterizing the evolution of cyber attacker-victim relation graphs, in *JMILCOM 2018–2018 IEEE Military Communications Conference (MILCOM)* (2018), pp. 70–75
11. Z. Zhan, M. Xu, S. Xu, Characterizing honeypotcaptured cyber-attacks: statistical framework and case study. IEEE Trans. Inf. Forensics Secur. 1775–1789 (2013)
12. X. Shouhuai, Cybersecurity dynamics: a foundation for the science of cybersecurity, in *Proactive and Dynamic Network Defense* (Springer, New York, 2019)
13. S. Banerjee, M. Jenamani, D.K. Pratihar, Properties of a projected network of a bipartite network, in *2017 International Conference on Communication and Signal Processing (ICCSP)* (2017), pp. 0143–0147
14. D. Koutra, J.T. Vogelstein, C. Faloutsos, DELTACON: a principled massive-graph similarity function, in *Proceedings of the 2013 SIAM International Conference on Data Mining* (2013), pp. 162–170
15. S. Mallissery, K. Praveen, S. Sathar, Correlation of alerts using prerequisites and consequences for intrusion detection, in *International Conference on Computational Intelligence and Information Technology* (2011), pp. 662–666

A Review on Open Challenges in Intrusion Detection System

Arun Kumar Singh, Ashish Tripathi, Pushpa Choudhary, and Prem Chand Vashist

1 Introduction

In general, the meaning of communication is the data flow from sender to receiver over a public communication channel, and always new threats arise due to existing vulnerabilities in the system. These threats exploit vulnerabilities in the form of attacks. These attacks in the digital world are known as "cyber attack" that affects the victim's network system in terms of loss of data and information. In cyber security, intrusion detection is treated as a critical function. The concept of the Intrusion Detection System (IDS) firstly comes in the late 1980s. An IDS is basically a security alarm to protect sensitive information against possible threats. The objective of the IDS is to monitor activities of the anomalous behavior of the communication system and generate reports as per the audit trails of the network traffic. After that, IDS does an analysis of the report and takes the necessary action to reduce the risk [1].

IDS basically keeps its eye on the events occurring in a network and communication system and analyzes them to predict violations of any security rules in the future through security breaches or compromising the security policy practices. Real-time monitoring and defensive action against the intrusion are performed by the IDS [2]. The intrusion detection system (IDS) is a very sensitive and critical tool for protection against possible threats in the network. Network traffic is analyzed along with their logs to detect intrusions and raise alerts [3]. The rest of the paper is organized into four sections. A literature survey that covers privacy and security issues, audit monitoring and false-positive rates in IDS are shown in Sect. 2. The concept of IDS is to keep an eye on the events occurring in a network and communication system and analyzing them for future predication of those events are violations of the security breaches or compromising the security policy practices.

A. K. Singh · A. Tripathi (✉) · P. Choudhary · P. C. Vashist
Department of Information Technology, G. L. Bajaj Institute of Technology and Management, Greater Noida, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_4

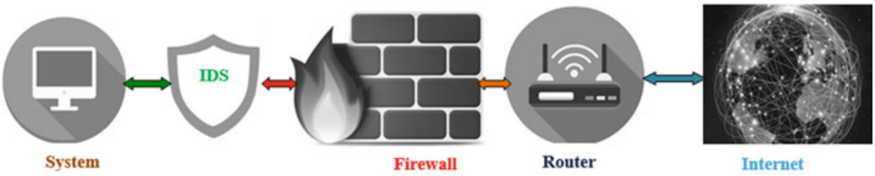


Fig. 1 Intrusion detection system architecture

Network monitoring and defensive strategies against the intrusion are performed by the Intrusion detection system. With the fast-growing of the internet, real-time monitoring of the IDS for events can be analyzed by ‘audit trails’ [2]. Intrusion detection systems (IDS) are very sensitive and critical tools for protection against intrusions in the networks. Analysis of the network traffic along with the logs is to detect an intrusion for raises the alert [3]. Figure 1 shows the basic architecture of IDS.

2 Literature Survey

Intrusion Detection System (IDS) acts as defensive techniques to sense the vulnerability and threat activity. IDS is only alert against the probability of suspicious incidents, which may occur in the future. The main aim of this research paper is to present the concept of IDS as well as an analysis of different security mechanisms in IDS and behaviors of the threats. Intrusion Detection System is to constrain access, to the authentication system.

Various pedagogical techniques for proving security against the new threats are Firewall, Virtual Private Network, Antiviruses, and authentication mechanism through an access matrix to create a shield of a virtual layer of protection [4]. As such now, no such security measure ensures ward off attacks.

Access to an object by unauthorized users or program is known as Intrusion, these are classified into two categories as Internal Intrusion and External Intrusion. Internal Intruder has limitations, whereas External intruders have got unauthorized access to damage big information system from outside of the organization. Whenever a new attack is happening, Intrusion detection system generates an alert signal, which contains the information of intrusion and its pattern or signature. An updated signature always detects possible attacks. The way of updating the signature is basically dependent on the wide range of knowledge of various intrusions [5].

For protection by the intrusions, a new system is called IDS, which are categorized into two categories, named signature-based intrusion detection system (SIDS) and anomaly-based intrusion detection system (AIDS) [6]. Detections of intrusions in the high-speed networks are flow-based IDS, which inspect the header information of that packet but generally not the analysis of the payload of the packet. IDS is a sensitive tool to protect IP networks, which used to analyze the system logs for finding any new attack of the network traffic [3]. Extension of security is the privacy issue to communication among users and all the personal sensitive date must not share by organizations or institutional to others for self-business purposes [7].

Online Intrusion detection system provide a dynamic inspection to identify unexpected a new threat from network traffic, these inspection help to investigate foot printing and instantaneously make the collective report based on the classification of threats, which is called auto-encoders [8]. Garcia gives the review of anomaly-based network intrusion detection system with a division of A-NIDS into two separate domains; statistical, knowledge-based, and machine learning-based with respect to its pros and cons [9].

Liao presents a review of IDS taxonomy based on the data source, timelines, and detection strategy along with future challenges of the new threats [10]. New threats are always more intelligent than the existing IDS [11]. Using genetic algorithms and multi-start meta-heuristic method, Tamer proposed for anomy detection by hybrid technique [12].

2.1 Privacy and Security in IDS

Although each country has separated law for privacy for maintaining sensitive personal information to collect data by surveillance through IDS, so for analyzing these data, such as log file or network traffic with compliance of privacy rules for reflecting the output [13].

Still, various challenges and open issue exist in IDS; user always trusts on the security policy of IDS but as such no guarantees on the third party, how much they compromise with Respect to privacy. For the confidentiality of data, it's very difficult to trust any third-party vendor to reveal the sensitive data of users.

Information security and privacy are the highest priority in today's digital modern world. To ensure security and privacy in communication, different security systems such as Intrusion Detection Systems, Encryption-Decryption techniques, firewall, and Honeypots systems are used. An effective system of Honeypots with the association of IDS is ensuring to provide better security [14]. Any unlawful evens may be entered into the unauthorized access to any network by the intrusion, such type of intrusion may be called "invasion of privacy". As per the oxford dictionary, intrusion is "the action of intruding".

2.1.1 Audit Monitoring of IDS

The basic functionality of the IDS is the postmortem of the network logs on the basis of the database of the predefined signature and computer forensic techniques [15]. The objective of the intrusion detection systems is to find out the sensitive intrusion techniques and mitigate the false-positive rate [16]. A very important tool needs to live monitor sensitive logs, which collect the log files in public network traffic. Its basic requirement for today to monitor real-time flow-based traffic logs with sensitivity. Still, it is very difficult to detect intrusions like SQL injection or cross-scripting [17]. Additional parameters for accessing matrix are required for accurate and efficient results.

The main issue in flow-based IDS is false positive due to the flaw of the sampling techniques [18]. Such false challenges are avoided by conducting an investigation on sampling strategies in order to get an efficient outcome. For modern e-palm-gazettes payload-based IDS is not much more successful because heavy traffic load on the website, mobile apps, and limited memory to work out on these apps [19]. IDS security access matrix provides for the global-level network traffic and protection against intrusion by the sensitivity of the detection mechanism [20].

Most of the researchers are finding the alternative mechanism of the intrusion detection system for the cloud and its services. Chirag et al focus on the various IDS and IPS techniques for the prevention of the network systems. The integration of soft computing techniques, which maybe enhance the security feature of the Intrusion detection system [21]. Eventually, the advancement of IDS services can come by the use of cloud services comes with the compliance of new technology, which provide the trusted and independent platform to enhance the security with the scale of the network traffics (Tables 1 and 2).

2.1.2 Merit and Demerit of IDS

See Table 1.

2.1.3 False-Positive Rates of IDS

False-positive rates cannot be removed, it only mitigates with the research of the great accuracy and find out the type of the attack categories. The intrusion may be insider or outsider under the categories of physical and virtual. Physically, it may be a human or e-gazettes in a virtual way, it may be a program or any type of script work in the form of the intrusions [25]. In the past few decades, large scale users of the modern Internet and computer systems have raised numerous security threats due to the explosive use of networks. Any vulnerabilities, malicious intrusion, or attack on the network or information systems may give rise to serious disasters, [10] and breach the policies of computer security, i.e. Confidentiality, Integrity, and Availability (CIA).

Various researchers work on a new paradigm of the intrusion detection system is called hybrid intrusion detection techniques that include misuse detection along with anomaly detection in a new system [26, 27]. According to Shi-Jinn Horng [28], hybrid intrusion detection techniques are a combination of the clustering algorithm that supports vector mechanism, and the feature is a simple selection algorithm.

Hybrid intelligent decision technique is proposed by Mrutyunjaya [29] for data filtering and association with a classifier to get more accuracy on network attack

Table 1 Merits and demerits of IDS

Serial Number	Type of IDS	Merit	De-merit
1	Host-IDS [22, 23]	(i) Host-IDS knows how to check cipher data with electronics intercommunication data (ii) Host-IDS are well aware of the acceptability of the actual attack, hence whether the attack was successful or not (iii) It does not require additional hardware, so it is easy to deploy, also does not affect the existing system design	(i) Host-IDS is broken if the attacker succeeds in breaking the OS vulnerability (ii) The limitation of Host-IDS is that it is not able to detect only network and DoS attacks
2	Network-IDS (NIDS) [24]	(i) NIDS is independent of the operating system environment, so this will not influence the execution of hosts	(i) Whether the attack is successful or not, it is never able to point out (ii) Encrypted traffic is very difficult to analyze, so it is not able to examine properly (iii) Network-IDS has exceptional partial transparency within the host

[30]. It gives a better algorithm to detect the intrusion over the network traffic [31]. Hong Kuan Sok proposed an algorithm for more accurate results with respect to existing intrusion systems. Combination of boosting and decision tree algorithms is represented by Yonav Freund [32].

Primarily, research issues in IDS are intrusion detection policy, false-positive response, audit data source, and performance [33]. Security of IDS by the concept of "fuzzy logic", the false-positive response can be mitigated with applying of efficient fuzzy-set policy for abnormal behavior of the intrusion detection system [2].

3 Network Monitoring Challenges in IDS

The various challenges such as human intervention, audit analysis, tools deployments, dependency on the sensors, false-positive alarm, existing signature collection, and monitoring techniques exist in IDS. The role of IDS is not only limited to monitor the traffic besides the alert against new security attacks too, but the tool may also be the desktop version or web version [34].

This study focuses on the challenges of the network traffics with the compliances of the new security systems. Most common challenges are as follows:

- **Monitoring of TLS security:**

When web communication starts with TLS security by using HTTPS, which is a request-response protocol for client–server communication using cryptographical techniques [1, 16]. Https communication provides encrypted traffic over the networks on the application layer TCP/IP model, where N-IDS monitors such type of traffics to access the private key of Secure Socket Layer certificates to prevent the security.

- **Role of Cloud Security in IDS:**

Cloud computing is basically a cloud of the virtual network, based on a shared cluster, which provides services on a pay as you use and services are in the form of software as a service (SAAS), platform as a service (PAAS) as well as Infrastructure as a service (IAAS) [1, 29]. There is no requirement to buy and physical infrastructure for any computation, only use that service for the particular time being and pay only for uses that services. The role of IDS is very important to enhance the security of these services and the perseverance of an active defense system against the new intruder maleficent attacks for any IT infrastructures [32].

In cloud computing, the applications are received on the remote server of the provider and they have control toward the usage of the data. IDMEF (Intrusion detection message exchange format) is the standard used in cloud for the communication purpose [8, 29].

3.1 Comparative Study of IDS

See Table 2.

4 Research Challenges in IDS

Although the current research of intrusion detection techniques and system researchers have gained a certain achievement, there are still some research problems and challenges that need to be dealt with.

(a) Lack of designing and non-compliance security products uses for IDS, which are not verified and validated. Avoiding these issues, designed IDS should be followed the standard security compliance.

(b) An open research issue false-positive alarm still exists in the IDS Systems.

(c) Risk assessment and countermeasure need when IDS communicates with other security applications like firewall, anti-malware, etc.

Table 2 Comparative study of IDS

Serial Number	IDS	Host-IDS	Network-IDS
1	Detection possibility of platform [35]	Host only	Networks or host
2	Structural design of network [36]	Control networks	Control networks
3	Input information [37]	Adaptation of security logs, activity logs of the application program, host activity logs, configuration of host	Monitor traffic packet move in the network, earlier measures, client reports
4	Types of attack in IDS [38]	Nasty succession of any sensitive data, bombarding of spam data, spyware programs, discover the pilfering, input data of key-logging, botnet activity, identify the logos for unauthorized users	End-user web attack through CSRF: cross-site request forgery, web attack through cross-site scripting (XSS), attack on the TCP-fragment packet, attack on TCP-SYN packets of TCP protocols
5	Database attack [39]	DBMS injection attack, SQL injection, and session attack	DBMS injection attack, SQL injection, and session attack
6	Source of information [40]	System call	Network traffic

Intrusions in a computing environment are a very common undesired malicious activity that is going on since the inception of computing resources. A number of security measures have taken place for the last three decades, but as technology has grown up, so as the security threats [17].

Lots of research is required in the intrusion detection system to make an efficient intrusion detection system [41]. There are a number of issues in the existing intrusion detection system, which are as follows:

(a) Ineffectiveness of Intrusion detection system designing: Organization has very sensitive threats that may occur against improper installation mitigate by ensuring proper vulnerability assessment of the IDS, for ensuring optimized installation.

(b) Sensitive alertness of the Intrusion Detection System: Mostly IDS generates alert to users with respect to a predefined signature, so that policy should be complying with new security standards.

(c) Real-time monitoring: Intrusion detection system should provide prevention by the real-time attacks and monitor unauthorized events.

(d) Mitigate false-positive rate: Due to false-positive rate, IDS suffer the false alarm will that should be mitigating for sensitivity and accurate result of Intrusion

Detection System. The category of IDS will be truly positive and false positive [42].

(e) Lack of design in Intrusion Detection System: Detection algorithm and pattern matching are two terms that are required to design in intrusion detection systems.

(f) Heterogeneous IDS: In the current scenario, various vendors' IDS products deployed in the organization, and still as such no security compliance has been followed for IDS policy. So lack of security breaches has happened, which will be a big vulnerability in the network system.

5 Conclusion

This paper discussed the concept of IDS and various IDS techniques and issues. There are two types of IDS host-based and anomaly-based IDS, to ensure the integrity of security policy. As per the networking divides in Network-based (NIDS) and Host-based (HIDS), network-based IDS monitors various hosts simultaneously, but they have issues for a monitor of high-speed networks, encrypted protocols, and no alert of attack success, whereas host-based IDS identifies at the application layer and no trouble with cryptography encryption and decryption. The drawback of host-based IDS attacker attacks on any host that are vulnerable due to applications or any program threats. Anomaly-based IDS easily identifies a new attack but gives a high false alarm rate.

References

1. S. Vijayarani, S. Maria Sylviaa, Intrusion detection system—a study. Int. J. Secur. Priv. Trust. Manag. (IJSPTM) **4**(1) (2015)
2. M.M. Hassan, Current studies on intrusion detection system, genetic algorithm and fuzzy logic. arXiv preprint. arXiv: 1304.3535 (2013)
3. M.F. Umer, M. Sher, Y. Bi, Flow-based intrusion detection: techniques and challenges. Comput. Secur. **70**, 238–254 (2017)
4. A. Lazarevic, V. Kumar, J. Srivastava, Intrusion detection: a survey, in *Managing cyber threats* (Springer, Boston, MA, 2005), pp. 19–78
5. N. Hubballi, V. Suryanarayanan, False alarm minimization techniques in signature-based intrusion detection systems: a survey. Comput. Commun. **49**, 1–17 (2014)
6. C. Zhou, et al., Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. IEEE Trans. Syst. Man Cybern. Syst. **45**(10), 1345–1360 (2015)
7. S. Niksefat, P. Kaghazgaran, B. Sadeghiyan, Privacy issues in intrusion detection systems: a taxonomy, survey and future directions.Comput. Sci. Rev. **25**, 69–78 (2017)
8. Y. Mirsky, et al., Kitsune: an ensemble of autoencoders for online network intrusion detection. arXiv preprint. arXiv:1802.09089 (2018)
9. P. Garcia-Teodoro, et al., Anomaly-based network intrusion detection: techniques, systems and challenges. Comput. Secur. **28**(1–2), 18–28. H.-J. Liao, C.-H.R. Lin, Y.-C. Lin, K.-Y. Tung,

Intrusion detection system: a comprehensive review. J. Netw. Comput. Appl. **36**(1), 16–24 (2013)

10. H.-J. Liao, et al., Intrusion detection system: a comprehensive review. J. Netw. Comput. Appl. **36**(1), 16–24 (2013)
11. S.-H. Ahn, N.-U. Kim, T.-M. Chung, Big data analysis system concept for detecting unknown attacks, in *16th International Conference on Advanced Communication Technology* (IEEE, 2014)
12. T.F. Ghanem, W.S. Elkilani, H.M. Abdul-Kader, A hybrid approach for efficient anomaly detection using metaheuristic methods. J. Adv. Res. **6**(4), 609–619 (2015)
13. A.F. Westin, Privacy and freedom. Wash. Lee Law Rev. **25**(1), 166 (1968)
14. M. Baykara, R. Das, A novel honeypot based security approach for real-time intrusion detection and prevention systems. J. Inf. Secur. Appl. **41**, 103–116 (2018)
15. K.A. Garcia, et al.,Analyzing log files for postmortem intrusion detection. IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.) **42**(6), 1690–1704 (2012)
16. R.S.M. Carrasco, M.-A. Sicilia, Unsupervised intrusion detection through skip-gram models of network behavior. Comput. Secur. **78**, 187–197 (2018)
17. N. Chakraborty, Intrusion detection system and intrusion prevention system: a comparative study. Int. J. Comput. Bus. Res. (IJCBR) **4**(2), 1–8 (2013)
18. M. Tavallaee, et al.,A detailed analysis of the KDD CUP 99 data set, in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications* (IEEE, 2009)
19. A. Sperotto, A. Pras, Flow-based intrusion detection, in *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops* (IEEE, 2011)
20. M.R.G. Raman, et al., An efficient intrusion detection system based on hypergraph-Genetic algorithm for parameter optimization and feature selection in support vector machine. Knowl. Based Syst. **134**, 1–12 (2017)
21. C. Modi, et al., A survey of intrusion detection techniques in cloud. J. Netw. Comput. Appl. **36**(1), 42–57 (2013)
22. F. Basicevic, M. Popovic, V. Kovacevic, The use of distributed network-based IDS systems in detection of evasion attacks, in *Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop (AICT/SAPIR/ELETE'05)* (IEEE, 2005), pp. 78–82
23. A.K. Tummala, P. Patel, Distributed ids using reconfigurable hardware, in *2007 IEEE International Parallel and Distributed Processing Symposium* (IEEE, 2007), pp. 1–6
24. A. Sultana, M.A. Jabbar, Intelligent network intrusion detection system using data mining techniques, in *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (ICATCCT)* (IEEE, 2016), pp. 329–333
25. M.R. Kabir, A.R. Onik, T. Samad, A network intrusion detection framework based on Bayesian network using wrapper approach. Int. J. Comput. Appl. **166**(4), 13–17 (2017)
26. R. Dharaskar, Inform. Technol. (IJCEIT) **8**(13), 12–15 (2010)
27. G. Kim, S. Lee, S. Kim, A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Syst. Appl. **41**(4), 1690–1700 (2014)
28. S.-J. Horng, et al., A novel intrusion detection system based on hierarchical clustering and support vector machines. Expert. Syst. Appl. **38**(1), 306–313 (2011)
29. M. Panda, M.R. Patra, A comparative study of data mining algorithms for network intrusion detection, in *2008 First International Conference on Emerging Trends in Engineering and Technology* (IEEE, 2008)
30. H.K. Sok, et al.,Using the ADTree for feature reduction through knowledge discovery, in *2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)* (IEEE, 2013)
31. F. Amiri, et al.,Mutual information-based feature selection for intrusion detection systems. J. Netw. Comput. Appl. **34**(4), 1184–1199 (2011)
32. A. Negi, M. Singh, S. Kumar, An efficient security framework design for cloud computing using artificial neural networks. Int. J. Comput. Appl. **129**(4), 17–21 (2015). Foundation of Computer Science (FCS), NY, USA

33. S. Han, et al., Intrusion detection in cyber-physical systems: techniques and challenges. IEEE Syst. J. **8**(4), 1052–1062 (2014)
34. N. Agarwal, S.Z. Hussain, A closer look at intrusion detection system for web applications. Secur. Commun. Netw. **2018** (2018)
35. N. Puketza, M. Chung, R.A. Olsson, B. Mukherjee, A software platform for testing intrusion detection systems. IEEE Softwa. **14**(5), 43–51 (1997)
36. M. Alicherry, M. Muthuprasanna, V. Kumar, High speed pattern matching for network IDS/IPS, in *Proceedings of the 2006 IEEE International Conference on Network Protocols* (IEEE, 2006), pp. 187–196
37. M. Murakami, N. Honda, A study on the modeling ability of the IDS method: a soft computing technique using pattern-based information processing. Int. J. Approx. Reason. **45**(3), 470–487 (2007)
38. O. Depren, M. Topallar, E. Anarim, M.K. Ciliz, An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert Syst. Appl. **29**(4), 713–722 (2005)
39. D. Wagner, P. Soto, Mimicry attacks on host-based intrusion detection systems, in *Proceedings of the 9th ACM Conference on Computer and Communications Security* (2002), pp. 255–264
40. K.J. Cox, C. Gerg, in *Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools* (O'Reilly Media, Inc., 2004)
41. P. Sadotra, C. Sharma, A review on integrated intrusion detection system in cyber security (2016)
42. J. Wang, Q. Yang, D. Ren, An intrusion detection algorithm based on decision tree technology, in *2009 Asia-Pacific Conference on Information Processing*, vol. 2 (IEEE, 2009)

Intelligent Computing and Communication Security

Big Data-Based Autonomous Anomaly Detection Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing

P. M. Diaz and M. Julie Emerald Jiju

1 Introduction

Virtualization is the potential of operating various control systems nearly unique physical machines and dividing the fundamental hardware resources. It is applicable to enhance everywhere along with costs by utilizing the physical resource quality group. Virtualized cloud-based computing deployed the essential platform to operating systems and storage units. Cloud virtualization handles the workload by converting usual data processing to make better hierarchal, cost-effective and powerful environments. One of the principal aspects of virtualizations is its capability to facilitate the combined use of applications toward different clients [1, 2].

For example, a recent study [3] proposed an unverified learning-based autonomous anomaly detection method that causes precise outcomes anomaly detection regarding a cost-effective method. It was not a unique impact through structures data, while may be able to manipulate alike common and separate anomalies successfully. In this method, [4] applies Autonomous anomaly detection to determine the statistics approach with an intention to seek particular rare occurrence techniques. Numerous enrolments encompass Autonomous anomaly detection; for instance, detect illegal activity, conflagration, human body monitoring, etc. The study in [5] described that virtualization is one of the enormous advances in cloud computing. Another example, [6] focuses only on the way to enlarge particular capability or else append distinctly feasible to the current configuration in recent infrastructure. Negi et al. [7] reported

P. M. Diaz (✉)
Department of Mechanical Engineering, Sreyas Institute of Engineering and Technology, Hyderabad, Telangana, India
e-mail: pauldiaz@sreyas.ac.in

M. Julie Emerald Jiju
Department of MCA, CSI Institute of Technology, Thovalai, Kanyakumari, Tamil Nadu, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*, Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_6

that Cloud Computing is a comparatively a new approach, which, moreover, provides a significant range suitable to anticipate end-user.

This [8] describes a file management system configured to store a large number of data throughout numerous nodes of commodity hardware. Hadoop was originally established in 2007, meanwhile open source Implementation of the MapReduce processing engine joined with a distributed file system. In this category, it [9] used Machine learning techniques to detect the unusual posture of services. Virtualization takes complex reliability and high availability process to meet the high solution for standard essential. For example, [10] described that Cloud computing leads to numerous securities to the organization. The component which affects cloud computing adoption and attacks is an applicable solution to build up surveillance and solitude within the Cloud environment.

It is considerable to refer that our research is diverse in accordance to the above stated investigation in different usages. On the other hand, most of the current analyses commonly assessed a large amount of data processing, anomaly detection, unsupervised learning mostly emphasized clustering processing as opposed to real-time processing. Conversely, we have mainly focused on autonomous anomaly detection security analytics for protecting virtualized infrastructures in cloud computing containing clustering and classification methods. Datasets collected from virtual machines are stored in Hadoop Distributed File System. A new method of autonomous anomaly detection centered on k-means clustering is used. It applies four different classification methods, such as K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Random Forest (RF) and Artificial Neural Network (ANN). Classification methods individually show the accuracy of ROC. Eventually, the Receiver Operator Characteristics Curve (ROC) shows the graphical way connection Specificity and Sensitivity.

The remainder of this paper is organized as follows. Section 2 briefly brings out the Literature review. Section 3 explains the methodology offered. Section 4 defines the investigational outcomes and discussion. Section 5 describes the conclusion.

2 Literature Review

Security data analysis for Virtualized Infrastructures in Cloud Computing by Autonomous Anomaly Detection depends on a dependable circumstance building approach; many academics have suggested various methods to create background models [11, 12].

An essential allusion for our research is the work on collocating [13]. This work showed that huge quantities of data processing and machine learning in anomalous detection have the explication to examine. The system is suggested for clustering/classification algorithms, big data processing technologies and analytics for anomaly detection. The author also shows accuracy and efficiency in the detection rate with the algorithm. The security cloud introduced by Wei et al. [14] states an accumulator security log for cloud customer’s data. Furthermore, it merely obtains the stored information besides that states security on computer-based information. Shantanu et al. [15] stated that security is a reasonable major challenge through storing data in the cloud computing system. This [16] described cloud computing, virtualization increases the security by securing both the integrity of guest virtual machines and the cloud infrastructure components. For example, the study in [17] contemplated the security problems in massive data, cloud computing and the Hadoop environment. The fundamental of this study emphasized the security issues, thereby processing big data in the data processing. It [18] examined the issue related to the security in virtualized infrastructure for identifying the current threats and complexity in the cloud platform. In which, [19] indicates that the detection of anomalies secures the environment in cloud computing based on the concept of Big Data, although it uses only one classification method to prove a highly accurate algorithm. In this analysis, Mahendiran et al. [20] put forward the K-Means clustering algorithm, one of the very popular and high-performance clustering algorithms was compared with other algorithms. A present study by Ahmad et al. [21] uses many unsupervised machine learning algorithms for anomaly detection. The recent study by Win et al. [22] figured out a model, which interpolates the attribute data items and assures that it is well generalized to detect unknown attacks.

3 Proposed Methodology

The fundamental principle of the proposed approach is to detect the autonomous anomaly detection analytics for protecting virtualized infrastructures in cloud computing, which, occasionally, collect the large dataset from Comodo Cloud Security Centre. Attributes, Pe-Files-Malwares, Malware Good ware and Malware-Analysis datasets are collected from virtual machines. Clustering and Classification method is preowned for security analysis. In the process, K-means algorithms perceive anomalies from the dataset. Later, Big Data-Based Autonomous Anomaly Detection Security Analytics applies four different classification methods like KNN, SVM, RF and ANN. Each classification separately checks the accuracy by Receiver Operator Characteristics (ROC).

3.1 Autonomous Anomaly Detection Using K-Means

Anomaly detection is the unity of outstanding events, module or identification of rare occurrences or events of concern due to their differing characteristics from majority of the processed data. It is used in applications such as fraud and intrusion detection, system health monitoring and ecosystem disturbance monitoring. The proposed method uses a novel method of Autonomous Anomaly Detection (AAD) to detect independent anomalies from a large dataset. The AAD method describes the anomaly detection approach, which is implemented using MATLAB.

3.2 K-Means

Clustering is one of the most common probing data analysis techniques used to get a hunch about the structure of the data. Clustering analysis is generally used in many applications in particular image processing, pattern recognition, data analysis and market research. K-means is one of the unsupervised learning algorithms that solves the common clustering problem. The algorithm recurrences to assign each data point to one of the K groups based on the features that are provided. The main idea is to define k centers, one for each cluster. Suppose, the required dataset has ‘n’ objects and the partitioning method (k-means) constructs ‘k’ partitions of data, each and every partition will signify as a cluster. It means that it will classify the data into k groups that satisfy the $k \leq n$ requirement. Using K-means, unrelated data will be modeled as clusters. Subsequently, it is described as similar and dissimilar groups. That is, in some of the rare cases, one or two separate data can be detected, in a way, that cases initiate it as a cluster. The K–Means clustering uses distance-based measurements to determine the similarity between data points. K-medoids clustering method is more similar to K-Means method. Compared to other cluster methods, AAD clustering method is well organized.

3.3 Classification Methods

In supervised learning, both input and output data are provided. Input and output data are labeled for classification to provide a learning basis for data processing. Two techniques used in supervised learning are linear regression and classification techniques. Linear regression model gives the relationship between quantitative data. It is a statistical method that is used for predictive analysis. Classification is used to group the uniform data points into different components to classify them. Particularly, this method consists of four classifications: (i) K-Nearest Neighbor, (ii) Support Vector Machine, (iii) Random Forest and (iv) Artificial Neural Network.

3.4 K-Nearest Neighbor

The k-nearest neighbor algorithm is a simple supervised machine learning algorithm. It can be used to solve both classification and regression problems. All the accessible data are stored and arranged in a new discrete unit of information based on the similarity. The nearest neighbor selects K training cases that have the smallest distance where ‘K’ denotes the required value whether it is maximum or minimum to the nearest neighbor.

3.5 Support Vector Machine

A support vector machine is a supervised machine learning algorithm that analyzes and recognizes patterns. Data are used to solve both classification and regression analysis. A support vector machine is also known as a support vector network. The algorithm creates a line or a hyper-plane, which separates the data into classes.

3.6 Random Forest

Random forest classifier is an entity classifier that produces multiple decision trees. It can be used for both classification and regression. A number of m input variables are used to regulate the decision at a node of the tree. Random forest algorithm gives a more accurate estimate of error rate when compared with the decision tree.

3.7 Artificial Neural Network

An Artificial Neural Network is an arithmetic model based on the structure and functions of biological neural networks. There are hundreds or thousands of artificial neurons called processing units, which are interlinked by nodes. These processing units are devised by input and output units. The artificial neural network is used as a random function estimate tool.

4 Experimental Result

MATLAB is a programming environment for algorithm development, data analysis, visualization and numerical computation developed by Math Works. The proposed Big Data-Based Autonomous Anomaly Detection Security Analytics was implemented using the MATLAB R2018a platform.

The succeeding datasets: (i) Attribute (ii) PE-Files-Malware (iii) Malware Good ware and (iv) Malware Analysis data sets are taken into consideration for execution. The pictorial imageries of both the feature (Dataset-1) and PE-Files-Malware (Dataset-2) datasets are provided in this article. Figures 1 and 2 depict Autonomous Anomaly detection using K-means clustering. In each data for classification, there is a positive and negative class. Positive class denotes blue and negative class denotes black. In 1 attribute dataset graph, x denotes x1 and y denotes x2. In PE-Files Malware dataset graph, x denotes E cblp *104 and y denotes E cp *104.

Figures 3 and 4 depict the ROC curve for KNN in two datasets. It measures the accuracy in the ROC of the system. The suggested techniques provide improved

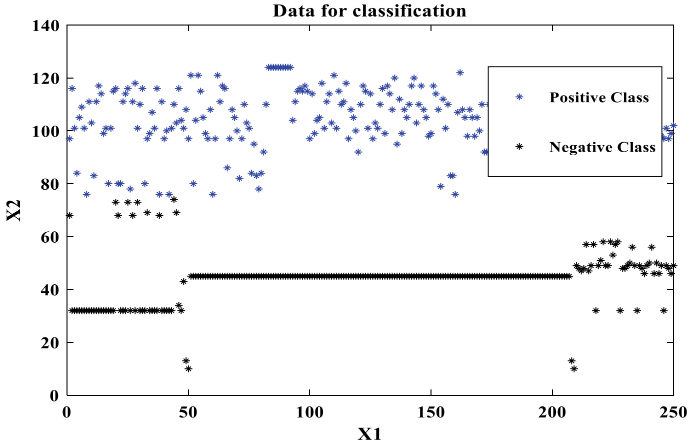


Fig. 1 Dataset 1—autonomous anomaly detection using K-means clustering

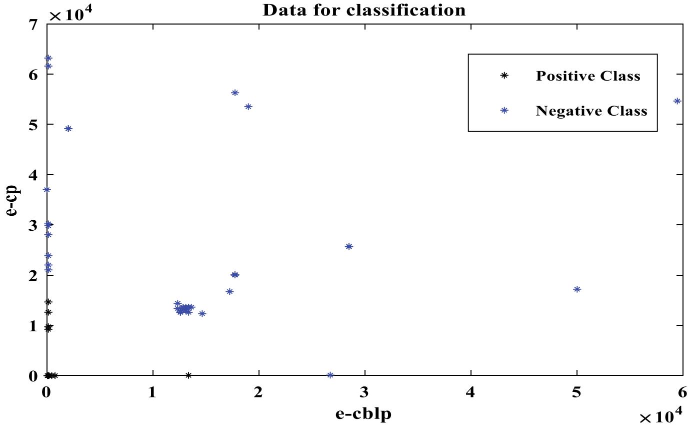


Fig. 2 Dataset 2—autonomous anomaly detection using K-means clustering

accuracy results for data classification. From the result, it is observed to have 1 sensibility and specificity. The effectiveness of a classifier is to identify positive labels and negative labels. The red circle denotes 1 sensibility and specificity.

Figures 5 and 6 illustrate the ROC curve for SVM in datasets. In accordance result, it determines accuracy in ROC of the method. The proposed method ensures enhanced accuracy in the classification of the datasets. From the result, it is found to have 1 sensibility and specificity. The performance of a classifier is to distinguish positive labels and negative labels. The red circle implies 1 sensibility and specificity.

Figures 7 and 8 demonstrate the ROC curve for RF in datasets. The implementation measures accuracy in the ROC of the system. The implied process affords more effective accuracy in the classification of the datasets. Through a result, it is observed

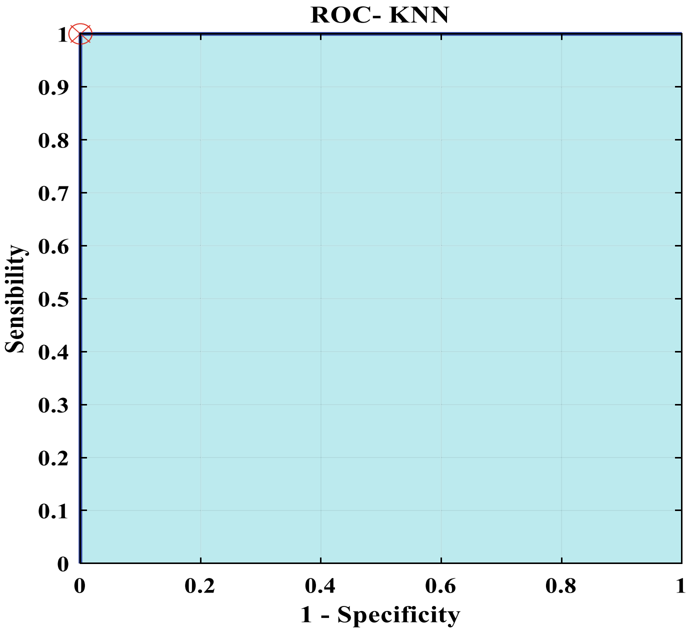


Fig. 3 Dataset 1—ROC curve for KNN

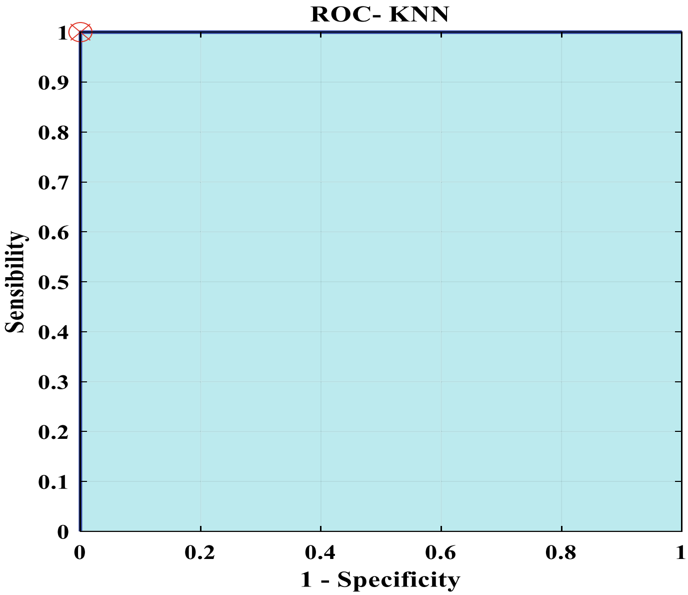


Fig. 4 Dataset 2—ROC curve for KNN

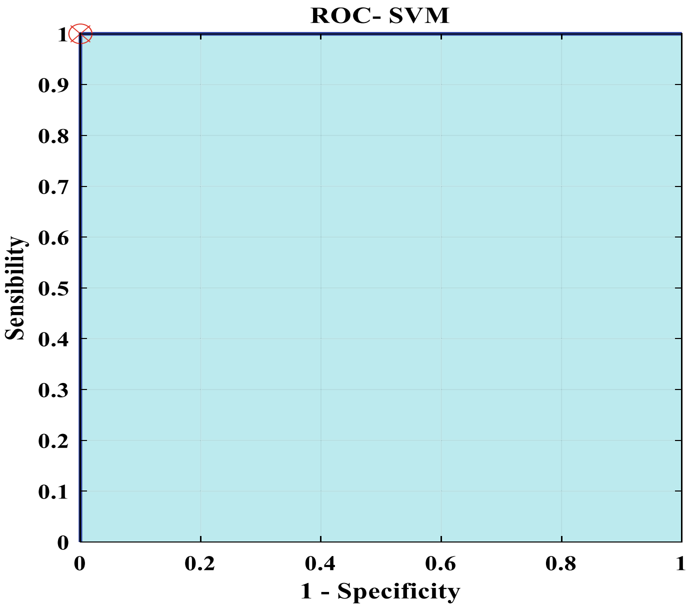


Fig. 5 Dataset 1—ROC curve for SVM

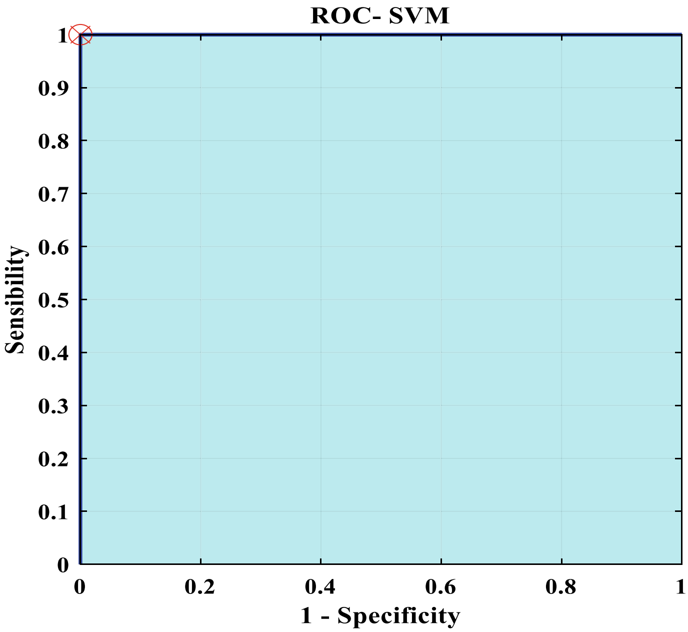


Fig. 6 Dataset 2—ROC curve for SVM

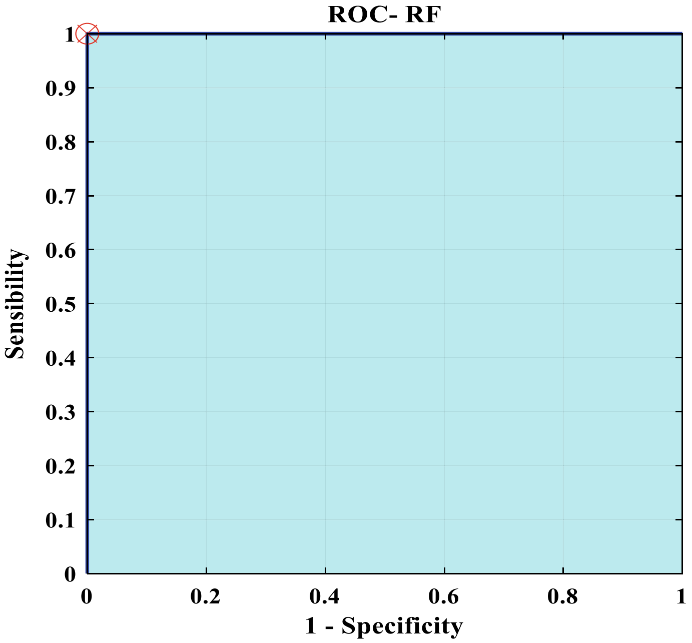


Fig. 7 Dataset 1—ROC curve for RF

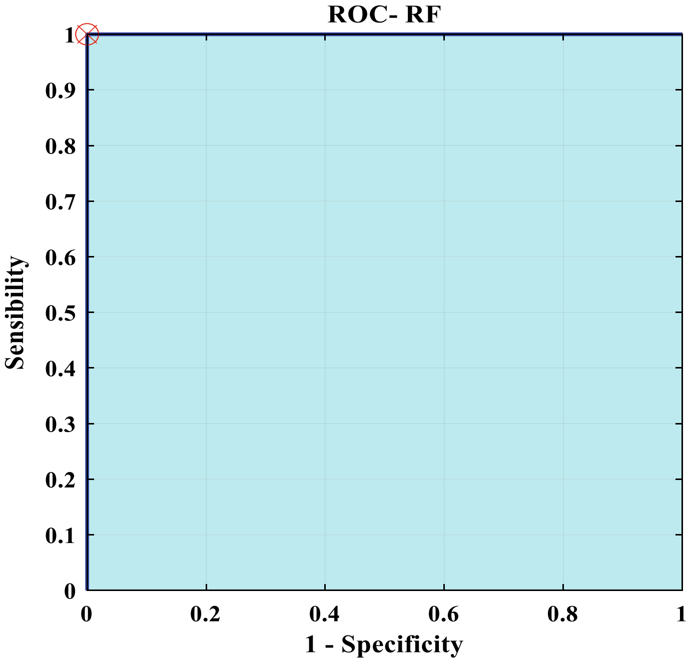


Fig. 8 Dataset 2—ROC curve for RF

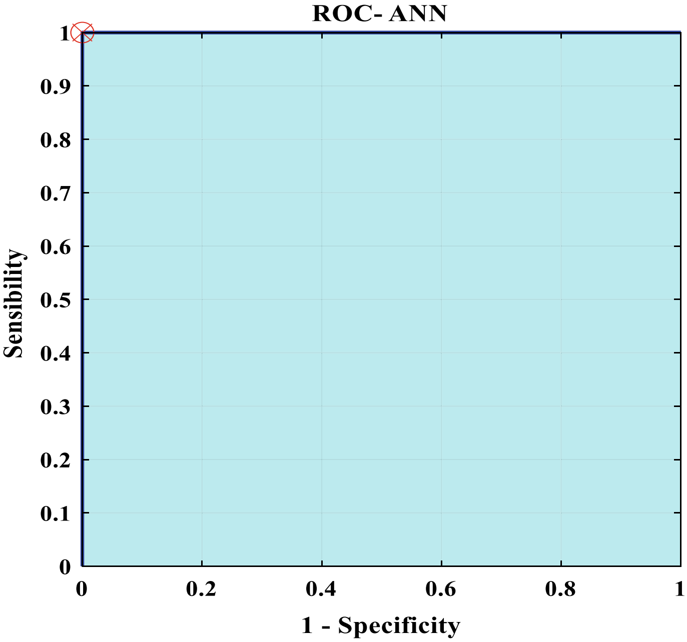


Fig. 9 Dataset 1—ROC curve for ANN

to have 1 sensibility and specificity. The influence of a classifier is to determine positive labels and negative labels. The red circle signifies 1 sensibility and specificity.

Figures 9 and 10 elucidate the ROC curve for ANN in datasets. From the result, it measures accuracy in the ROC of the system. The indicated expertise contributes to rectified accuracy in the classification of the datasets. Among results, it is observed to have 1 sensibility and specificity. The effectiveness of a classifier is to specify positive labels and negative labels. The red circle designates 1 sensibility and specificity.

Datasets are collected from the virtual machine and stored in Hadoop Distributed System, and K-means clustering is done with four classifications. In each dataset for classification, there is a positive and negative class. In the Roc curve, there is a graphical way connection between sensitivity and specificity. We discuss each of the classifications with accuracy 1. The proposed approach can detect anomalies in high accuracy by the datasets. In some cases, the best accuracy is produced at the cost of high computational processing and time. ROC curve is a graph airing the performance of a classification model at all classification thresholds. It contains two parameters: True Positive and True Negative. Sensitivity identifies positive labels and specificity identifies negative labels. The result highlights four datasets. An attribute dataset is an important type of semantic property shared among different activities. In attribute dataset, the accuracy and ROC of four classifications are 1. It gives more information about the functionality of the malware and how the malware interacts with OS. In the four classifications, PE-file's malware dataset contains the accuracy 0.9998 and ROC

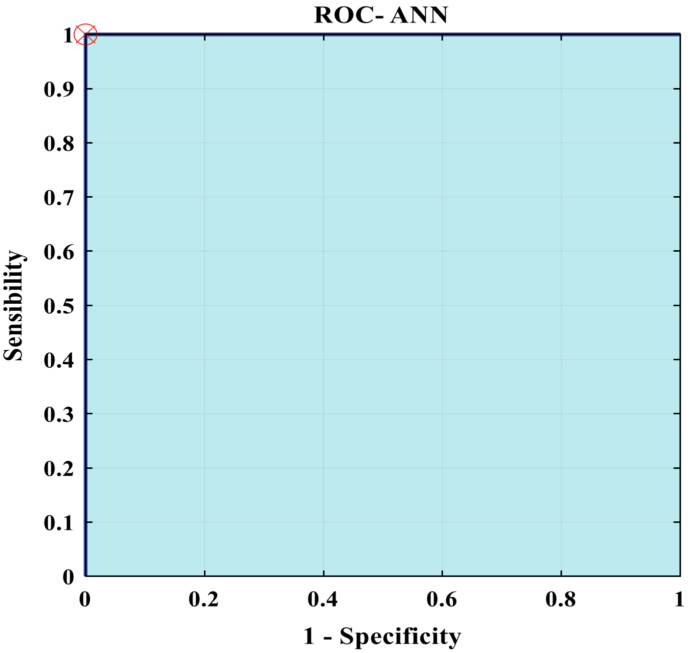


Fig. 10 Dataset 2—ROC curve for ANN

1. Malware analysis dataset contains static analysis data, the accuracy is 0.9946 and ROC is 1. In the Malware Good Ware dataset, the accuracy is 0.9946 and ROC is 1. In the approach, four classifications calculate the Receivers Operating Characteristic Curve, which represents 1—Specificity and Sensitivity.

5 Conclusion

This paper proposed a novel autonomous anomaly detection technique for securing the virtualized infrastructure in cloud computing based on clustering and classification. In this approach, the datasets are initially filtered by using K-means clustering. The clustered data are then directed into classifiers to obtain accurate classification outcomes. Different classifiers considered for evaluation include KNN, SVM, RF and ANN. The performance of classification can be observed through ROC parameters of individual models. The proposed method is found to achieve the best results in all the datasets. Therefore, it can be applied in virtual computer networks to provide full data security with attack detection. The future work is to integrate a DaaS software-defined networking with the present security analytic system to establish advanced security to the cloud networks. It is also significant to improve the framework through the experience acquired from the developers.

References

1. V. Ratten, Cloud computing technology innovation advances: a set of research propositions, in *Disruptive Technology: Concepts, Methodologies, Tools, and Applications* (2020), pp. 693–703
2. H. Shukur, S. Zeebaree, R. Zebari, D. Zeebaree, O. Ahmed, A. Salih, Cloud computing virtualization of resources allocation for distributed systems. J. Applied Sci. Tech. Trends. **1**(3), 98–105 (2020)
3. P.P. Angelov, X. Gu, Applications of autonomous anomaly detection. Stud. Comput. Intell. 249–259 (2018)
4. X. Gu, P. Angelov, Autonomous anomaly detection, in *Evolving and Adaptive Intelligent Systems (EAIS)* (2017)
5. B. Rohit, C. Rituparna, C. Nabendu, S. Sugata, A survey on security issues in cloud computing. Acta Tehnica Corviniensis – Bull. Eng. Tome. 160–177 (2014)
6. K. Rakesh, Applications of cloud computing in academic libraries. Library Waves **3**(1) (2017)
7. A. Negi, M. Singh, S. Kumar, An efficient security farmework design for cloud computing using artificial neural networks. Int. J. Comput. Appl. **129**(4), 17–21. November 2015. Published by Foundation of Computer Science (FCS), NY, USA
8. S. Liu, T.M. Khoshgoftaar, A.N. Richter, T. Hasanin, A survey of open source tools for machine learning with big data in the Hadoop ecosystem. J. Big Data **2**(1) (2015)
9. A. Gulenko, M. Wallschlager, F. Schmidt, O. Kao, F. Liu, Evaluating machine learning algorithms for anomaly detection in clouds. IEEE Int. Conf. Big Data (Big Data) (2016)
10. C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajarajan, A survey on security issues and solutions at different layers of Cloud computing. J. Supercomput. **63**(2), 561–592 (2012)
11. B. Asvija, R. Eswari, M.B. Bijoy, Security in hardware assisted virtualization for cloud computing—state of the art issues and challenges. Comput. Netw. **151**, 68–92 (2019)
12. M. Jouini, L.B.A. Rabai, A security framework for secure cloud computing environments, in *Cloud Security: Concepts, Methodologies, Tools, and Applications* (2019), pp. 249–263
13. H.R.A. Ariyaluran, F. Nasaruddin, A. Gani, H.I.A. Targio, E. Ahmed, M. Imran, Real-time big data processing for anomaly detection: a Survey. Int. J. Inf. Manag. (2018)
14. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing. Inf. Sci. **258**, 371–386 (2014)
15. K. Shantanu, J. Hiteshkumar, U. Kaushiki, Providing classification and security of Big Data in Cloud computing. Int. J. Tech. Res. Appl. **4**(2), 302–304 (2016)
16. F. Lombardi, R. Di Pietro, Secure virtualization for cloud computing. J. Netw. Comput. App. **34**(4), 1113–1122 (2011)
17. V.N. Inukollu, S. Arsi, S.R. Ravuri, Security issues associated with big data in cloud computing. Int. J. Netw. Secur. App. **6**, 39–45 (2014)
18. A.S. Ibrahim, J. Hamlyn-Harri, J. Grundy, Emerging security challenges of cloud virtual infrastructure (2016)
19. H. Zhengbing, G. Sergiy, K. Oksana, G. Viktor, B. Serhii, Anomaly detection system in secure cloud computing environment. Int. J. Comput. Netw. Inf. Secur. **4**, 10–21 (2017)
20. A. Mahendiran, N. Saravanan, S.N. Venkata, N. Sairam, Implementation of K-means clustering in cloud computing environment. Res. J. App. Sci. Eng. Tech. **4**(10), 1391–1394 (2012)
21. S. Ahmad, A. Lavin, S. Purdy, Z. Agha, Unsupervised real-time anomaly detection for streaming data. Neurocomputing **262**, 134–147 (2017)
22. T.Y. Win, H. Tianfield, Q. Mair, Big data based security analytics for protecting virtualized infrastructures in cloud computing. IEEE Trans. Big Data **4**(1), 11–25 (2018)

A Study on Clustering Facebook Multimedia Based on Metadata—A Comparative Analysis

Prashant Bhat and Pradnya Malaganve

1 Introduction

Knowledge discovery designates achieving useful or most important information among huge set of data which is gathered from several data warehouses [1] and other data sources. To attain this, data mining techniques are essentially used. In our research we are utilizing cluster techniques and algorithms to extract useful information by grouping the instances in different Clusters. Cluster is an unsupervised approach for grouping the instances of a data set [2]. The word unsupervised means there is no label for the instances where in supervised method contains label for the instances. In the present work we have explained the process of three clustering algorithms that are Expectation Maximization (EM), Simple K-Means, and Hierarchical Clusterer. These algorithms are applied on a data set of a cosmetic company's Facebook page. This data set contains 19 attributes such as total interactions, type, likes, and shares. These attributes are considered as Metadata of the dataset and 500 instances are present in the dataset. The attribute "type" has taken for the observation which further contains four kinds of instance that are Link, Status, Photo, and Video. We have used a method, i.e., Classes to Cluster Evaluation for all three Cluster algorithms and tested using WEKA data mining tool to get the essential results [3]. Based on the confusion matrix, time taken to build the model and number of incorrectly clustered instances, the comparison of all three algorithms is made and result is carried out to analyze in depth to prove the best suitable clustering algorithm for Facebook data set [4, 5].

P. Bhat · P. Malaganve (✉)
Garden City University, Bengaluru, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_7

1.1 Expectation Maximization

Expectation Maximization is a method of estimating max probable variables even when missing values present in the data set [6]. It is a repetitive process which generates the loop between two modes, namely, E-mode, i.e., estimation mode and M-mode, i.e., maximization mode [7]. In this approach E-mode strives to estimate the missing variables then the M-mode strives to develop the variables present in the data set to put the data into the model in a better way [8].

Expectation Maximization Algorithm

Step 1: Estimating latent or missing variables of the data set.
Step 2: Maximizing the variables that are present in the data set.

1.2 Simple K-Means Cluster

It is unsupervised learning algorithm that divides same number of instances [9, 10] to all the clusters as the algorithm shown below [11].

Simple K-Means Cluster Algorithm

Step 1: "n" number of instances are considered.
Step 2: All the instances are classified in "k" number of clusters.
Step 3: Mean value of the instances is calculated for "k" number of clusters.
Step 4: All the instances are compared with the mean value.
Step 5: The values which are near to mean value are exchanged to respective Clusters.
Step 5: Form new Cluster.
Step 6: Repeat Step 4 and Step 5 till instances are grouped correctly in each Clusters.

1.3 Hierarchical Clusterer

Rather than unstructured cluster, Hierarchical Clusterer is more informative and well-structured cluster. Below algorithm shows the process of Hierarchical Clusterer.

Hierarchical Clusterer Algorithm

Step 1: Form the Proximity or similarity matrix.
Step 2: Let each instance be a cluster.
Step 3: Combine two nearest clusters.
Step 4: Repeat Step 3 till single Cluster remains (Fig. 2).

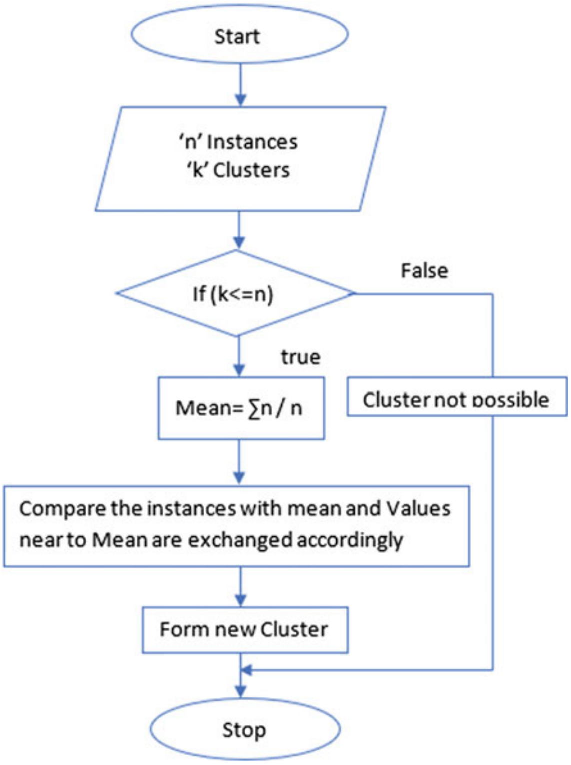


Fig. 1 Flowchart for simple K-means algorithm

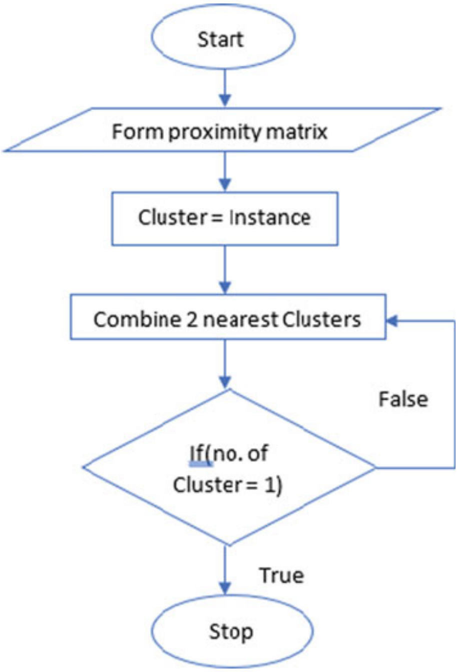
1.4 Classes to Cluster Evaluation

In the present work we have used a single method, i.e., Classes to Cluster Evaluation for all three above explained algorithms. This method applies Brut Force approach to find minimum class label errors to Clusters followed by a constraint that one class label can be assigned to only one Cluster. If any Cluster returns "No Class" that indicates all the instances under that particular Cluster are considered as incorrectly Clustered instances. In WEKA, Classes to Cluster Evaluation method initially ignores the instances and directly generates the Clusters. Then at the time of testing, it assigns the instances to the Clusters based on majority values of instances within each Cluster. And related confusion matrix will be formed.

2 Proposed Model for Clustering Multimedia Based on Metadata

Figure 3 represents the methodology that carries out achieving the detailed compar-

Fig. 2 Flowchart for hierarchical clusterer algorithm



ison analysis of Expectation Maximization, Simple K-Means, and Hierarchical Clusterer algorithms expecting for knowledge discovery and group data into respective clusters. We have shown five steps in the proposed model to achieve cluster algorithm results.

(1) Meta Data extraction process
(2) Pre-processing
(3) Cluster techniques
(4) Classes to Cluster Evaluation
(5) Result Analysis

Meta Data can be determined as data about data. As we have used cosmetic company's Facebook page data in the present work hence the Meta Data are URL of web page, number of likes, shares, comments type of the content uploaded, etc. These Meta Data need to be extracted from the web [12].

In this work, Info extractor tool is used for extracting the dataset that contains 19 attributes and 500 instances. Extracted data is stored in .CSV (Comma Separate Value) or .ARFF (Attribute Relation File Format) files for further findings. Initially the extracted data will be unrefined or raw.

Hence, we move to the next stage, i.e., Pre-processing. The term Unrefined means the dataset may contain huge amount of noise in it. For example, missing values in the dataset or the dataset may contain such values which cannot be understood and are meaningless. So, the unrefined data will be purified. In data mining several [13]

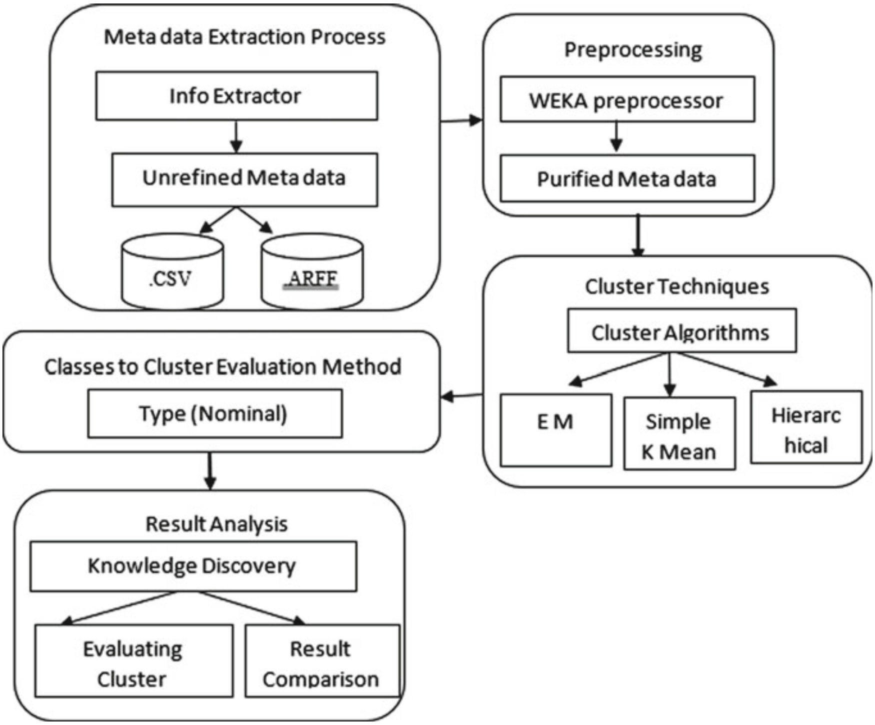


Fig. 3 Proposed model for clustering multimedia based on metadata

techniques are available to fill the missing values. For example, we can use most frequently appeared value of the respective column to fill the gap, by calculating the mean value of remaining instances the missing value can be filled, one global value can be declared such as “null” to fill the missing and so on. Using these techniques manually we can fill the gap in the dataset which is termed as pre-processing the noisy data. In present work we have used WEKA tool for pre-processing as the dataset is large in size.

The very next step carries three cluster algorithms that are Expectation Maximization, Simple K-Means, and Hierarchical Clusterer algorithm for the experiment. All three respective algorithms and flowcharts are defined in the introduction section algorithms are to be applied on the dataset for knowledge discovery. The resultant parameters are compared and analyzed in detail.

In the introduction section we have explained the process of the method, Classes to cluster evaluation. To group four instances that are Photo, Status, Video, and Link into four different clusters this method is used. And these four instances belong to “type” Metadata. “Type” contains nominal values, i.e., non-numeric.

The final step is to determine the relationship between variables and to compare the findings of all three algorithms considered in this research work. Evaluating cluster results and analyzing the result in depth leads to knowledge discovery.

2.1 Attributes Descriptions of Table 1

Page total likes: It indicates the total number of users those who have liked the cosmetic company's Facebook page.

Type: This attribute indicates the content type, whether the content is link, video, photo, or status.

Category: It indicates the characterization of the manual content.

Post month: This attribute indicates in which month the post is published.

Post week: This attribute indicates in which week the post is published.

Post hour: This attribute indicates at what time the post is published.

Table 1 Attributes descriptions

Name of attribute	Data type	Description
Page total likes	Numeric	Number of users who liked the company's page
Type	String	Type of content (Link, Photo, Video, Status)
Category	Numeric	Manual content characterization
Post month	Numeric	Post published month
Post week	Numeric	Post published week
Post hour	Numeric	Post published hour
Paid	Numeric	Company paid to the Facebook for advertising
Lifetime post total reach	Numeric	Number of unique users who saw the page post
Lifetime post total impression	Numeric	Number of times a post from a page is displayed
Lifetime engaged users	Numeric	Number of unique users clicked anywhere in the post
Lifetime post consumers	Numeric	Number of users clicked anywhere in the post
Lifetime post consumptions	Numeric	Numbers of clicks anywhere in the post
Lifetime Post Impressions by people who have liked your Page	Numeric	Number of impressions by users who have liked the page
Lifetime Post reach by people who like your Page	Numeric	Number of unique users saw a page post because they have liked it
Lifetime People who have liked your Page and engaged with your post	Numeric	Number of unique users liked and clicked anywhere in the post
Comment	Numeric	Number of comments of the post
Like	Numeric	Number of likes of the post
Share	Numeric	Number of shares of the post
Total interactions	Numeric	Sum of comments, likes and shares of the post

Paid: This attribute shows whether the cosmetic company has paid to the Facebook for its advertisement. Attribute values will be in the form of yes/no.

Lifetime post total reach: It shows the number of unique users who have seen the page post.

Lifetime post total impression: It indicates the number of times the post from company's page has appeared whether it is clicked or not. For example, first time when it is updated, second time, if a friend put any comment on it or if a friend shares it.

Lifetime engaged users: It shows the number of unique users who have clicked anywhere in a post.

Lifetime post consumers: This attribute indicates the total number of users who have clicked on the page.

Lifetime post consumptions: It shows the total number of clicks anywhere in a post.

Lifetime Post Impressions by people who have liked your Page: It shows the number of impressions only from the users who have liked a page.

Lifetime Post reach by people who like your Page: It is the total number of unique users who saw a page post only because they have liked it.

Lifetime People who have liked your Page and engaged with your post: It shows the number of unique users who have liked a page and also clicked anywhere in a post.

Comment: Total number of comments present on a post.

Like: Total number of likes present on a post.

Share: Total number of shares on a post.

Total Interactions: This attribute is the total number of comments, number of likes, and number of shares on a post.

3 Results and Analysis

3.1 Confusion Matrix

Confusion Matrix is to identify all the clustered instances of a dataset. By this matrix formation, we can identify correctly clustered and incorrectly clustered instances. The confusion matrix of all three algorithms is shown in Tables 2, 3, and 4.

Table 2 is formed using WEKA and the first row of the confusion matrix is assigned to classes, i.e., Cluster 0, Cluster 1, Cluster 2, and Cluster 3. And the remaining values of the matrix indicate all the instances of the dataset which are grouped as different clusters. Table 2 delivers that Expectation Maximization algorithm has formed four clusters and it has divided the instances in respective clusters as below.

Cluster 0 is holding 34 "status" instances that are clustered correctly.

Cluster 1 is holding 183 correctly clustered instances which are "photo".

Cluster 2 is holding 4 correctly clustered instances which are "video".

Table 2 Confusion matrix expectation maximization

0	1	2	3	← Assigned to Class
101	183	47	95	Photo
34	1	9	1	Status
8	7	2	5	Link
3	0	4	0	Video
Cluster 0 ← Status				
Cluster 1 ← Photo				
Cluster 2 ← Video				
Cluster 3 ← Link				

Table 3 Confusion matrix simple K-means

0	1	2	3	← Assigned to Class
40	51	307	28	Photo
8	0	35	2	Status
4	0	16	2	Link
4	0	3	0	Video
Cluster 0 ← Status				
Cluster 1 ← No Class				
Cluster 2 ← Photo				
Cluster 3 ← Link				

Table 4 Confusion matrix hierarchical clusterer

0	1	2	3	← Assigned to Class
40	51	307	28	Photo
8	0	35	2	Status
4	0	16	2	Link
4	0	3	0	Video
Cluster 0 ← Status				
Cluster 1 ← No Class				
Cluster 2 ← Photo				
Cluster 3 ← Link				

Cluster 3 is holding 5 “link” instances that are clustered correctly.

Table 3 represents the confusion matrix of Simple K-Means algorithm and the number of correctly clustered instances belong to four different categories are shown below which is determined using WEKA Data Mining tool.

Cluster 0 is holding 8 “status” instances that are clustered correctly.

Cluster 1 is holding 0 instances.

Cluster 2 is holding 307 correctly clustered instances which are “photo”.

Cluster 3 is holding 2 “link” instances that are clustered correctly.

Simple K-Means is containing Cluster 1 as null or no class that indicates the algorithm has not clustered video instances from the dataset.

Table 4 represents the confusion matrix of Hierarchical Clusterer algorithm and below are the number of correctly clustered instances which are formed with the help of WEKA.

Cluster 0 is holding 423 “photo” instances that are clustered correctly.

Cluster 1 is holding 0 instances.

Cluster 2 is holding 0 instances.

Cluster 3 is holding 0 instances.

In Hierarchical Clusterer, Cluster 1, Cluster 2, and Cluster 3 are having 0 instances. This indicates that the algorithm has not clustered video, status, and link instances correctly in particular group.

3.2 Analysis of Table 5

Table 5 gives the distinct result of all three algorithms. As we observe all the readings of Table 5, Expectation Maximization has incorrectly clustered 274 instances out of 500 instances, i.e., 54.8% instances are clustered wrong. Hence correctly clustered instances are 226. In Simple K-Means algorithm findings, incorrect clustered instances are 183, i.e., 36.6% instances are not clustered correctly. Hence correctly clustered instances are 317. Compared to Expectation Maximization algorithm, Simple K-Means algorithm has better numbers while clustering the instances in particular group. The algorithm Hierarchical Clusterer has incorrectly clustered 77 instances and 15.4% instances of the whole dataset is incorrect. Hence correctly clustered instances are 423 and by observing incorrectly clustered values of all three algorithms, we can say that Hierarchical Clusterer is having very less instances which are clustered incorrectly. Hence Hierarchical clusterer can produce the best accuracy in clustering the Facebook dataset in a better way.

The time taken to build all three models is minimum as all the algorithms have taken less than 1 s to get executed. And according to the observations, it clearly indicates that the Simple K-Means cluster takes the least time to generate the model.

Table 5 Comparison analysis based on correctly clustered instances and time taken to build the model

	Expectation maximization	Simple K-means	Hierarchical clusterer
Incorrectly clustered instances	274.0	183.0	77.0
	54.8%	36.6%	15.4%
Time taken to build the model	0.42 s	0.02 s	0.83 s

4 Conclusion

After analyzing all the variables and readings of all three algorithms, it's proven that Hierarchical Clusterer is the best suitable algorithm for clustering Facebook pages dataset in a better way, as the algorithm has correctly clustered 423 instances out of 500 instances which is highest compared to Simple K-Means and Expectation Maximization algorithms. Hence, we would like to conclude that, because of the structure and formation of Hierarchical Clusterer, the algorithm is capable of clustering the instances in a better way as it considers every instance as a cluster and go on combining nearest clusters until formation of a single cluster.

References

1. C. Maionea, D.R. Nelsonb, R.M. Barbosa, Research on social data by means of Cluster analysis. 2210–8327/Ó2018 Production and hosting by Elsevier B.V.
2. S. Ding, F. Wu, J. Qian, Research on data stream clustering algorithms. Artif. Intell. Rev. **43**, 593–600 (2015)
3. P. Bhat, P. Malaganve, P. Hegade, A new framework for social media content mining and knowledge discovery. IJCA **182**(36), 17–20 (2019)
4. A. Shensa, J.E. Sidani,' M.A. Dew,' C.G. Escobar-Viera, B.A Primack, Social media use and depression and anxiety symptoms: a cluster analysis. **42**(2), 116–128 (2018)
5. C.C. Aggarwal, C. Zhai, A survey of text clustering algorithms, in *Mining Text Data,* ed. by C. Aggarwal, C. Zhai (Springer, Boston, MA). https://doi.org/10.1007/978-1-4614-3223-4_4
6. https://machinelearningmastery.com/expectation-maximization-em-algorithm/
7. C.K. Reddy, H. Chiang, B. Rajaratnam, TRUST-TECH-based expectation maximization for learning finite mixture models. IEEE **30**(7), 1146–1157 (2008). https://doi.org/10.1109/TPAMI.2007.70775.
8. S.P. Algur, P. Bhat, Web video object mining: expectation maximization and density based clustering of web video metadata objects. I. J. Inf. Eng. Electron. Bus. **1**, 69–77 (2016). https://doi.org/10.5815/ijieeb.2016.01.08
9. Y.G. Jung, M.S. Kang, J. Heo, Clustering performance comparison using K means and expectation maximization algorithm. Biotechnol. Biotechnol. Equip. **28**(sup1), S44–S48. https://doi.org/10.1080/13102818.2014.949045
10. N. Dhanachandra, K. Manglem, Y.J. Chanu, Image segmentation using K means clustering algorithm and subtractive clustering algorithm, in *IMCIP* (2015)
11. https://www.tutorialride.com/data-mining/KMeans-Clustering-in-data-mining.htm
12. M. Othman, S.A. Mohamed, M.H.A. Abdullah, M.M. Yusof, R. Mohamed, A framework to cluster temporal data using personalised modelling approach, in *Ghazali, SCDM 2018. Advances in Intelligent Systems and Computing*, vol. 700 (Springer, Cham, 2018)
13. S. Harifi, E. Byagowi, M. Khalilian, *Comparative Study of Apache Spark MLlib Clustering Algorithm: DMBD 2017* (Springer International Publishing AG, 2017). LNCS **10387**, 61–73 (2017). https://doi.org/10.1007/978-3-319-61845-6_7
14. H. Jia, S. Ding, X. Xu, The latest research progress on spectral clustering. Neural Comput. Appl. **24**, 1477–1486 (2014)
15. R. Vaarandi, M. Pihelgas, LogCluster—a data clustering and pattern mining algorithm for event logs, in *CNSM*, Barcelona (2015), pp. 1–7
16. **81**, 1 March 2015. https://doi.org/10.1016/j.energy.2014.12.054
17. S. Ajani, M. Wanjari, An efficient approach for clustering uncertain data mining based on hash indexing and voronoi clustering, in *5th International Conference and Computational Intelligence and Communication Networks,* Mathura (2013), pp. 486–490

18. H. Nguyen, Y. Woon, W.A. Ng, Survey on data stream clustering and classification. Knowl. Inf. Syst. **45**, 535–569 (2015). https://doi.org/10.1007/s10115-014-0808-1
19. F.T. Giuntini et al., How do i feel? Identifying emotional expressions on facebook reactions using clustering mechanism. IEEE Access **7**, 53909–53921 (2019). https://doi.org/10.1109/ACCESS.2019.2913136
20. S. Moro, P. Rita, B. Val, Predicting social media performance metrics and evaluation of the impact on brand building: a data mining approach. J. Bus. Res. (Elsevier) (2016)

A Big Impact of Social Network Analysis and Machine Learning Algorithms for Predicting Facts of Covid-19 Pandemic

Sonam and Surjeet Kumar

1 Introduction

On the basis of report covered under 'survey of Global Digital Growth 2019–20', there were 304 million people as an active social network users, of which, 2498 people were Facebook users. Therefore, Facebook is a good platform from where people may access to the facts about Covid-19. People share their physical and psychological impact on Facebook portal and subsequently follow the suggestions [1]. People are joining with like, comment, and share on all the posts by WHO at Facebook platform and getting updates related to Covid-19 every day. The algorithm has a crucial role for the advancement of Facebook posts. Day by day, varieties of useful data are handled by using 'big data' analysis [2]. Facebook generates 4 Petabyte data each day. All stored data known as hive that contains 300 Petabyte of data. After analyzing social network we can boost our attractive and quantitative graph metric that provides relationship between nodes and edges. We generally face major challenges choosing appropriate algorithm for social network analysis and prediction. Machine learning algorithms have vital role to make all information available on one platform just like Facebook.

2 Impact of Algorithm on Social Network

Every Facebook user's action starts with commenting on photos, liking to post messages or posting videos [3]. All are shown by algorithm in the final analysis. The goal is to satisfy everyone to ensure the customers only receive information that is valuable to them [4].

Sonam (✉) · S. Kumar
Department of Computer Applications, VBS Purvanchal University, Jaunpur, UP, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_8

Since Facebook algorithms esteem the quality of post and express main factors of audience engagement [5]. Then, work of algorithm on Facebook is [6]:

- Affection
- Variety of theme or text
- Communication
- Contemporary
- Variation
- Productive outcome by Links

3 Major Role of Covid-19 Information Center Posts on Facebook

We have identified Covid-19 information center menu that is available on Facebook [7]. It contains.

Latest updating post—post source is WHO related to India and global Covid-19 cases.

Fact about Covid-19—WHO posts are accurate free from day to day rumors about covid-19.

Recent post—Post from government community and public health organization pages such as recent post on Facebook by WHO, MyGovCoronaHub, MoHFW India, UNICEF, and ABHWCs, etc.

All the request, help, suggestions, and prevention tips are available on Facebook about Covid-19. We collected some unique post from Facebook through WHO pages and plotting data for" like", "comment" and "share". We are showing by Fig. 1.

There are 6 lakhs "likes" on the posts, posted by WHO at Facebook.

According to comment distribution, there are 10,000 comments on posts that are shown in Fig. 2.

There are 50,000 people, sharing WHO posts that is shown in Fig. 3.

4 Using Networkx Technique for Analysis of Facebook

We are using "Networkx" [8] for analyzing social network that draw a specific graph for node and edges on the basis of attributes which are available in dataset [9]. Graph G works as a container for adding the collected form of edges and nodes [10].

It is expressed by properties of graph such as G.node, G.edge and G.degree used to express every value [11]. We generated graph to identify all nodes for multiple public health organization and expressing node.

On the base of WHO Post, the list of all nodes, edges, and degree values is shown in Table 1.

Graph shown in below that expresses all nodes and edges (Fig. 4).

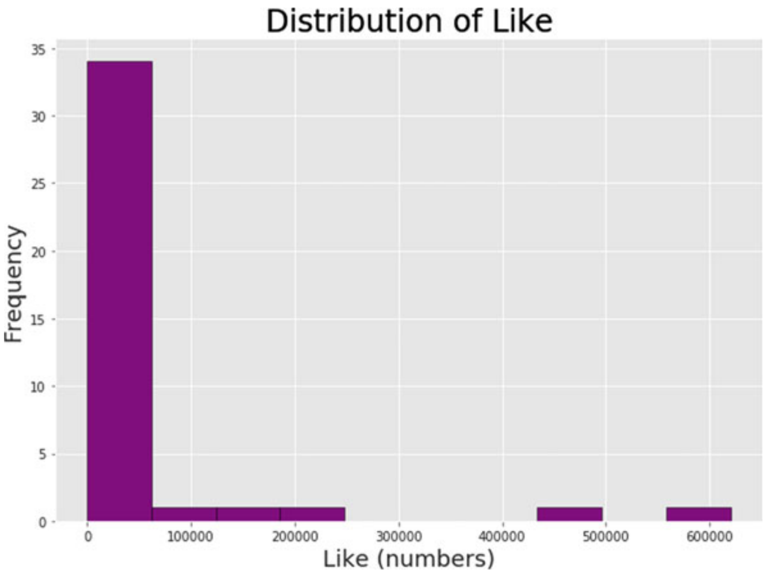


Fig. 1 Distribution of Like

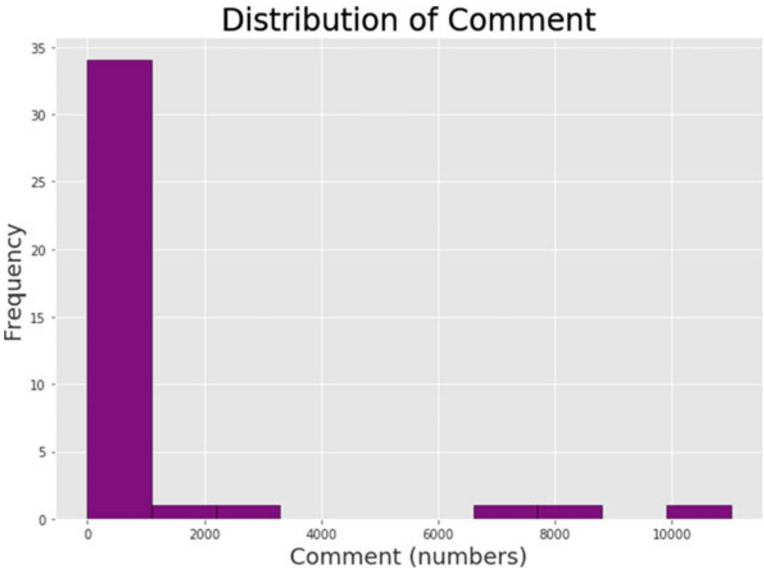


Fig. 2 Distribution of Comment

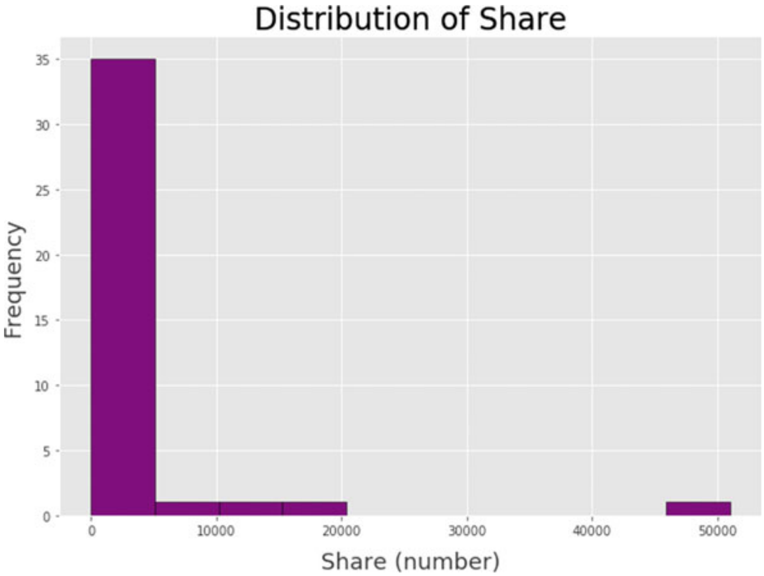


Fig. 3 Distribution of Share

5 Experimental Work and Deliberation of Algorithms

5.1 Random Forest Regressor to Predict Interaction Among People with Public Health Organization

Integrating several decision trees into one model that is the random forest regression technique which is a supervised machine learning method [12]. It mostly uses an ensemble learning algorithm [13]. It also makes a decision tree accompanying of training and generates results as a mean prediction. Hyper parameter [14] refers to attributes which is used for splitting data and identifying accurate percentage.

A big advantage of this ensemble method [15] is to recognize all predicted features. Output would be generated as an average into a specific ensemble property that gets output for every decision tree [8].

We collected 500 posts from all public health organization that is accessible on Facebook social networking sites. We applied algorithm of random forest regressor [16] with splitting train and test with number of estimators is 50 and random state 1 Correlated data are depicted from correlation map among all features. It predicts accurate values on the basis of independent and dependent variable and identifies approximately 6 lakh people are interacting with sWHO posts among 500 posts.

People are interacting with all public health organization on the base of their post shown in Fig. 5.

Table 1 Feature of networkx

Total _Number_of _nodes: 60
Total_Number_of_edges: 10
List of all nodes: [‘1’, ‘2’, ‘3’, ‘4’, ‘5’, ‘6’, ‘7’, ‘8’, ‘9’, ‘10’, ‘11’, ‘12’, ‘13’, ‘14’, ‘15’, ‘16’, ‘17’, ‘18’, ‘19’, ‘20’, ‘21’, ‘22’, ‘23’, ‘24’, ‘25’, ‘26’, ‘27’, ‘28’, ‘29’, ‘30’, ‘31’, ‘32’, ‘33’, ‘34’, ‘35’, ‘36’, ‘37’, ‘38’, ‘39’, ‘40’, ‘41’, ‘42’, ‘43’, ‘44’, ‘45’, ‘46’, ‘47’, ‘48’, ‘49’, ‘50’, ‘60,400’, 1, 2, 6, 3, 4, 5, 8, 9, 7]
List of all edges: [(1, 2, {}), (1, 6, {}), (2, 3, {}), (2, 4, {}), (2, 6, {}), (6, 7, {}), (3, 4, {}), (3, 5, {}), (4, 8, {}), (4, 9, {})]
Degree for all nodes: {‘1’: 0, ‘2’: 0, ‘3’: 0, ‘4’: 0, ‘5’: 0, ‘6’: 0, ‘7’: 0, ‘8’: 0, ‘9’: 0, ‘10’: 0, ‘11’: 0, ‘12’: 0, ‘13’: 0, ‘14’: 0, ‘15’: 0, ‘16’: 0, ‘17’: 0, ‘18’: 0, ‘19’: 0, ‘20’: 0, ‘21’: 0, ‘22’: 0, ‘23’: 0, ‘24’: 0, ‘25’: 0, ‘26’: 0, ‘27’: 0, ‘28’: 0, ‘29’: 0, ‘30’: 0, ‘31’: 0, ‘32’: 0, ‘33’: 0, ‘34’: 0, ‘35’: 0, ‘36’: 0, ‘37’: 0, ‘38’: 0, ‘39’: 0, ‘40’: 0, ‘41’: 0, ‘42’: 0, ‘43’: 0, ‘44’: 0, ‘45’: 0, ‘46’: 0, ‘47’: 0, ‘48’: 0, ‘49’: 0, ‘50’: 0, ‘60,400’: 0, 1: 2, 2:4, 6: 3, 3: 3, 4: 4, 5: 1, 8: 1, 9: 1, 7: 1}
Total_Number_of_self-loops: 0
List of all nodes with self-loops: []
List of all nodes we can go to in a single step from node 1:50 [2, 3, 5, 6]

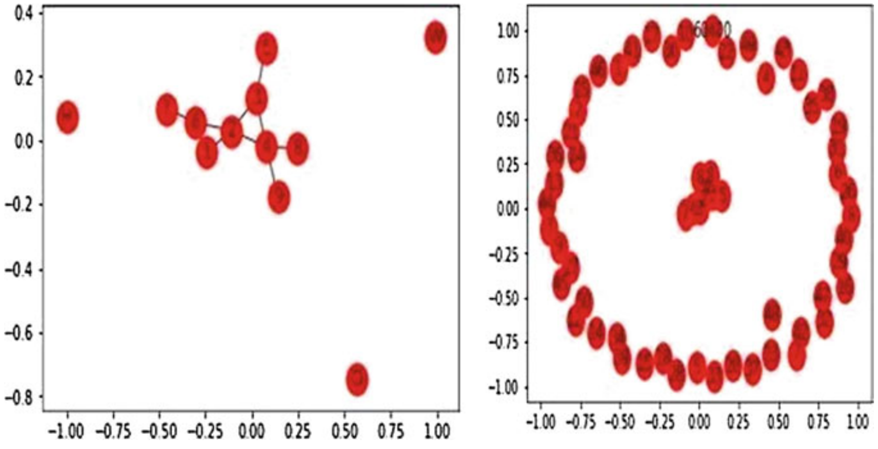


Fig. 4 Networkx: nodes and edges

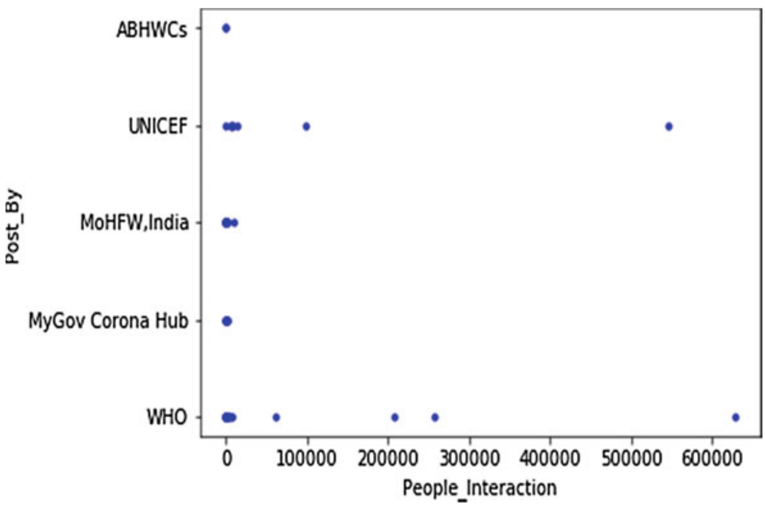


Fig. 5 People interaction with all health community

Interaction between people with WHO post that is depicted on plot shown in Fig. 6.

On the base of our dataset we applied train and test after that we identified predicted value (Fig. 7).

After training dataset we applied algorithm for relation between predicted and test values shown in Fig. 8.

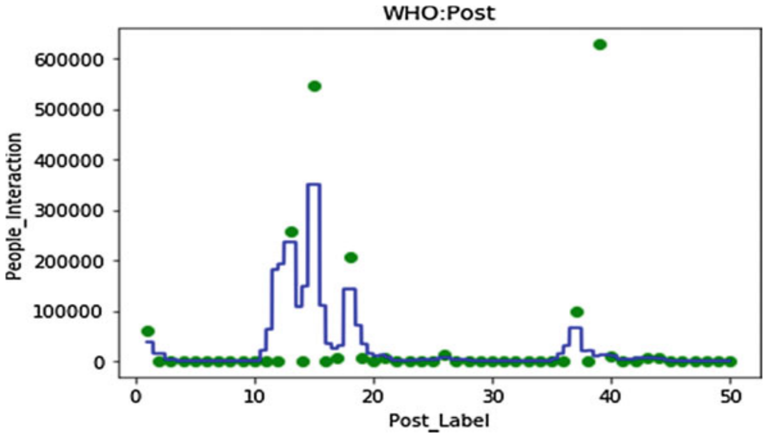


Fig. 6 People interaction with WHO

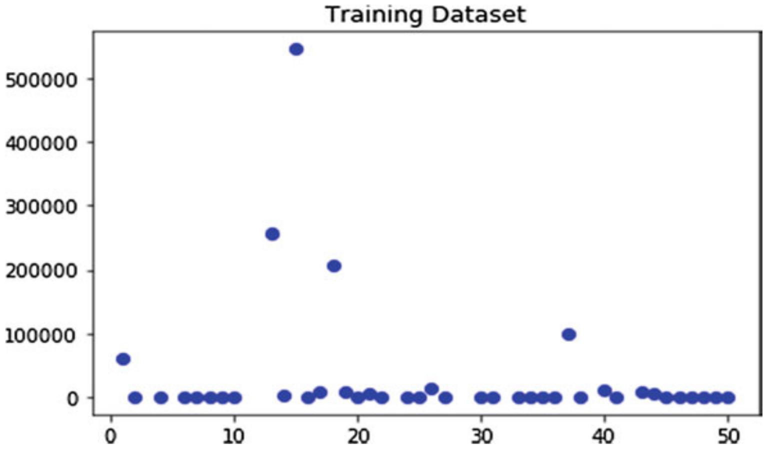


Fig. 7 Analyze for training data

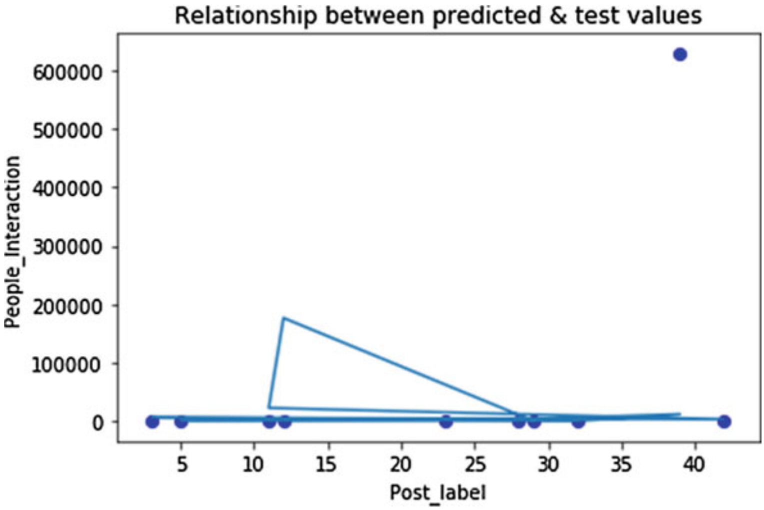


Fig. 8 Analysis for test data and predicted value

5.2 Analysis Feature of Time Series Forecasting: Arima and Sarima Model

A time series is a sequencing step of recording metrics at regular intervals, whereas forecasting is nothing but which step and on where we identify to predict future values that the series will adopt. We have applied model that is Arima [17] and Sarima to predict new case of Covid-19 disease till October.

Arima model is the best forecasting method. It refers as automatic regression integrated moving average which is a forecasting algorithm that is based on some ideas such as data available according to the previous values of time series for predicting future values. Arima model can be applied that exhibits pattern by non-seasonal time series and are not random white noise. Autoregressive [18] as a linearly regression model that uses lags as predictor.

An Arima model combines three methods—Autoregressive, Integrated, and moving average that takes 3 parameters such as p, d, q.

p—Order of automatic regression terms.

d—Difference that requires for making time series stationary.

q—Order of moving average terms. It refers to the number of lagging prediction errors that should be entered into the ARIMA model.

Purely, autoregressive model in which Yt refers as past values that have own lags [19]. That's why Yt is used as a function for Lags of Yt. Arima algorithm is identified by formula such as Eq. 1.

$$Yt \;= \alpha + \beta 1\ Yt - 1 + \beta 2\ Yt - 2 + \ldots\ \beta p\ Yt - p + €1 \tag{1}$$

In this model, the time series differs at least once to stabilize it, and then AR and MA terms are combined. Therefore, Predicted value of Yt = constant + linear combination lags of Y (up to p lags) + linear combination of lagged forecast errors (up to q lags). That's why equation becomes as Eq. 2.

$$Yt \;= \alpha + \beta 1\ Yt - 1 + \beta 2\ Yt - 2 + \ \ldots\ \beta p\ Yt - p\ \ €t\ + \Phi 1\ \ €t - 1\ \ + \Phi 2\ \ €t - 2 + .. + \Phi q\ €t - q \tag{2}$$

5.3 How Arima Model Works on Dataset?

At first we collected data for predicting new case of Covid-19 disease for India, downloaded from WHO link [20] https://covid19.who.int/region/searo/country/in. We found 184 rows and 5 columns of data from January to July. After that we identified new cases from 30th January to 31st July, 2020. The best solution is applying common method to differentiate it. We are showing dataset as a plot expresses as (Fig. 9).

According to plotting figure we have found everyday cases are different so the series is not stationary, it can be made after differencing. After differencing once, series is called a unified order 1 and denotes as I(1) or I(d)1. If autocorrelation is positive for several delays such as 10 or above, sequences need to be different. In another hand, if lag 1 autocorrelation is too negative, series may be overly differentiated. According to p-value time series [19] is indeed stationary.

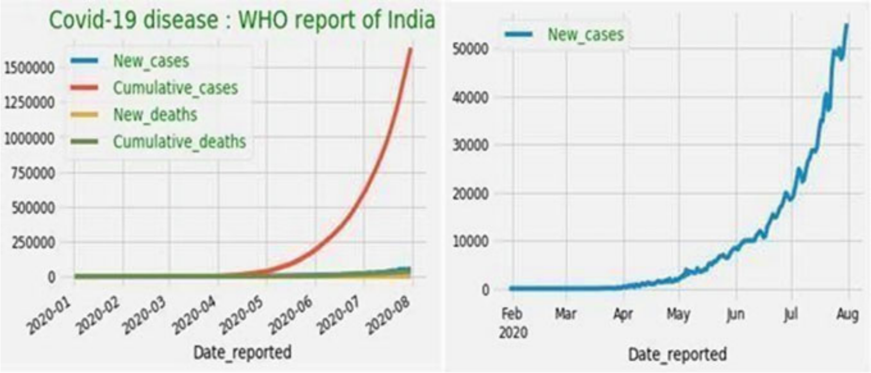


Fig. 9 Plotting data from WHO dataset

So, convert from series to stationary, the method is differentiation that means subtract past value from current value. The value of d is least number of differentiation need to make from series to stationary. If d = 0, then time series is stationary.

In our cases, we calculated the differentiates of data frame values that is comparing with other next value.

That is cases_diff = cases.diff (periods = 1) we used periods = 1 shifted to calculate difference that accepts neutralize value that is showing on autocorrelation figure.

Autocorrelation is the similarity between observations as a function at the time lag between them –1 to +1. The AIC is defined by a simple equation from the sum of squares and aggregate degree of freedom for the two models.

Mean square error indicates distances between regression line and set of points. Distances refer as error that mean using mean squared error we found average according to set of errors. We used Arima order to identify AIC value and extract mean square error [21]. After fitting Arima model. We deducted AIC values and minimum value indicates better model and predicted value on test dataset [22] (Fig. 10).

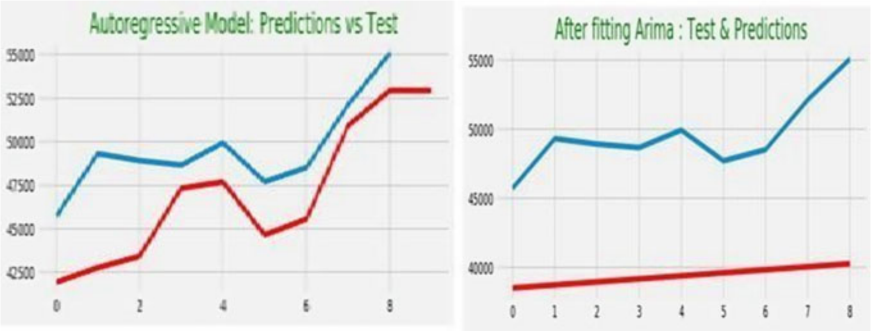


Fig. 10 Autoregressive: test and prediction

P = d = q = range (0, 2) is better for predicting AIC value that's order is (0, 1, 1) and same as AIC value with fitting ARIMA model [23].

To determine a proper model for a given time series data, it is necessary to carry out the ACF analysis.

5.4 Seasonal Autoregressive Integrated Moving Average (SARIMA) Model

This proposed model is known as the Seasonal ARIMA (SARIMA) model. In this model seasonal differencing of appropriate order is used to eliminate non-stationarity from the series. A first-order seasonal difference is the difference between an observation and the corresponding observation from the previous year and is calculated as Z t = Y t – Y t – S during month-wise time series $s = 12$ and for quarterly time series $s = 4$.

This model is generally termed as the SARIMA (p, d, q) × (*P*, *D, Q*) *s* model. The seasonal period, s, defines the number of observations that make up a seasonal cycle. The value of s is fixed in the series. If we have daily data and the seasonal period is the length of the month, s will be approximately 30, but it will vary from month to month. Histogram features is shown in Fig. 11.

With daily data we can have weekly seasonality, with s = 7, monthly, with s = 30 and yearly, with s = 365. We have assumed that there is only one type of seasonality and at the ending of section we will observe how to extend the methods presented to various seasonal periods [24] (Fig. 12).

Using algorithm we have observed forecast analysis which successfully predict values for upcoming months from August to October (Fig. 13).

Finally, we have predicted New Cases value is up to 104,894 on Date 23/10/2020 that would be approximate value of WHO dataset.

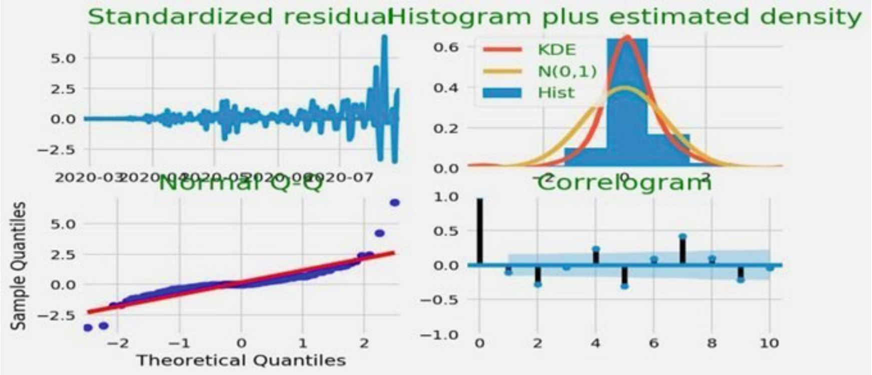


Fig. 11 Histogram features

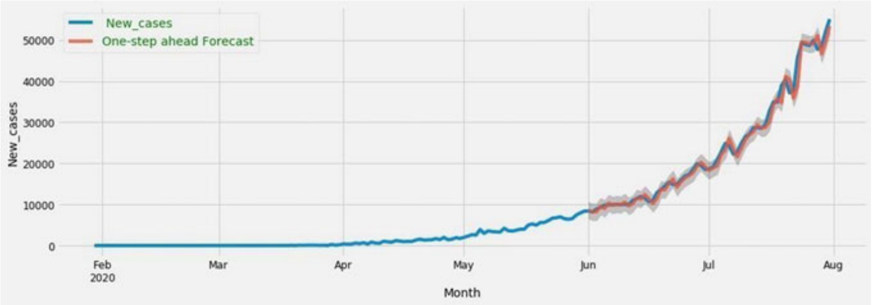


Fig. 12 Analysis for daily cases

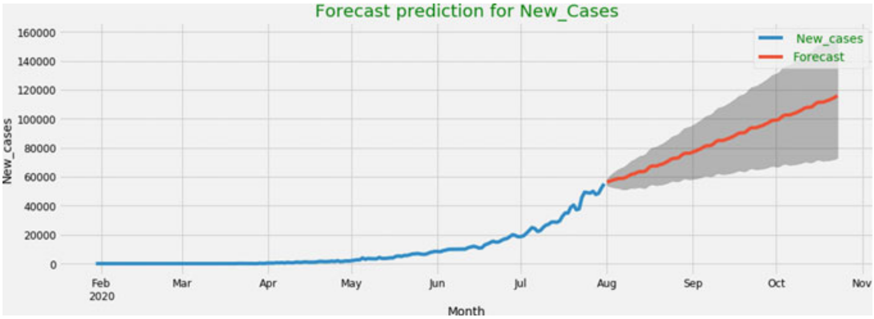


Fig. 13 Forecast future prediction for new cases

6 Conclusion

This work is an attempt to elucidate the importance of employing machine learning tools for getting a meaningful result to receiving ends. The work at first collects dataset of interaction between people and all the respective agencies like AB- HWCs, UNICEF, MoHF, MyGov corona Hub and WHO and proves through applying random forest regressor technique that out of all the agencies, WHO receiving maximum interaction. Also, our work validates the previous notion about the credibility of the two presently available tools ARIMA and SARIMA for future prediction. Here it has been proved by mining dataset up from January to July 2020 and employing the machine learning tool ARIMA and SARIMA to predict new Covid cases up to October 2020. By varying further about the predicted result with WHO database about new cases, it matches approximately validating these two open-source tools. The prediction can generously be used for deploying help, prevention, and propagating public awareness about this pandemic Covid-19.

References

1. G. Bello-Orgaz, J. Jung, D. Camacho, Social big data: recent achievements and new challenges. J. Info. Fusion **28**, 45–59 (2016)
2. H.A. Chalabi, U.C. Apoki, A. Hibah, A. Alsaad, Big data analysis using social networks, in *Conference* (IEEE, Iraq, 2017)
3. H.J. Esfahani, K. Tavasoli, A. Jabbarzadeh, Big data and social media: a scientometrics analysis. J. Dat. Net. Sci. **3**, 145–164 (2019)
4. S. Stieglitz, M. Mirbabaie, B. Ross, C. Neuberger, Social media analytics–challenges in topic discovery, data collection, and data preparation. J. Inf. Manag. **39**, 156–168 (2018)
5. M.M. Mariani, M. Di Felice, M. Mura, Facebook as a destination marketing tool: evidence from Italian regional destination management organizations. J. Tour. Manag. **54**, 321–343 (2016)
6. R. Devakunchari, C. Valliyammai, Big social data analytics: opportunities, challenges and implications on society, in *Conference on Communication, Media, Technology and Design*, Zagreb–Croatia (2016), pp. 27–29
7. Fact of Covid-19 information center, https://www.Facebook.com/coronavirus_info/?page_source=bookmark
8. K.S. Sonam, Analyzing and predicting social networking big data: using network and regression techniques. J. Adv. Sci. Technol. **29**(03), 8087–8096 (2020)
9. R.K. Devi, A machine learning-based online social network analysis for 360-degree user profiling. J. Innov. Tech. **9**(2S2), 2278–3075 (2019)
10. N.B. Lassen, L. Cour, R. Vatrapu, Predictive analytics with social media data, BK-SAGE-SLOAN_QUAN-HAASE-160238-CHP20.indd, in The *Sage Handbook of Social Media Research Methods* (2016)
11. T. Kaushik, S. Singhal, J. Mandan, K. Sharma, Social networking analysis: a case study in tools. J. Eng. Adv. Tech. **8**(2), 2249–8958 (2018)
12. C.C. Hsu, Y.C. Lee, P.E. Lu, S.S. Lu, Social media prediction based on residual learning and random forest, in *Conference. SERSC* (2017)
13. X. Gao, J. Wen, C. Zhang, *An Improved Random Forest Algorithm for Predicting Employee Turnover* (2019)
14. M. Fadhil, P. Andras, A systematic analysis of random forest based social media spam classification, in *11th International Conference, NSS 2017, Proceedings*, Helsinki, Finland (2017), pp. 427–438
15. K. Sridevi, B.V.S. Samrat, S. Srihari, Traffic analysis by using random forest algorithm considering social media platforms. J. Res. Tech. **7**(6S), 2277–3878 (2019)
16. V.M. Herrera, M. Taghi, F.B. Khoshgoftaar, Random forest implementation and optimization for big data analytics on Lexis Nexis's high performance computing cluster platform. J. Big Data **68** (2019)
17. V. Chaurasia, S. Pal, Application of machine learning time series analysis for prediction of Covid-19 pandemic. Res. Biomed. Eng. (2020)
18. L.V.D. Alquisola, J.A.B. Coronel, M.F. Reolope, J.N.A. Roque, Pre-diction and visualization of the disaster risks in the Philippines using discrete wavelet transform (DWT), autoregressive integrated moving average (ARIMA), and artificial neural network (ANN), in *3rd International Conference on Computer and Communication Systems (ICCCS)* (2018), pp. 146–149
19. R. Adhikari, R.K. Agrawal, An introductory study on time series modeling and forecasting. J. LAP (Lambert Academic Publishing, Germany) (2013)
20. Collection of dataset for covid19 cases, https://covid19.who.int/dataset
21. Q. Yang, X. Wang, Research on covid-19 based ARIMA MODEL—Taking Hubei, China as an example to see the epidemic in Italy. J. Inf. Pub. Health (2020)
22. D. Benvenuto, M. Giovanetti, L. Vassallo, S. Angeletti, M. Ciccozzi, Application of the Arima model on Covid2019 epidemic dataset. J. Data In Brief **29** (2020)

23. A. Hernandez-Matamoros, H. Fujita, P. Meana, Forecasting of covid19 per regions using Arima models and polynomial functions. J. Elsev. Pub. Health Emerg. Collect. **96** (2020)
24. A. Tarsitano, I.L. Amerise, Short-term load forecasting using a two-stage sarimax model. J. Econpaper Energy **133**, 108–114 (2017)

A Framework for Crowdfunding Platform Using Ethereum Blockchain Technology

Jatin Manav Mutharasu, Utshav Pandey, B. Rethick, Bhavika Kulkarni, and Prof. Mohandas Pawar

1 Introduction

1.1 Crowdfunding

In crowdfunding, companies pitch their idea to a large network of people and provide them an opportunity to invest in it if they find it promising rather than call for a small knowledgeable group of investors as mentioned in [1]. Crowdfunding has become a valuable means of raising capital investment and has given non-traditional projects, such as ideas of start-ups or hopeful creatives, a new audience to pitch their idea. Small Companies especially benefit from the use of crowdfunding as discussed in [2]. Such businesses may find it hard to obtain funding from traditional sources such as bank loans due to their lack of historical data. There are different types of crowdfunding:

1.1.1 Equity-Based Crowdfunding

The investors will be granted a share in the enterprise or startup with equity-based crowdfunding, depending on how much money they invest. Equity-based crowdfunding is linked to complex contracts involving due diligence and a high degree of investment, which means that funders are fully aware of the advocates and the company. It could make equity investments in an online audience seem nonsensical [3].

1.1.2 Reward-Based Crowdfunding

The bonuses are earned by crowd funders who donate funds or contribute to the fundraising, depending on the amount of the money raised by the organization or project. The reward might be a product or other goodies that they develop. Crowd-

J. M. Mutharasu (✉) · U. Pandey · B. Rethick · B. Kulkarni · Prof. M. Pawar
MIT School of Engineering, Pune, India
e-mail: mohandas.pawar@mituniversity.edu.in

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_9

funding on a reward basis is particularly popular among entrepreneurs as described in [4].

1.1.3 Donation-Based Crowdfunding

With donation-based crowdfunding, people contribute different sums of money according to the idea put forward by the beneficiaries without any hopes and rewards or costs. Such crowd financing usually starts to support voluntary organizations, disaster relief, and the collection of emergency funds [5].

1.2 Blockchain

Blockchain is an upcoming comprehensive system used in areas such as cryptocurrency, banking, insurance, government, music, identification, supply chain, information management, and many others. By understanding the underlying mechanisms that power blockchain, one can join the discussion and explore use cases for blockchain in your own life and work. It is a distributed ledger which permits storing of the data, as mentioned in [6], in an immutable and auditable way. Two types of blockchains exist private and public blockchains. There are nevertheless also numerous variations, such as hybrid blockchains and consortium blockchains. Let us research what characteristics all blockchains share before we concentrate on the individual characteristics of each blockchain. A collection of nodes running in a peer-to-peer network (P2P) is included in each blockchain. Every node in a network has a shared copy of the ledger which is updated in regular intervals. Each node can validate transactions, begin or accept transactions and generate blocks. Now let's have a look in detail about the four types of blockchains that are possible as seen in [7].

1.2.1 Public Blockchain

A public blockchain is essentially a shared ledger network which is not limiting and can be accessed without permission. Anyone who has a way to the internet can sign up for an approved node on a blockchain platform and join the blockchain network. This enables the delivery of the data and guarantees its integrity as seen in [8]. A node or user in the blockchain is allowed to view, inspect transactions, or perform proof of work on a block input [9] and also mining for current block. The primary use of public blockchains is in cryptocurrencies mining and exchange. Ethereum [10] and Bitcoin [11] are the most frequently used public blockchains.

1.2.2 Private Blockchain

A private or permissioned blockchain is essentially a blockchain operated in a closed network. Private blockchains are used in an organization or company where only a few predefined members participate in the blockchain network. The controlling association shall be responsible for the degree of protection, permits, accessibility. So, private blockchains have a small, restrictive network but are similar to public blockchains. First, permission must be given to any node in a private blockchain, leading to greater confidence. As studied in [12], this contributes to improved results. Private blockchain networks are utilized in many domains which include voting [13] and supply chain management [14] and Digital ID [15].

1.2.3 Consortium Blockchain

A blockchain consortium is semi-permissioned in which multiple organizations control a blockchain network. This is contrary to what we have seen in a private blockchain that is operated by only one entity. In [7] we saw that in this type of blockchain, several associations can act as a node and trade commercial data, or mine. Consortium Blockchains are typically used by banks [16], energy trading [17], etc.

1.2.4 Hybrid Blockchain

A hybrid blockchain is a public and private blockchain aggregate. It uses the attributes of both, hence a private permission operation and a public permission-free operation can both be performed. Users control who has access to data stored in a blockchain via such a hybrid network. Only a predefined division of blockchain records can be accessed publicly and designating the rest as confidential in a privately owned network. The hybrid blockchain framework can be expanded to allow users to search easily for a private blockchain with multiple public blockchains. A transaction is typically performed inside the private network of a hybrid blockchain. But users can also issue it for verification in the public blockchain. The public blockchains extend the hashing process and include other verifying nodes. As defined in [7], this improves the certainty and clarity of the blockchain.

1.3 Ethereum

While every blockchain can process code, most are severely restricted. Ethereum is distinctive. Rather than providing a collection of restricted services, Ethereum provides developers to implement whatever services they want. This implies developers

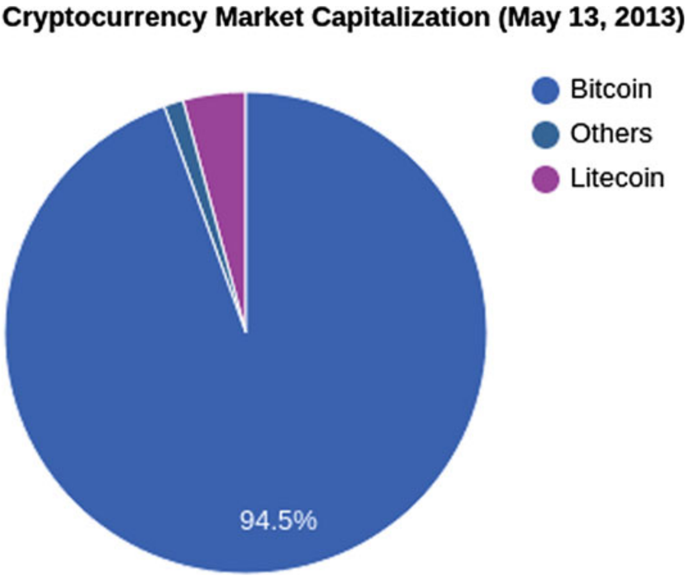


Fig. 1 The market share of different cryptocurrencies as of May 13, 2013

can make thousands of diverse applications that operate way past anything we have witnessed before as explained in [10] (Fig. 1).

Buterin was fascinated by the blockchain technology and co-founded Bitcoin Magazine. He began imagining a network which would go beyond Bitcoin's financial use cases and publish a 2013 White Paper explaining, with a general scripting language, how it would become Ethereum. The main Bitcoin differentiator was the network's ability to trade more than cryptocurrencies. Buterin and the other Ethereum founders started a campaign to encourage crowdsourcing in 2014, selling participants Ether to raise more than 18 million dollars from their vision. Ethereum began its first live release in 2015, known as Frontier. Since then, the platform has evolved steadily and hundreds of developers are now interested.

1.4 Smart Contracts

A Smart Contract is just an expression to describe a code of machines that can facilitate trade in money, material, property, shares, or anything that is of significance. When operating on the blockchain a smart contract becomes like a self-operating computer application that executes when explicit requirements are satisfied. As mentioned in [18, 19] they run on the blockchain because smart contracts operate accurately as configured without any licencing chance, downtime, fraud, or interference from third parties. While every blockchain can process code, most are firmly lim-

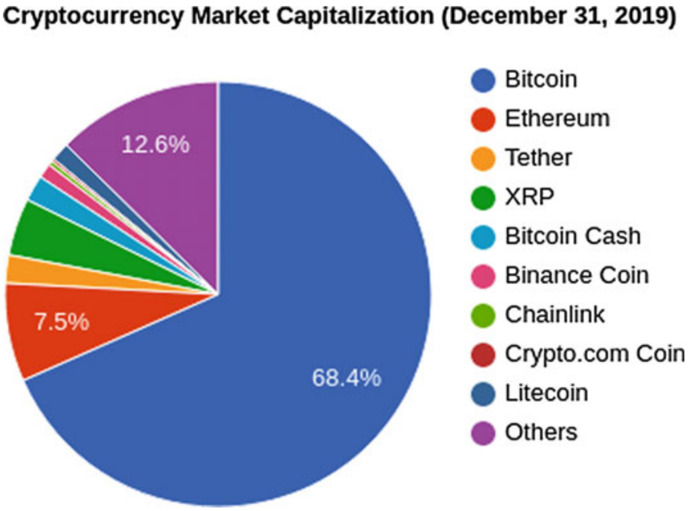


Fig. 2 The market share of different cryptocurrencies as of December 31, 2019

ited. Ethereum is unique in this aspect. Ethereum allows developers to offer whatever resources they need rather than offering a small amount of help. This allows developers to produce thousands of distinct applications that work way beyond anything we have thought of earlier (Fig. 2).

1.5 Blockchain-Based Crowdfunding

Though traditional crowdfunding systems do well, there are major concerns from the sponsors of the project. As stated in [20] for example, incentive-based crowdfunding or reward-based crowdfunding projects give the project supporter some incentive depending on how much money they deposit but, sometimes they're conned or the incentives are given very late. These issues can be solved using a blockchain-based approach to these issues that delivers faster transfers and withdrawals as compared with normal means. Another major issue that blockchain solves is fake data and misleading transactions, which could pose problems for the company. Many Blockchain technologies use proof of work which guarantees that there are no fraudulent transactions or false data present that can impact the initiative as well as removing the need for an intermediate portal to commit their valuable assets to the proposed project. This can be an important aspect of improving the initiative. Reward-based crowdfunding is a modern concept that promotes and democratizes the process of fundraising for launching risky and creative ventures in a range of economic fields. Reward-based blockchain platforms are really great for launching new products, services, and brands since It's one of the cheapest ways to raise capital. They are also preferable to other platforms for expanding into new territories as the process is fairly simple with no previous experience needed and the exposure on the platform can help to build awareness of customers and brands.

2 Literature Survey

Research work in the field of blockchain-based crowdfunding deals with the effects of blockchain-based technology in initial coin offerings [21, 22], donation-based crowdfunding [18], and general comparisons between traditional and blockchain-based approaches [20, 23]. There is a lack of research work in the field of reward-based crowdfunding using blockchain technology. This paper hopes to solve this research gap by providing a framework for reward-based crowdfunding using blockchain technology.

In 2019, Hartmann et al. [23] presented what blockchain-based crowdfunding is, how it is comparable to that of the traditional crowdfunding system, and what makes it unique and different from the conventional system. Although both traditional crowdfunding and blockchain-based versions are popular, understanding is insufficient when it comes to blockchain-based explications, and it is important to understand that to solicit investors. Understanding these certain concepts will help others to know how blockchain frameworks work and how it supplements the existing traditional system.

In 2019, Saadat et al. [20] inscribed that although initially blockchain has been implemented only for cryptocurrencies, now there is a surge in the use of blockchain as many foundations are preferring the use of it. Soon, blockchain will replace all other transaction platforms. One such platform is crowdfunding because some of the campaigns are not standardized and some turn out to be a fraud. It explores the use of Ethereum-based dApp to solve many issues. It exploits the use of smart contracts and how it will be automatically used and how it will help solve problems in the current system.

In 2019, Brennecke et al. [21] formulated that crowdfunding has been gaining acknowledgment from entrepreneurs for raising resource funding. It explains crowdfunding as a public solicitation to invest in a project which is published by the ones in need via the internet. It exploits the use of ICO's for developing blockchain-based variants for crowdfunding as this crowdfunding ecosystem relies on P2P transactions. Thus it will make the crowdfunding notion between the ones seeking funds and the ones helping them to raise it fascinating. It will make transactions more reasonable, more productive, and more transparent.

In 2016, Jacynycz et al. [24] inferred crowdfunding being implemented over centralized platforms and these platforms are commission-based ones. It discussed the use of an Ethereum-based decentralized platform being implemented for crowdfunding campaigns. The pros of using this approach are that no one can tamper with its code and charge commissions to its users. This system will not only be used by the ones proposing the project but also the ones funding it. The blockchain-based approach will meddle the frauds in this field and empower its users in a more decentralized fashion.

In 2015, Ante et al. [22] explored the determinants of a blockchain-based Initial Coin Offering's Success based on varied factors. They have found that ICOs resemble established crowdfunding and venture capital markets and that the funds raised by an ICO depend on factors such as human capital, consistency of the business model, project growth, and their presence on social media. They have stated that the importance of social media cannot be quantified and further analysis is needed. Hence they have concluded that ICOs are a neoteric way to fund start-ups that shift closer to conventional structures as markets develop and blockchains become widely accepted.

In 2019, Zichichi et al. [18] constructed a blockchain-based Crowdfunding built over the Ethereum network called LikeStarter. They have chosen a donation-based approach to crowdfund and place emphasis on funding creative pursuits. It has been built in the form of a social networking site to promote able artists hence raising money for their future projects. Published content receives appreciation in the form of likes, comments, and shares. Every like corresponds to a transaction transferring ether to the crowdfunding beneficiary. A beneficiary can also offer rewards to his fans to attract further contributions.

In 2018, Zheng et al. [18] discussed the advantages and disadvantages of blockchains. They noticed that no blockchain study existed both in technology and implementation and tried to fill this void. Blockchain is lauded for its decentralized infrastructure and peer-to-peer nature. It has shown the potential to transform traditional industries with its anonymity, persistence, and decentralization. They have also studied the typical consensus algorithms used and compared them with each other. They have analyzed the praxis of blockchain and further studied the factors which may inhibit the widespread adoption of such applications. They have also inferred solutions that can rectify this and further improve the existing solutions.

In 2019, Yaga et al. [25] provided a technical overview and tried to help people understand the workings of blockchain technology. They began with the history and implementation of blockchain in Bitcoin. Bitcoin has played an indispensable role in the popularity of blockchain technology. They have further classified the types of blockchain present and the advantages of each. They have explained the working of blockchain along with a thorough explanation of each component. They have thoroughly explained why the blockchain functions as it does. They have compared various consensus models in depth and stated each of their advantages and disadvantages. They have further stated that a blockchain relies on existing technologies but uses them in new and compelling ways (Table 1).

3 Proposed System

Proof of work is a consent protocol in which transactions are checked and fraudulent transactions are prevented by nodes on a blockchain network. It varies from other

Table 1 Literature Survey

Year	Methodology	Features	Challenges
2019 [18]	This uses blockchain, digital signature, taxonomy of blockchain, consensus algorithms, finance, IoT, selfish mining, big data analysis, smart contracts, artificial intelligence	There is a broad range of blockchain implementations which vary from cryptocurrency, financial services, risk, IoT, public to social services	This article provides Taxonomy of bitcoin, Typical implementations of Consensus Network Algorithms, reviews software blockchain, and addresses the technological issues and new trends in task management
2019 [20]	In order to solve fraud problems, this project uses Ethereum's intelligent site contracts to provide the contracts within the prescribed time period	The Highlight of Crowdfunding is that in a short time it can collect the sum of money needed. This plans to add ERC-223 tokens in contracts as they provide further advantages	The biggest issue with the present world-wide crowd financing scene is that campaigns are not monitored and some crowd financing projects have been fraudulent
2019 [21]	Initial coin offer (ICOs) for peer-to-peer (P2P) funding was listed as one of the most promising and recognizable applications	These tokens can reflect any typical category of asset, and are now being used, for example, to define shareholdings in an organisation, consumer trust in online applications, fiat currency deposits, and cryptocurrency applications balances	The problem is to describe the core concepts and the variations between the ICOs and conventional financing and their possible effects on crowdfunding are discussed
2018 [22]	In this initial coin offering (ICO) success, investment fund blockchain, and crowdfunding was used.	ICOs are the big function which presents parallels with the traditional market for venture capital and crowdfunding	The major issue is to identify correlations between characteristics of funding performance including characteristics of human capital, efficiency of business model, project creation, and events in social media
2019 [23]	The Initial Coin Offerings (ICO), and recently Security Token Offers (STOs), are represented in this blockchain-based crowdfunding	The key function is to help regulations and market participants understand blockchain-based crowdfunding	The concern is that in comparison to conventional crowdfunding over recent years there has been a lack of clear understanding of the success of blockchains based ventures

(continued)

Table 1 (continued)

Year	Methodology	Features	Challenges
2016 [24]	In this paper, Bitcoin, Blockchain, Bounty, Crowdfunding, Cryptocurrencies, Distributed Applications, Ethereum, Peer-to-Peer Networks, and Smart contract are used	This method does not need a central and trustworthy agency unlike traditional crowdfunding platforms	The issue is the idea, the reward and also enticing future developers to do so, is completed in a given time period
2019 [25]	The technologies used are blockchain, consensus model, cryptocurrency, cryptographic hash function, asymmetric-key cryptography, distributed ledger, distributed consensus algorithm, smart contracts, data oracle	Blockchain allows the user group to archive related transfers in a ledger within that group, so that it is under regular service in the network with blockchain and there should be no trade changed after it has been released	The challenge is to help readers understand how blockchain technology works
2020 [26]	In this paper, effective crowdfunding is implemented to fabricate a trustworthy current model, transparently, honestly, decentrally and cost-effectively	The function of the blockchain crowdfunding tools including anti-tampering, anti-fraud, open leather solutions can aid to provide information and data security	The challenge is to make the existing model of a pool of people contributing a small amount of money for the scheme or maybe cause and predict some Economic, or non-economic returns to a network focused on blockchain crowdfunding
2020 [27]	It is centered on the need for an innovative crowdfunding site for the creation of smart regions and the intrinsic functionality of blockchain technology	The two key aspects are a balanced project distribution that empowers developers and adjust the parameters iteratively in order to find the optimum solution, the latter is the effect of other developers' bids on the winning solution	The problem is that the numerous middlemen and intermediaries do not encourage the skilled professional tools to be used appropriately mostly because of their self-interest and lack of an effective structure or a platform to connect the talent with the appropriate talent hunters

negotiation processes, such as Proof of Stake which are used in the same way but have different approaches. In proof of work, mining is a part of the process of consensus, whereas in proof of stake, blockchain network mining is not accessible. All the participants have each got stakes instead. Smart Contracts are written in Solidity and then deployed to the Ethereum blockchain. Smart Contracts use a Programming code agreement between the two entities. Once the data is stored in the blockchain, the data can not be manipulated in the public database. These contracts are compiled to Application Binary Interfaces which provide an interface to interact with the blockchain. This system uses ReactJS to provide a seamless front-end user experience. Node.js and Express.js are used to build the backend API. When a new request is sent by the user, it is handled by calling the respective function from the ABI with the help of Web3.js which in turn adds a transaction to the blockchain. Web3.js is a javascript library that allows you to interact with a local or a remote Ethereum node. It provides an interface that allows the user to call functions from the ABI. This way the Web App is used to interact with the blockchain. All transactions in the Ethereum blockchain require gas to be validated. Hence, a small amount of ether is required to fund the transaction. This is accomplished by using a browser extension known as MetaMask. MetaMask is a bridge that allows users to have access to tomorrow's distributed platform. It allows running Ethereum-based decentralized apps in your browser without using a full Ethereum node. Every time a transaction is to be performed a small amount of ether will be deducted as gas to fund the validation of the transaction. It makes the device connect to another Ethereum node called Infura by which smart contracts can be executed. It manages the Ethereum wallet. All the transactions both sending and receiving happen through it which uses ether as the medium for the transaction. This transaction is then added to the pending queue in the Ethereum network with a bounty of the gas money that you paid. After the transaction is validated by a miner, It is appended to the Ethereum Network (Fig. 3).

This system also uses a No-SQL database called MongoDB. to save details about the user and the projects proposed. It is an alternative for relational databases. As compared to the relational database, MongoDB stores data in JSON format as key-value pairs instead of storing them as tables. These key-value pairs are stored as documents and all these documents add on to make a collection. A collection can contain any number of documents. A document may have multiple key-value pairs. MongoDB stores this data in BSON format which stands for binary JSON, which is an extended version of JSON which supports more data types than JSON. Every time a user proposes a new project, a new entry is added to the database. This entry contains all the details about the system including the funding target, the project idea, the rewards to be distributed et cetera. After a crowdfunding campaign is successfully set up, it can start receiving funds. Different investors can invest in different projects to their likability. After an investment, a reward is promised from the company or individual who owns the campaign to each individual who invested a certain sum of money. The rewards may differ depending on the sum of money invested in the campaign. If it is a small amount then some goodies may be promised and in case of a hefty sum, a sample of their product is given to the investor.

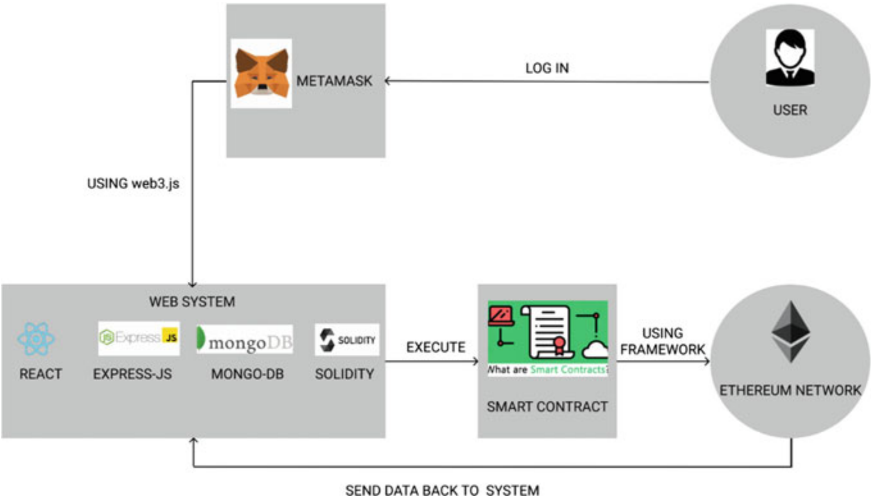


Fig. 3 The proposed system

4 Result

The Traditional Crowdfunding model is inefficient. It follows a centralized approach similar to venture capital firms with a single controlling platform. Funders have no assurance whether their funds are going toward the promised product. Traditional Crowdfunding platforms do not provide any assurance and this may scare potential investors. This affects entrepreneurs who have a good idea but do not have the funds required to start a business. Crowdfunding, with it's nature of multiple involved parties, can benefit immensely with the introduction of a decentralized approach. As seen in Fig. 4, blockchain-based crowdfunding is burgeoning in recent years. When a user first enters the platform's website, he is greeted by a home page where he can choose to create a new account, login, or explore existing campaigns. The homepage can additionally also highlight popular campaigns.

4.1 Campaign Creation

When a user decides to create a new campaign, they enter any details associated with the campaign in the website. After entering all associated data, they can create a transaction to deploy the data to a blockchain. This entry will contain all associated details such as campaign id, target amount, campaign name, campaign address, and incentives for funders. This way the data that is stored is immutable. This entry ensures that there is proof of the initial promise by the company which hence provides

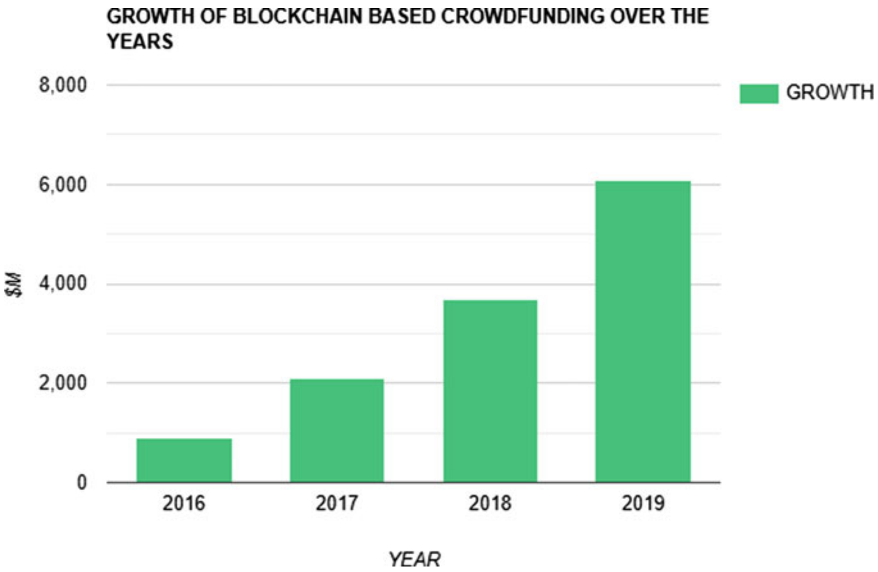


Fig. 4 Capital raised by blockchain-based crowdfunding platforms

a testament in case they try to renege. This initial deployment will also take a small amount of gas in the form of ether.

4.2 Explore Campaigns

The explore page provides new users the opportunity to view all the existing crowdfunding campaigns along with the capital raised by them. It contains a catalogue of all the campaigns that are started by the user and have not yet reached their target amount. Each campaign has a small card along with some associated information about the campaign. The user can then choose to click on the campaign and view all the information provided by the company. If the user is logged in, the user can then decide if he wants to invest/donate in the campaign.

4.3 Invest in Campaign

If a user finds the company's pitch appealing, he can choose to donate to the campaign. All of the transactions take place using ether. A user can enter the amount he wants to invest in the provided field. Then the respective function from the smart contract will be called. This transaction will be added to the blockchain. The incentive obtained will be based on the initial contract decided upon by the founding company.

4.4 Campaign Failure

If the campaign fails to reach the target amount in the specified duration, the smart contract ensures that the investors receive their originally invested amount. This data is present in the blockchain in the form of transactions and can be used for the same. This way every investor receives their investment back.

4.5 Campaign Success

If the campaign reaches the target amount in the specified duration, every investor receives the promised reward. The list of rewards offered is stored in the blockchain along with the list of all the investors and the amount invested. Since all of the data is stored in a blockchain, it cannot be modified later.

5 Conclusion

This paper presents the working model consisting of Ethereum and Crowdfunding which in turn provides a prominent platform. Crowdfunding helps in launching new businesses and a reward-based approach helps start-ups maintain their equity early on unlike an ICO approach. At the same time, Ethereum ensures that the business remains accountable and does not renege on its terms while also increasing the confidence of investors. This also encourages more people to invest in the product. Hence, both the business and the consumer benefit from an Ethereum based crowdfunding approach. With each passing day, people are understanding Blockchain technology much better and thus the scope for attracting interested audiences for our crowdfunding platform increases. Though this paper won't be the elixir to existing problems, we believe that combined with the understanding of the readers there will be desirable results.

References

1. P. Belleflamme, T. Lambert, A. Schwienbacher, Crowdfunding: tapping the right crowd. J. Bus. Ventur. **29**(5), 585–609 (2014)

2. A. Schwienbacher, B. Larralde, Crowdfunding of small entrepreneurial ventures, in *Handbook of Entrepreneurial Finance* (Oxford University Press, Forthcoming, 2010)
3. N. Vulkan, T. Åstebro, M.F. Sierra, Equity crowdfunding: a new phenomena. J. Bus. Ventur. Insights **5**, 37–49 (2016)
4. B. Mundial, Crowdfunding's potential for the developing world. Finance Private Sec. Dev. Depart. 1–102 (2013)
5. D. Freedman, M.R. Nutting, *A Brief History of Crowdfunding* (Debt Equity Platforms USA, Including Rewards, Donation, 2015)
6. M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman et al., Blockchain technology: beyond bitcoin. Appl. Innov. **2**(6–10), 71 (2016)
7. M.K. Shrivas, D. Yeboah, The disruptive blockchain: types platforms and applications, in *Fifth Texila World Conference for Scholars (TWCS) on Transformation: The Creative Potential of Interdisciplinary* (2018)
8. R. Yuan, Y.B. Xia, H.B. Chen, B.Y. Zang, J. Xie, Shadoweth: private smart contract on public blockchain. J. Comput. Sci. Technol. **33**(3), 542–556 (2018)
9. A. Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016), pp. 3–16
10. V. Buterin, et al., A next-generation smart contract and decentralized application platform. White Paper **3**(37) (2014)
11. S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. Technical Report Manubot (2019)
12. T.T.A. Dinh, J. Wang, G. Chen, R. Liu, B.C. Ooi, K.L. Tan, Blockbench: a framework for analyzing private blockchains, in *Proceedings of the 2017 ACM International Conference on Management of Data* (2017), pp. 1085–1100
13. F. Hjálmarsson, G.K. Hreiarsson, M. Hamdaqa, G. Hjálmtỳsson, Blockchain-based e-voting system, in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (IEEE, 2018), pp. 983–986
14. K. Biswas, V. Muthukkumarasamy, W.L. Tan, Blockchain based wine supply chain traceability system (2017)
15. J.H. Lee, Bidaas: Blockchain based id as a service. IEEE Access **6**, 2274–2278 (2017)
16. Y. Guo, C. Liang, Blockchain application and outlook in the banking industry. Financ. Innov. **2**(1), 24 (2016)
17. Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium blockchain for secure energy trading in industrial internet of things. IEEE Trans. Ind. Inf. **14**(8), 3690–3700 (2017)
18. M. Zichichi, M. Contu, S. Ferretti, G. D'Angelo, Likestarter: a smart-contract based social dao for crowdfunding, in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (IEEE, 2019). pp. 313–318
19. M. Bartoletti, L. Pompianu, An empirical analysis of smart contracts: platforms, applications, and design patterns, in *International Conference on Financial Cryptography and Data Security* (Springer, 2017), pp. 494–509
20. M.N. Saadat, S.A.H.S.A. Rahman, R.M. Nassr, M.F. Zuhiri, Blockchain based crowdfunding systems in Malaysian perspective, in *Proceedings of the 2019 11th International Conference on Computer and Automation Engineering* (2019), pp. 57–61
21. L. Arnold, M. Brennecke, P. Camus, G. Fridgen, T. Guggenberger, S. Radszuwill, A. Rieger, A. Schweizer, M. Urbach, Blockchain and initial coin offerings: blockchain's implications for crowdfunding, in *Business Transformation Through Blockchain* (Springer, 2019), pp. 233–272
22. L. Ante, P. Sandner, I. Fiedler, Blockchain-based ICOS: pure hype or the dawn of a new era of startup financing? J. Risk Financ. Manage. **11**(4), 80 (2018)
23. F. Hartmann, G. Grottolo, X. Wang, M.I. Lunesu, Alternative fundraising: success factors for blockchain-based vs. conventional crowdfunding, in *2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* (2019), pp. 38–43
24. V. Jacynycz, A. Calvo, S. Hassan, A.A. Sánchez-Ruiz, Betfunding: a distributed bounty-based crowdfunding platform over ethereum, in *Distributed Computing and Artificial Intelligence, 13th International Conference* (Springer, 2016) pp. 403–411

25. D. Yaga, P. Mell, N. Roby, K. Scarfone, Blockchain technology overview. arXiv preprint arXiv:1906.11078 (2019)
26. H. Baber, Blockchain-based crowdfunding, in *Blockchain Technology for Industry 4.0* (Springer, 2020), pp. 117–130
27. V. Hassija, V. Chamola, S. Zeadally, Bitfund: a blockchain-based crowd funding platform for future smart and connected nation. Sustain. Cities Soc. 102145 (2020)

Data Science: Concern for Credit Card Scam with Artificial Intelligence

Neha Tyagi, Ajay Rana, Shashank Awasthi, and Lalit Kumar Tyagi

1 Introduction

As of now, Unlawful use of a cc and obtaining its private information without the owner's knowledge is considered cc fraud [2]. Credit card fraud is increasing day by day with the development of technology leading to the loss of billions of dollars of customers around the world every year. Hence, Fraud detection involves identifying fraudulent activity scattered across many legal transactions as quickly as possible. This is a widespread event problem called outlier analysis, anomaly detection, exception retrieval, rare class retrieval, unbalanced data retrieval, and so on the amount of fraud transitions is much less than the total number of transitions, so the accurate detection of the fraud transition is very difficult and questionable for this, we must use very efficient methods and algorithms. Therefore, in this article we try to collect and integrate the whole series of research in the literature and to analyze it from various aspects. According to the World Payment Report, in 2016 total non-cash transactions increased 10.1% from 2015 for a total of 482.62 billion transactions. Actually, the credit card fraud techniques are mainly categorized into two category application fraud and the behavioral fraud. Application fraud occurs when scammer request new cards from the bank or issuing companies using the wrong information or obtain the wrong information from the other [3]. However, multiple requests can be made by a single user with the same user details or by a different user with identical details. On the other hand, behavioral fraud has four main types: mail theft, fake card, stolen/lost card, and the cardholder has no fraud [5]. Although Due to the

N. Tyagi (✉) · S. Awasthi · L. K. Tyagi
G.L Bajaj Institute of Technology & Management, Greater Noida, India

A. Rana
Amity University, Noida, India
e-mail: ajay_rana@amity.edu

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_10

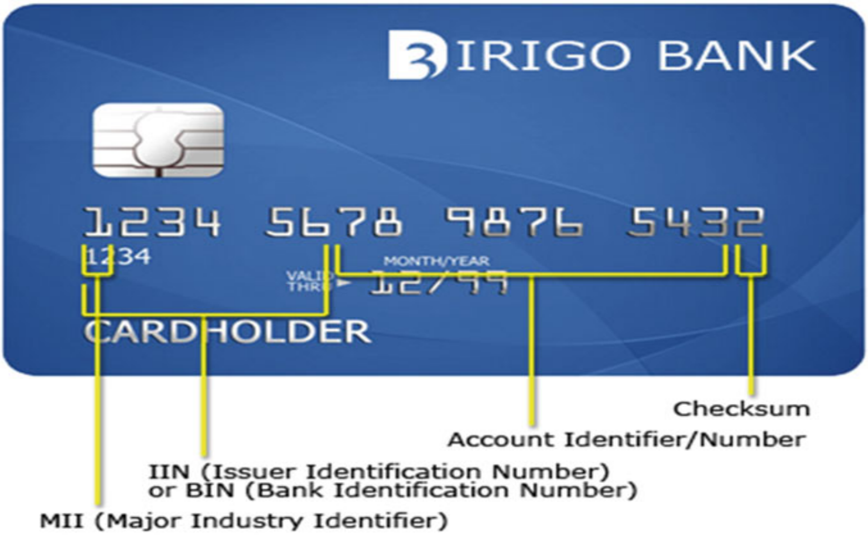

IRIGO BANK
1234 5678 9876 5432
1234
VALID THRU
MONTH/YEAR
12/99
CARDHOLDER
Checksum
Account Identifier/Number
IIN (Issuer Identification Number)
or BIN (Bank Identification Number)
MII (Major Industry Identifier)

Fig. 1 The data of credit card that needs to be confidential by the owner of the credit card in the credit card to protect it from the hacker [6]

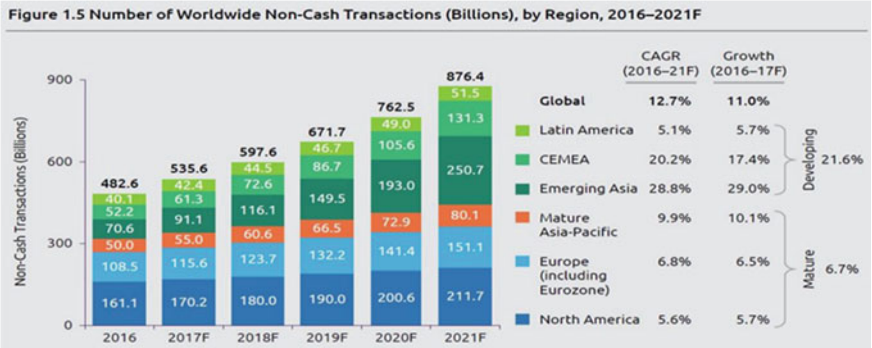


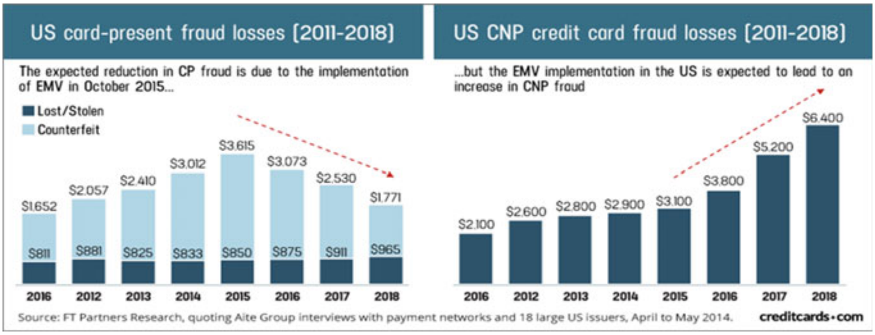
Fig. 2 The steady growth of the non-cash transactions [2]

fraudment of the credit card the flip side fraudment rise we move to the EVM smart chip-based card for security purposes (Figs. 1, 2 and 3).

1.1 Categories of Credit–Card Fraud Finding

There are two kinds of main findings:

a. Finding of misuse

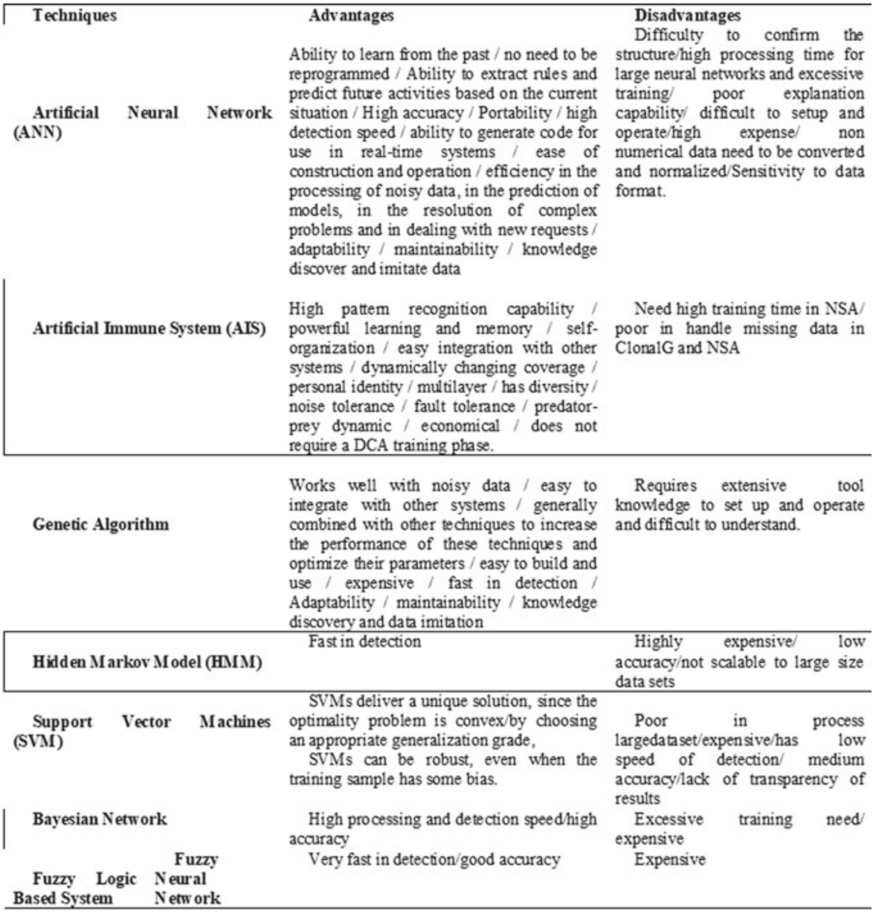


Source: FT Partners Research, quoting Aite Group interviews with payment networks and 18 large US issuers, April to May 2014.

Fig. 3 Due to the fraudment of the credit card the flip side fraudment rise we move to the EVM smart chip-based card for security purposes [5]

b. Finding of Anomaly.

Extortion of misuse identification is a procedure that manages directed grouping movement at the exchange level. In these strategies, exchanges are hailed as extortion or ordinarily dependent on verifiable information from the client's past progress model [4]. This dataset is utilized to make the grouping model that can foresee the state (typical or false) of new records. There are numerous models for making techniques for the common two-class grouping task, for example, rule enlistment, choice trees, and neural systems. This methodology has demonstrated to be the dependable identification of the majority of the misrepresentation recommendations that have been seen previously. It is otherwise called misuse location. Utilization conduct examination misrepresentation (abnormality recognition) manages solo location techniques dependent on account conduct [3]. In this strategy, an exchange is identified as extortion in the event that it clashes with typical client conduct. This is on the grounds that we don't anticipate that con artists should act similarly as the record holder or to know about the proprietor's example of conduct [5]. To do this, we have to remove the real client conduct model, for example, the client profile for each record and afterward recognize false exercises dependent on it by contrasting new practices with agreeing with this model, various exercises that are adequately extraordinary are viewed as misrepresentation. Profiles may contain data about record movement, for example, trader types, sum, spot, and season of exchanges. This strategy is otherwise called irregularity detection [5]. In the table beneath, a few strategies are quickly introduced speaking to some current extortion discovery methods that are applied to the assignments of the charge card misrepresentation recognition framework. It additionally speaks to the favorable position and detriment of each approach [5, 5] (Fig. 4).



Techniques	Advantages	Disadvantages
Artificial Neural Network (ANN)	Ability to learn from the past / no need to be reprogrammed / Ability to extract rules and predict future activities based on the current situation / High accuracy / Portability / high detection speed / ability to generate code for use in real-time systems / ease of construction and operation / efficiency in the processing of noisy data, in the prediction of models, in the resolution of complex problems and in dealing with new requests / adaptability / maintainability / knowledge discover and imitate data	Difficulty to confirm the structure/high processing time for large neural networks and excessive training/ poor explanation capability/ difficult to setup and operate/high expense/ non numerical data need to be converted and normalized/Sensitivity to data format.
Artificial Immune System (AIS)	High pattern recognition capability / powerful learning and memory / self-organization / easy integration with other systems / dynamically changing coverage / personal identity / multilayer / has diversity / noise tolerance / fault tolerance / predator-prey dynamic / economical / does not require a DCA training phase.	Need high training time in NSA/ poor in handle missing data in ClonalG and NSA
Genetic Algorithm	Works well with noisy data / easy to integrate with other systems / generally combined with other techniques to increase the performance of these techniques and optimize their parameters / easy to build and use / expensive / fast in detection / Adaptability / maintainability / knowledge discovery and data imitation	Requires extensive tool knowledge to set up and operate and difficult to understand.
Hidden Markov Model (HMM)	Fast in detection	Highly expensive/ low accuracy/not scalable to large size data sets
Support Vector Machines (SVM)	SVMs deliver a unique solution, since the optimality problem is convex/by choosing an appropriate generalization grade, SVMs can be robust, even when the training sample has some bias.	Poor in process largedataset/expensive/has low speed of detection/ medium accuracy/lack of transparency of results
Bayesian Network	High processing and detection speed/high accuracy	Excessive training need/ expensive
Fuzzy Logic Based System Fuzzy Neural Network	Very fast in detection/good accuracy	Expensive

Fig. 4 Due to the fraudment of the credit card the flip side fraudment rise we move to the EVM smart chip-based card for security purposes

2 Methodology

User comes and selects the transaction methods and after that the process is matched with the stored datasets and is seen that is there any issues in the process of the transaction if the datasets find any issues then the transitions are rejected and the fraud is confirmed [6]. For further if there is any issues like the user isn't fraud then security questions are checked and if the security question can't be answered then it is a complete fraud and the system exits the user from the transaction. The flow chart diagram of the Credit Card Fraud detection technique that is used by us is of the user behavioral model that is shown in the figure below. In this the new transition is matched with the past transition pattern such as amount of transition pattern, location of the transition and the type of purchasing the transition if the

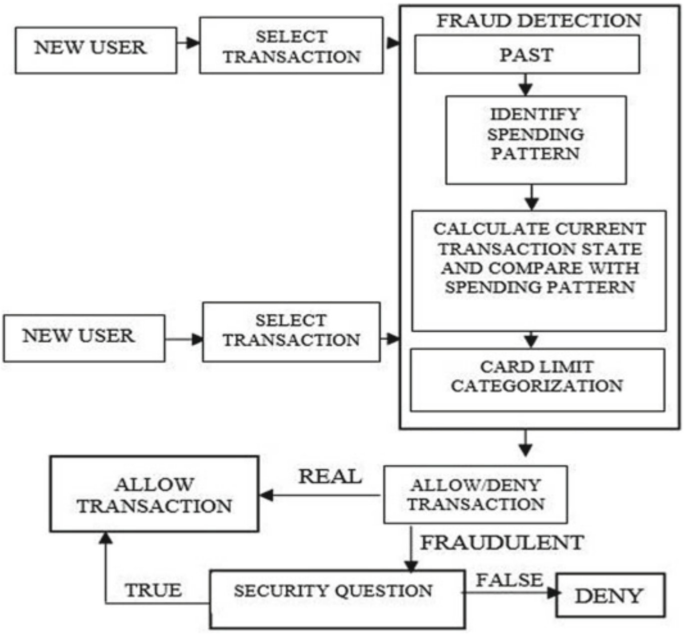


Fig. 5 Block diagram of credit card fraud detection system

system found it fraud than it raises the security question if it answered than transition further proceed otherwise the system will abort the transition and report to the holder about the fraudment of the transition [10] (Fig. 5).

2.1 *Stages of CC Fraud Detection Classification Methods*

The **Credit card Fraud Detection** system is an 8 step process in which we will use different machine learning algorithms and use them to analyze data import dataset plot different graphs use ANN that is artificial neural network to recognize patterns will see different curves.

1. Importing Datasets
2. Data Exploration
3. Data manipulation
4. Data Modeling
5. Fitting Logistic Regression Model
6. Fitting Decision Model
7. Artificial Neural Network
8. Gradient Boosting.

In the very first step import the library and different datasets and then when it is successful then move to our second step and which is data exploration. After that there is a need to explore the imported data that will manipulate it with step called data manipulation and after that Model the data. The Data Modelling is an important part as it will compare with many states and transactions with this modeled data and if there is any issue in modeled data then the system won't work properly [].

Now from the next step start using different ML algorithms, at first do fitting logistic Regression Model. Then apply fitting Decision Model after that apply ANN artificial neural networks and at the end do gradient boosting [].

a. **Importing Datasets**: Here import the datasets that contain exchanges made by Visas or check card holders. We have utilized Kaggle.com which has the premade informational collections which contained 285,500 lines of information and 32 sections. Out of the apparent multitude of segments, the main ones that are the most sense were Time, Amount, and Class (misrepresentation or not extortion). The other 29 sections were changed by utilizing what is by all accounts a PCA dimensionality decrease so as to ensure the client personality [11].

b. **Data Exploration**: In this we will investigate the information that take a gander at various fields' tables and different subtleties like kind of charge card utilized generally the territory which has more number of fakes. We investigate the information that is contained in the MasterCard information outline. We will continue by indicating the charge card utilizing the head () and the tail () work.

   Now the data that use to run through a few initial comparisons between the three columns that Time, Amount, and Class (Fig. 6).

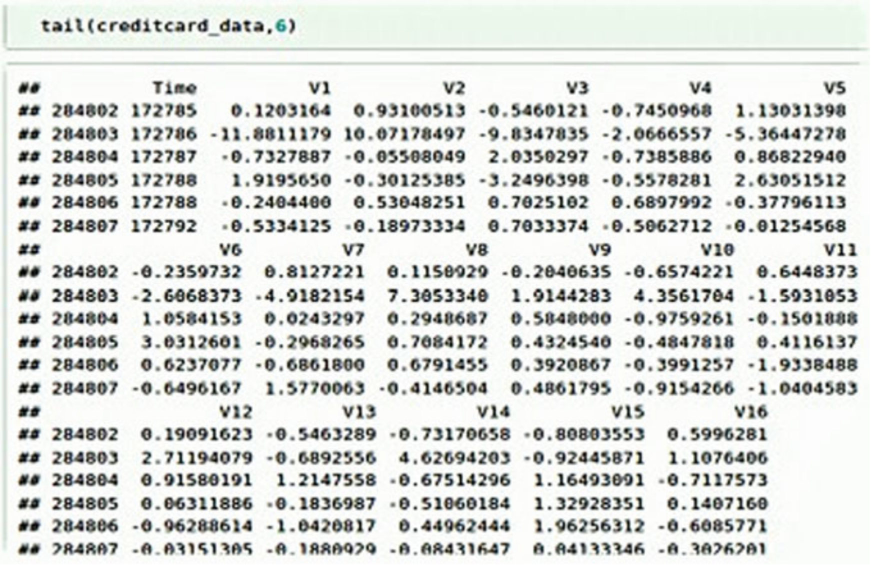
   Now we have the data that we want to run through a few initial comparisons between the three columns that **Time, Amount, and Class**.

   Figure 7 is depicting that, while most of the big deals are very small, this distribution is also planned. Most of the time, day-to-day transactions aren't overly expensive (most are <$50), but they're probably the most fraudulent transactions to happen too.

   Figure 8 is depicting that the visible distribution is valid data for two days. It is for regular consumers for most purchases made during the day and when people leave work/school and go home, purchases decrease overnight. Figure 9 is illustrating the Class (Fraud/Not Fraud).

   In the dataset, there is only 493 fraud transactions, i.e., Only the approx. 0.179% of all of the transactions in this dataset.

c. **Data Manipulation**: The information control is applied to the sum part of Visa informational collection. In this we do Scaling. Scaling is otherwise called the exceptional normalization by the assistance of which the scaling of information is organized as indicated by a particular range. When we've normalized our whole dataset, we'll split our dataset into a preparation set and a test set with a split proportion of 0.83. This implies 83% of our information is given to preparing information while 17% of information is given to test information [12] (Fig. 10).



```
tail(creditcard_data,6)
```

```
##            Time          V1          V2         V3         V4          V5
## 284802 172785   0.1203164  0.93100513 -0.5460121 -0.7450968  1.13031398
## 284803 172786 -11.8811179 10.07178497 -9.8347835 -2.0666557 -5.36447278
## 284804 172787  -0.7327887 -0.05508049  2.0350297 -0.7385886  0.86822940
## 284805 172788   1.9195650 -0.30125385 -3.2496398 -0.5578281  2.63051512
## 284806 172788  -0.2404400  0.53048251  0.7025102  0.6897992 -0.37796113
## 284807 172792  -0.5334125 -0.18973334  0.7033374 -0.5062712 -0.01254568
##                V6         V7         V8         V9        V10        V11
## 284802 -0.2359732  0.8127221  0.1150929 -0.2040635 -0.6574221  0.6448373
## 284803 -2.6068373 -4.9182154  7.3053340  1.9144283  4.3561704 -1.5931053
## 284804  1.0584153  0.0243297  0.2948687  0.5848000 -0.9759261 -0.1501888
## 284805  3.0312601 -0.2968265  0.7084172  0.4324540 -0.4847818  0.4116137
## 284806  0.6237077 -0.6861800  0.6791455  0.3920867 -0.3991257 -1.9338488
## 284807 -0.6496167  1.5770063 -0.4146504  0.4861795 -0.9154266 -1.0404583
##                V12        V13         V14         V15        V16
## 284802  0.19091623 -0.5463289 -0.73170658 -0.80803553  0.5996281
## 284803  2.71194079 -0.6892556  4.62694203 -0.92445871  1.1076406
## 284804  0.91580191  1.2147558 -0.67514296  1.16493091 -0.7117573
## 284805  0.06311886 -0.1836987 -0.51060184  1.32928351  0.1407160
## 284806 -0.96288614 -1.0420817  0.44962444  1.96256312 -0.6085771
## 284807 -0.03151305 -0.1880929 -0.08431647  0.04133346 -0.3026201
```

Fig. 6 Comparison train data of time, amount and class

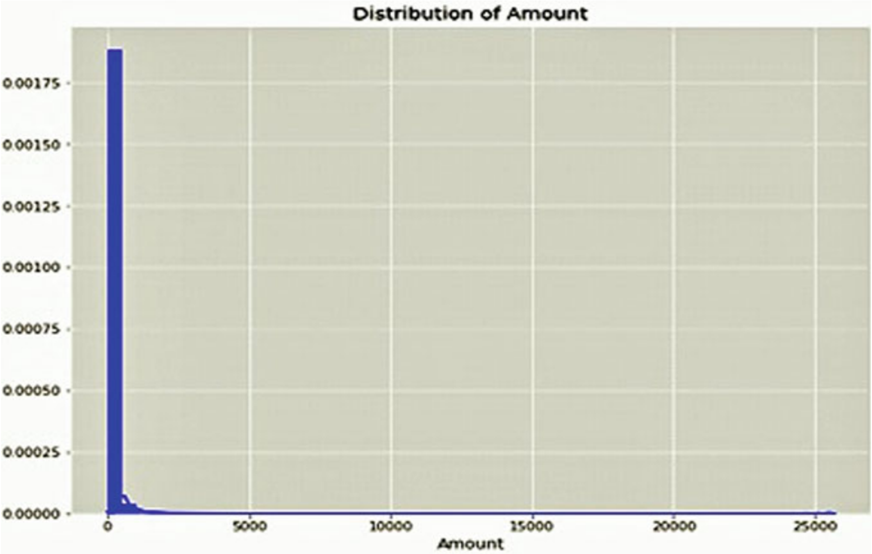


Fig. 7 Distribution of amount of credit card data

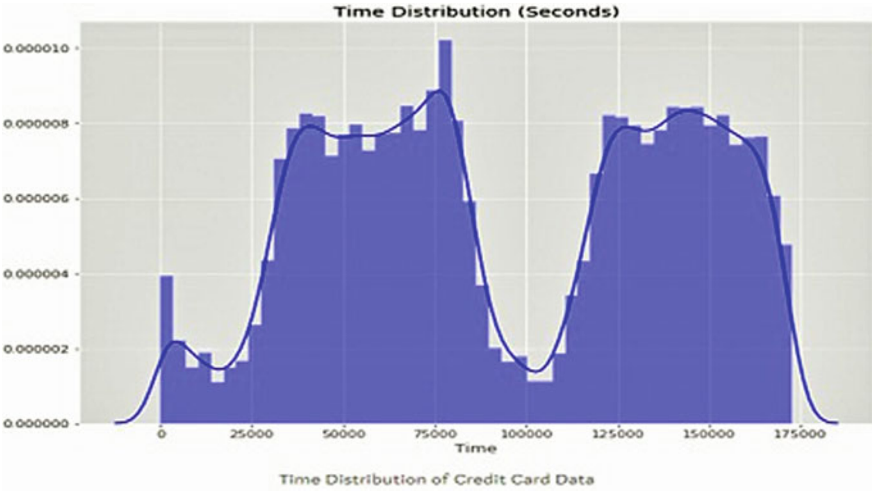


Fig. 8 Time distribution of credit card data

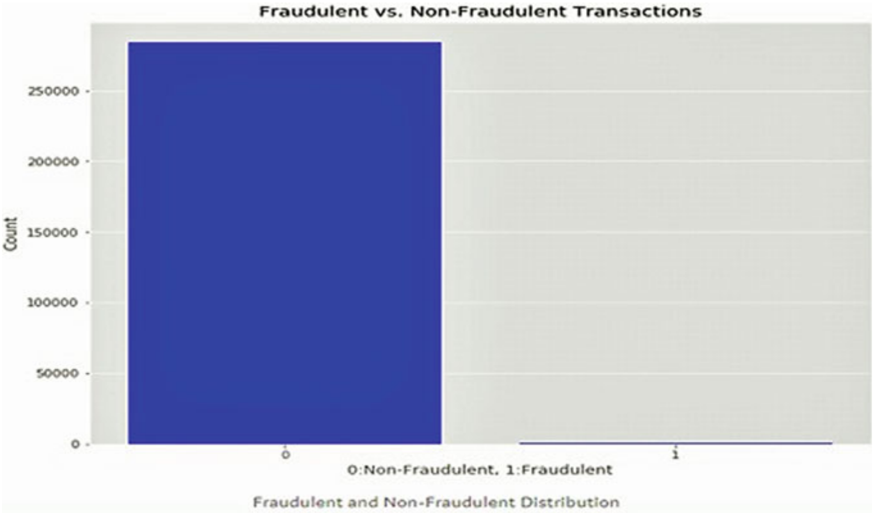
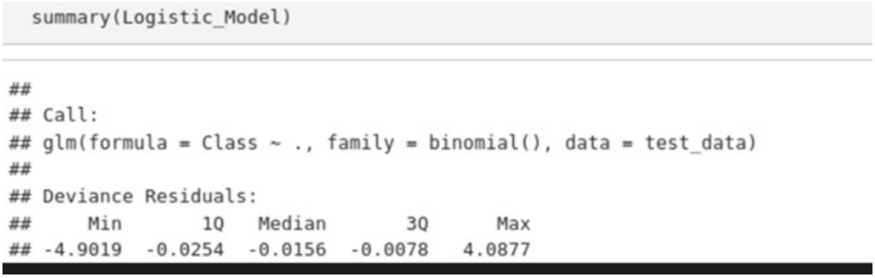


Fig. 9 Fraudulent and Non-Fraudulent distribution of credit card data

d. **Data Modeling**: Later we have normalized our whole dataset, we will partition our dataset into preparing set just as test set with the split proportion of 0.83 which implies that 83% of the information is ascribed to the preparation information though 17% of the information is given to the test information [9, 9].

Figure 11 is depicting that, here not added any numbers because it would be



```
summary(Logistic_Model)
```

```
##
## Call:
## glm(formula = Class ~ ., family = binomial(), data = test_data)
##
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -4.9019  -0.0254  -0.0156  -0.0078   4.0877
```

Fig. 10 Divison of test data and train data

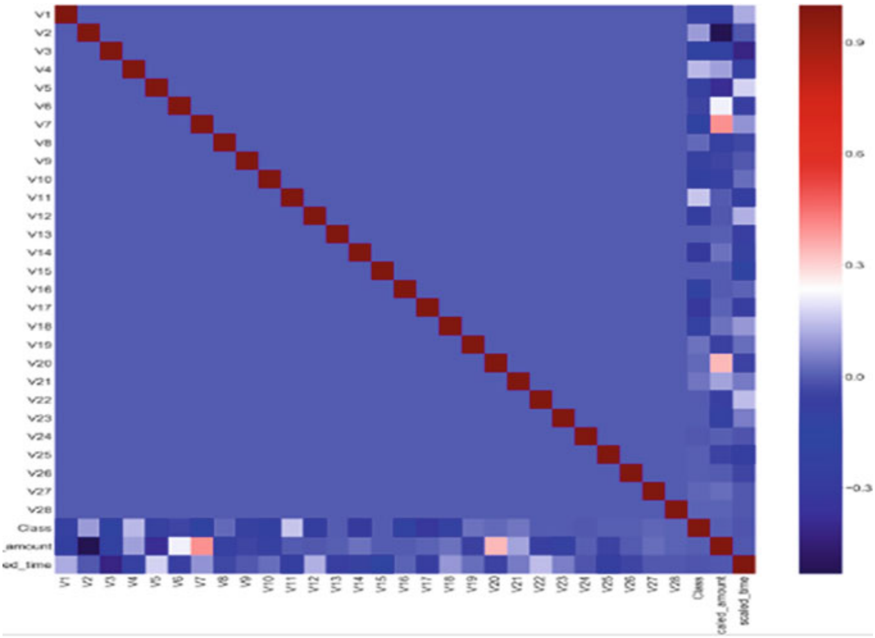


Fig. 11 Correlation among time and amount of credit card fraud

very, very difficult for the reader to see. So look for anything that shows strong correlation.

e. **Logistic Regression and Random Forests**: Calculated relapse is a factual model that endeavors to decrease the expense of an awful gauge. The Random Forests calculation is a gathering of choice trees that all things considered anticipate whether the change is a misrepresentation or not. In the event that progressing is a fake, I run my information through these two models and get extraordinary outcomes. The complete score for calculated relapse and arbitrary woods models is exceptionally encouraging for our dataset. Each model

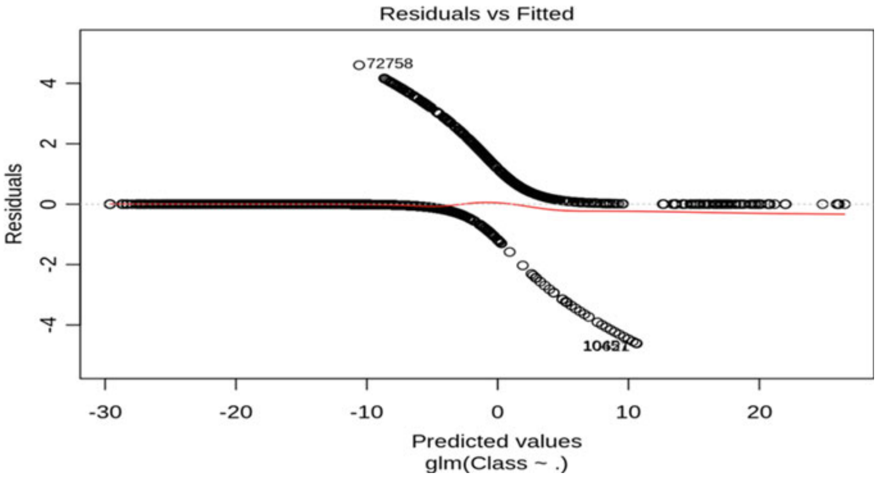


Fig. 12 Logistic regression of credit card fraud/non-fraud transition

has a high evident positive rate and takes into consideration a bogus positive rate which we need here [14].

f. **Fitting Logistic Regression Model**: In this credit card fraud detection system project, we will adapt to our standard model. So let's start with logistic regression. In our case, we are trying to find out if it is a fraud/non-fraud transition. [6, 6] (Fig. 12).

g. **Decision TREE**: In the choice tree—Regression, the choice tree makes relapse or characterization models as a tree structure. We partition the dataset into littler and littler subsets and simultaneously build up a related choice tree. The final product is a tree with choice hubs and leaf hubs. The choice tree can contain both numeric and clear cut information (Fig. 13).

h. **ANN Artificial Neural Network**: ANN's are the sort of AI calculation (ml) methodology displayed based on the human sensory system. ANN models picked up utilizing authentic information and rank dependent on input information. The information imported from the neural system bundle permits us to actualize our ANN. At that point we can plot it utilizing the plot work. Presently, on account of fake neural systems, there is a scope of qualities somewhere in the range of 1 and 0. We characterize limit esteem. 0.5 Otherwise the worth more prominent than 0.5 will be 1 and the rest is 0 [9] (Fig. 14).

3 Proposed Algorithm

Some common methods are used for making the system. Algorithm used: HMM (Hidden Markov Model (HMM)); Semi HMM; Multiple HMM; Optimized HMM, and Advanced HMM.

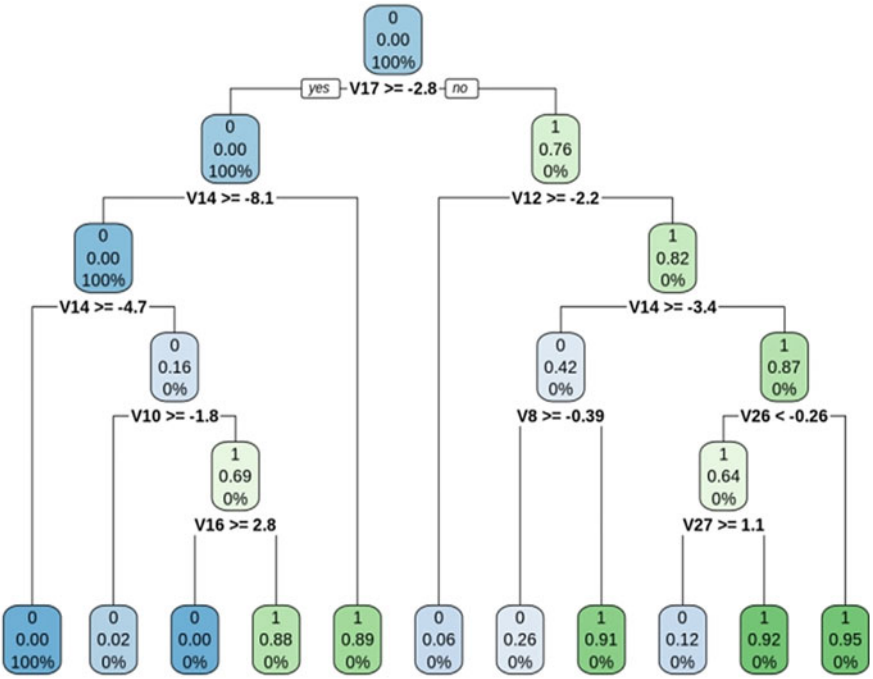


Fig. 13 Decision tree—regression model for credit card fraud/non-fraud transition

The comparison between different algorithms on their accuracy here the optimized HMM is most accurate in the functioning whereas the HMM is lead Functioning. Whereas the dataset trading using R language is also a good accurate algorithm this functionally performs equally to the optimized HMM. Among all the methods of finding the fraud detection technique system build the Hidden Markov Model (HMM) is the one of the best and accurate method for the detection of the fraud transition [7]. HMM method has the very high accuracy among all the methods as shown in the figure below among all the methods of building the fraud detection system techniques (Fig. 15).

3.1 ROC Curve of the Algorithms

A Receiver Operator Characteristics curve (ROC) is a graphical diagram used to show the diagnostic capability of binary classifiers. It was first used in the theory of signal detection but it is now used in many other field such as medicine, radiology, natural hazards, and machine learning [8] (Fig. 16).

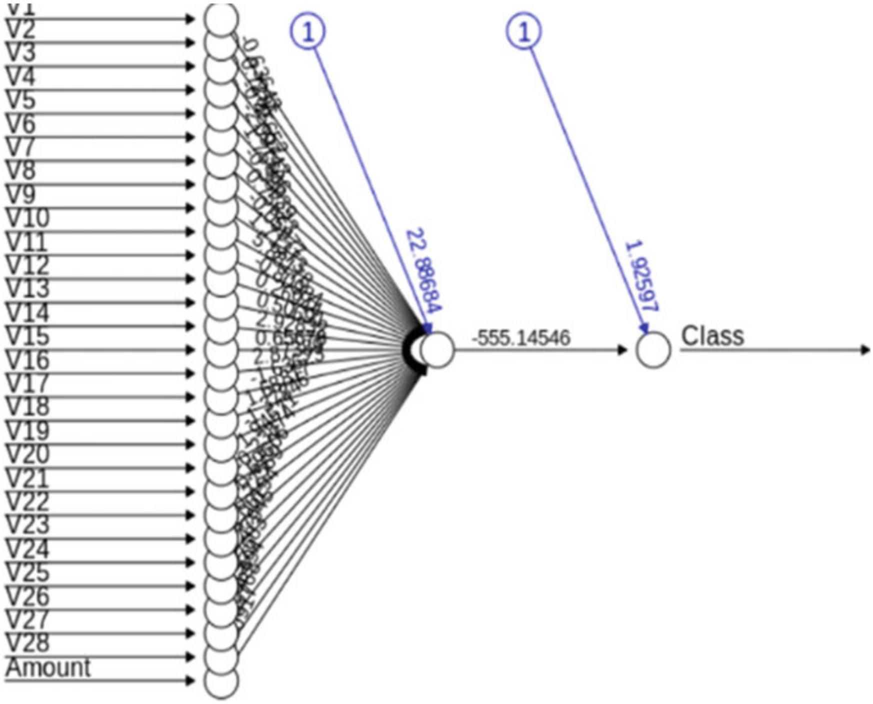


Fig. 14 Artificial neural networks for credit card fraud/non-fraud transition

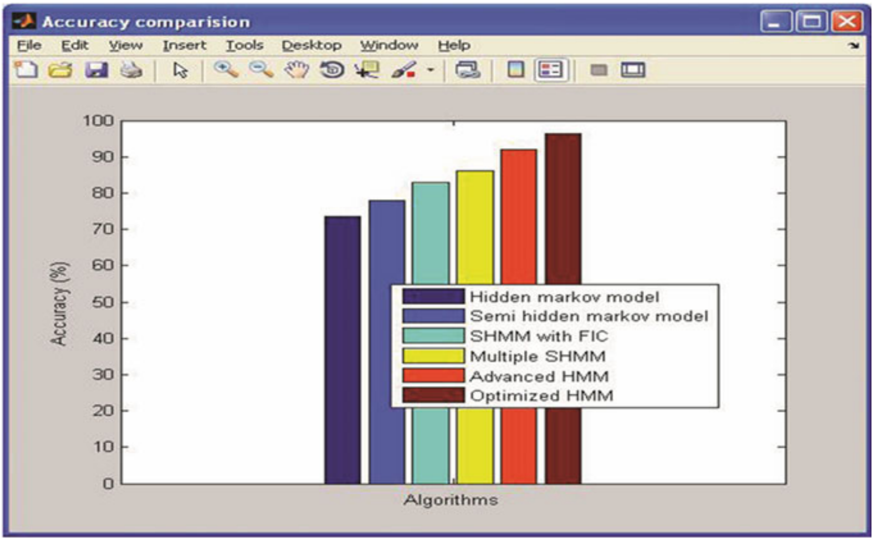


Fig. 15 Accuracy comparison of different methods

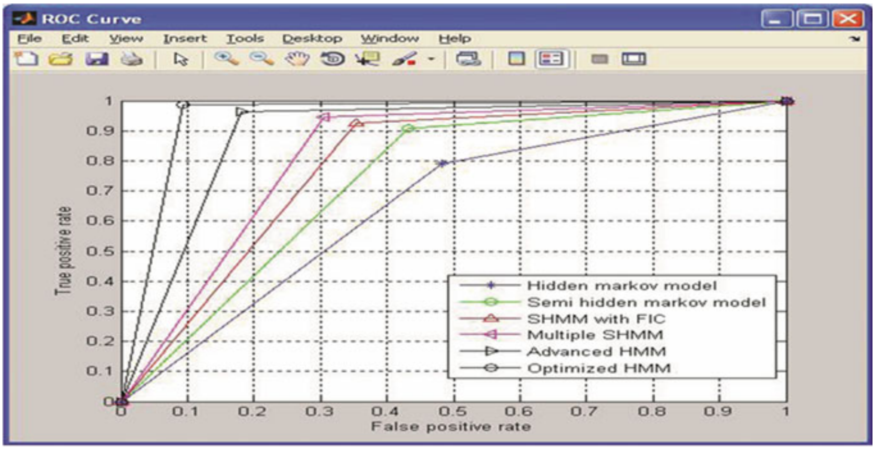


Fig. 16 Receiver operator characteristics curve of various methods

4 Issues: CC Fraud—Detection

Fraud detection system is subject to a lot of trouble and has a lot of problems mentioned below. Effective fraud detection techniques that most should have the ability to eliminate these difficulties to obtain and achieve the best performance.

a. Data Misbalancing: credit card data fraud detection is skewed, which means that a very small percentage of all credit card transactions are fraud. This makes detection difficult and inaccurate fraudulent transactions.
b. Misclassification of data: In a fraud detection system tasks, different misclassifications have different interests. One classifies normal transactions such as fraud harmless as normal detection fraudulent transactions. Because in the first case of misclassification are identified by further investigation [].

5 Conclusion

To find the fraud transactions with credit cards are actually important specifically in digital society. So detection of credit card fraud is very multifarious and important matter that entails the large number of data analysis and a very precise system which will detect fraud in maximum number of cases and also able to handle error and some other inputs. It can be considered as part of machine learning and data science and this type of system ensures the customer and organization that the money transfer is always safe and there is no loss of the money or anything. Future work will focus on more about the fake bin detection which authors covered in the introduction part. This is one of the most important things to look on as there is much fraud using this bin system that authors analyzed. Another thing is the POS hacking or hijacking which is also an important task to add in it. The POS hacking is also a big fraud and we should always look on that to and try our system to tackle this problem also.

References

1. K. Chaudhary, J. Yadav, A review of fraud detection techniques: credit card. Int. J. Comput. Appl. **45** (2012)
2. M. E. Edge, P. R. Falcone Sampaio, A survey of signature based methods for financial fraud detection. J. Comput. Sec. **28**, 381–394 (2009)
3. L. Delamaire, J. Pointon, Credit card fraud and detection techniques: a review. Banks Bank Syst. **4**(2) (2009)
4. S. J. Stolfo, D. W. Fan, W. Lee, A. L. Prodromidis, Credit card fraud detection using meta-learning: issues and initial results. Department of Computer Science Columbia University (1999)
5. S. Maes, K. Tuyls, B. Vanschoenwinkel, B. Manderick, Credit card fraud detection using bayesian and neural networks. Vrije University Brussel–Belgium (2002)
6. https://towardsdatascience.com/credit-card-fraud-detection-a122c7e1b75f59
7. Machine Learning Group—ULB, Credit Card Fraud Detection, Kaggle (2019)
8. Visualizing High-Dimensional Data Using t-SNE, J. Mach. Learn. Res. (2013)
9. S. J. Stolfo, W. Fan, W. Lee, A. L. Prodromidis, Cost-based modeling for fraud and intrusion detection: results from the JAM Project. 0-7695-04910-6/99 (1999)
10. N. Tyagi, A. Katiyar, S. Garg, S. Yadav (2017) Methods for protection of key in private key cryptography. Int. J. Innov. Res. (2017)
11. N. Tyagi, A. Agarwal, A. Katiyar, S. Garg, S. Yadav, Information security: a saga of security measures. Int. J. Eng. Comput. (2017)
12. N. Tyagi, Algorithm for protection of key in private key cryptography. Int. J. Eng. Res. Comput. Sci. (2017)
13. N. Tyagi, Security issues, research and challenges in cloud computing. Int. J. Eng. Res. Comput. Sci. (2017)
14. N. Tyagi, Protection of key in private key cryptography. Int. J. Adv. Res. (2017)
15. N. Tyagi, Function codes for protection of key in private key cryptography. J. Emerg. Technol. Innov. (2017)
16. L. K. T. Neha Tyagi, Need of combining symmetric key cryptosystem with public key cryptosystem, in International Conference on Issues & Challenges in Networking, Intelligence (2011)

Offline Handwritten Hindi Character Recognition Using Deep Learning with Augmented Dataset

Ajay Indian, Karamjit Bhatia, and Krishan Kumar

1 Introduction

In the early recent years, tremendous developments have been observed in solving curious tasks by adopting Deep learning. Although neural networks have been utilizing by researchers for the last few decades, their real strength has only been unraveled in recent years. This advancement is because computer systems are well equipped with Graphics Processing Units (GPUs), enabling them to facilitate a superior computational power for improved learning [1]. The improvement and previously obtained great results have directed us to a fact where it is believed that DNNs are proficient enough to solve virtually any problem, provided a sufficient number of training samples are supplied. The main problem of concern in our study is to prepare a vast amount of data samples adequate to build an opposite model for the recognition of offline characters of Hindi script. In this paper, a handwritten dataset is prepared by collecting the samples of handwritten characters from various individuals. This dataset is then augmented by introducing some hypothetical variations in collected samples to enhance the variety of samples such that overall improvement in recognition is attained.

Extracting features has been a crucial stage of any pattern recognition system. This phase generally involves using domain-centric knowledge to extract the features from the image such that extracted features can be used to develop an efficient model. Therefore, one of the characteristics of such techniques that hamper generality is to rely on domain-specific features. To neutralize this phase, the use of Convolution Layers is proposed to extract the implicit features of character images instead of

A. Indian (✉)
Central University of Rajasthan, Ajmer, India
e-mail: ajay.indian@curaj.ac.in

K. Bhatia · K. Kumar
Gurukula Kangri Vishwavidyalaya, Haridwar, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_11

extracting some domain-specific features. These layers are capable of mining features from the character images supplied as input matrix, irrespective of their size, and pass on to the subsequent layer [1]. The models based on the concept of these layers are called Convolutional Neural Networks (CNNs). The best fascinating characteristic of these layers is that they are not known to extract a similar set of features. Rather, they evolve and learn over time.

Apart from these layers, the dataset adopted for the CNN model's training may also be limited to the level of variations in the shape of characters captured during collection [2]. For instance, in our study, it is described how an OCR system can be restricted to some samples when trained with inappropriate parameters using a restricted dataset. Thus, the proposed method is a combination of the two techniques. Convolution layers are employed to extract the features from the original dataset and augmented dataset of offline handwritten Hindi characters. Original dataset, augmented dataset, and the architecture of CNNs are elaborated in Sects. 3, 4 and 5.

2 Literature Review

A concise overview of the work done in the field of offline handwritten Hindi character recognition is presented in this section, including traditional method like Hidden Markov Models (HMMs), Support Vector Machines (SVMs), Decision Trees (DTs), Regular Expressions (REs), etc. to Deep Learning (DL) methods.

Siddhartha et al. [3] proposed the graph matching scheme to compute the similarity among the characters extracted from bank cheques with the samples of characters in the database to recognize the characters. The proposed method was able to identify the characters written on bank cheques with 87.2% accuracy. Gauri et al. [4] presented a hybrid feature extraction scheme and a feature selection technique based on a genetic algorithm with adaptive MLP classifiers to improve overall performance. Kamble et al. [5] proposed a technique for extracting features from handwritten offline Marathi characters using the features based on connected pixel-like area, perimeter, orientation, Euler number, and eccentricity. An accuracy of 85.88% was reported using the proposed technique with the k-NN classifier with fivefold validation. Indian and Bhatia [6] suggested a handwritten offline Hindi vowel "Swar" recognition method by employing a new wave-based feature extraction "Tarang" with back-propagation and attained the accuracy of 96.2%.

Anuvadiya et al. [7] stated that encouraging recognition rate can be achieved with CNN by considering some particular issues. This way, the CNN-based system for recognizing handwritten characters offers an improved recognition rate compared to other CNN-based recognition systems. Indian and Bhatia [8] projected a combinational feature vector using Gradient, Zernike moments, and wave-based features for Hindi numerals recognition and achieved 96.4% accuracy with Zernike complex using BPNN classifiers. Alom et al. [9] presented the experimental results. They revealed the higher performance of the Deep Convolutional Neural Network (DCCNN) model compared to other prevalent object recognition methods. It shows that a DCNN can be a virtuous choice to develop an automatic system for handwritten Bangla character recognition for hands-on applications. Puri et al. [10] presented a proficient Devnagari character recognition method by utilizing SVM for handwritten and printed monolingual documents having Hindi, Sanskrit, and Marathi text. The experiments conducted on the projected system achieved moderate recognition accuracies of 98.35% handwritten characters. Recently, Indian and Bhatia [11] report the efficacy of Zernike moments and Zernike complex moments using a backpropagation neural network classifier for Hindi numeral recognition and accuracy of 80.8% and 94.8%, respectively, is achieved.

It is observed that neural networks, particularly CNN, are being utilized widely to recognize handwritten and printed characters. Yet, traditional methods, e.g., HMM, SVM, DT, etc. are also being adopted in combination with CNN. Memon et al. [12] presented a systematic literature review on OCR and confirmed the same observations.

3 Model Description

An artificial neural network can be best described by its underlying topology, which can be described with the help of different layers utilized in its topology. The current section is dedicated to elaborate two essential layers used in the proposed topology.

3.1 Convolution Layers

The convolution layer is the first and fundamental layer utilized in the proposed scheme. Convolutional layers are responsible for carrying out inference precisely; these layers work as a pre-processing tool with a key objective to extract features from a given input. This task is carried out by employing convolution kernels and convolution operations.

Each convolution layer is equipped with some fixed number of filters, also called kernels. When these layers are supplied with the input, all filters are convoluted for the given input, and each filter produces a single output. All convolution layers possess a crucial characteristic that if more kernels are applied for an input, which is generally not done in deep learning, then extracted features gradually become more abstract. It is critically essentials it supports the model to attain generalization. Moreover, these layers can be further improved to increase their competency and correctness.

3.2 Fully Connected Layers

Fully connected layers are other essential layers in the proposed model. Convolution layers are responsible for extracting specific significant features from supplied input data. The features received from the convolution layer are supplied to a fully connected layer, which produces the results. These layers of CNN are also used in the traditional neural network.

The convolution layer produces the 2D form output, but fully connected layers require input in the 1D form, preferably. Therefore, the output produced from the previous layer is first transformed into a 1D form. So, after converting the output into 1D, it is passed to the fully connected layer. Each of the output values is considered as distinct features and used to characterize the image. These layers carry out two transformations on the received data—a linear and a non-linear transformation. First, a linear transformation is done on the input data.

$$Z = W^T.X + b, \tag{1}$$

where X denotes the input data vector, W is the randomly initialized weight matrix, and b signifies a constant bias value (Fig. 1).

At this moment, only non-linear transformation is left in the forward propagation. Merely performing linear transformation cannot acquire complex relationships hidden in data. Therefore, a component is introduced in the architecture, which enhances non-linearity in the data, known as the activation function. The activation functions support the network to utilize vital information and suppress inappropriate data [14]. Activation functions are used at every layer of the network. The specific activation function to be adopted for a problem depends on the problem's complexity being solved. As our problem is multi-class, so ReLU (Rectified Linear Unit) is used to solve the problem, which is a non-linear activation function widely used in deep learning. The key benefit of adopting the ReLU function as activation functions is that it does not activate all neurons simultaneously, specifically if the output of the linear transformation < 0.

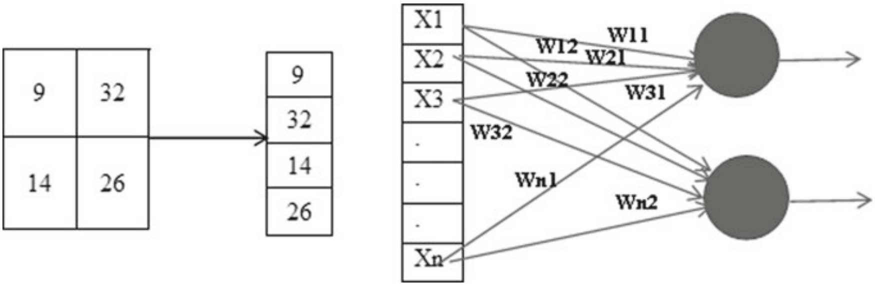


Fig. 1 Depicting the working of fully connected layer

$$f(x) = max(0, x) \tag{2}$$

If input values are negative, it will return zero that means corresponding neurons will not be activated [14]. ReLU will activate the selected number of neurons. The ReLU function is very efficient in computation compared with other functions (such as sigmoid and tanh).

$$f(x) = \begin{cases} 0, x < 0 \\ x, x \geq 0 \end{cases} \tag{3}$$

4 Dataset Description

Our study has used two different datasets- one is collected samples of 46 handwritten characters (10 numerals, 36 consonants) from different individuals of varying groups initially. Two hundred samples were collected for each character, making the complete dataset of 9200 samples (ORG). The second one is the augmented dataset (AUG) derived from the original dataset. With the help of randomized data augmentation, one can grow the size and variations in the training data. Distortions to the image data can be made invariant with the use of augmentation. For instance, randomized rotations can be added to input images such that a network is made invariant to the existing rotation found in input images. An augmented dataset is a handy technique to apply a fixed number of augmentations to 2D images to carry out classification tasks.

For conducting the experiments, the original dataset (ORG) was utilized to construct the model. However, the core competence of this dataset lies under the augmented dataset for the sake of generalization. In the process of augmentation, few image samples of the original dataset are randomly augmented. This augmented dataset is then used for the construction of the classifier. These augmentations comprise

- Random rotation of images in a direction with random value ranges from 10 to 10 and 15 to 15.
- Random translation of images in the horizontal direction.
- Random translation of images in the vertical direction.

As mentioned above, the augmentations are the key to enriching the original dataset with many image variations, which helps defend the key argument of this study to obtain an efficient model for handwritten Hindi character recognition utilizing this augmented dataset. Similar approaches for creating an artificial dataset for a specific problem have also been effectively adopted in other areas, such as scene-text recognition [13], where an appropriate number of data samples were not readily available. For both datasets, 85% of samples were utilized for training, and

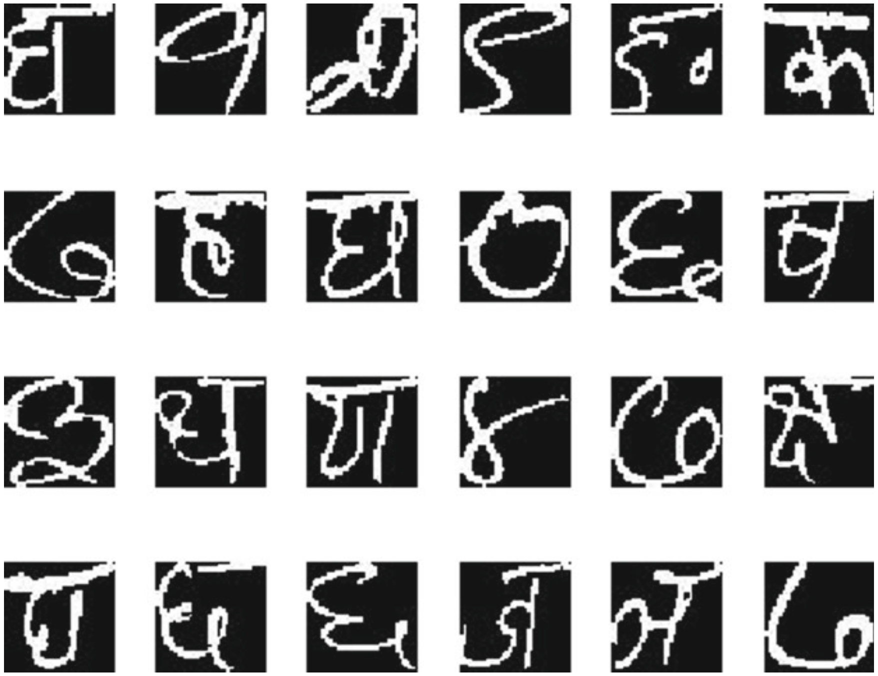


Fig. 2 Random samples of consonants and numerals of hindi script

the rest 15% of samples were utilized to validate the model. Hence, the efficacy of the original dataset over the augmented dataset was verified using the experiments. In this paper, a discussion on the model developed using the original dataset followed by a discussion on how augmented dataset enhances the model's performance over the original dataset is presented. In the validation phase, 15% of each dataset's samples were used to assess the models' performances for handwritten character recognition. Some random samples of characters from the prepared dataset can be found in Fig. 2.

5 Implementation

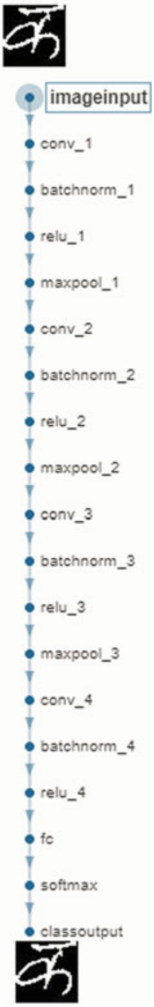
The proposed model based on CNNs for recognizing handwritten Hindi characters is implemented using MATLAB 2019a, and the model is trained and assessed on the above-stated datasets. The preceding sections cover the description of the layers adopted in the proposed model. First, several convolution layers are employed to extract the features of character images. These 2D features are then transformed into a linear vector and then supplied to the fully connected layer. At last, a fully connected layer reduces the size of the linear vector corresponding to the number of target class labels (in our case, 46 class labels for 36 consonants and 10 numerals).

Four strategies are formed using the original dataset and augmented dataset to assess the efficacy of the proposed model:

Strategy-I: CNN models without a dropout layer on original data.
Strategy-II: CNN models with a dropout layer on original data.
Strategy-III: CNN models without a dropout layer on augmented data.
Strategy-IV: CNN models with a dropout layer on augmented data.

An outline of the network layers adopted in the proposed model (*Dropout Layer are only adopted in Strategy-II and Strategy-IV) is presented in Table 1, and the overall flow of the data in the model is depicted in Fig. 3.

Fig. 3 The flow of the data in the proposed CNN model



Another vibrant characteristic of this neural network model is that layers are facilitated to attain maximum generalization and performance gain. Following are the layers:

5.1 Dropout Layers

Neural networks based on deep learning paradigm can quickly over-fit with a training dataset having a small number of examples. Ensembles of network models with different configuration parameters are popularly acknowledged to overcome overfitting problems up to an extent. Still, they incur the extra computational cost to train and maintain multiple models. Preferably, a single model can be utilized to simulate with a huge number of various network structures by randomly dropping out the nodes while training the model. Which is known as dropout, which incurs less computational cost with a remarkable efficient regularization technique to reduce overfitting and improve generalization error in deep neural networks [15, 16].

5.2 Pooling Layers

Next to the convolutional layer, a novel-pooling layer is added to the network. Precisely, after a non-linear activation function (e.g., ReLU) is applied to the feature maps received from the convolutional layer. Adding a pooling layer next to the convolutional layer is a very general phenomenon adopted for sequencing layers in the CNN model, which can be used one or more than one time in a given model. These layers work upon all feature maps individually to produce a new set of pooled feature maps. Pooling comprises selecting a pooling operation similar to a filter to be applied to feature maps. The pooling or filter size remains smaller than the size of the feature maps [18]. The pooling is specified rather than learned. Generally, pooling is done by employing two functions:

- *Average Pooling*: Computes the average value for all the patches on the feature map.
- *Maximum Pooling*: Computes the max value for all the patches on the feature maps, called max-pooling [18].

5.3 Batch Normalization Layer

This layer is used to normalize each input channel across a mini-batch. These layers first normalize all channels' activations by subtracting the mini-batch mean and dividing by the mini-batch standard deviation. Small batches of mini sizes are adopted throughout the training phase to speed up the training of CNNs and reduce the sensitivity to network initialization. Challenges that come with small size batches are resolved using the covariance shift [17, 19] and batch normalization.

6 Result and Discussion

Based on the strategies mentioned above, all the models, I, through IV, are trained with a hyper-parameter, ***tolerance***, and dynamically defined tolerance—all the models assessed using the validation dataset by using the estimated heir accuracies and losses. If the loss decreases after some no. of epochs, concluded that convergence had occurred; hence, training was halted. Here, the maximum number of epochs was decided based on the performance. If the performance of the model stabilizes after some number of epochs, training was stopped. Empirically observation has been made that all models based on the strategies mentioned above converged comparatively better with small datasets than some other state of the art where large datasets were used. A summary of all the outcomes obtained after experimentation is presented in Table 2.

Based on the original dataset (ORG), strategy-I achieved the recognition rate of 90.78% with an average training time/epoch of 13.7 s and a total training time of 6 min 51 s. Whereas the Strategy-II based on the original dataset (ORG) with dropout layer performed better, giving an accuracy of 91.90%, an average training time/epoch of 12.31 s, and total training time of 7 min 11 s that shows that for dataset (ORG) network generalizes well with dropout layer.

Strategy-III, based on the augmented dataset (AUG), achieved the recognition rate of 92.18% with an average training time/epoch of 12.47 s and a total training time of 9 min 34 s. Whereas, the Strategy-IV based on the augmented dataset (AUG) with the dropout layer performed better as compared to Strategy-I, Strategy-II, and Strategy-III. It achieved an accuracy of 94.19% with an average training time/epoch of 8.43 s and a total training time of 6 min 38 s, which is the highest accuracy achieved in the proposed work. Performance of the Strategy-IV affirms that the network generalizes very well with the dropout layer and improves the model's performance in terms of speed and accuracy. Performance and loss estimation of the Strategy-IV is shown in Figs. 4 and 5 while training the model. Performance comparison of the proposed strategy with other existing models based on CNN are presented in Table 3, which shows that the performance of the proposed approach (94.19%) is comparable to the performance (95.46%) of [21] as in the proposed work dataset is smaller, and numbers of classes are more than double. Performance of the strategies discussed in [20, 22] are much better than the proposed approach as the numbers of samples in these strategies are ten times more, but the average training time/ epoch is very high. It shows that a higher accuracy rate can be achieved by increasing the dataset's size in the proposed strategy.

Table 1 Outline of the network layers adopted with various parameters

Layers	Parameters used
Input layer	40*40
Convolutional	4 Filters of size 3*3, Stride of [1 1], with Padding “same”
Normalization	Batch
Activation function	ReLU
Pooling	2*2 Max-pooling, Stride [2 2], with Padding [0 0 0 0]
*Dropout	0.5
Convolutional	8 Filters of size 3*3, Stride of [1 1], with Padding “same”
Normalization	Batch
Activation function	ReLU
Pooling	2*2 Max-pooling, Stride [2 2], with Padding [0 0 0 0]
Convolutional	16 Filters of size 3*3, Stride of [1 1], with Padding “same”
Normalization	Batch
Activation function	ReLU
Pooling	2*2 Max-pooling, Stride [2 2], with Padding [0 0 0 0]
Convolutional	32 Filters of size 3*3, Stride of [1 1], with Padding “same”
Normalization	Batch
Activation function	ReLU
Fully connected	46 Fully connected layers
Softmax	Softmax
Classification	Crossentropyex

7 Conclusion

The work done in this paper is limited to study the performance of augmented dataset (AUG) for Hindi characters over the original dataset (ORG) of small size using a CNN with a dropout layer for the recognition of characters. The current study has shown that the augmented dataset (AUG) outperforms the original dataset, signifying the augmented dataset’s importance. Using the dropout layer also enables the model to overcome over-fitting as the dataset used in this paper is comparatively small compared to other states of the art problem. Hence, the use of a dropout layer increases performance. In the future, this technique can be enhanced for the recognition of words as this study only focused on recognizing individual characters of Hindi script and some other scripts.

Table 2 Performances of the proposed strategies

Strategy	Dataset	Epoch number with best accuracy	Average training time/epoch (s)	Total training time	Accuracy (%)
Strategy-I	ORG (Collected Samples)	30	13.7	6 min 51 s	90.78
Strategy-II	ORG (Collected Samples)	35	12.31	7 min 11 s	91.90
Strategy-III	AUG (Augmented Collected Samples)	46	12.47	9 min 34 s	92.18
Strategy-IV	AUG (Augmented Collected Samples)	46	8.43	6 min 38 s	94.19

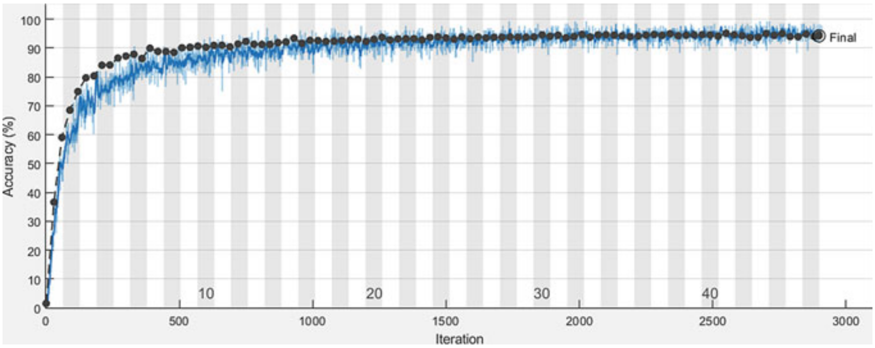


Fig. 4 Performance of the Strategy-IV in terms of accuracy versus iteration

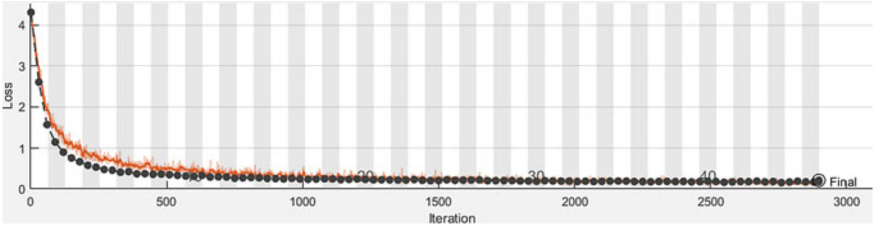


Fig. 5 Performance of the Strategy-IV in terms of loss versus iteration

Table 3 Performance comparison of strategies adopted in study

Authors	Dataset	No. of samples in the dataset	No. of distinct characters/class labels	Average training time/epoch	Accuracy (%)
Baranidharan et al. [20]	UC irvine machine learning repository	92,000	46	47 s	98.66
Aneja and Aneja [21]	UC irvine machine learning repository	92,000	46	16.3 min	99
Sonawane et al. [22]	Own created dataset	16,870	22	–	95.46
Proposed	AUG dataset	9200	46	8.43 s	94.19

Further, the offline handwritten character recognition system can be integrated with the security system to develop a more interactive and more secure system in this digital era. The user will be able to interact with the system and get authenticated by using his handwritten text. Hence, the system will be more personalized and secured for the individual users.

References

1. A. Krizhevsky, I. Sutskever, G.E. Hinton, ImageNet classification with deep convolutional neural networks. Commun. ACM **60**(6), 84–90 (2017)
2. K. Peymani, M. Soryani, From machine-generated to handwritten character recognition: a deep learning approach, in *3rd International Conference on Pattern Recognition and Image Analysis (IPRIA)*, Shahrekord, pp. 243–247. https://doi.org/10.1109/PRIA.2017.7983055 (2017)
3. S. Banerjee, B.R. Ghosh, A. Kundu, Handwritten character recognition from bank cheque. Int. J. Comput. Sci. Eng. EISSN: 2347–2693, **4**(1), 099–104 (2016)
4. G. Katiyar, S. Mehfuz, A hybrid recognition system for off-line handwritten characters. Springer Plus **5**(1), 1–18 (2016)
5. P.M. Kamble, R.S. Hegadi, Geometrical features extraction and KNN based classification of handwritten marathi characters, in *World Congress on Computing and Communication Technologies (WCCCT)*, pp. 219–222 (2017)
6. A. Indian, K. Bhatia, Offline handwritten hindi 'SWARs' recognition using a novel wave based feature extraction method. Int. J. Comput. Sci. Issues **14**(4), 8–14 (2017)
7. H.D. Anuvadiya, A.A. Abhangi, A research on improve handwritten character recognition by using convolutional neural network. Int. J. Adv. Eng. Res. Dev. **5**(05), 20–25 (2018)
8. A. Indian, K. Bhatia, Off-line handwritten hindi consonants recognition system using zernike moments and genetic algorithm, in *Proceedings of the IEEE Conference International Conference on System Modeling & Advancement in Research Trends, (SMART-2018)*, pp. 10–16 (2018)
9. Z. Alom, P. Sidike, M. Hasan, T.M. Taha, V.K. Asari1, Handwritten bangla character recognition using the state-of-the-art deep convolutional neural networks. Hindawi Computat. Intell. Neurosci. **2018**, Article ID 6747098, pp 1–13. https://doi.org/10.1155/2018/6747098 (2018)

10. S. Puria, S.P. Singh, An efficient devnagari character classification in printed and handwritten documents using SVM, in *International Conference on Pervasive Computing Advances and Applications—PerCAA 2019, Procedia Computer Science*, vol. 152, pp. 111–121 (2019)
11. A. Indian, K. Bhatia, Offline handwritten hindi numerals recognition using zernike moments. Int. J. Tomograp. Simul. **32**(2), 68–82 (2019)
12. J. Memon, M. Sami, R.A. Khan, Handwritten Optical Character Recognition (OCR): a comprehensive Systematic Literature Review (SLR), Cornell University (2020)
13. M. Jaderberg, K. Simonyan, A. Vedaldi, A. Zisserman, Synthetic data and artificial neural networks for natural scene text recognition (2014)
14. C.E. Nwankpa, W. Ijomah, A. Gachagan, S. Marshall, Activation functions: comparison of trends in practice and research for deep learning. arXiv:1811.03378v1 [cs.LG] 8.(2018)
15. H. Wu, X. Gu, Max-pooling dropout for regularization of convolutional neural networks. (2015)
16. N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, R. Salakhutdinov, Dropout: a simple way to prevent neural networks from overfitting. J. Mach. Learn. Res. **15**, 1929–1958 (2014)
17. I. Sergey, C. Szegedy, Batch normalization: accelerating deep network training by reducing internal covariate shift. arXiv:1502.03167 (2015)
18. J. Brownlee, A gentle introduction to pooling layers for convolutional neural networks, in *A Web Article on Deep Learning for Computer Vision*, April 22 (2019)
19. https://in.mathworks.com/help/deeplearning/ref/nnet.cnn.layer.batchnormalizationlayer.htm
20. B. Baranidharan, A. Kandpal, A. Chakravorty, Hindi handwritten character recognition using CNN. Int. J. Adv. Sci. Technol. **29**(6), 58–66 (2020)
21. P. K. Sonawane, S. Shelke, Handwritten devanagari character classificationusing deep learning, in *IEEE International Conference on Information, Communication, Engineering and Technology (ICICET)*, Zeal College of Engineering and Research, Narhe, Pune, India, pp. 1–4, Aug. 29–30 (2018)
22. N. Aneja, S. Aneja, Transfer learning using CNN for handwritten devanagari character recognition, in *Accepted for publication in IEEE International Conference on Advances in Information Technology (ICAIT)* (2019)

Handshake Comparison Between TLS V 1.2 and TLS V 1.3 Protocol

Abhay Pratap Singh and Mahendra Singh

1 Introduction

The benefits of the Internet include easy retrieval of information, communication, Internet banking, e-commerce, and several others, enhancing living standards. Simultaneously, the Internet also has some shortcomings as much as its advantages. With the increasing development of cyber security threats to provide Web communications security and wireless cellular networks over the Internet has grown to be a significant concern in the digital era [1, 2]. The sensor network security is essential for transferring reliable data from sensor devices to distant sinks and maintaining network availability [3]. The data transmission between two entities must be carefully secured and protected while they are communicating across unsecured networks or unprotected networks. For this purpose, the SSL/TLS protocol provides the mechanism to protect the Internet traffic during data transmission. The TLS protocol is one of the most popular enciphered communication protocol among the Internet [4]. The TLS protocol facilitates the Web-client and Web-server to verify both sides to negotiate to encipher algorithms and cryptographic keys in the handshake process before retrieving essential information over the Web [5]. Today, almost 75% of all Web application requests are secured and protected utilizing the TLS encipher-based methods [6]. It is also utilized by other Internet protocols, including IMAP (Internet Message Access Protocol) or SMTP (Simple Mail Transfer Protocol) (email communication), HTTP or HTTPs (Hypertext Transfer Protocol or Secure) (Web communication), and LDAP (Lightweight Directory Access Protocol) (for accessing directories) [7]. Applications running on computer devices, servers, and mobile phones heavily rely on it [8]. The TLS protocol devised to deliver network security features for protocols operating on the application layer. TLS works across transport layer protocols, as

A. P. Singh (✉) · M. Singh
Department of Computer Science, Gurukula Kangri Vishwavidyalaya, Haridwar, India
e-mail: rs.abhaypratapsingh@gkv.ac.in

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_12

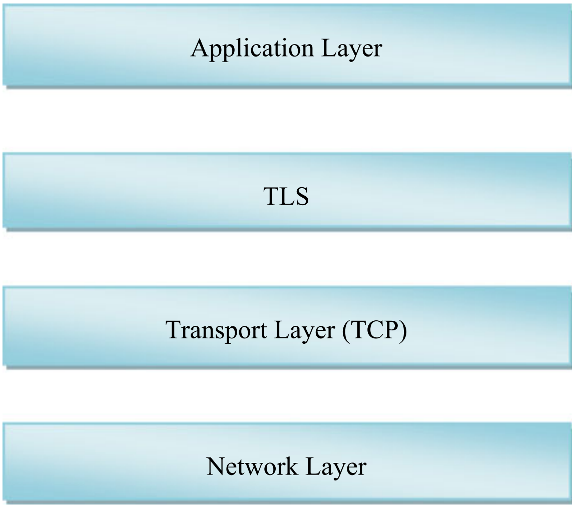


Fig. 1 Flow of TLS in communication layers

shown in Fig. 1. Particularly, TLS operates over the Transmission Control Protocol (TCP) [9], a reliable or secure network protocol that ensures the delivery of network messages in order. The fundamental purpose of TLS protocol is to expedite the establishment from a safe and reliable medium within two connecting parties, for example, Web-client to Web-server; therefore, third parties cannot obtain transmitted data. By using SSL/TLS, an attacker can still hijack the session or data. Though, as the data is enciphered, the attacker cannot retrieve any meaningful information from transmitted packets over Web communication. Therefore, the message's integrity and confidentiality are preserved. The TLS protocol can also be utilized to safeguard the privacy and authenticity among the clients communicating over unsecured channels. Simultaneously, attackers can also be used to conceal malicious activities due to the nature of encrypted traffic.

In this paper, we will consider the TLS protocol as one of the most extensively recognized enciphered network traffic protocols. First, we captured network traffic (PCAPs) using packet capturing tool Wireshark [10] and performed passive monitoring to inspect the TLS v 1.2 handshake and TLS v 1.3 handshake metadata. The rest of this paper is prepared as follows: in Sect. 2, discussed the background and architecture of SSL/TLS. Sections 3 and 4 present a passive inspection of TLS v 1.2 and TLS v 1.3 handshake metadata through Wireshark. Next In Sect. 5, discussed the improvements of TLS v 1.3 over TLS v 1.2. Finally, Sect. 6 presents the conclusion of this paper.

2 Background of SSL/TLS

This section presents the history and architecture of the SSL/TLS protocol. Netscape Company introduced SSL protocol in 1994, which was later, renamed the TLS protocol. SSL/TLS is cryptographic protocols that aim to provide secure and safe data transmission across a computer network. It is a standard mechanism that establishes an encipher communication between Web-client to Web-server. TLS is one of the most extensively utilized network security protocols today. It is also utilized for Internet browsers and other Web applications that need to exchange data securely over the network, for instance, VPN and data file transfers [11]. SSL comprises 1.0, 2.0, and 3.0 versions, including its historical development, and then convert it to the TLS protocol to make it more efficient and secure. On the other hand, four various versions of the TLS protocol are currently in use, including TLS 1.0, TLS 1.1, and TLS 1.2, of which TLS 1.3 is the safest and secured new protocol.

SSL v 1.0 was developed in 1994 by the Netscape Internet browser, which refers to the Netscape communications organization. However, it is criticized and could not open for public use because it contains many vulnerabilities. After making several changes for the previous version, Netscape communications launched SSL v 2.0 in February 1995. This version explored several security flaws like lack of missing handshake authentication, utilizing a weak algorithm through the handshake process, etc. SSL v 3.0 [12] was formed in 1996 to enhance the security and operationally of SSL v 2.0. Nonetheless, since 2014, this version has again deemed insecure, as it is exposed to several methods of an attack affecting block encryption. Only the RC4, a stream cipher algorithm, support this version, but this algorithm is not adequate to make SSL v 3.0 reliable as it can be disclosed to numerous attacks.

TLS v 1.0 RFC 2246 is an upgraded version of SSL v 3.0, first confirmed in January 1999 [13]. The primary security flaw in TLS v 1.0 implementation is the support for the downgrade negotiation mechanism where the Web-client and Web-server can allow on a weaker SSL protocol. TLS v 1.1 RFC 4346 was described in April 2006 [14]. TLS v 1.1 prohibits the usage of insecure cipher suites. The critical vulnerability of the TLS v 1.1 implementation is utilizing an amalgamation of MD5 and SHA-1 hash functions that have been proven to be broken [15]. The significant change from TLS v 1.0 is that this variant introduced security features toward cipher-block chaining attacks. TLS v 1.2 RFC 5246 was first settled in August 2008[16] and updated the previous version of TLS. One of the main goals of this version was to eliminate the protocol's dependence on MD5 and SHA1 hashing algorithms. TLS v 1.3 RFC 8446 was well-defined in August 2018 [17]. TLS v 1.3, the most updated version of the protocol offers many features to significantly improve the performance especially TLS handshake, simplify the protocol, and many other things [18]. It is also based on TLS v 1.2, but it is different from the preceding version. It eliminated the MD5 and SHA-224 support as hash functions. This version also eliminated some ciphers which have been vulnerable and considered as insecure. Some of them are RC4, ciphers using block chaining, and RSA key transport. This version has also

Table 1 SSL/TLS protocol versions

Version number	Year
SSL 1.0	1994
SSL 2.0	1995
SSL 3.0	1996
TLS 1.0	1999
TLS 1.1	2006
TLS 1.2	2008
TLS 1.3	2018

improved the load time for Web pages. An outline of the variations from SSL/TLS protocol versions is shown in Table 1.

2.1 SSL/TLS Architecture

HTTPs (also termed as HTTP over TLS) are HTTP (Hypertext Transfer Protocol) protected by SSL or TLS. The primary functioning of SSL/TLS is made possible by the other related systems, such as the operating system and network connectivity through TCP/IP [19]. In addition, the root or system director, which also supports the authentication process, and the trusted certificate authorities (CA) play a significant role in enabling proper SSL/TLS functioning. TLS is not a sole protocol, but consists of two protocol layers, as shown in Fig. 2.

Primarily, the handshake protocol manages the authentication process between the Web-client and Web-server by first allowing the negotiation of the algorithm for encryption and exchanging the subsequent the encryption keys [21]. The top layer comprises the three handshaking sub-protocols: the Handshake, the Change Cipher Specification, including the Alert protocol. Fundamentally, the handshake protocol maintains the authentication process within the client to server by negotiating the cryptographic parameters which are explained below:

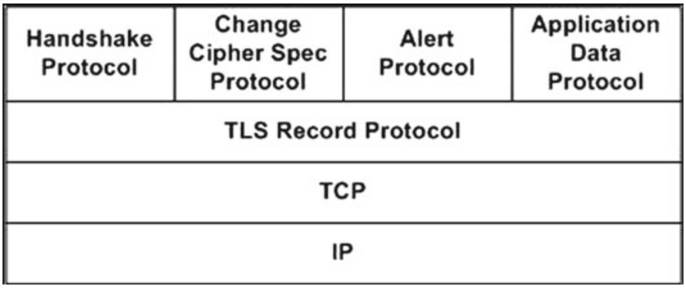


Fig. 2 Architecture of SSL/TLS [20]

- **Session identifier**—An arbitrary byte sequence is determined via the server to recognize a session state.
- **Compression method**—the algorithm is also applied to compress data.
- **Peer certificate**—X.509v3 digital certificate used.
- **Cipher suite**—It is a combination of several cryptographic algorithms, including the encipher algorithm, key exchange algorithm pseudorandom function (PRF), and MAC algorithm applied for key generation.
- **Master secret**—It is acquired during the handshake and used for generating both cryptographic keys (MAC and encryption keys).
- **Is resumable**—A flag showing whether the session can be utilized to start novel connections.

The change cipher spec protocol is mainly deal with to change the encryption utilized by both client and server. It is usually used as a part of the handshake process to shift to symmetric key cipher. The CCS protocol notifies the message to the sender wants to change to a distinct collection of keys, and created information transferred by the handshake protocol.

On the other side, the alert protocol provides information regarding the authentication process, for example, authentication failure, an error that occurred during the process, or an alert to end the connection. There are two kinds of alert messages: first, warning it can be ignored, and the second fatal, the connection will be terminated immediately.

Once the authentication process is finished, the Record protocol is accountable for dividing data into chunks, which are optionally compressed, authenticated with MAC, encrypted, and ultimately transmitted [22]. On the receiving side, the received data is deciphered, verified by calculating MAC, decompressed, reassembled, and then gets conveyed to the calling application on the recipient's side. The following figure below depicts the overall functioning of the SSL/TLS record protocol (Fig. 3).

In the Figure shown, the initial phase is fragmentation. Each application data gets fragmented within blocks of fixed size. Here, compression is optionally used. There is no compression algorithm specified in SSL v 3.0, therefore, compression algorithm utilization is insignificant by default. However, it depends on the implementation; the record protocol may select a compression algorithm.

In a further step, a message authentication code gets calculated over compress data. A hash code is calculated by combining the compressed data, a secret key, and some padding. In order to do this, clients and servers are utilized MAC secret keys. The receiver executes similar calculation and compares the calculated MAC value, including the incoming MAC value. If both the values match, the receiver is ensured that the message did not change during transmission. Besides, with MAC, the receiver will have the certainty regarding the authenticity of the sender. Now, the compressed data and associated MAC are enciphered utilizing a symmetric key cipher. Lastly, the SSL record protocol pre-adds the SSL record header and transmits the whole unit to the receiver.

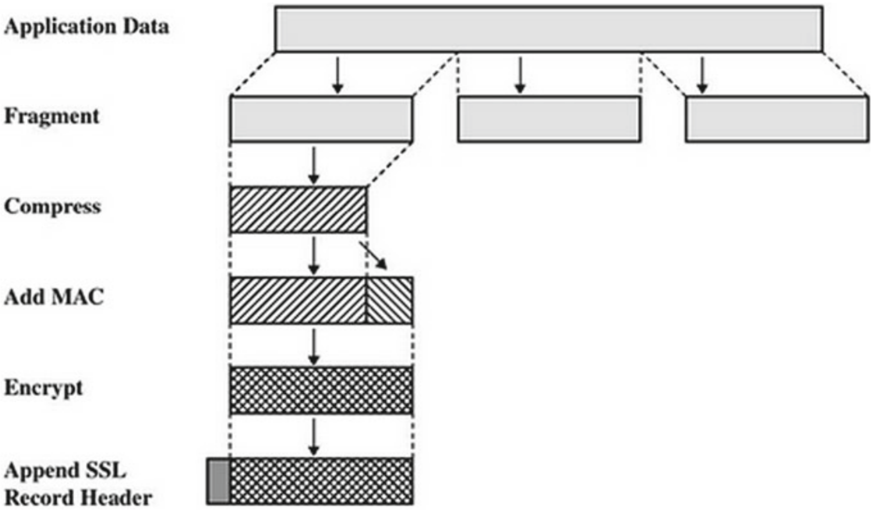


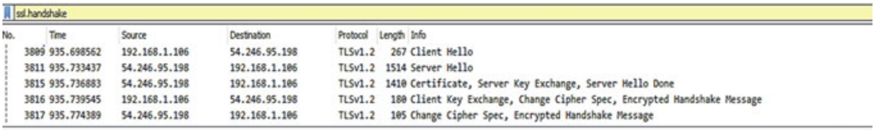
Fig. 3 SSL/TLS record protocol [20]

3 Passive Inspection of TLS V 1.2 Handshake Through Wireshark

The following image is an illustration of the TLS v 1.2 handshake between the client to server captured via Wireshark. This packet analyzer tool inspects the browsing of TLS v 1.2 handshake parameters (Fig. 4).

3.1 Client Hello

In the handshake process, hello message to the client is the initial move in initiating a TLS session since the user wants to communicate with TLS. It contains a version number, cipher suites and, session-related data.



```
ssl.handshake
No.    Time        Source          Destination     Protocol Length Info
  3809 935.698562  192.168.1.106   54.246.95.198   TLSv1.2   267 Client Hello
  3811 935.733437  54.246.95.198   192.168.1.106   TLSv1.2  1514 Server Hello
  3815 935.736883  54.246.95.198   192.168.1.106   TLSv1.2  1410 Certificate, Server Key Exchange, Server Hello Done
  3816 935.739545  192.168.1.106   54.246.95.198   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  3817 935.774389  54.246.95.198   192.168.1.106   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
```

Fig. 4 TLS v 1.2 handshake process

3.2 Server Hello

The second step is the answer of the server to the client hello message to communicate with TLS. It also contains a version number, cipher suites, and session-related data. Furthermore, this step holds the server's public key along with the server's digital certificate.

3.3 Server Key Exchange and Certificate

The Web-server's public key is used to encipher a session key which is generated for the secure communication. It is essential to say that both the Web-client and the Web-server will utilize similar key to encipher session specific data. On the other hand, digital certificates are used to guarantee that the genuine Web-client wants to correspond with legitimate Web-server. This certificate includes public keys and connects it to the certificate owner.

3.4 Server Hello Done

When the server transfers a digital certificate along with public key, and server hello done process finished on the server-side. The client also notifies that server hello done message, which authenticates that the server received his client hello message.

3.5 Client Key Exchange

Now, The client key exchanged message is sent after the client receives the server hello done message. This message is computed by the use of received parameters in the server key transfer message. This public value will be utilized through the server to determine the similar premaster secret key which the client has already selected. Premaster secret key is consequently applied to encipher and decipher application data transferred within the two communication parties.

3.6 Change Cipher Spec

In this step, both the parties agree upon the same premaster secret key to change the session specific-data transmission from an insecure channel to a secure channel.

3.7 Finished

After all these steps finish, the safe and secure communication through TLS completed.

4 Passive Inspection of TLS V 1.3 Handshake Through Wireshark

The following Wireshark TLS v 1.3 PCAPs is clearly shown that the multiple of TLS handshake messages is being decreased compared to TLS v 1.2. The TLS v 1.3 all handshake steps are defined below.

4.1 Client Hello

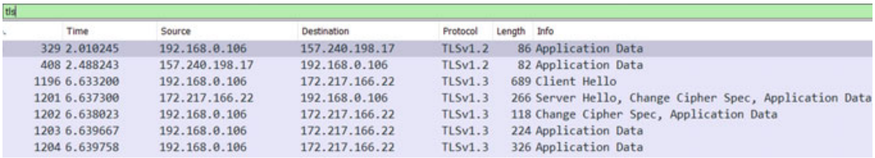
Similar to the TLS v 1.2 handshake message, the TLS v 1.3 handshake message also starts with one important change. The Web-client sends out the detailed set of approved cipher suites and preemptively assumes what key agreement protocol the Web-server is possible to choose. The Web-client also subsequently sends its key part for that particular key agreement protocol later, which will be helpful to make a secure connection.

4.2 Server Hello

The Web-server responds to the message on behalf of the Web-client and meets with the already selected key agreement protocol. The hello message from the server also includes the server's key part along with digital certificates as well as the server finished message.

4.3 Client Reply to Server

The Web-client inspects the digital certificate of the Web-server, creates keys as it has the key part of the web-server, and transfers the client ended message. Now, it is ready to send the encrypted request, after only one round trip time.



tls

.	Time	Source	Destination	Protocol	Length	Info
329	2.010245	192.168.0.106	157.240.198.17	TLSv1.2	86	Application Data
408	2.488243	157.240.198.17	192.168.0.106	TLSv1.2	82	Application Data
1196	6.633200	192.168.0.106	172.217.166.22	TLSv1.3	689	Client Hello
1201	6.637300	172.217.166.22	192.168.0.106	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Data
1202	6.638023	192.168.0.106	172.217.166.22	TLSv1.3	118	Change Cipher Spec, Application Data
1203	6.639667	192.168.0.106	172.217.166.22	TLSv1.3	224	Application Data
1204	6.639758	192.168.0.106	172.217.166.22	TLSv1.3	326	Application Data

Fig. 5 TLS v 1.3 handshake process

5 Improvements TLS V 1.3 Handshake Over TLS V 1.2 Handshake

As we already discussed in the previous section, the internal working of TLS v 1.3 and TLS v 1.2 handshake metadata was explored through the Wireshark tool and studied both the protocol version. Here, the list of some significant improvements which are shown below.

5.1 Speed and Performance Benefits

Concerning speed and performance, TLS v 1.3 takes one round trip time to make secure the connection with in Web-client and Web-server, as shown in Fig. 5. While in TLS v 1.2, it gets two round trips time to establish a connection. Compared with TLS v 1.3, it is slower with regard to network performance [23]. Another advantage is when a user visits a website that he has already visited, then a user does not require to establish a handshake process again. This mechanism is called as "zero round trip time" (0-RTT). The shorter TLS handshake has made TLS v1.3 faster than TLS v1.2. In TLS v 1.3, pre-shared key utilized to resume a connection, while TLS v 1.2 applies several forms to continue, i.e., session tickets and session IDs (Fig. 6).

5.2 Security and Privacy Benefits

The problem with TLS v 1.2 is that it is not configured properly and provides an open way concerning web attacks. The release of TLS v 1.3 removes all vulnerable features and outdated ciphers for instance AES-CBC, DES, RC4, and eliminating session renegotiation. TLS v 1.3 enables PFS (perfect forward secrecy) by default. It also adds another layer of confidentiality to an enciphered session, which ensures that only two communication parties can decrypt the traffic. A PFS means if another person somehow captured an enciphered session, and later gain access to the Web-server private key, then they could not use that key to decrypt the session [24].

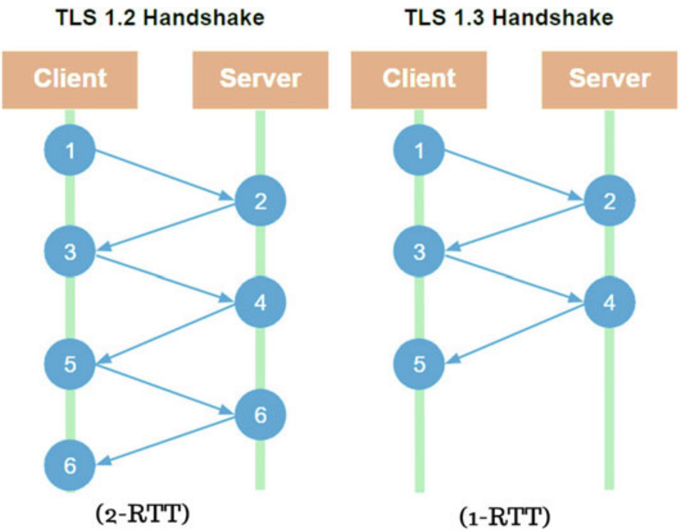


Fig. 6 TLS Handshake Comparison

5.3 TLS Version Negotiation

Earlier version of TLS, Web users were entitled to renegotiate cipher suites through merely ordering the server hello preference list. It can start downgrading attacks, where an intruder may simply reshuffle the cipher suite list and downgrade the Web-client to an unprotected version of SSL or TLS, exploiting its vulnerabilities [25]. TLS v 1.3 forbids renegotiation and utilizes the "legacy version" and "supported version".

5.4 Cipher Suites Simplified

The TLS v 1.3 handshake eliminates negotiation, and this handshake process appears to reduce the size of the cipher suites. TLS v 1.2 and other versions use sophisticated cipher suites, while TLS v 1.3 assists cipher suites that do not involve the key transfer and signature algorithms. The main disadvantage in TLS v 1.2 is that many cipher combinations bring nightmares to all communication parties involved in the handshake process; it also lags in guiding the determination of cipher suites to provide proper security [26]. By comparison, TLS v 1.3 only supports five ciphers, all of that enable perfect forward secrecy and secure protection.

TLS v 1.3 has five diverse cipher suites, which can be utilized as follows:

TLS_AES_256_GCM_SHA384.

TLS_CHACHA20_POLY1305_SHA256.

TLS_AES_128_GCM_SHA256.
TLS_AES_128_CCM_8_SHA256.
TLS_AES_128_CCM_SHA256.

5.5 Encrypted Server Name Indication (ESNI)

SNI is an essential element of the TLS handshake process, which hosts several TLS-based websites on a similar IP address set. In other words, it is a convenient way to track which service is accessed by a novel TLS connection. SNI information also provides the Web-server to know what type of certificate and configuration to utilize [27]. In TLS v 1.2, SNI is clear text value (un-encrypted) from the TLS handshake messages, which provides a way to eavesdroppers to track activities between two communication parties, leading to privacy concerns. However, in TLS v 1.3, SNI is encrypted, which prevents attackers or hackers from identifying the domain name of the website network users is communicating it. It enables another layer of privacy for Internet users.

The comparison of TLS v 1.2 and TLS v 1.3 handshake can be seen in Table 2.

Table 2 A comparative study of TLS v 1.2 and TLS v 1.3 handshake

Factors	TLS v 1.2	TLS v 1.3
R.F.C number	5246 [16]	8446 [17]
Handshake messages	Handshake messages are not encrypted	Handshake messages are encrypted after the server hello step
RTT (round trip time) [23]	2-RTT requires for completing handshake	1-RTT requires for completing handshake
Communication Time [23]	It takes more load time	It takes less load time
PFS (perfect forward secrecy) [24]	It does not provide PFS	It provides PFS
Cipher suites [26]	Support complex cipher suites	Support simplified and secure cipher suites
SNI (server name indication) [27]	SNI is un-encrypted	SNI is encrypted
Cryptographic algorithms	Legacy algorithms are used	Authenticated encryption with associated data (AEAD) algorithms are used
Passive interception	Content type is not encrypted	Content type is encrypted
Latency	Encryption latency is higher	Encryption latency is lower

6 Conclusion

The SSL/TLS protocol allows Web applications to connect across the Internet in such a way as to thwart tampering, theft of information, and data forgery. It provides several algorithms to be utilized in operations, for instance, identifying the authentication between Web-clients to Web-servers through exchanging the digital certificates, achieving privacy through encryption, and maintaining a secure and safe connection via message integrity inspection. In this paper, the TLS v 1.2 and TLS v 1.3 handshake metadata have been explored through one of the most comprehensive Wireshark network monitoring tool. A comparative study shows that TLS v 1.3 is significantly more secure and faster compared to its previous versions. It completely mitigates the previous security loopholes and vulnerabilities and the goal of reducing latency and optimizing the Web worldwide. It also contributes a safer and faster Internet for all.

References

1. S. Kumar, M.S. Gaur, Call admission control in mobile multimedia network using grey wolf optimization, in *Intelligent Computing in Engineering. Advances in Intelligent Systems and Computing*, vol. 1125, eds. by V. Solanki, M. Hoang, Z. Lu, P. Pattnaik (Springer, Singapore, 2020)
2. S. Kumar, M.S. Gaur, Handoff prioritization to manage call admission control in mobile multimedia networks for healthcare, in *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India* (2019), pp. 1–7
3. S. Kumar, K. Kumar, Neuro-fuzzy based call admission control for next generation mobile multimedia networks. Int. J. Eng. Adv. Technol. (IJEAT) **8**(6) (2019)
4. P. Kotzias, A. Razaghpanah, J. Amann, K.G. Paterson, N. Vallina-Rodriguez, J. Caballero, Coming of age: a longitudinal study of TLS deployment, in *Proceedings of the Internet Measurement Conference* (2018), pp. 415–428
5. F. Qi, Z. Tang, G. Wang, J. Wu, User requirements-aware security ranking in SSL protocol. Int. J. Supercomput. 762–776 (2013). Springer
6. HTTP Archive Report: State of the Web. Available at: https://www.httparchive.org/reports/state-of-the-web. Last accessed 25 Jan 2020
7. M. Kohlweiss, U. Maurer, C. Onete, B. Tackmann, D. Venturi, (De-) constructing TLS 1.3, in *International Conference on Cryptology in India* (Springer, Cham, 2015), pp. 85–102
8. R. Holz, J. Amann, A. Razaghpanah, N. Vallina-Rodriguez, *The Era of TLS 1.3: Measuring Deployment and Use with Active and Passive Methods* (2019). arXivpreprint arXiv:1907.12762
9. J. Postel (ed), DOD standard transmission control protocol. Defense advanced research projects agency, information processing techniques office, RFC 761, IEN 129. ACM Comput. Commun. Rev. **10**(4), 52–132 (1980)
10. Wireshark homepage, https://www.wireshark.org/. Last accessed 10 March 2020
11. L. Waked, M. Mannan, A. Youssef, The sorry state of tls security in enterprise interception appliances. Digital Threats Res. Pract. **1**–**2**, 1–26 (2020)
12. A.O. Freier, P. Karlton, The SSL protocol version 3.0. Internet draft. Netscape Commun. (1996)
13. C. Allen, T. Dierks, The TLS Protocol Version 1.0. Tech. rep. RFC 2246 (1999)
14. T. Dierks, The Transport Layer Security (TLS) Protocol Version 1.1. Tech. rep. RFC 4346 (2006)

15. C. Meyer, J. Somorovsky, E. Weiss, J. Schwenk, S. Schinzel, E. Tews, Revisiting SSL/TLS implementations: new Bleichenbacher sidechannels and attacks. In USENIX Security **14**, 733–748 (2014)
16. Rescorla, E RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2 (2008)
17. E. Rescorla, DierksRFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3. (2018)
18. C. Cremers, M. Horvat, J. Hoyland, S. Scott, T. van der Merwe, A comprehensive symbolic analysis of TLS 1.3, in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security* (2017), pp. 1773–1788
19. A. Uzunov, E.B. Fernandez, K. Falkner, Securing distributed systems using patterns. A Surv. Comput. Secur. **31**(5), 681–703 (2012). https://doi.org/10.1016/j.cose.2012.04.005
20. W. Stallings, W. Stallings, *Cryptography and Network Security. Principles and practice* (Prentice Hall, Upper Saddle River, N.J, 1999)
21. S. Thomas, *SSL & TLS Essentials* (New York, 2020), p. 3
22. M. AsadzadehKaljahi, A. Payandeh, M.B. GhaznaviGhoushchi, Improving SSL/TLS protocol by trust model. Secur. Communi. Netw. 1659–1671 (2015)
23. Dev Community, *Advantages of TLS 1.3 Over TLS 1.2.* https://dev.to/https_india/advantage-of-tls-1-3-over-tls-1-2-6ig. Last accessed 25 April 2020
24. SSL/TLS ORCHESTRATION, F5, TLS 1.3, *Are You Ready?* www.f5.com/pdf/products/tls1-3_are-you-ready.pdf. Last accessed 12 April 2020
25. TLS 1.3—Status, Concerns & Impact A10 Networks. www.a10networks.com/blog/tls-13-status-concerns-impact/. Last accessed 2020/4/17.
26. TLS Version 1.3, *What To Know About The Latest TLS Version | Infosec Insights*. [online] InfoSec Insights. Available at: https://sectigostore.com/blog/tls-version-1-3-what-to-know-about-the-latest-tls-version/. Last accessed 10 May 2020
27. W.M. Shbair, T. Cholez, J. Francois, I. Chrisment, Improving SNI-based HTTPs security monitoring, in *IEEE International Conference on Distributed Computing Systems Workshops* (2016), pp. 72–77

Secure Communication in Peer-to-Peer Network Based on Trust-Based Model

Vijay Paul Singh, Tulika Vijay, Tushita, Sonal, Rigzin Angmo, and Naveen Aggarwal

1 Introduction

Peer-to-peer network approach has evolved over the years. It has been accepted as an efficient communication model because of its distinctive characteristics and applications such as self-scalability, dynamic nature, content distribution, and effective search [1]. In terms of computer networks, it refers to a network that uses a distributed network architecture. Whereas the devices or computers or nodes that are part of this network are called peers [2] and are completely independent of each other without any central authority. In this paper, we use the acronym P2P for peer-to-peer network.

Earlier, for communication, a simple client–server architecture was followed over the Internet and flourished throughout the 1990s. During the late 1990s, new technologies of data compression for mp3, MPEG, etc. became popular and the traditional systems were unable to deal with the increase in overall demand of data consequently, it was difficult to manage the increase in bandwidth costs for the clients. P2P network provides solutions for this problem by introducing applications like “Napster” that can be used to download and share free mp3 files. In a P2P network, delivery costs get reduced further with the increase in demand of a file which leads to more seeding of that file in the network by the peers [3]. The availability, cost, and capability of personal computers and broadband Internet services to the general population also led to an inevitable increase of interest in the P2P architecture. Since the 90s there has been a sudden boom in P2P network applications to share multimedia files. Some of the most famous file-sharing protocols used are Freenet, Napster, Direct Connect, Gnutella, eDonkey2000, and Bit Torrent [4].

In P2P communication, file sharing with the help of peers, akin to Napster, Bit Torrent both uses centralized directory server, Gnutella that uses Query Flooding to provide an easy way and avoids the central point of failure [5]. Usually, in the

V. P. Singh (✉) · T. Vijay · Tushita · Sonal · R. Angmo · N. Aggarwal
CSE, UIET, Panjab University, Chandigarh, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_13

file system, security breaches due to infected files sharing with this whole peer get affected or even other files get affected. To resolve the risk of file sharing and to provide secured documents from malicious, a trust-based P2P system is needed [6]. Trust is a widely used term whose definition differs among researcher and application areas [7]. Trust can be measured numerically for a specific level of the subjective with which other nodes or agents will perform a particular action and take further action [8]. In addition, the Trust often refers to the mechanisms to ensure that the source of information is actually what claims to be a source [9]. The trust in network communication is further categorized [10].

(i) Policy-based trust: Establish trust using the third party or trusted third party to serve as an authority for issuing verified credentials [11].
(ii) Reputation-based trust: It is based on past interaction performance or history of an entity action/behavior [12].
(iii) General model of trust: It is also based on transaction and reputation.
(iv) Trust in information resources: It is related to web resources and websites in which rating by the user about the quality of information and services [13].

To provide trust in communication, various trust-based model techniques are there, some of them are described in this paper. It is the most cited trust and name primarily based model employed in peer to see system [14]. It fights against malicious peers and permits peers to see file sharing. Every peer maintains a neighborhood trust with another peer and every peer calculates international trust worth by all alternative peers:

(i) Eigentrust: It is the most usable and cited trust. It identifies trustable versus non-trustable peers during file sharing using the reputation-based model. Each peer maintains local trust with another peer and global trust by all alternative peers [15, 16].
(ii) Peer trust: It measures trust factor based on two important factors, i.e., transaction feedback collected from other peers and general metric, using these two parameter peer credibility measures [17].
(iii) Cuboid trust: It is based on global trust and pre-trusted peer involvement; these two techniques support identifying trustable peers in the network [12, 18].
(iv) Ant reputation: It maintains a trustable table similar to the distance vector routing protocol table, in which peer information is maintained related to the trust factor [9].

Eigenvalue uses almost every reputation-based model, based on that local trust, global, the number of transactions, and also the past reputation of the peer are important factors to identify trustable peers in the network. There are three possibilities during file sharing in the P2P network [9, 12, 15], i.e., Only a few responses, No one Response, and Everyone Response. This peer requires its acquaintances about their opinions about the other peer, which affects it to decrease the number of unauthenticated files. In this, the system should be self-policing and should maintain anonymity, not assign any profit to newcomers, minimal overhead. Each peer *i* can store the information of successful transactions with peer *j* [19].

Each peer i can store the information of successful transactions with peer j [19].

$$S_{ij} = Sat(i, j) - Unsat(i, j). \tag{1}$$

In Eq. (1), *Sat* is a satisfaction transaction, *Unsat* is an un-satisfaction transaction.

$$C_{ij} = \max\left(S_{ij}, 0\right) / \sum j \max\left(S_{ij}, 0\right). \tag{2}$$

In Eq. (2), C_{ij}, compute local trust value using max function which finds out higher values between S_{ij} and zero based on that local trust value calculated. To mitigate the risk during file sharing in such systems, we have proposed the model to improve the system scenario, proposed model is using trust and reputation mechanism to find the malicious nodes. The proposed model categorizes the peers into two main categories: (i) trusted nodes and (ii) normal nodes, based on their defined access level. In this paper, eigenvalue is used to measure the trust value, and the reputation analysis is done based on time. In the proposed network, nodes are rated by each other and based on this rating they communicate with each other in the network. To validate the approach, simulation using simply has been implemented. The implementation is aimed to figure out the presence of malicious peers in the network based on the trust mechanism. With the help of graphs, it can be visualized that outcome has been achieved. In a decentralized network, this mechanism to find the malicious node is effective and sensitive. This paper is organized as: the next section, i.e., Section 2, pointed to some related work; Sect. 3, problem statement; Sect. 4, proposed model; Sect. 5, discuss implementation and experimental results; and Sects. 6 and 7, compare, conclude, and discuss future work.

2 Related Work

P2P network is an example of Bit Torrent [20] in which each node depends on each other. In client–server model, information is not revealed to the client but in P2P some internal information may be exposed and attackers can easily attack or communicate with these nodes through various tactics [21, 22]. There are various levels of P2P networking [23] such as Hybrid P2P in which the central server keeps the information about the network, Pure P2P, where there is no absolute server, Mixed P2P similar to Gnutella no central server but a cluster of nodes. There are various attacks which can be possible in the P2P network such as DoS, DDoS, Masquerade, Man-in-the-middle Attack, Worm Propagation, Rational Attacks, File Poisoning, Eclipse Attack, Sybil Attack, and many more [24–26]. These attacks are generally possible due to several vulnerabilities. DoS is an attack in which a network or node loses the service. Detecting a DoS attack is a challenging task [27]. El Defrawy et al. [19] make use of the BitTorrent system and perform real-life experiments that demonstrate the practicability and severity of such attacks. Yusof et al. [28] surveyed

DDoS attack, where they had provided answers to the 6 proposed research questions and 48 techniques that are used to DDoS attack on various kinds of the network system in which one of them is P2P. Man-in-the-middle attack is common in file sharing where an attacker easily inserts in the network and spreads polluted files on behalf of the authorized node [29]. To mitigate this attack in P2P, trustable authority is required, which generally does not exist in P2P. Worm propagation is the biggest threat, popular worms are Code Red or Nimda that can infect thousands of nodes within an hour [30]. There are various factors that make P2P worms infected such as using the same software by all nodes of P2P [21], during transfer of large file set limit in order to hold one TCP packet [30], and easily accessing normal user computers and retrieving sensitive information. Once a worm propagates inside the network then its next goal is to launch the DDoS attack [21]. The human is also one of the factors of attacks, sometimes novice users download files that are infected, and due to their inaction with regard to security created difficulties [31]. Whereas rational attack, file poisoning, and Sybil attack are enormously possible in the P2P network. In the rational attacks in P2P, a large number of nodes consume system resources and less involvement in the network [31]. File poisoning, the actual file has been spoofed by the attacker. This attack is controlled by deleting corrupted downloaded files on the user's end or by trying not to download unauthorized files and is detected by various smart algorithms. Finally, there is the Sybil attack in which a single malicious identity can present multiple identities that effectively take control of the network [32]. To handle Sybil attacks one approach is the trustable central authority which is not possible in P2P. Another approach is a reputation-based system which might be able to control this attack. In this paper, we have used a trust-based model which is related to the reputation of nodes in the network.

3 Problem Statement

In peer-to-peer communication, the security threats mainly seen in file systems are attacks by malicious nodes or malicious collective, while using the eigentrust concept in P2P might be less control of malicious nodes due to an increase in satisfactory transaction Eq. (1). These security threats make the system unreliable and non-robust. The lack of any scrutiny and the open nature of decentralized systems have made it prone to security hazards that adversely affect the performance of the network. To mitigate this situation, we have proposed an approach that can easily disallow the malicious node to communicate in the network.

4 Proposed Model

The proposed model states that the peers are categorized into two nodes: (i) trusted node and (ii) normal nodes. The access permissions are provided to these nodes according to their categories. The trusted nodes are those that make the network and are provided with all kinds of access permissions. Whereas all other nodes that subsequently join the network are normal nodes with restricted permissions. In the proposed model, the trust and reputation mechanism is used to track the behavior of the nodes. Within the network, a normal node records local trust values about its experience with some nodes and the trusted nodes record the aggregate trust values that summarize the experiences of all nodes in the network with some nodes. The main contributions of the paper are as follows:

- It presents a simple and easy-to-implement model for P2P network security by providing the categorization of nodes, differentiation in access permissions, and monitoring of the behavior of peers based on trust and reputation mechanism.
- The model also provides a fair and unbiased opportunity to peers that enhance their access permissions.
- The malicious nodes are efficiently detected in the network with the help of this model and used for the prevention of the underlying security risk in an advanced file-sharing system.
- The experimental results under various cases indicate that our approach is more effective and sensitive in detecting malicious peers as compared to other similar trust models.

Table 1 contains symbols related to the proposed approach.

A. ***Algorithm for Joining of Nodes***

1. Each node joins the network as a normal node.

B. ***Algorithm for Trust Calculation***

1. Each node i in the network maintains local *eigentrust value* $S_{i,j}$ and normalized local trust value $C_{i,j}$ based on the number of successful and unsuccessful transactions with peer j.
   for each node i

Table 1 Symbol table

T_i	Trusted nodes
U_i	Normal nodes
$Sat_{(i,j)}$	Successful transaction between nodes i and j
$Unsat_{(i,j)}$	Unsuccessful transaction between nodes i and j
$S_{i,j}$	Local trust values of node i with node j
$C_{i,j}$	Normalized local trust between node i and node j
G_i	Aggregate trust

$$S_{ij} = Sat(i, j) - Unsat(i, j) \tag{3}$$

$$C_{ij} = \max\left(S_{ij}, 0\right) / \sum j \max\left(S_{ij}, 0\right). \tag{4}$$

2. T_i stores aggregate trust values of each node in the network
   for each T_i

$$Gi = \left(\sum Sat(i, j) - \sum jUnsat(i, j)\right) / (\sum Sat\left(i, j + \sum jUnsat(i, j)\right). \tag{5}$$

3. The trusted nodes maintain a minimum threshold value. If the aggregate trust value of any node becomes less than this value, the node can be identified as harmful to the network and its access permissions are further decreased.
4. The trusted nodes maintain a maximum threshold value. If the aggregate trust value of any node becomes greater than this value, the node can be identified as reliable and its access permissions are increased.
5. The measure of aggregate trust G_i is a probabilistic and normalized measure and thus is successful in differentiating between two peers whose difference between successful and unsuccessful transactions is the same but one peer has a higher probability of unsuccessful transactions than the other.
6. The threshold calculation by the trusted node is assumed to be dependent on various reputation parameters like the amount of time spent in the network, the number and type of transactions done, and the study of how malicious nodes have behaved in the past in the same network or in peer-to-peer networks in general.

III. *Algorithm for Upgradation of Nodes*

Some nodes may be upgraded from the normal category to the trusted one, according to the following algorithm:

```
1. The trusted node keeps track of the total
   number of nodes in the network.

2. If total number of($U_i$)>> total number of($T_i$),
   then

3. $G_{max}$ is set as $U_i$ and j=0
4. For each node i,
       if ($U_i$>$G_{max}$), then
         $G_{max}$ is set as $U_i$
5. End for
6. For each node i,
       (If $U_i$== $G_{max}$)
                j=j+1
7. End for
8. If j==1, then
9. Ui with $G_{max}$ is set as Ti
10.Else
11.Reputation parameter based on time of the node
   that is the amount of time node has spent in
   the network is used (Ri).
12.The node with $G_{max}$ and $R_{max}$ is upgraded.
13.End if
14.End if
```

The trusted node keeps track of the total number of nodes in the network. If there is an imbalance between the number of trusted and normal nodes, they take the decision of upgrading certain nodes from the normal category to the trusted one.

When there is a need for upgradation, trusted nodes find a node with maximum aggregate trust.

(a) If there is no other node with the same aggregate trust the node is upgraded.

(b) If there are more than one node in the network with this same aggregate trust, we use a reputation parameter based on time of the node, which is the amount of time it has spent in the network. The node which has this maximum aggregate trust and has been in the network for a longer time is upgraded.

IV. *Algorithm for Leaving of Nodes*

```
If the node which wants to leave is a normal node($U_i$), then
    Delete ($U_i$).
End if
If leaving node is a trusted node($T_i$), then
    If total number of($U_i$)>> total number of($T_i$), then
        Call upgradation function.
    Else
        Delete($T_i$)
    End if
End if
```

From the above algorithm, if the leaving node is a normal node, then it is a simple leave operation. If the leaving node is a trusted node, the remaining trusted nodes use the *UPGRADE* algorithm.

5 Implementation and Results

To simulate the peer-to-peer network, we use SimPy [33] which is a discrete-event, process-based simulation platform based on standard Python. The implementation is aimed to figure out the presence of malicious peers in the network based on the trust mechanism. The simulation implements the presented algorithm, calculates local trust, normalized local trust and aggregate trust of each peer, and enlists nodes that are harmful to the network.

We assume that the network consists of a total of 50 nodes consisting of five peers that are labeled trusted and 45 other nodes. The trusted nodes are provided with read and write access and the others are provided only read access. The connections formed between the nodes are random and they are assumed to communicate using three types of messages—read, write, and inauthentic. All peers in the network can send a read message as they all have the read permission. The write message by any normal node notifies them that the write access is denied. The inauthentic messages which represent malicious behavior are sent only by the malicious nodes that decrease their reputation in the network.

The nodes maintain a record of their communication. Each node *i* maintains a log of the number of successful and unsuccessful transactions it has with node *j* which is used to calculate the local trust.

At the end of simulation, aggregate trust is calculated for each peer which is a measure of its overall behavior and helps to determine which nodes are malicious in the network. In this paper, three cases are presented to understand the effectiveness of the model to provide secure communication based on the trust model in P2P communication network.

Case 1: A trusted peer communicates with any other peer: The trusted peers have all access permissions and they can communicate successfully with any peer in the network.

Case 2: A normal node communicates with any other peer: All other nodes in the network except the trusted nodes have only read permissions. When a node sends a read message, the transaction can be successful or unsuccessful based on the delay which is calculated using randomly allotted bandwidth. When a node sends the write message, it is alerted that this access is not provided to it.

Case 3: A malicious node communicates with any other peer: The model deals with read and write messages sent by the malicious node in a similar manner as that of a normal node discussed above. The malicious behavior of such nodes is simulated by using a third type of message, inauthentic, which decreases their reputation in the network considerably.

As per the above cases, we have implemented and visualized in graph form. In Fig. 1, the graph depicts local trust values for each connection (over a range of positive and negative values) as the number of connections increases. Here, peers are chosen randomly and sequential numbers are assigned to the connections established.

In Fig. 2, the graph depicts local trust values for each connection as the number of connections increases but the values are normalized (in the range (0, 1)).

Note: peers are chosen randomly and sequential numbers are assigned to the connections established.

In Fig. 3, It affirms that the peers numbered 40, 41, 42, 43, 44 are malicious nodes as they have the least aggregate trust values.

In Figs. 1 and 2, the graph depicts local trust values for each connection (made up of two nodes) as the number of connections increases. Figure 2 is a modification of Fig. 1 as it shows normalized local trust values. In Fig. 3, the graph depicts the aggregate trust (calculated with the help of local trust) for each peer, and as a result

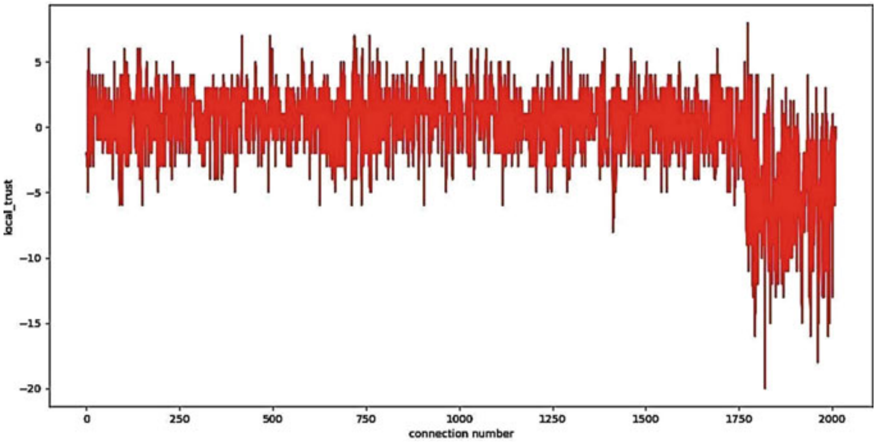


Fig. 1 Local trust values versus the number of connections

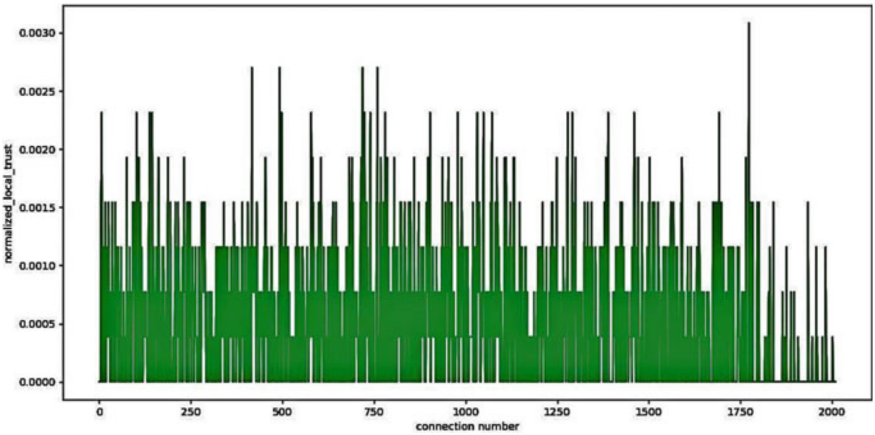


Fig. 2 Normalized local trust values versus the number of connections

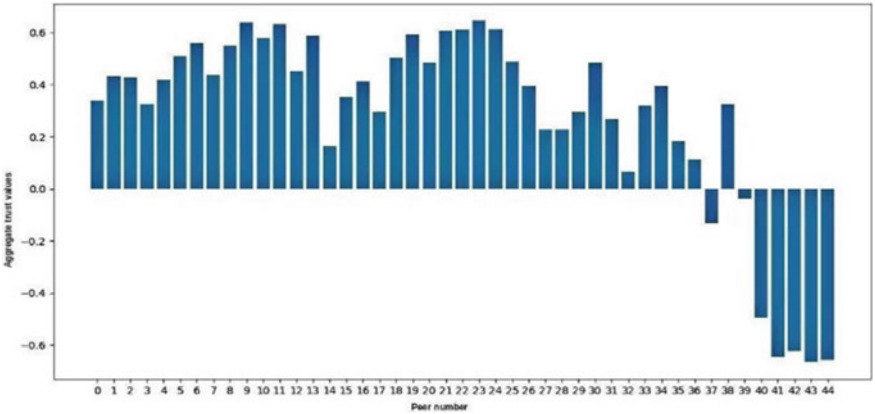


Fig. 3 Aggregate trust values versus the peer number

we are able to distinguish between non-malicious and malicious peers, with Fig. 4, we are able to see the activity of the malicious peer (in this case the most malicious peer) an amount of time the number of connections it forms increases. In Fig. 5, we are able to see the activity of a non-malicious node (in this case, the most trustworthy node) after a short interval the number of connections it forms increases.

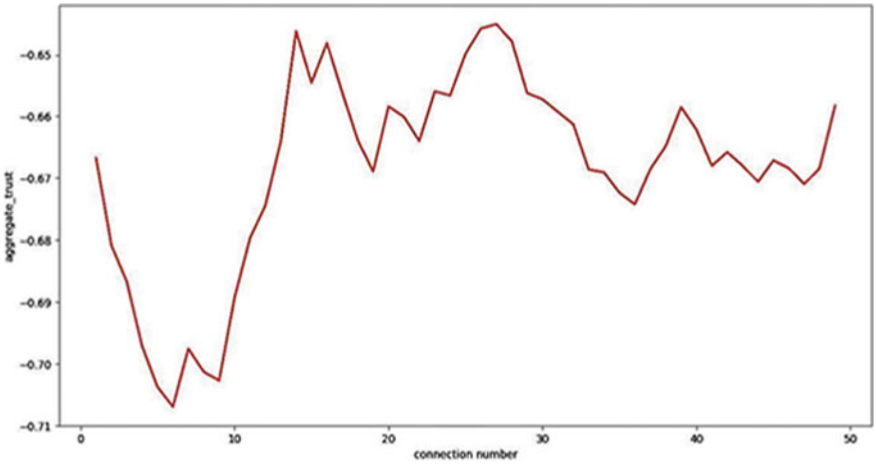


Fig. 4 Aggregate trust values of the most malicious peer (P43) versus the connections made by the said peer over a period of time

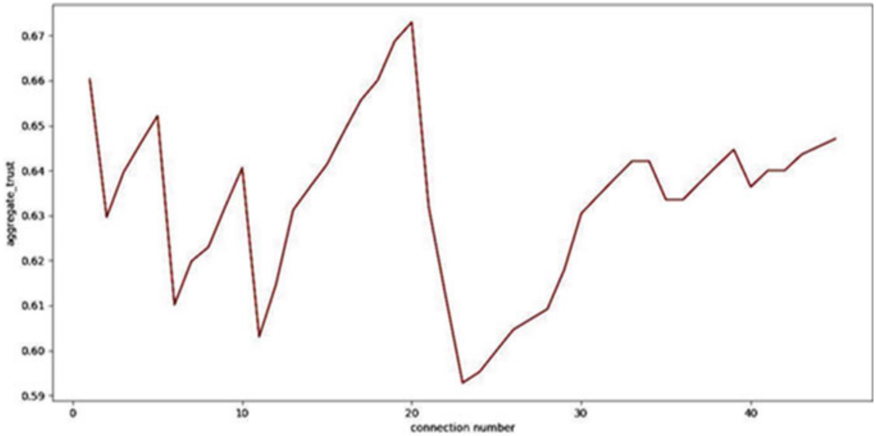


Fig. 5 Aggregate trust values of the most trustworthy peer (P23) versus the connections made by the said peer over a period of time

6 Comparison of Proposed Trust-Based Models

Peer-to-peer network has many implementations—one of the implementations is in electronic markets where SLA (service-level agreement) is used to state agreements based on transactions between client and service provider [31, 34] deals with the same problem as the one discussed in this paper, that is, in a network of clients and service providers as peers, malicious behavior in a network can affect the overall trust values of the peers. The ground of comparison is that our proposed model categorizes the nodes into (i) trusted and (ii) normal with differentiation in access permissions and the rearrangement of permissions based on the trust values (upgradation of normal peers to trusted peers).

In a peer-to-peer network, peers can review each other negatively or positively. In the team-based learning model, [35] peers can assign biased scores to other peers to inflate or deflate grades. Similarly, this paper deals with malicious nodes which can increase their trust values in the network with other malicious nodes to increase their aggregated trust value. The cited paper proposes Michaelsen, Fink, Kole methods to build a trust model while we propose a model based on eigentrust algorithm with aggregated and local trust values. In paper, [32] proposes a model for secure transaction in mobile P2P networks. It defines an adaptive reputation factor similar to the trust values in our proposed model. With historical interactions of the peers, Bayesian game theory is used to design the trust model in MP2P network whereas our model uses the eigentrust algorithm with a record of transactions to maintain local trust and aggregate trust to build a secure network.

7 Conclusion

In the evaluation of the proposed model, the experimental results under various cases evince that our approach is more effective and sensitive in detecting malicious peers as compared to other similar trust models. This paper presents a simple and easy-to-implement model for P2P network security. The model is based on the categorization of nodes, differentiation in access permissions, and monitoring of the behavior of peers based on trust and reputation mechanism. The model also provides the opportunity to peers to enhance their access permissions with being fair and unbiased. It is found to be efficient in detecting the presence of malicious nodes in the network and thus preventing the underlying security risk in an advanced file-sharing system.

Acknowledgements Authors would like to thank the team of DIC, Chandigarh, India (dic.puchd.ac.in) and are grateful to the Ministry of Human Resource Development (MHRD) of Government of India for supporting this research under Design Innovation Center (MHRD-DIC).

References

1. S. Androutsellis-Theotokis, D. Spinellis, A survey of peer-to-peer content distribution technologies. ACM Comput. Surv. (CSUR) **36**(4), 335–371 (2004)
2. J. Risson, T. Moors, Survey of research towards robust peer-to-peer networks: Search methods. Comput. Netw. **50**(17), 3485–3521 (2006)
3. S. Nakamoto, A. Bitcoin, A peer-to-peer electronic cash system. Bitcoin. https://bitcoin.org/bitcoin.pdf. 4 (2008)
4. J. Li, A survey of peer-to-peer network security issues. Retrieved November 29 (2007), 2010

5. S. Saroiu, K.P. Gummadi, S.D. Gribble, Measuring and analyzing the characteristics of Napster and Gnutella hosts. Multimedia Syst. **9**(2), 170–184 (2003)
6. H. Tran, M. Hitchens, V. Varadharajan, P. Watters, A trust based access control framework for P2P file-sharing systems, in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences* (Big Island, HI, USA, 2005), pp. 302c–302c
7. M. Momani, S. Challa, Survey of trust models in different network domains. arXiv:1010.0168 (2010)
8. D.J. Kim, D.L. Ferrin, H.R. Rao, A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Syst. **44**(2), 544–564 (2008)
9. A.A. Selcuk, E. Uzun, M.R. Pariente, A reputation-based trust management system for P2P networks, in *IEEE International Symposium on Cluster Computing and the Grid, 2004*. CCGrid 2004 (IEEE, 2004)
10. D. Artz, Y. Gil, A survey of trust in computer science and the semantic web. J. Web Semant. **5**(2), 58–71 (2007)
11. P. Bonatti et al., An integration of reputation-based and policy-based trust management. Networks **2**(14), 10 (2007)
12. L. Xiong, L. Liu, Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. Know. Data Eng. **16**(7), 843–857 (2004)
13. S.A. Morris, T.E. Marshall, R.K. Rainer Jr., Impact of user satisfaction and trust on virtual team members. Inf. Res. Manage. J. (IRMJ) **15**(2), 22–30 (2002)
14. F.G. Mármol, G.M. Pérez, Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. Comput. Stand. Interfaces **32**(4),185–196 (2010)
15. S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina, The eigentrust algorithm for reputation management in p2p networks, in *Proceedings of the 12th International Conference on World Wide Web* (2003)
16. A. Abdul-Rahman, S. Hailes, A distributed trust model, in *Proceedings of the 1997 Workshop on New Security Paradigms* (1998)
17. G. Suryanarayana, R.N. Taylor, A survey of trust management and resource discovery technologies in peer-to-peer applications (2004)
18. R. Chen et al., CuboidTrust: a global reputation-based trust model in peer-to-peer networks, in *International Conference on Autonomic and Trusted Computing* (Springer, Berlin, Heidelberg, 2007)
19. K. El Defrawy, M. Gjoka, A. Markopoulou, BotTorrent: misusing BitTorrent to launch DDoS attacks. SRUTI **7**, 1–6 (2007)
20. B. Cohen, The BitTorrent protocol specification, 11 October 2013. Retrieved April 24, 2017, from http://www.bittorrent.org/beps/bep0003.html
21. N. Naoumov, K. Ross, Exploiting p2p systems for ddos attacks, in *Proceedings of the 1st International Conference on Scalable Information Systems* (2006).
22. J. Liang, N. Naoumov, K.W. Ross, The index poisoning attack in P2P file sharing systems. INFOCOM (2006)
23. J. Buford, Y. Heather, E.K. Lua, *P2P Networking and Applications* (Morgan Kaufmann, 2009)
24. J. Mirkovic, P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput. Commun. Rev. **34**(2), 39–53 (2004)
25. J. Seedorf, Security challenges for peer-to-peer SIP. IEEE Netw. **20**(5), 38–45 (2006)
26. B. Pretre, Attacks on peer-to-peer networks. Dept. of Computer Science Swiss Federal Institute of Technology (ETH) Zurich Autumn (2005)
27. G. Carl et al., Denial-of-service attack-detection techniques. IEEE Int. Comput. **10**(1), 82–89 (2006)
28. A.R. Yusof, N.I. Udzir, A. Selamat, Systematic literature review and taxonomy for DDoS attack detection and prediction. Int. J. Digi. Enterprise Technol. **1**(3), 292–315 (2019)
29. D.S. Wallach, A survey of peer-to-peer security issues, in *International Symposium on Software Security* (Springer, Berlin, Heidelberg, 2002)

30. V. Vlachos, S. Androutsellis-Theotokis, D. Spinellis, Security applications of peer-to-peer networks. Comput. Netw. **45**(2), 195–205 (2004)
31. J. Dinger, H. Hartenstein, Defending the Sybil attack in p2p networks: taxonomy, challenges, and a proposal for self-registration, in *First International Conference on Availability, Reliability and Security (ARES '06)* (IEEE, 2006)
32. Z. Li, J. Bi, An adaptive trusted request and authorization model for mobile peer-to-peer networks, in *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing* (Zhangjiajie, 2013), pp. 1274–1280. https://doi.org/10.1109/HPCC.and.EUC.2013.181
33. SimPy. https://simpy.readthedocs.io/en/latest/. Accessed 1 May 2019
34. I. Petri, O. Rana, Y. Rezgui, G.C. Silaghi, Evaluating trust in peer-to-peer service provider communities, in *7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)* (Orlando, FL, 2011), pp. 407–414. https://doi.org/10.4108/icst.collaboratecom.247125 (2011)
35. M.S. Patil et al., Trusted relative peer review: A novel approach to assess an individual in team based learning, in *2016 IEEE 4th International Conference on MOOCs, Innovation and Technology in Education (MITE)* (Madurai, 2016), pp. 54–59. https://doi.org/10.1109/MITE.2016.021
36. B.N. Levine, C. Shields, N.B. Margolin, A survey of solutions to the Sybil attack. University of Massachusetts Amherst, Amherst, MA 7, 224 (2006)

Efficient Mechanism for Multicasting in IoT-Enabled Wireless Sensor Network

Shiv Ashish Dhondiyal, Sushil Chandra Dimri, and Deepak Singh Rana

1 Introduction

Internet of Things is one of the rapidly growing technologies that is used these days to connect and communicate among various devices. The devices connected through Internet means Internet of Things is growing with a rapid pace. In the upcoming years, the use of IOT will grow more and more [1]. In 2020, nearly about 26 billions of devices will be joining through IOT by wirelessly or wired. Internet provides such an interconnected system through which different devices can connect with each other across the world using a set of various communication protocols [2]. The IOT devices have become a necessity for all of us which can connect different things remotely at any point of time. Various smart devices coming in market day by day, which is becoming a large number, so managing and monitoring these devices is only possible through IOT [3]. With the increase in the number of smart devices day by day, the Internet of Things (IoT) can be ideal solution for management of these smart devices. Internet of Things is basically a network of interconnected things. The things here refer to the devices such as sensors or actuators. These IOT devices collect different types of information as data sources [4]. These devices may produce a large amount of information, measuring lots of values in different timestamps. This collection of data values can be assumed as a continuous flow of data in stream. This stream consists of information of various types (e.g., temperature, pressure, and humidity or air pollution) and always also contain meta-data (self-describing data) [5]. The complexity of its processing requires machines and applications that may merge and analyze the data, reacting in a clever way to get the best decision out of it [6]. The devices connected in the Internet of Things are mostly heterogeneous entities. The communication patterns in Internet of things may be directly from human to human or human to things or things to things [7].

S. A. Dhondiyal (✉) · S. C. Dimri · D. S. Rana
Graphic Era Deemed to be University, Dehradun, Uttarakhand, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_14

As users of the Internet, it is necessary to have more trust that the Internet, its uses, and the devices connected to IOT are secure that whatever activities we want to do we can do securely [8]. The Internet of things must be secure so that the people must have trust in the environment in which they are using their devices. If a less secured device gets connected to the Internet, it can compromise security of the whole network [9]. Gradually we are becoming more and more dependent on IoT devices for essential services. There is a need that the devices connected to the Internet must be secure, while we know that no device can be completely secure [10]. The Internet of things must have security so that the people those have devices connected with the internet have trust in the environment [11]. If a poorly secured device is connected with the internet, it will affect the security of the whole network [2]. This rapidly increasing level of dependence on IoT devices and the services provided by Internet they interact with increases risk in the network security. For example, if smart TV gets accessed by attacker, we can unplug that smart TV, at the same time we cannot turn off a smart power meter so easily if getting attacked. That's why IOT security is still a burning research topic [12].

2 Literature Review

Pawani Parambage et al. have defined a hybrid key establishment algorithm based on public key establishment algorithm by public key nature protocols for symmetric key cryptography based on certificates. They proposed elliptic curve cryptography and have shown the utilization of certificates for deriving pair-wise link keys in a WSN [1].

Shahid Raza et al. proposed lithe for IOT which is the combination of COAP and DTLS. Moreover, with this they also proposed one scheme called DTLS header compression by maximizing the 6LOWPAN standard which results in the gain of packet size with better processing time [2]. Rene. Hummen, Jan H. Ziegeldorf et al. give main load calculation for the certificate-based DTLS handshake and argue that certificates with improvements to the handshake are a viable method of authentication in many network scenarios [3].

Chunyao Fu, Zhifang Jiang et al. give a new technology that gives very less energy consumption and improves the lifetime of the network [4]. Yuebin Bai et al. give the distance between the nodes based on the availability of the nodes. Experimental results clearly show that current approach is far better than existing approach [5]. Shiv Ashish et al. explain working of sleeping mode mod-leach protocol which is modification of mod-leach protocol. The simulation result shows that proposed protocol is far better than the original one [6].

Wei Yuan et al. have proposed Harn and lin's protocol that cannot bear man-in-the-middle attack and explained the reasons that the active attacker owns the group key and that attacker is not included in that group [7]. Anar A. Hadly et al. provide leach-cs protocol for WSN. Depending on the data sensed leach-cs provides better performance as compared to leach protocol [8]. H. R. Hussen et al. proposed a scheme which enables a 6LoWPAN device to securely authenticate with the remote server with a session key established between them. The security proof by the protocol composition logic can prove the logic correctness of the proposed scheme [9].

Debabrata Singh, Sanjeet Kumar et al. give E-Modleach algorithm which is used for homogenous network model [10]. D. J. Cook et al. give AI-based smart environment which defines problems toward the performance of the intelligent surrounding [11].

Debmalya Bhattacharya et al. made a system of wireless hubs that have the ability to sense a parameter of surrounding. Sensors of different sorts are sent universally and pervasively in shifted situations, for example, office structures, untamed life stores, war zones, versatile systems, and so forth [13].

R. Hummen, H. Wirtz, et al. give an algorithm based on public key operation on resource-constrained IoT devices [12]. F. Bouhafs, M. Merabti et al. provide an overview of remote sensing process. As such, it is aimed at introducing the students to the science, art, and technology of Remote Sensing (RS) [14].

Gogu, A. et al. analyze probably the most central optimization issues identified with coverage, topology control, scheduling, routing, and mobility in WSNs [15].

J. Pouwelse, K. Langendoen, et al. explain the voltage scaling key technique for exploiting the hardware characteristics of processors to reduce energy dissipation by lowering the supply voltage and the operating frequency [16].

3 System Design

The purposed scheme takes an encrypted image as the key element. In this technique, no separate key is transmitted with data. Multi-level security is provided, at first level group key is checked [14] by the receivers sent by the sender once the key gets acknowledged, then receiver sends the signature to the sender, and then finally send verify the signature if the signature is correct and then it forms the connection otherwise connection not formed.

3.1 System Model

Our security model is based on two-level security check, in which first group key is checked, verified, and then signature is checked and verified. Image is worked as key element in our protocol. Connection between sender and receiver is formed only after both level security is verified [15]. If at any level security fails then connection is not formed. There is no separate key transmitted in the network along with data.

3.2 System Flowchart

The system flowchart below describes the work flow of proposed algorithm. We choose images and encrypt them using proposed algorithm. These encrypted images are used as group key. Each group has its own group key which is distributed at the factory resetting phase to the initiator. The initiator also stores the signature for each node. Every responder of a group has the same original image. Sender sends request to receiver to establish the connection using key element. The receiver decrypts image and compares it with stored image, if images matched then the signature is sent by responder. The signature is verified at initiator and the connection is established (Fig. 1).

3.3 Proposed Algorithm

Initialization phase

There are two steps in network initialization phase:

- Sender first forms a cluster of similar kind of nodes and advertises the information to all receiver.
- For each cluster there is key which is generated by proposed protocol. And signature is also provided to each group and then both signature and key were sent to each sender.

Connection establishment phase

There are four steps to form connection between sender and receiver

- Sender requests the receiver by using key element that means encrypted image.
- Receiver decrypts the image and verifies it. If the image is found within its database then it sends the acknowledgement to sender.
- The sender compares the received signature with stored signature. If it matches it sends an acknowledgement (Acki) to the receiver.
- Lastly receiver receives and verifies ack and finally forms the connection.

There are two algorithms used for transferring of data between sender and receiver which are as follows:

- Encryption algorithm.
- Decryption algorithm.

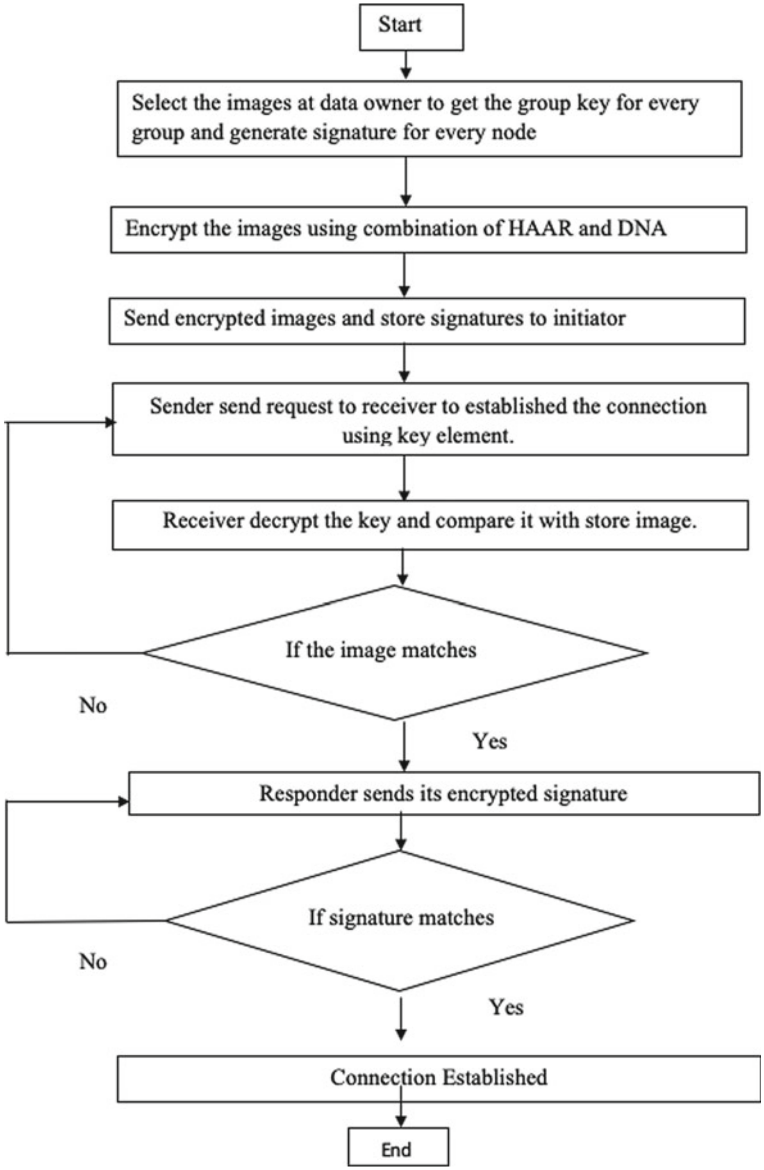

Start
Select the images at data owner to get the group key for every group and generate signature for every node
Encrypt the images using combination of HAAR and DNA
Send encrypted images and store signatures to initiator
Sender send request to receiver to established the connection using key element.
Receiver decrypt the key and compare it with store image.
If the image matches
No
Yes
Responder sends its encrypted signature
If signature matches
No
Yes
Connection Established
End

Fig. 1 System flowchart

3.3.1 Encryption Algorithm

```
Begin
Step 1: Create the network environment.
Step 2: Initialize the Encryption process.
Step 3: Store the number of images.
Step 4: Loop till all images get traversed
Step 5: Scan the image
Step 6: Calculate image size
Step 7: Loop1 till all channels get scan
Step 8: Loop2 traverse all rows
Step 9:         Loop3 traverse all column.
Step 10: Calculate sum by subtracting array of [row, column, channel] and array
of [row, column, channel+1].
Step 11: Find new Image by assign sum to array of row and column.
Step 12:        End loop3
Step 13:    End loop2
Step 14: End loops1
Step15: Use HAAR technique to find sum.
Step 16: Use DNA technique to encrypt the image.
Stop
```

3.3.2 Decryption Algorithm Begin

```
Begin
Step 1: Create the network environment.
Step 2: Initialize the decryption process.
Step 3: Extract the number of images.
Step 4: Loop till all images get traversed
Step 5: Scan the received image
Step 6: Calculate image size
Step 7: Loop1 till all channels get scan
Step 8: Loop2 traverse all rows
Step 9:         Loop3 traverse all column.
Step 10: Exchange the pixel of the image.
Step 11: End loop3
Step 12:    End loop2
Step 13: End loops1
Step14: Get the final decrypted image by reversing the image.
Stop
```

4 Simulation and Results

Complete analysis is conducted in MATLAB 2017a tool and firstly the network environment is created by pressing the prepare network button, then sensor node gets deployed by using the deploy button, and then finally algorithm starts execution by using the start button in Fig. 2. Then authentication process starts as shown in Figs. 3 and 4 by formation of the groups of the sensor node. Results clearly show that the significant improvement in time, energy, and bandwidth in data transmission for proposed scheme in Figs. 5, 6, and 7, respectively, is compared to base schemed.

The time consumption in Fig. 5 shows that initially nearly same time is expended but at that point when proposed framework starts saving more time as compared to the exiting frame then the performance is getting improved. It is clear that the proposed protocol performs better as compared to the existing method.

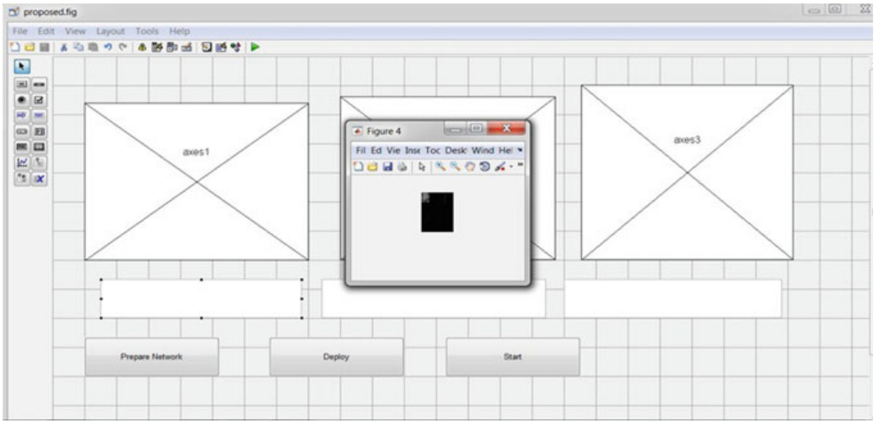

proposed.fig
File Edit View Layout Tools Help
axes1
Figure 4
Fil Ed Vie Inse Too Desk Wind Hel
axes3
Prepare Network
Deploy
Start

Fig. 2 Distribution of sensor nodes in the field

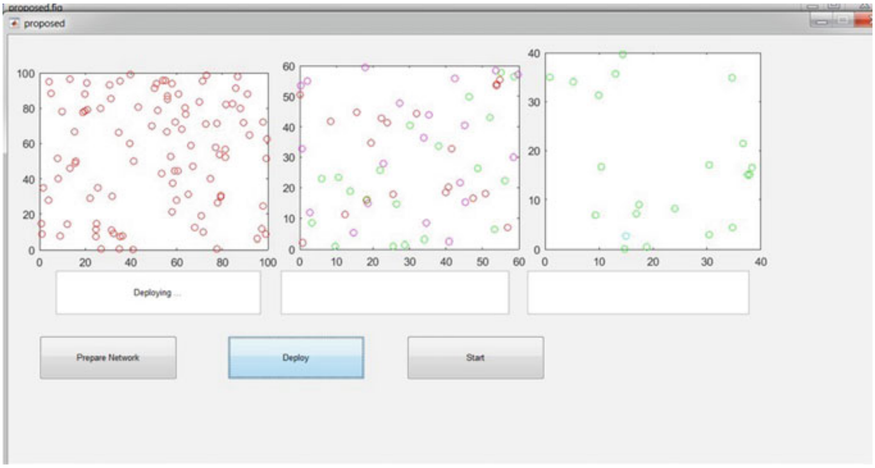


Fig. 3 Authentication process for first group

The energy consumption in Fig. 6 is clearly showing that energy consumed by the proposed protocol shown is much less than existing procedure in spite of the fact that the energy climbs as the organized advances but indeed at that point it remains much lower at that point of the existing protocol.

Figure 7 is showing the bandwidth required for the transmission of data. It is very clear that bandwidth required by proposed protocol is much lesser than the exiting protocol.

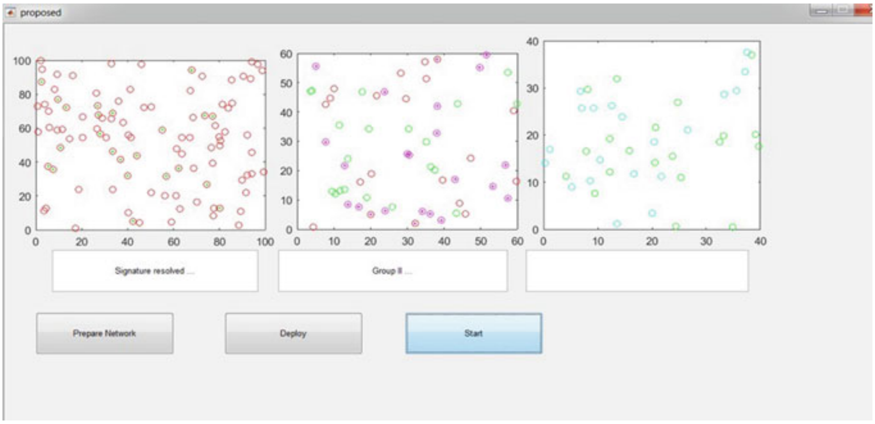


Fig. 4 Authentication process for second group

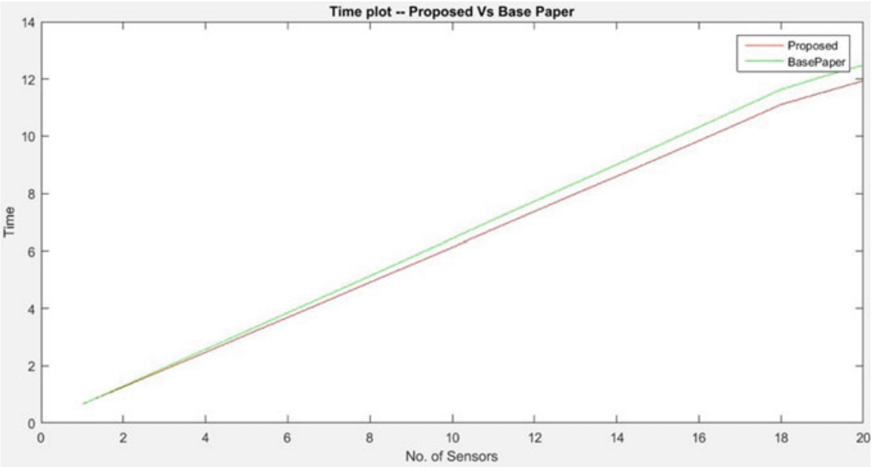


Fig. 5 Comparison of time consumption

5 Conclusion and Future Scope

The proposed protocol is made to provide more efficiency to IOT networks with real-time support. In this research work, first image which is encrypted is considered as a main key element and the verification to every node is provided by the signature. The network is spitted into various groups where each group has sender and receiver. The encrypted algorithm uses HAAR and DNA as combined protocol to encrypt the given image. The proposed protocol is split into two states. The first state is steady state in which key element that mean image is elected for each node which is encrypted with the given algorithm and then both the image and signatures are stored

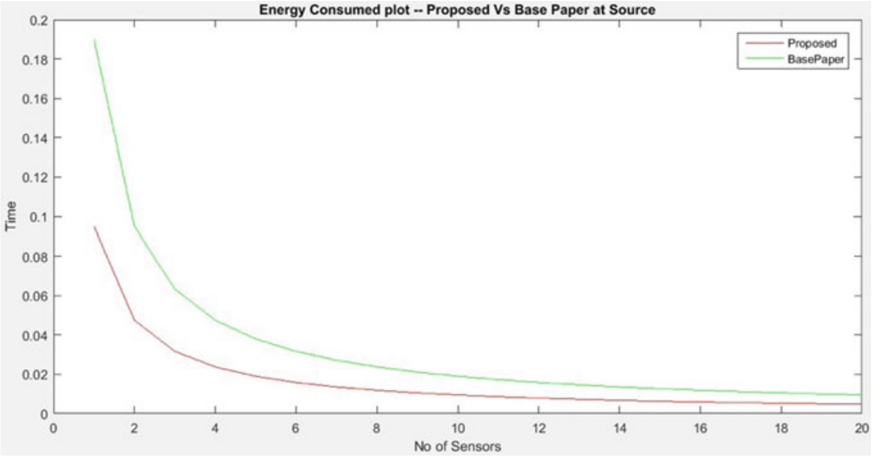


Fig. 6 Comparison of energy consumption

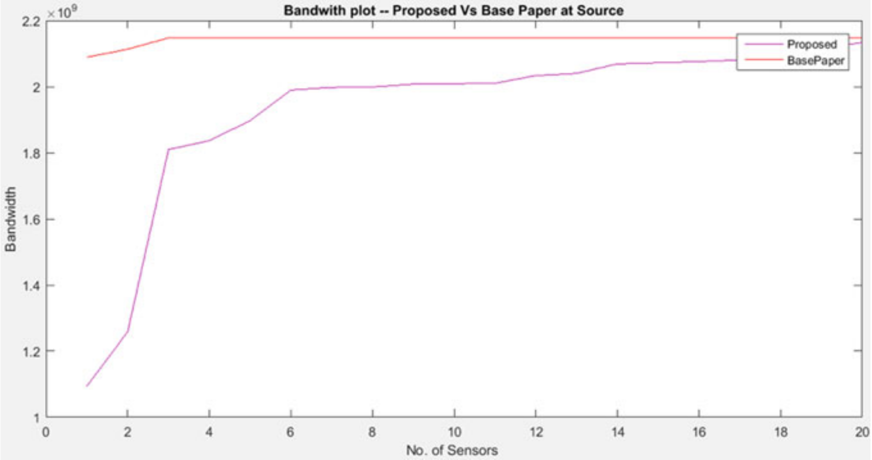


Fig. 7 Comparison of bandwidth utilization

manually into the sender. The second state called as connection establishment state in which the sender requests the receiver for the encrypted image, then the image is decrypted by receiver to authenticate that image, and then after authentication, the signature is being sent to the sender for authentication of node, if authenticated, the connection made gets established, otherwise connection not formed.

References

1. P. Porambage, P. Kumar, C. Schmitt, A. Gurtov, M. Ylianttila, Certificate-based pairwise key establishment protocol for wireless sensor networks, in *2013 IEEE 16th International Conference on Computational Science and Engineering* (IEEE, 2013), pp. 667–674
2. S. Raza, H. Shafagh, K. Hewage, R. Hummen, T. Voigt, Lithe: lightweight secure coap for the internet of things. IEEE Sens. J. **13**(10), 3711–3720 (2013)
3. R. Hummen, J.H. Ziegeldorf, H. Shafagh, S. Raza, K. Wehrle, Towards viable certificate-based authentication for the Internet of Things, in *Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy* (2013), pp. 37–42
4. C. Fu, Z. Jiang, W. Wei, A. Wei, An energy balanced algorithm of LEACH protocol in WSN. IJCSI **10**, 354–359 (2013)
5. Y. Bai, J. Huang, Q. Han, D. Qian, Link availability based mobility-aware max-min multi-hop clustering (M4C) for mobile ad hoc networks. IEICE Trans. (2009)
6. S.A. Dhondiyal, D.A. Rana, Sleeping mode MODLEACH protocol for WSN. IJARCCE **7**, 112–116 (2018). https://doi.org/10.17148/IJARCCE.2018.7823
7. W. Yuan, L. Hu, H. Li, J. Chu, Security and improvement of an authenticated group key transfer protocol based on secret sharing. Appl. Math. Inf. Sci **7**(5), 1943–1949 (2013)
8. A. Ahady, S.M. Abd EI-Kader, H.S. Eissa, Intelligent sleeping mechanism for wireless sensor network. Egypt. Inf. J.
9. H.R. Hussen et al., SAKES: secure authentication and key establishment scheme for M2M communication in the IP-based wireless sensor network (6LoWPAN) (2013)
10. D. Singh, S. K. Nayak, Enhanced modified Leach (EMODLEACH) protocol for WSN, in *2015 International Symposium on Advanced Computing and Communication (ISACC)* (2015)
11. D.J. Cook, S.K. Das, *Smart Environments: Technologies, Protocols, and Applications* (Wiley, New York, 2004)
12. R. Hummen, H. Wirtz, et al., Tailoring end-to-end IP security protocols to the Internet of Things (2013)
13. D. Bhattacharya, R. Krishnamoorthy, Control optimisation in wireless sensor networks. IJCSI **8**, 415–419 (2011)
14. F. Bouhafs, M. Merabti, H. Mokhtar, A hub recuperation plot for information scattering in remote sensor systems, in *IEEE International Conference on Correspondences, 2007*. ICC'07 (2007), p. 3876
15. A. Gogu, D. Nace, A. Dilo, *Optimisation Problems in Wireless Sensor Networks* (IEEE, 2011), pp. 302–309
16. J. Pouwelse, K. Langendoen, H. Tastes, Dynamic voltage scaling on a low-control microchip, in *Proceedings of the Seventh Yearly Global Gathering on Mobile Registering and Systems Administration* (ACM Press, New York, NY, USA, 2001), pp. 251–259

Wired Communication Technologies and Networks for Smart Grid—A Review

S. Vikram Singh, Aizad Khursheed, and Zahoor Alam

1 Introduction

The beginning of the twenty-first century was distinct by the escalation in smart grid development. The objectives of this development are unlimited, which include encouraging the extensive and distributed use of sustainable sources of energy, increasing energy efficiency, limiting the power generation to reach its peak, automatically responding to demand, increasing reliability, reducing cost of energy, and end user participation in management of energy. This development will influence all aspects of the electrical network, which has not changed much from the time of its origination at the winding up of the nineteenth century.

To achieve the goals of developing an intelligent grid, it is necessary to modernize network components, introduce latest control techniques, up-to-date monitoring strategies, and continuous study and evolution of new technologies. Smart grid judgment depends on real-time sharing of control and measurement data between a huge network of equipment devices installed in households as well as enterprises, in transmission and distribution networks, as well as in substations, control, centers and generating stations, etc. Therefore, a powerful, dependable, safe, and expandable communication network is an important element in the development of an intelligent network [1].

At present, the networks for communication in most of the electric utilities are not well equipped to cater the obstacles produced by the smart grid evolution. To

S. V. Singh · A. Khursheed (✉)
EEE Department, Amity University, Greater Noida, India
e-mail: akhursheed@gn.amity.edu

S. V. Singh
e-mail: svikram@gn.amity.edu

Z. Alam
IME Department, Indian Institute of Technology Kanpur, Kanpur, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_15

support the discrete applications, most of the communication networks are specifically designed: distinct networks for the System for Management of Energy (EMS), SCADA, distribution management services, smart metering, etc. Aforesaid networks depend on wired or wireless communication technologies. The ever-growing network extremities and applications with smart grid expansion make the present-day practices supportable. What is needed is a new consolidated network structure that routes traffic for each application while catering different requirements for performance, security, and reliability [2].

The application-oriented approach for the design of communication network for the smart grid and network transformation depends on this design which has been studied in detail. Hence, an appreciable portion of this article is dedicated to the description of progressive smart grid applications like the distribution automation and advanced metering infrastructure and conventional utility applications like SCADA.

The electricity grid comprises bulk power generating stations tied to a transmission line network operating at a very high voltage to supply electricity to end users through electricity distribution network [1]. During second half of the twentieth century, communication networks were used for grid monitoring but were restricted to SCADA and protection systems based on substations only. The obligation for clean energy with widespread use of sustainable energy sources, the benefits of limiting the power generation to reach its peak for ecological, and cost-effective reasons and consumer involvement in management of energy are few reasons for the advancement of grid from conventional to the smart one. While the smart grid is the updated version of the conventional power grid, the development has acquired a sense of haste over the past few years.

The structuring of this review paper is done as follows: a run through of power sector and by what means the current infrastructure can be combined with recent communication technologies in power system is covered in Sect. 2. Section 3 deals with the different types of smart grid communication networks. A detailed comparison of different types of wired communication technologies used in power sector is covered in Sect. 4. Different utility applications that are critical to smart grid operation are discussed in Sect. 5. The summarizing remarks are given in the last section, i.e., Sect. 6.

2 Power Sector

The design of a conventional power grid is such that the flow of electricity, information, and revenue is a one-way process. The power plant generates electricity, and a very high-voltage transmission of generated power is done before distributing this power across distribution lines of medium and low voltage levels (Fig. 1). The design of a modern power grid is such that the flow of electricity, information, and revenue is a two-way process as shown in Fig. 2. Due to the integration of traditional grid with information grid, a traditional grid is converted into a smart grid.

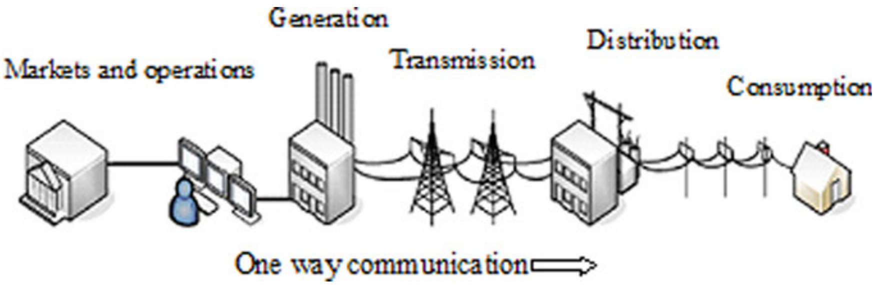


Fig. 1 Traditional electricity grid

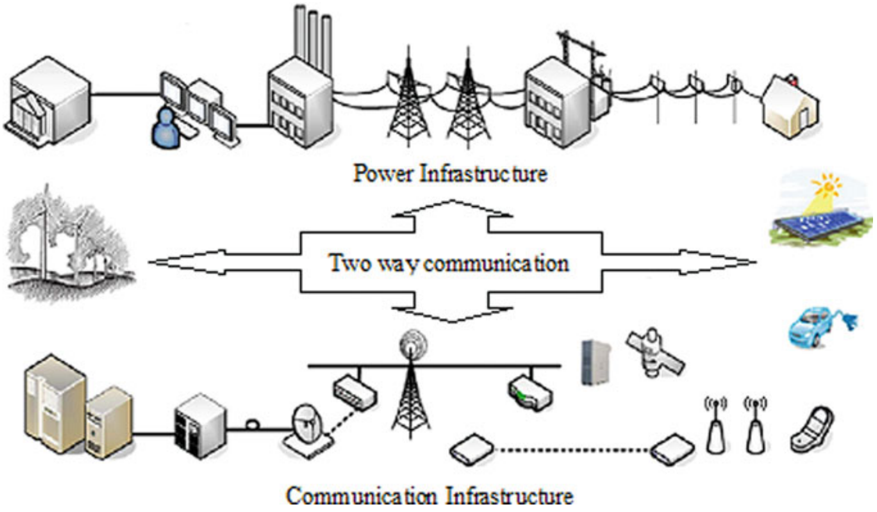


Fig. 2 Modern electricity grid

Conventional grids utilizing the computer-based technologies of automation and remote control are generally referred to as smart grid. Smart grid has become reality due to two-way digital communication technologies and computer-based processes that are in use in other industries from decades. A major improvement in power system reliability and energy efficiency is the important benefit which a smart grid offers to the utilities and the consumers [1, 2].

Nowadays, it is a matter of debate whether to make investment into long-distance high-voltage transmission lines or into technologies facilitating bulk storage of power. Indeed, the distributed generation of electricity and its storage for localized distribution is a cost-saving, less complicated, faster, and efficient substitute to unified generation of electricity and transmitting generated power over long distances through transmission network of high-voltage lines.

The implementation of Automated Meter Reading (AMR) and SCADA/EMS by electricity distribution and transmission companies, respectively, was the first step in the implementation of machine-to-machine (M2M) communication in the energy sector. For electricity consumers as well as utilities, the advantages of smart metering are manifold, that is, being able to take readings remotely and remote control of load, implementing tariffs according to the time of the day, faster detection of outages, etc. A much improved reliability of the grid is achieved by Wide Area Monitoring System (WAMS) through phasor measurement of voltage and current vectors [3].

For the purpose of reducing the environmental pollution, aggressive and far-sighted targets are set by the authorities and the regulators to generate electricity through sustainable energy sources. In addition to providing cost-effective and clean mode of transportation, the electric vehicles may also act as virtual generators, which, in the event of a breakdown, could possibly provide electricity to the grid. Also, the generators and the loads can be controlled intelligently by setting up smart micro-grids. The aforesaid micro-grids can be isolated from the major grid in the event of an outage or a data breach. It is expected that the electricity grid will transform into "Grid of Things" in a similar way the Internet has been transformed into "Internet of Things". Integration of "Internet of Things" and device-to-device communication with "Grid of Things" is known as "Internet of Energy". Figure 3 illustrates this concept in more detail.

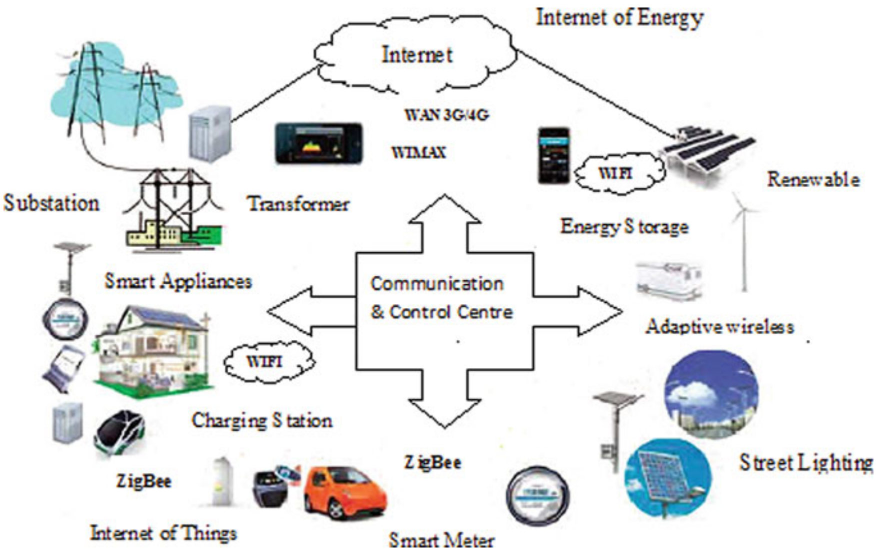


Fig. 3 Modern power sector

3 Communication Networks of Smart Grid

The structure of communication networks of smart grid supports exchange of information between end points of the network present between and within the distribution, transmission, and areas of operation of smart grid architecture. The support for connectivity of smart meters and Intelligent Electronic Devices (IEDs) installed at the distributed generation (DG) and customer domains is also provided by the communication network structure. The network structure is required to help extranet connections to establishments in other areas that is bulk power generation, service provider areas, etc. The types of networks on which the communication architecture may be based are wide area network, neighborhood area network, and home area network. Based on the aforesaid networks, the communication architecture representational diagram of the smart grid is depicted in Fig. 4.

The area of installation and operation of HAN is very small, i.e., tens of meters, which may be house or a small office. As compared to other two networks, the rate of data transmission of HAN is relatively low, i.e., hundreds of bps-bits per second [4]. The standard application of HAN comprises sharing of a wideband Internet connection by many users via wireless or wired modem. This allows resource sharing and communication between mobiles, computers, and other devices via network connection. As far as smart grid applications are concerned, the smart meters and in-home smart devices consuming energy may be connected to HAN. The data from the smart devices is fetched and fed to the smart meter via HAN, allowing cost-effective energy management at home.

Neighborhood area network is installed and operated over an area of few hundred meters, which are in fact only a few buildings. The energy consumption data of each building is transmitted to neighborhood area network by connecting the discrete home area networks to a neighborhood area network. The data is forwarded further

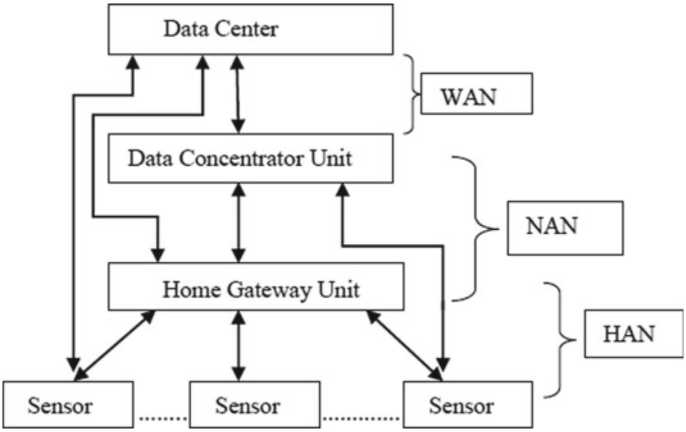


Fig. 4 Smart grid communication networks

by NAN for storage at local data centers. The stored data is significant for recognizing the pattern of generation and demand through data analysis and for consumer billing purposes. The maximum speed at which data transmission can be done in NAN is 2 Kbps.

Wide area network is installed and operated over a large area in the range of tens of kilometers. It contains discrete neighborhood area networks as well as home area networks. In addition, the communication between all the components of smart grid including conventional and sustainable energy generation, transmission and distribution, operator control center, etc. is based on wide area network. WAN supports high-speed transmission of data at a rate of few Gbps. The implementation of HAN, NAN, and WAN can be done through various wired or wireless communication technologies.

The various elements in M2M communication are backhaul network or WAN, field area network or NAN, HAN, various sensors, some home gateway, and a data center with data concentrator unit. The home gateway may or may not be present depending upon the characteristics of the application that is supported. A core (or backbone) network would also be available. Figure 4 shows a theoretical representation of M2M communications, in which several sensors in a HAN, NAN, WAN would communicate with the home gateway, data concentrator unit, or data center [5].

M2M device will receive the IP (Internet Protocol) address when these devices are connected to the gateway from the central dynamic host configuration protocol server. After validation, the session manager/BRAS create the session and access to the Internet is given. The in-operation architecture for M2M communications might have its foundation on the one M2M architecture or on any other if it is pertinent to our requirement for its usage in the energy sector. Although the positive outcome of implementing existing technologies or that shall be introduced in the future depends totally upon all the connected devices in the system and also on the interoperability with IP networks. The in-existence breakup of wireless wide area network technologies utilized in the M2M field is illustrated in Section IV. GPRS communication has a major share among the wide area network communication technologies.

4 Wired Communication Technologies

As already explained, smart grid is a combination of conventional grid and information technology, but we know that without communication technology we cannot imagine about information. Therefore, best communication technologies must be applied for collection of information. At present, the prime objective is to develop a communication system architecture which can provide solution to the interconnected system problems and can be used in future smart grid applications [2]. In this paper, only wired communication technologies have been discussed. The wired communication technologies use power line or data cables as propagation mediums for transmission of electromagnetic signals. Dedicated data cable networks require additional capital for the cable deployment, but they have greater communication capabilities and lower communication delay. Some of the potential wired communication solutions in smart grid are discussed in this section such as Power Line Communication (PLC), Fiber to the x (FTTx), Serial Interfaces (RS232/RS422/RS485), Digital Subscriber Line (DSL), and Ethernet.

In addition to the distribution of electrical power, the utilization of power lines for communication purpose has gained popularity in recent years. The advantage of PLC is that no additional wiring is required, but its practical applications are difficult [6, 7]. The signal frequency variation and length of communication channel play a critical role in the channel performance [8, 9]. In PLC technology, a modulated carrier is introduced over the power line cable for establishment of two-way communication [10]. The modulated carrier introduction on the power line allows utilities to use power infrastructure for exchanging data and monitoring control messages. This technique is a cost-efficient method of smart grid [11] communication and is extensively used in deployment of AMR applications [1].

Several areas of smart grid, including bulk generation, distribution, as well as consumers use PLC technology. The utilities prefer PLC technology over other methods of communication because it is more reliable than others. As a right solution to the smart grid communication infrastructure, PLC can be taken into consideration [4]. Due to shortfall in interoperability and standards in the multi-protocol and the multi-vendor surroundings of HAN networks, PLC is not considered as a practical solution in a HAN environment till date [10]. Narrowband PLC and broadband PLC are two major subcategories of PLC.

FTTx or fiber in the loop is a term that is generally used for any broadband network architecture that uses the optical fiber to provide a part or all of the local loop used for last-mile communication. Since fiber optic cables can hold and carry more amounts of data for longer distances, the copper-based telephone networks developed in the twentieth century are being substituted with fiber optic cables. Optical communication is extensively used for connecting operation and control centers with substations in the backbone network, due to its lot of advantages like ability to broadcast over large distances with higher bandwidth and greater opposition to electromagnetic and radio interferences, thus making it a good choice for high-voltage environments. In our opinion, fiber optic communication will play an important role in smart grid infrastructure. The deployment of Optical Power Ground Wire (OPGW) technology in transmission and distribution lines is appropriate because the amalgamation of grounding and optical communication permits transmission of signal over longer distances with higher rates of data transfer. One more use of fiber optic technology would be to give services to customer domain [12] using Passive Optical Networks (PON) as these utilize only the splitters to collect optical signals, not requiring any switching equipment. Ethernet PON (EPON) is also attracting grid operators and it seems to be appropriate technology for smart grid access segment. The operation of EPON depends on interoperable IP-based Ethernet protocols over optical network technology [10].

Table 1 Protocol comparison

Parameters	RS232	RS422	RS485
Cable used	Single ended	Single ended Multi-drop	Multi-drop
Maximum devices	1 transmitter 1 receiver	1 transmitter 10 receivers	32transmitters 32 receivers
Communication systems	Full duplex	Full duplex Half duplex	Full duplex Half duplex
Distance range	50 feet at 19.2 kbps	4000 feet at 100 kbps	4000 feet at 100 kbps
Data rate (50 feet)	1 Mbps	10 Mbps	10 Mbps

The method of transmitting data, one bit at a time, in sequence, over communication channel, or computer bus is called serial communication. In parallel communication, quite a few bits are sent as complete, over a link with various parallel channels. Serial communication is implemented in all the haul communications and in almost all computers in which higher cable cost and synchronization problems make parallel communication not feasible practically. Some of the most widely used communication protocols are RS232, RS485, RS422, USB, and Ethernet. In USB and Ethernet, there are requirements of complex protocols and powerful interfaces. A lot of devices utilize RS232, RS485, and RS422. The comparison of these protocols is given in Table 1. The RS232, RS485, and RS422 serial protocols are relevant to hardware interface only. These are not software protocols which are used to initiate communication between devices.

DSL is a suite of communication technologies that allow data transmission through telephone lines. The advantage of using telephone lines for data transfer is that the utilities can transmit data without investing in deployment of additional lines. DSL substitutes like Asymmetric DSL (ADSL), ADSL 2+, and VDSL (very high bit DSL) support data transfer rate of up to 8 Mbps, 24 Mbps, and 52 Mbps, respectively, for downstream and up to 640 Kbps, 1 Mbps, and 16 Mbps, respectively for upstream but VDSL is suitable for data transfer to shorter distances only [10].

The advantages of Ethernet such as versatility, higher speed, and better compatibility make it the most preferable choice for the substation automation system. Due to the substantial increase in the number of IEDs, there is a need to create networks in substations. The detailed comparison of wired communication technologies which are used in power sector [13] is given in Table 2.

5 Smart Grid

Smart grid can be defined as an integrated network that would support all the utility and smart grid applications that are being put into practice presently as well as in future. A detailed study of the recent utility applications that are an integral part of the

Table 2 Wired communication technologies used in power sector

Technology	Frequency bands	Advantages	Drawbacks
PLC	Narrowband: 200 Hz to 500 kHz Broadband: MHz	1. Use existing infrastructure 2. Long technological life cycle 3. Many standards and protocols available	1. Good condition power cable required 2. O & M cost is high 3. Point-to-point communication gets affected during outage 4. Absence of regulation on frequency bands
FTTx	According to use	1. Superfast 2. Very high bandwidth 3. Very low attenuation	1. Less availability 2. Installation cost is more
Serial interfaces RS232 RS422 RS485	Depends on the signal frequency	1. Mature protocols 2. Easy to implement 3. Inexpensive installation	1. Wires increase complexity 2. Less range 3. Extremely less throughput
DSL	0–0.2.208 MHz	1. Economical 2. Time saving 3. Inherent redundancy	1. Less secure
Ethernet	a. 16 MHz b. 100 MHz c. 250 MHz d. 500 MHz e. 600 MHz f. 1 GHz g. 1.6–2.0 GHz	1. Economical 2. Excellent throughput 3. Lesser installation time 4. Easily scalable	1. Least secure 2. Highest latency 3. Bursts of additional bandwidth not possible

smart grid evolution is presented in this section. The utility applications include AMR and AMI, transmission management system, DMS, DG, energy storage, Distributed Control System (DCS) for production units, substation automation and distribution automation, electric vehicles, energy storage, micro-grids, home/building energy management and enterprise networks.

Advanced metering infrastructure is a term used for the network infrastructure linking smart meters installed at consumer premises, meter data management system installed at utility Data and Control Center (DCC), and other intermediary network devices that support the exchange of data or information among the smart meters and the Meter Data Management System (MDMS). Nowadays, the smart meters have replaced the conventional electric meters which are located at the consumer locations. Regular analysis of electrical parameters fetched by the meters is not only utilized in billing the consumers, but it also assists several utility operations and business functions like tracking the voltage, power, usage of energy, and other customer-oriented functions. AMI is one of the major functions of smart grid [1].

In general, a system that assists the functions required to manage the transmission network is called Transmission Management System (TMS) regardless of whether the TMS is actualized as a centralized one or a system spread over various servers. Flexible AC Transmission System (FACTS), SCADA, EMS, digital fault recorder, dynamic line rating, wide area situational awareness and control, etc. are some of the important applications and the functions of TMS. Similar to transmission corporations, Distribution Management System (DMS) is the term used by distribution companies for a system that assists the functions required to manage the distribution network regardless of whether the DMS is actualized as a centralized one or a system spread over various servers. SCADA, digital fault recorder, outage management system, MDMS, multilevel feeder reconfiguration, distribution operation model and analysis, voltage control, active and reactive power control, etc. are some of the important applications and the functions of DMS. Furthermore, TMS and DMS are installed at utility Data and Control Center (DCC). Although the DCC might be centralized or made to spread over various places for the purpose of back up [14], sometimes the utilities install TMS and DMS at discrete locations.

The stand-alone plants or grid/distribution system connected sources of power generation situated either near the load centers or at consumer locations and are usually having smaller generation capacity and fall into the category of Distributed Generation (DG). The power generated through DG is mostly consumed locally and only the power which is surplus is supplied to the grid. The current-feasible technologies for DG, being a part of a large establishment or a micro-grid, contribute a maximum of 10 MW power to the grid [15]. Furthermore, the DG output depends on the localized load demand and the nature of DG installed (solar, small hydro, wind, biogas, etc.). The mutual agreement between the consumer and the utility should benefit both the parties.

It is difficult for the utilities to maintain a satisfactory and cost-efficient balance between demand and generation during day-to-day operations. The storage of electrical energy has an advantage that the energy pulled out from energy storage could be utilized to make up for the changes in load demand. Storing electrical energy in bulk is a tough task, especially when the storage is needed for longer periods. A grid-connected energy storage arrangement reserves excess incoming energy from the grid and supplies this energy back to the grid when required, which is generally referred to as Distributed Storage (DS) [16]. The fuel cells do not fall into the DS category because the energy stored in fuel cells is not taken from the grid.

A micro-grid is a decentralized group of distributed energy sources and loads that can be operated in a regulated and coordinated manner. It is either linked to the major grid or may operate in “islanded” mode and sometimes it can be completely disconnected from the main grid. Micro-grids are low- or medium-voltage grids situated at or near the load centers. The consumers connected to the micro-grid are supplied either from the utility grid or from the distributed sources of power within the micro-grid. A residential or a commercial building having solar photovoltaic modules installed at top of the building can be called as a micro-grid. Micro-grids are very important in case of an emergency situation like islanding during an outage, when it is required to run essential loads like lighting, lifts, security devices, etc. Also, the flexibility to put a micro-grid deliberately into the islanding mode and its capability to supply power to the critical loads is another important feature of micro-grids.

The smart grid aims to control and optimize the energy consumption through a combination of advanced communication technologies and the power grid. Providing a dedicated and efficient network for the power grid is a challenge, given the infrastructure architecture, communication technologies, and quality of service requirements. Both wired and wireless communications play a key role in the mix of communication technologies needed for future smart grid communications. An extensive range of wired and wireless communication technologies are available. However, technologies should not mean different networks. The different technologies should be merged into a single, hybrid communication technology for optimal smart grid communication. Hybrid communication architectures may prove to be a promising solution to smart grid communication infrastructures because of the balanced trade-off between investments and benefits and meeting the critical requirements of smart grid applications [17–20].

6 Conclusion

The conventional grid can be made more efficient by introducing advanced smart metering, remote sensing, and remote control of its main components but these features rely on relevant communication technologies. In the near future, by combining the information technology with conventional power system infrastructure, most of the vital components of the power system can be made automatic, intelligent, and smart. Therefore, twenty-first-century information technology is the foundation of a smart power grid and future of smart grids relies on relevant communication technologies which should be secure, reliable, fast, flexible, and robust. A comparison between conventional and futuristic communication networks and an overview of existing communication infrastructure and technologies relevant to smart grid has been put up in this review paper. Also, the limitations and challenges associated with communication technologies and communication networks and protocols are summarized in this paper.

These comparisons reveal that the technologies have the capability to support the operation of smart grid but are very less exposed to external factors like wholesale pricing of electricity and consumer behavior and other control issues. As the present range of bandwidth is not sufficient to cope up with ever-increasing consumers and businesses in the utility sector, the communication infrastructure should facilitate in accommodating a rapidly growing number of devices. Also, due to the implementation of new technologies, there should not be any appreciable increase in price of energy.

The utilities are looking for alternatives to wired communication technologies as wired technologies are not cost-efficient, their installation is difficult, the cables used are vulnerable to theft, etc. Also, the wireless communication technologies are gaining more popularity as a better alternative over wired technologies. By improving the data encryption techniques, they can offer enhanced security, which is their major drawback compared to wired technologies. A hybrid network, which is a combination of different wired and wireless technologies, may prove to be a better alternative. Hybrid networks can be more cost-efficient, less power consuming, and will be more feasible for remote networks through lower hardware costs.

References

1. K. C. Budka, J. G. Deshpande, M. Thottan, *Communication Networks for Smart Grids* (eBook) (Springer). ISBN: 978-1-4471-6302-2
2. A. Usman, S. Shami, Evolution of communication technologies for smart grid applications. Renew. Sustain. Energy Rev. 191–199 (2013).
3. V.K. Sood, D. Fischer, J.M. Eklund, T. Brown, Developing a communication infrastructure for smart grid, in *Proceedings of IEEE Electrical Power and Energy Conference* (Montreal, QC, Canada, 2009), pp. 1–7
4. W. Wang, Y. Xu, M. Khanna, A survey on the communication architectures in smart grid. *Computer Networks*, 3604–3629 (2011)
5. C. Strauss, *Practical electrical network automation and communication systems* (Newnes, Oxford, 2003)
6. C. Konate, M. Machmoun, J. F. Diouris, Multipath Model for power line communication channel in the frequency range 1 MHz to 30 MHz, in *Proceedings of The International Conference on Computer as a Tool* (Warsaw, Poland, 2007)
7. A. Tonello, F. Versolatto, Bottom-up statistical PLC channel modeling part I: random topology model and efficient transfer function computation. IEEE Trans. Power Delivery **26**(2), 891–898 (2011)
8. Z. Alam, A. Khursheed, R. Kant, Modeling, simulation and performance evaluation of low voltage power line communication channel. Int. J. Adv. Technol. Eng. Explorat. IJATEE **5**(46), 308–317 (2018)
9. Z. Alam, A. Khursheed, S.V. Singh, Modeling of power line for home-building automation, in *Proceedings of IEEE International Conference on Automation, Computational and Technology Management* (London, UK, 2019), pp. 111–115
10. V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, A survey on smart grid potential applications and communication requirements. IEEE Trans. Indus. Inf. **9**(1) (2013)
11. S. Galli, A. Scaglione, Z. Wang, Power line communications and the smart grid, in *Proceedings of First IEEE International Conference on Smart Grid Communications* (Gaithersburg, MD, USA, 2010), pp. 303–308
12. Y. Gobena, A. Durai, M. Birkner, V. Pothamsetty, V. Varakantam, Practical architecture considerations for smart grid WAN network, in *Proceedings of IEEE PES Power Systems Conference and Exposition* (Phoenix, Arizona, USA, 2011)
13. V.C. Güngör, D. Sahin, T. Kocak, S. Ergüt, C. Buccella, C. Cecati, G.P. Hancke, Smart grid technologies: Communication technologies and standards. IEEE Trans. Industr. Inf. **7**(4), 529–539 (2011)
14. J. Belagur, R. Schmidt, IP communication for substation automation, distribution automation, and other utility applications—a business case, in *Proceedings of IEEE PES Transmission and Distribution Conference and Exposition* (Chicago, IL USA, 2008), pp. 1–9
15. H. Khan, Z. Xu, H. Iu, V. Sreeram, Review of technologies and implementation strategies in the area of smart grid, in *Proceedings of 19th Australasian Universities Power Engineering Conference (AUPEC)* (Adelaide, Australia, 2009), pp. 1–6
16. N. Ansari, C.-H. Lo, The progressive smart grid system from both power and communications aspects. IEEE Commun. Survey Tutor. **14**(3), 799–829 (2012)

17. H. Hu, A. Doufexi, S. Armour, D. Kaleshi, A reliable hybrid wireless network architecture for smart grid neighborhood area networks, in *Proceedings of IEEE Wireless Communications and Networking Conference* (San Francisco, CA, USA), pp. 1–6 (2017)
18. J. Zhang, A. Hasandka, J. Wei, S. Alam, T. Elgindy, A. Florita, B. Hodge, Hybrid Communication architectures for distributed smart grid applications. Energies **11**(4) (2018)
19. B. Williams, Advantages of hybrid wireless field communication networks for smart grids. Electrical Energy Online, January/February (2017)
20. J. Zhang, A. Hasandka, J. Wei, S. Alam, T. Elgindy, A. Florita, B. Hodge, Analysis of hybrid smart grid communication network designs for distributed energy resources coordination, in *Proceedings of IEEE Power and Energy Society Innovative Smart Grid Technologies Conference* (Washington, DC, USA, 2019), pp. 1–5

Simulation of Firefly Algorithm-Based Routing Technique for Wireless Sensor Networks

Shilpa Choudhary, Purneshwari Varshney, Arpana Mishra, Vidit Shukla, and Shradha Gupta

1 Introduction

In wireless sensor network, number of independent sensor nodes is deployed in a certain manner to gather information like temperature, humidity, pollution, etc. In order to overcome the limitations of traditional monitoring technologies (e.g., those relying on wired networks), more and more real-time status monitoring systems based on wireless sensor networks (WSNs) are employed in smart grids to provide a strong service guarantee for monitoring and communication of electrical grids. With the use of wireless communication channels and possible deployment in harsh environments or unattended areas, they are subject to many types of attacks. Also, there are some limitations on deployed security mechanisms in these environments. Therefore, such systems are vulnerable to cybersecurity risks. Recently, numerous system analysts are taking into account systems dependent on latest resemblance methods, like never before wireless communication. Wireless systems enable hosts to meander without the imperatives of wired associations. Wireless systems have a significant job in both military and regular citizen frameworks. A wireless sensor network is a collection of center points sifted through into a framework. Each middle

S. Choudhary (✉) · V. Shukla
Department of Electronics & Communication Engineering, G.L. Bajaj Institute of Technology and Management, Greater Noida, India

P. Varshney
Department of Electronics & Communication Engineering, MBM Engineering College, Jodhpur, India

A. Mishra
Department of Electronics and Communication Engineering, IIMT, Greater Noida, India

S. Gupta
Department of Applied Science and Humanities, G. L. Bajaj Institute of Technology and Management, Greater Noida, UP, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_16

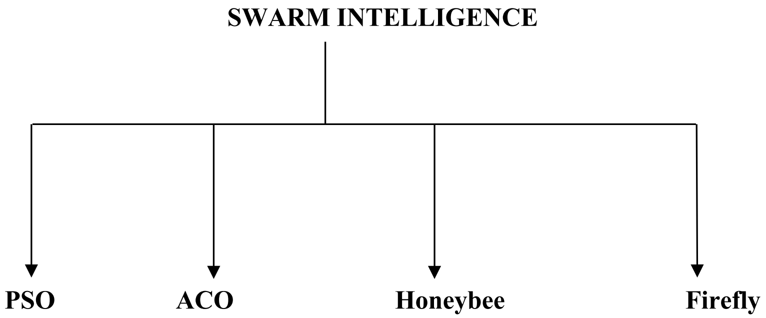


Fig. 1 Sub-domains of swarm intelligence

point incorporates dealing with limit, may contain different sorts of memory, have a RF handset, a power source, and suit different sensors and actuators. Many directing, control the board, and data spread shows have been expressly expected for WSNs where essentialness care is a key structure issue. Swarm Intelligence (SI) [1] is an artificial intelligence technique subject to the examination of total direct in decentralized, self-sifted through systems. Swarm information was exhibited by Beni and Wang in the year 1989, in the assistance of cell mechanical systems. Swarm understanding is given as "The rising total information on social affairs of essential administrators" [1]. It helps many-sided and sagacious direct through clear, independent relationship between a total amounts of self-ruling swarm people (Fig. 1).

Swarm intelligence is just another dimension of computational intelligence which offers response for complex streamlining issues which are not successfully taken care of by various systems. Swarm is portrayed as a great deal of versatile authorities that everything considered light up bothers. Every person of the swarm has simple guideline of activity and approach to a constrained measure of data through its prompt neighbor. Then again, even with restricted data and basic activities of individuals, the swarm, in general, is skilled to achieve exceptionally difficult issues of the calculation and streamlining. Swarm intelligence comprises Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), honeybee, and firefly ideal models. These models duplicate the conduct of genuine creepy crawlies for nourishment looking, sorted out living, and self-defensive styles for computational issues. The SI-based strategies are increasingly reasonable for the steering and energy assets advancement, because of the nature, design, topology, and usefulness of impromptu and remote sensor systems.

2 Related Work

J. Kennedy et al. proposed an idea of optimization with the implementation of swarm technology. There is the use of paradigms out of which one is implemented and explained with the help of tests. Explanation of the genetic life and particle algorithms is given in this paper. This explains the implementation of paradigms [2]. R. Schoonderwoerd et al. paper was in inspiration of the ant colony that they had observed and took it as their base to find useful results in the field. The very known ant colony was used in this paper to be the inspiration behind it [3]. S Choudhary et al. in their paper discussed about how the WSN has been used in military and biological fields. The new field discussed in the paper is processing to reduce the replication of information shared by the sensor nodes and to increase the reliability of end-to-end data transmission. This paper helped people from across the fields to get research-driven solutions [4]. I. F. Akyildiz et al. designed a low-cost sensor which was used in military area, healthcare, and the paper included the solutions of protocol stack layer section. The paper is not just limited to more fields to be developed in the same, and hence a cross-field paper [5]. Kwang Mong Sim et al. did modifications and detailed study in the field of ant colony optimization and models of collective intelligence were then converted to better and more implementable techniques. They also provided comparison between the techniques [6]. Mishra et al. in their paper discussed about the LEACH with the pheromone energy-efficient routings in WSN. It also discussed the performance evaluation of the SWARM intelligence alongside with the routing in wireless sensor networking in ad hoc networks. This paper clearly explains the ACO, SWARM technology so that performance can be evaluated in better manner [7]. K. Akkaya et al. did a thorough research on the wireless sensor networks connectivity. The paper focuses and also provides us with different techniques that can be used for connecting WSN to external networks and hence provides useful results [8]. JN Al-Karaki et al. in their paper explained the design challenges that were being faced while routing the WSN and also did an extensive survey. They classified them based on the protocol operation. The design trade-off is mentioned and also how the process of energy trade happens. This survey-based paper provided data and trends which could provide predictions for the same [9]. A. Mishra et al. in their paper explained and discussed about the pheromone energy-efficient routing which was useful in wireless sensor networks. It considered LEACH with pheromone energy. Hence, the paper gave beneficial results for further analysis [10]. C. Ramachandran et al. in their paper discussed about the swarm intelligence and ant model-based detection network which was based on the wildfire detection. It focused on the detection of wildfire using swarm intelligence. This paper provided much insight on the practical implementations of the said technology [11]. E. Baburaj et al. used the swarm technique in a different way. An intelligent mesh-based technique, multicast routing algorithm was implemented using MANET's [12]. Y-F Yen in his paper used the ant-based network with the help of wireless network and also routing in this energy [13]. Zulfiqar Ali et al. in their paper gave details about analysis carried out in swarm intelligence. It included routing protocols as well as the communication between the sensors wirelessly [14]. Saleem M. et al. in their paper discussed about the reverse techniques used in the swarm technology. They also provided an overall evaluation on the ant colony optimization which was evaluated and expressed as a discussion [15]. Raghvendran V. et al. in their paper explained the routing techniques that concerned the ad hoc mobile networks that also included swarm technology [16]. Sachan S. et al. in their paper “Comparative analysis of clustering algorithm for wireless sensor networks” did extensive analysis on the clustering algorithm that concerned the wireless sensor network, and they worked on the algorithm side of the technology to get useful results [17]. Jabeur et al. in the paper explained a new clustering approach that was based on the firefly approach that has micro- and macro-clustering approach for the WSN [18]. Dorigo M. et al. in the paper of ant colony optimization explained the metaheuristic techniques for their approach in the new ideas for optimization. Hence, it gave results that were helpful in further experimentation [19].

3 Swarm Intelligence-Based Routing Protocols and Algorithms

In the ongoing section, we surveyed the selected SI steering protocols for WSNs and feature their resources concerning the scientific bifurcations of directing conventions. The next few sections are a part of the larger picture where we talk about PSO- and FFA-based conventions.

3.1 Particle Swarm Optimization

Particle swarm optimization is another field of the SI that adventures the conduct of swarms for the arrangement of complex issues. PSO-natured calculation keeps up a swarm of particles. It misuses the common insight just as the data sharing limit of swarms. The PSO tries to put in the possibility of social cooperation for the arrangements of both hard and improvement issues. It was being created [2] in the year 1995 by the James Kennedy and the Russell Eberhart. In PSO, every molecule independently rose as a potential answer for the difficult issue to be comprehended. The working of PSO depends on the situation of molecule and speed of the molecule at some random time.

3.2 Centralized Particle Swarm Optimization (PSOC)

N. A. Latiff et al. presented [20] the energy mindful bunching for remote sensor systems utilizing Particle Swarm Optimization (PSO) calculation that is actualized at the base station. PSO expects to discover the molecule position that outcomes in the best assessment of a given wellness work. During every age, every molecule utilizes the useful data about its prior best individual position and worldwide finest position to refresh its up-and-comer arrangement.

3.3 Firefly Algorithm-Based Routing Protocol

Yang [21] built up the firefly calculation in 2008 dependent on this blazing conduct of fireflies. The target of firefly calculation is to discover the situation of the molecule that gives best outcomes in assessing a wellness work. The light force changes as indicated by the converse square law. The light power can be resolved as demonstrated as follows:

$$I(r) = I_0 \exp\left(-\gamma r^2\right), \tag{1}$$

where $I(r)$ refers to light intensity at a distance r, I_0 is the intensity at the source, and γ is the absorption coefficient of the medium.

The firefly's allure is straightforwardly relative to the light force observed by different fireflies; we presently characterize the engaging quality β with the separation r as

$$\beta = \beta_0 \exp\left(-\gamma r^m\right), \tag{2}$$

where β_0 is the appeal at $r = 0$. $r_{i,j}$ is the separation linked any two fireflies I and j, which are at positions xi and xj each one by one, individually. The Cartesian separation is given by the condition

$$r_{ij} = \sqrt{\sum_{k=1}^{d} (xi, k - xj, k)^2}, \tag{3}$$

where xi, k is the kth component of the spatial arrange xi of the firefly I and d is the quantity of measurements. The development of firefly I toward progressively another (more brilliant) firefly j is given by

$$x_i = x_i + \left[\beta_0 \exp\left(-\gamma r_{i,j}^2\right)\right]\left(x_j - x_i\right) + \alpha\varepsilon, \tag{4}$$

where the subsequent term is because of fascination and α is an arbitrary factor.

3.4 Group Arrangement Using Firefly Calculations

The base station runs the count as it is consolidated. The best K cluster heads that minimize the cost function are obtained.

$$\cos t = \beta \times d_1 + (1 - \beta) \times d_2, \tag{5}$$

$$d_1 = \max_{k=1,2,3\ldots k} \sum_{\forall ni \in Cp,k} \frac{d(ni, CHp, k)}{Cp, k}, \tag{6}$$

$$d_2 = \frac{\sum_{i=1}^{N} E(ni)}{\sum_{k=1}^{k} E(CHp, k)}, \tag{7}$$

where d_1 is the most extreme normal Euclidean separation of individual nodes to the related bunch heads, $|Cp, k|$ is the quantity of nodes that have a place with group C_k of molecule p, d_2 is the capacity which is the proportion of aggregate of beginning energy of all nodes ($n_i = 1, 2, 3 \ldots N$) to the total of the present energy of the group heads in the present cycle, and β is a client characterized consistent.

4 Customized Firefly Algorithm

There is a wide scope of divergence among the network of live people as far as wellness and quality. On the off chance that an individual have high wellness esteem, at that point it plays out its activity adequately than others and achieve superior. The part with low quality doesn't accomplish such superior. So as to improve the presentation of the network by making changes in the person's position another calculation dependent on firefly calculation is created. The new calculation permits making changes in the situation of the people and expanding the plausibility of getting the ideal arrangement in the firefly populace.

4.1 Proposed Methodology

This segment manages the modified firefly calculation (CFFA) with the suppositions made for building this novel convention. Suspicions are

- Every one of the nodes can speak with one another and with the base station (BS) directly.
- There is a solitary jump from customary node to cluster head (CH) and from CH to BS.
- Each one of the nodes is static, where the calculation runs at a specific time moment and updates for next round, and each one of the nodes is area mindful. They update their area data to the BS before going into the setup stage.
- 2-D space is considered for deployment of sensor node.

5 Simulation Environment

A lot of perceptible matrix can be utilized for assessing the presentation of routing protocols in WSN.

5.1 *Performance Matrices*

The following measurements are used for assessing the presentation of two directing conventions PSOC (centralized particle swarm optimization) and CFFA (customized firefly algorithm):

- Delay (second): The delay consolidates all reasonable and existing delay realized by buffering in between course disclosure dormancy, lining at the interface line, retransmission deferral, multiplication, and move time. The same is described as
  D = (Tr − Ts)
  Here Tr is receive time and Ts represents sent time.
- Energy Consumption: When transmission is done or getting information to/from neighbors, some energy of nodes get dispersed. So alongside the progression of time the rest of the energy or lingering energy of nodes diminishes.

5.2 *Simulation Setup*

As effectively laid out we have taken steering conventions, to be specific PSOC and tweaked FFA. For every one of the recreations, a similar development models were utilized and reproduction time is differed as 5, 15, 25, 35, 45, and 55 s. The presentation investigation is done on Ubuntu Operating System. Ns-3 was introduced on the stage. In this situation, a few parameters with a particular worth are considered. Those are as given in Table 1.

6 Results and Discussion

6.1 *Delay*

In Fig. 2, CFFA exhibits the minimum delay along with the increase in simulation time. It means packet delivery in between source and final destination requires less time as simulation time peaks in CFFA.

a. **Energy Consumption**

Figure 3 exhibits the connection between energy consumed at y-axis and simula-

Table 1 Scenario for implementation of PSOC and CFFA

Operating system platform	Ubuntu
Simulator used	NS-3
Protocols followed	PSOC, CFFA
Type of channel	Wireless channel
Traffic type	Constant bit rate (CBR)
Number of nodes	40
Area size of simulation	500 × 400
Mobility model	Random way point mobility
Antenna model	Antenna/omnidirectional
Packet size	712 Bytes
Max. packet in ifq	50

tion time at x-axis for PSOC and CFFA routing protocol. CFFA displays least value for the same. Therefore, CFFA is more energy efficient.

7 Conclusions

Energy efficiency is a basic factor in WSN so as to drag out framework lifetime. Because of the time-changing nature of the wireless channel, the throughput is extremely delicate to the packet size. The following paper presents an examination of the distinctive swarm-based steering methods for WSNs from the ongoing work. In this paper, grouping utilizing redid firefly calculation has been finished. Here cost capacity utilizes the separation between the nodes and the group head and the energy of the nodes. The re-enactment results show that the calculation gives low energy utilization and delayed system lifetime than the other convention. Future extension incorporates blend of other bio-enlivened calculations and presents crossover methods for effective clustering in WSNs. In future, much of the research work is required to reduce the security risk in wireless sensor network so that the data privacy may not get hampered.

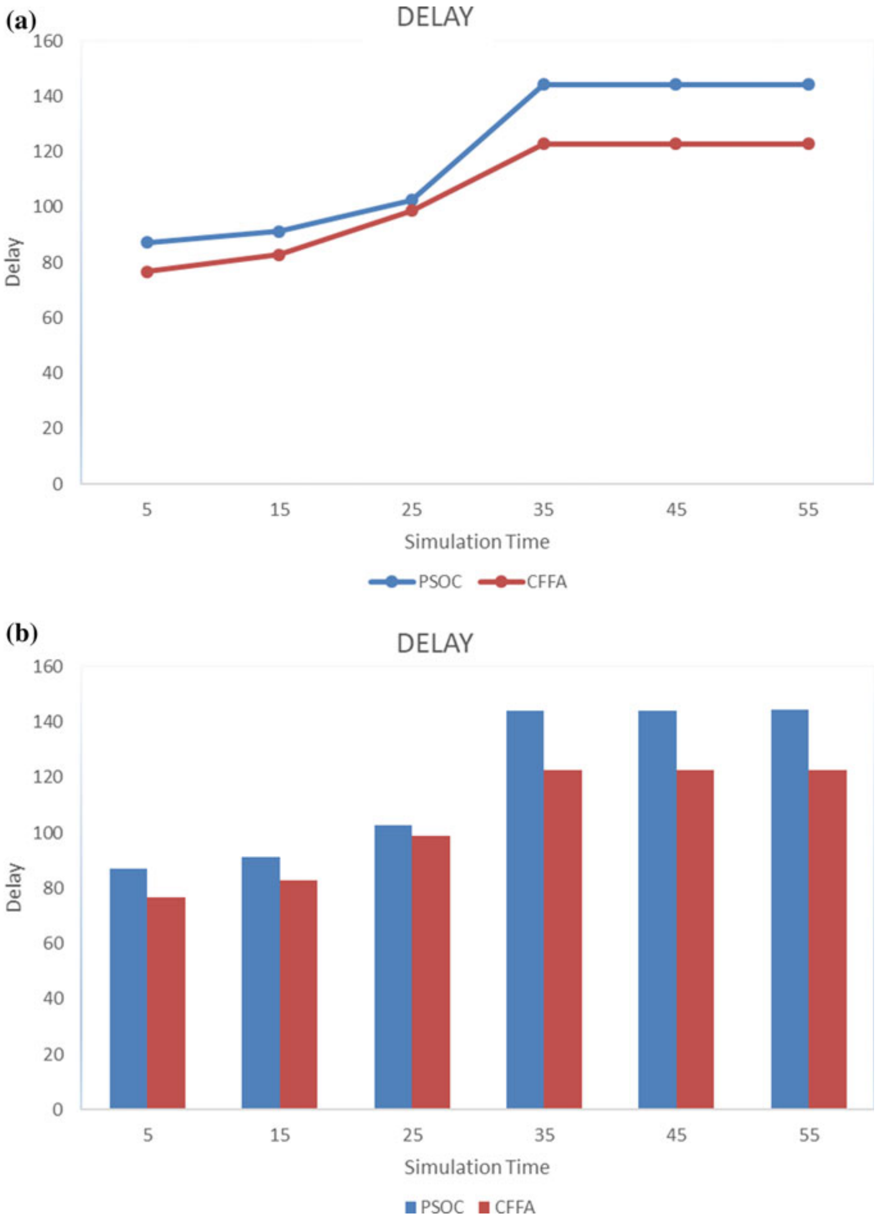


Fig. 2 Delay versus simulation time for PSOC and CFFA

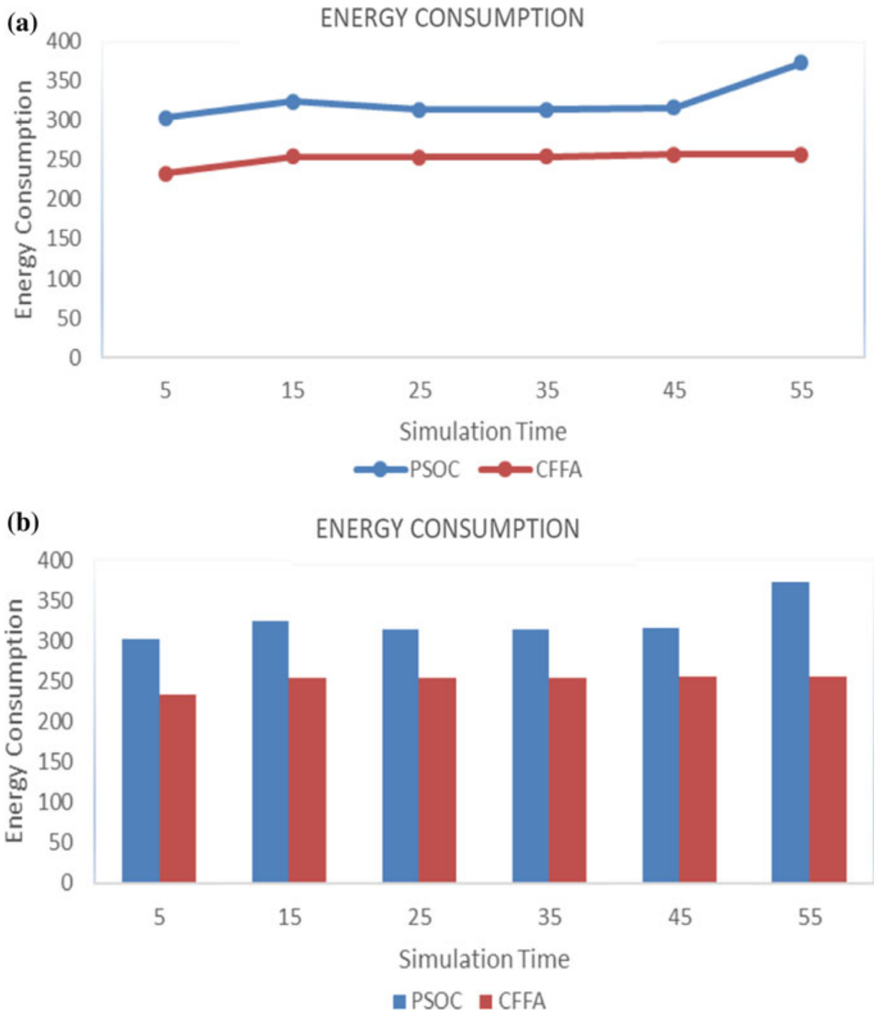


Fig. 3 Energy consumption versus simulation time for PSOC and CFFA

References

1. E. Bonabeau, M. Dorigo, G. Theraulaz, *Swarm Intelligence: From Natural to Artificial Systems*, 1st edn. (Oxford University Press, New York, USA, 1999)
2. J. Kennedy, R. Eberhart, Particle swarm optimization, in *IEEE International Conference on Neural Networks* (Perth, Australia, 1995), pp. 1942–1948
3. R. Schoonderwoerd, O. Holland, J. Bruten, L. Rothkrantz, Ant-based load balancing in telecommunications networks. Adapt. Behav. **5**(2), 169–207 (1996)
4. S. Choudhary, L. Sharma, A.K. Kaushik, A. Mishra, Novel approach to reduce the replication of information and to increase the reliability of end to end data transmission in WSN, in *2nd International Conference on Intelligent Communication and Computational Techniques*

(ICCT) (Manipal University Jaipur, 2019), pp. 36–83

5. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A Survey on sensor networks. IEEE Commun. Mag. **40**(8), 102–114 (2002)
6. K.M. Sim, W.H. Sun, Ant colony optimization for routing and load-balancing: survey and new directions. IEEE Trans. Syst. Man Cybernet.—Part A: Syst. Humans **33**(5), 560–572 (2003)
7. S. Mishra, P. Varshney, S. Choudhary, R. Purohit, Performance evolution of conventional and swarm based routing methods in mobile ad-hoc networks, in *2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC)* (Greater Noida, India, 2019), pp. 528–531
8. K. Akkaya, M. Younis, A survey of routing protocols in wireless sensor networks. Elsevier Ad Hoc Netw. J. **3**(3), 325–349 (2003)
9. J.N. Al-Karaki, A.E. Kamal, Routing techniques in wireless sensor networks: a survey. Wireless Commun. IEEE **11**(6), 6–28 (2004)
10. A. Mishra, S. Choudhary, M. Vats, S. Sachan, LEACH with pheromone energy efficient routing in wireless sensor network, in *Intelligent Computing in Engineering. Advances in Intelligent Systems and Computing*, ed. by V. Solanki, M. Hoang, Z. Lu, P. Pattnaik, vol. 1125 (Springer, Singapore, 2020), pp. 91–98
11. C. Ramachandran, S. Misra, M.S. Obaidat, A probabilistic zonal approach for swarm-inspired wildfire detection using sensor networks. Wiley InterSci. Int. J. Commun. Syst. **21**(10), 1047–1073 (2008)
12. E. Baburaj, V. Vasudevan, An intelligent mesh based multicast routing algorithm for MANETs using particle swarm optimization. IJCSNS Int. J. Comput. Sci. Netw. Secur. **8**(5), 214–218 (2008)
13. Y.F. Wen, Y.Q. Chen, M. Pan, Adaptive ant-based routing in wireless sensor networks using energy delay metrics. Springer's J. Zhejiang Univ.-Sci. A **9**(4), 531–538 (2008)
14. Z. Ali, W. Shahzad, Critical analysis of swarm intelligence based routing protocols in ad hoc and sensor wireless networks, in *IEEE International Conference on Computer Networks and Information Technology (ICCNIT)* (Abbottabad, Pakistan, 2011), pp. 287–292
15. M. Saleem, G.A. DiCaro, M. Farooq, Swarm intelligence based routing protocol for wireless sensor networks: survey and future directions. Inf. Sci. **181**, 4597–4624 (2011)
16. V. Raghavendran, N. Satish, P. Varma, Intelligent routing techniques for mobile ad hoc networks using swarm intelligence. I.J. Intell. Syst. Appl. **01**, 81–89 (2013)
17. S. Sachan, M. Vats, A. Mishra, S. Choudhary, Comparative analysis of clustering algorithm for wireless sensor networks, in *Intelligent Computing in Engineering*, ed. by V. Solanki, M. Hoang, Z. Lu, P. Pattnaik. Advances in Intelligent Systems and Computing, vol. 1125 (Springer, Singapore, 2020), pp. 63–71
18. N. Jabeur, A firefly-inspired micro and macro clustering approach for wireless sensor networks, in *International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2016)*, Procedia Computer Science, vol. 98 (2016), pp. 132–139
19. S. Kumar, M.S. Gaur, Call Admission control in mobile multimedia network using Grey Wolf optimization, in *Intelligent Computing in Engineering*, ed. by V. Solanki, M. Hoang, Z. Lu, P. Pattnaik. Advances in Intelligent Systems and Computing, vol. 1125. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-2780-7_27
20. N.A. Latiff, C. Tsimenidis, B. Sharif, Energy aware clustering for wireless sensor networks using particle swarm optimization, in *The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '07)* (Athens, Greece, 2007), pp. 1–5
21. X. Yang, *Nature-Inspired Metaheuristic Algorithms*, 2nd edn. Luniver Press, UK (2008)

Security Resilient Smart Applications

Securing Cyber-Resilience in Healthcare Sector

Pankaj Kumar, Amit Singh, and Aritro Sengupta

1 Introduction

In recent years, we have seen a surge in cybersecurity incidents in the healthcare industry. These incidents mainly include ransomware attacks, malware infections, theft of patient data, and selling of the patient data in exchange for bitcoins or other monetary benefits. In the present scenario, the healthcare industry is understandably busy, caring for COVID-19 patients. Taking advantage of this situation, cybercriminals are trying to disrupt healthcare provider's systems and access sensitive medical records.

World Health Organization, United States Department of Health and Human Services, and UK-based Hammersmith Medicines Research facility have fought off cyberattacks recently. Other key healthcare organizations such as Medtronic, Fujifilm, Philips, Johnson and Johnson, GE Healthcare, and Siemens Healthineers [1–4] have also dwarfed many attempts to steal millions of medical records. Medical records contain valuable and sensitive personal data, including personal health records, ID numbers, addresses, contact numbers, and much more.

However, medical data records are not the only target in the healthcare domain. Wireless sensors network, Implantable Medical Devices (IMDs), medical imaging devices, and IT systems and processes in the hospital are the major target for cyber-attacks. A report published by Greenbone networks [5] reveals that the WannaCry wave in May 2017 affected the National Health Service (NHS) in the UK. The ransomware encrypted data on numerous computers of the NHS. To do this, the attacker used a security gap in Windows systems. 81 of the 236 trusts were affected and 6912 appointments had to be rescheduled, including many critical operations.

In the U.S. in January 2018, the SamSam ransomware penetrated the network of the Hancock Health Hospital in Indiana and infected some of the hospital's IT

P. Kumar (✉) · A. Singh · A. Sengupta
Ministry of Electronics and Information Technology, Government of India, New Delhi, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_17

systems. The attacker exploited open/poorly configured Remote Desktop Protocol (RDP). Hancock Health paid the attackers around $60,000 to get its systems up and running again. Cyberattacks against hospitals have also been reported in Germany. In 2016, Klinikum Arnsberg and Lukas Krankenhaus in Neuss were victims of the Locky ransomware attack. Both systems were locked, and the attacker demanded ransom to make the system running again. Finally, Lukas Krankenhaus paid the ransom about €1 million.

As per another report published by Greenbone [6], medical data of more than one twenty million patients who underwent treatment in India have been leaked. These medical data are available on the Internet for free. One of the states, Maharashtra, have been affected the most by the medical data theft, with more than 69 million images of patients available online. The report also ranked the affected countries in terms of the action taken by their respective federal governments in stopping the data leak of patients. India is at number two in the ranking after the U.S. Apart from this, in the year 2019, several CVEs and research articles have been published which focus on vulnerable medical network, file-sharing formats, and access to the medical system framework [7].

We reviewed several research papers that discussed cyberattacks, challenges, and mitigations. The literature needs to be updated to cater to the evolving threat landscape. Based on new threats and cybersecurity dimensions, new mitigation strategies need to be prepared. Healthcare industry is complex and requires involvement of manufacturers, hospitals, and end users in reducing cybersecurity risks. This paper aims to bridge this gap and cover the latest cyberattack trends, including their mitigation policies. We also discuss cybersecurity challenges faced by the healthcare industries and end users in recent years.

The structure of the rest of the paper is as follows: Sect. 2 provides a detailed overview of a typical healthcare system and discusses its components that are vulnerable to cyberattacks. In Sect. 3, we explore different cyberattacks and vulnerabilities related to healthcare systems (implantable medical devices, wireless networks, data storage servers, hospital management systems) and measures to mitigate weaknesses. In Sect. 4, we discuss challenges and different risks related to cybersecurity. In Sect. 5, we discuss future directions and conclude the paper.

2 An Overview of a Typical Healthcare System and Its Major Components

A variety of network-connected devices are in use in the healthcare system. These devices vary from IoT-based hardware to a software-based hospital management system. In this section, we have discussed the popularly used devices and technologies used in the healthcare system.

2.1 Wireless Implantable Medical Devices (IMDs)

Implantable Medical Devices (IMDs) are electronic devices or artificial tissues that are implanted inside the body or on the surface of the skin of a medical patient.

These IMDs are linked to various communication networks which are known as “telemetry”. These devices are aimed to provide more sophisticated computing competence. Medical representatives can access the implanted devices and control or configure them remotely. This has made the implants more intelligent and granted autonomy in controlling the health parameters of a patient. [8, 9]. The most common IMD devices include pacemaker devices, neurostimulators, drug delivery systems, biosensors, etc. The various IMDs are shown in Fig. 1.

Implantable cardioverter defibrillators (ICDs) and cardiac resynchronization therapy defibrillators (CRT-Ds) are two widely used **implantable pacemaker devices** [9, 10]. The physician uses these devices to monitor the heartbeat of the patient remotely. **Brain stimulator** devices work by transmitting electrical signals of low amplitude through electrodes placed in the brain of a patient. It is used in the treatment of diseases such as Parkinson, epilepsy, depression, etc. [11]. **Drug Delivery Systems (DDS)**, a pump, and a tube are implanted under the skin of a

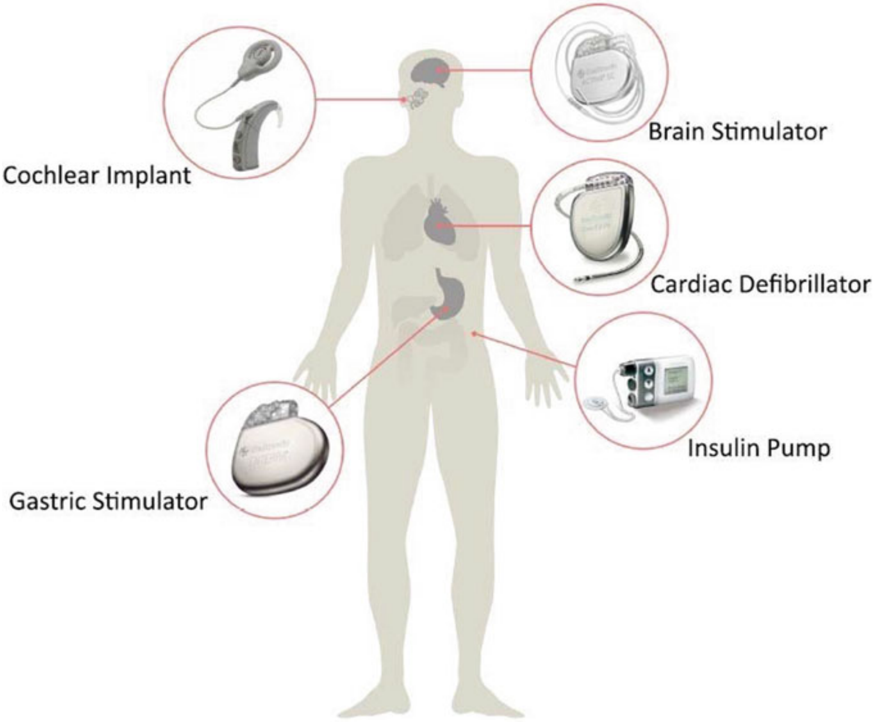


Fig. 1 Wireless implantable medical devices

medical patient. The purpose of the DDS is to supply medication to the patient in a measured, confined, and optimal way. **Biosensors are having** miniature sensors capable of sensing limited activities that are placed inside the body of a patient to monitor physiological parameters. Apart from the sensors, there exists a control node that communicates with the sensors and the controller. The sensors along with the central control node are termed as wireless biosensor networks. These IMDs are highly prone to cyberattacks as they are controlled through wireless network systems.

2.2 Medical Imaging Devices

These include devices that record medical images of the patient. For example, radiology devices that have imaging devices such as radiography, ultrasound, computed tomography (CT), nuclear medicine (positron emission tomography), and magnetic resonance imaging (MRI) which are used to diagnose or treat diseases. These machines record the medical images of the part of the body. The recorded image files are stored at the PACS/RIS server.

These devices are highly prone to cyberattacks. The medical images of patients are of high value to cybercriminals and they are selling it in the darknet at a towering price. Due to this, medical imaging devices are highly susceptible and are at the risk of being attacked by cybercriminals. In addition to the concern, most of the systems that are connected to these machines run outdated software versions that are vulnerable to various exploits. An attacker may use this loophole to exploit the vulnerability and gain access to the system.

2.3 Data Storage Server

These include the Picture Archiving and Communication System (PACS) server and Radiology Information System (RIS) server that store the medical image files of the patient. PACS is an Ethernet-based network which involves a server. The server receives scanned images from the imaging devices connected in the network, stores the images in the database for retrieval at a later point of time, and fetches the images for radiologists to analyze and prescribe. These support imaging modalities such as X-Ray, CT scan, MRIs, etc. [12, 13]. DICOM stands for Digital Imaging and Communications in Medicine and is a very old file format that is used for storing and sharing medical images. A DICOM viewer is used to view these files. A workflow diagram is given in Fig. 2.

These systems are responsible for collecting and storing sensitive data. These systems comprise a large number of software and hardware which are embedded in nature. Hence, if the systems are not patched from time to time, attackers may target these systems to exploit and gain access to the affected systems.

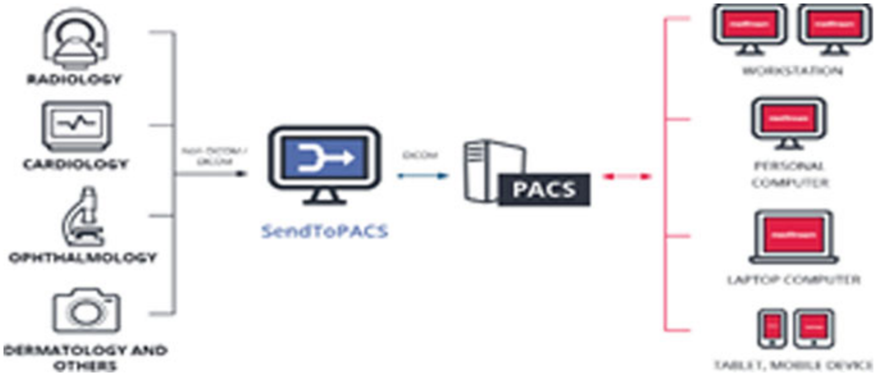


Fig. 2 PACS to DICOM workflow [14]

2.4 Hospital Management Network

As we know that hospitals have to collect patient's general information along with patients' medicine prescriptions, previous examination results such as X-Ray images, patient's documents of sterilization of surgical instruments, and other information about the stay. With the increasing number of patients, it is tedious and practically infeasible to store and maintain these data manually. To ease this, hospital management uses a dedicated software to store and manage these data. At the backend of the software, the storage servers (like SQL server) are connected to store the data. For example, patient management systems (PMS) are commonly used for admission and administration. Hospital information systems (HIS) support administrative processes in the hospital, such as in the areas of billing, controlling, order management, and care documentation. Radiology information systems (RIS) are used in radiology. These softwares are often found to be outdated as hospital managements fail to update the software patches on a routine basis. As a result, the vulnerabilities in the outdated software may be exploited by the cybercriminals, and subsequently they can get access to the patient's information. The information has enormous value in the black-market such as Darknet.

Cybercriminals have been using various types of cyberattacks such as DDoS, man-in-the-middle (MITM) attack, SQL injection, malicious code injection, phishing, ransomware, etc. to compromise integrity of healthcare devices and gain access to the systems. **DoS attack** is used to disrupt service and prevent users from getting access to service. This type of attack is done by flooding devices with unwanted and irrelevant requests. An attack where an attacker intercepts and alters the data sent between two nodes is known as **MITM** [15]. This is used to modify and gather data that breaches confidentiality. **SQL** is used by websites to manage their databases. SQL vulnerability may be exploited by an attacker to access the databases of healthcare organizations. In ransomware attacks, the attackers shut down the healthcare systems that may arise a severe issue for monitoring and caring/treatment of the patients. In

Table 1 Types of cyberattacks and affected healthcare systems

Types of attack	IMDs	Medical imaging devices	Data storage server	Hospital management network
Denial of service	✓			✓
MITM	✓		✓	✓
SQL injections exploit			✓	✓
Remote code execution and malicious software	✓	✓	✓	✓
Open SSH vulnerability	✓	✓	✓	
Ransomware	✓	✓	✓	✓
Phishing			✓	✓

Table 1, we have categorized different types of cyberattacks and relate to affected healthcare systems.

3 Recent Case Studies of Cyberattacks in Healthcare Systems

Currently, we are facing a global healthcare sector battle due to the ongoing COVID-19 pandemic. This has surged the number of cyberattacks in the healthcare sector. In this section, we shall discuss case studies related to recent cyberattacks observed in the healthcare domain (Table 2).

In coming sections, we shall also address vulnerabilities related to healthcare systems (implantable medical devices, medical image devices, data storage servers, hospital management systems) and steps to its mitigation.

3.1 Cyberattacks on Implantable Medical Devices

IMDs as discussed in Sect. 2.1 use wireless telemetry protocol, which enables them to communicate with each other and allows programmers and monitoring devices to do allotted tasks. The wireless telemetry protocol does not use basic security features such as encryption, authentication, or authorization. So this protocol has cybersecurity vulnerabilities. These vulnerabilities, if exploited, could allow an unauthorized individual to access and possibly manipulate the functioning of an implantable device, home-based monitor, or programmer. In recent years, multiple vulnerabilities

Table 2 Recent cyberattacks case studies

Organization	Type of breach	Month and year	No. of records	Breached devices/severs	Nature of lost data
Brno University Hospital, Czech Republic [16]	Ransomware	March 2020	20,000–30,000	IT networks	Name, date of birth, medical identification, address, and email
US Dept. of Health and Human Services	DDoS attack	March 2020	40,000–50,000	Network server	User credentials, medical information
World Health Organization [16]	Malicious code injection	April 2020	–	Email server	Login ID and password of users
Dominion National Insurer [17]	Information disclosure	April 2019	200,000	Network sever	Name, date of birth, medical identification
UK Healthcare Trust [17]	WannaCry attack	2017	30,000–35,000	Computer system	Login ID and password of systems

have been found in the IMDs. A summary of medical device vulnerabilities, along with their severity and impact, is shown in Table 3.

Steps to Mitigate

- Increase awareness among all stakeholders, including medical physicians and clinical IT teams about current and potential medical device vulnerabilities.
- Restrict unauthorized access to the network and networked medical devices through the implementation of AAA (authentication, authorization, and accounting) systems.
- An external device may be used that acts as a proxy between the device programmer and IMDs. Also, this proxy will perform the authentication process on behalf of the IMD. The proxy restricts the messages to/from the IMD and prevents attackers from decrypting them, while IMDs being able to decode them successfully [21].
- A pairing protocol may be enforced between the device programmer and medical devices to authenticate the communication. In this system, there is no need to share any prior key/password.
- A cryptographic key exchange may be used between the programmer and the medical devices through an auxiliary or Out-Of-Band (OOB) channel to authenticate the communication [22].
- Implement appropriate ACLs (access control lists) for IP addresses and/or port filters.

Table 3 Medical devices vulnerabilities and its impact

Medical devices	Vulnerability	Severity	Vendor	CVE	Vulnerability impact
Cardiac pacemakers, implantable neurostimulators, and implantable infusion pumps	Dropbear SSH server <2016.72 multiple vulnerabilities	Critical	GE healthcare, Animas, Bionet and Roche	CVE-2016-7407 [18]	It can disclose sensitive information held on the database server
MRI scanners and X-ray machines	Microsoft windows SMB server (4013389) security update (un-credentialed check) [19]	Critical	Carefusion and ReliOn	CVE-2017-0143** and CVE-2017-0144** [20]	Attackers can execute remote code on susceptible machines and run commands and gain access to the local machine
X-Ray machines	Denial of service (DoS)	High	Fujifilm	CVE-2019-10948 [20]	It allows an attacker to flood a network server with enormous traffic that requires a manual reboot of the device
CT scanners	OpenSSH vulnerability	High	Philips	CVE-2018-8853 [20]	It allows attackers to bypass authentication and gain access to sensitive patient information with the device
Blood gas analyzers	Remote code execution	High	Siemens Healthineers	CVE-2018-4845 [18]	Remote attackers access to the "Remote View" feature, may be able to gain privileges of the system

(continued)

Table 3 (continued)

Medical devices	Vulnerability	Severity	Vendor	CVE	Vulnerability impact
PET/CT and SPECT/CT medical imaging products	Remote code execution	High	Siemens Healthineers	CVE-2015-1635 [20]	It can access remotely and execute an arbitrary malicious program and gain access

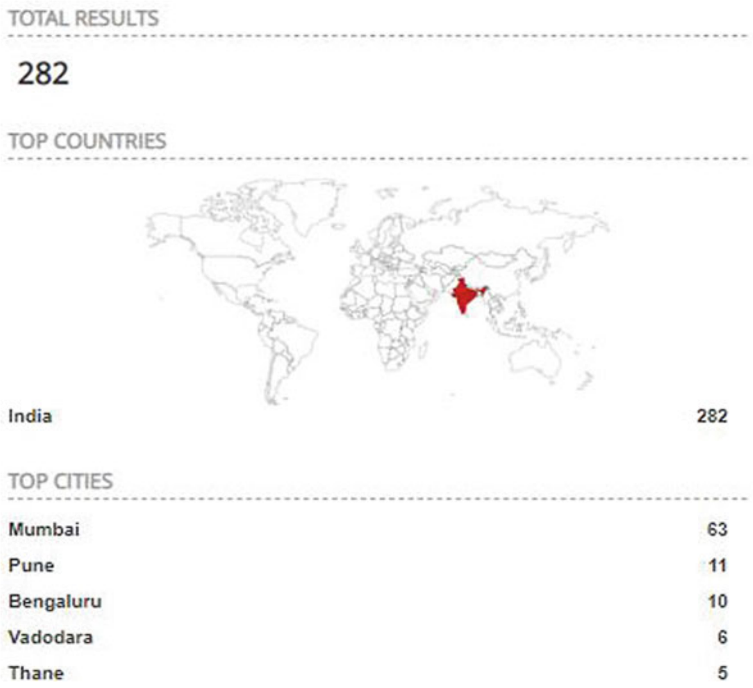
- Medical devices should be designed in such a way that they have good communication competence and be more secure in a network system. The communication system should not depend only on external mechanisms like firewalls, intrusion prevention systems, or any other third-party solutions.

3.2 Cyberattacks on PACS Server

As on date 13.08.2020, there are 282 PACS servers available in India as per open-source intelligence (OSINT) feed as shown in Fig. 3.

Many systems are available without any restrictions or any access control mechanisms.
PACS servers allow direct access to patient data via DICOM viewer. This access is possible without authentication, and in most of the servers, the data is transmitted via HTTP, i.e., unencrypted in plain text. This may be targeted to access and alter a patient's DICOM imagery. In addition to this, PACS are not directly connected to the Internet but connected via health care's internal network. This may allow an attacker to exploit vulnerabilities through social engineering attacks, insider attacks, etc. [23]. A workflow of tempering the medical imagery between the investigation and diagnosis stage has been shown in Fig. 4.
Restriction of Malicious HL7 messages in the network: In a PACS environment, DICOM communicates using HL7 version messages. These are used to keep consistent information through all hospital information systems, RIS, and PACS server. Information of patients (like name, hospital ID, address, etc.) can be continuously updated without human intervention using HL7 messages across multiple systems. Unfortunately, the HL7 message protocol does not provide any way to prevent a malicious attack on the messages. An attacker can observe the network traffic of HL7 messages, learn about patient data, or modify the genuine messages during transmission [24].

A summary of the PACS server and DICOM file vulnerabilities along with its severity and impact is shown in Table 4.



TOTAL RESULTS

282

TOP COUNTRIES

India	282

TOP CITIES

Mumbai	63
Pune	11
Bengaluru	10
Vadodara	6
Thane	5

Fig. 3 PACS server available in India as on date 13.08.2020.

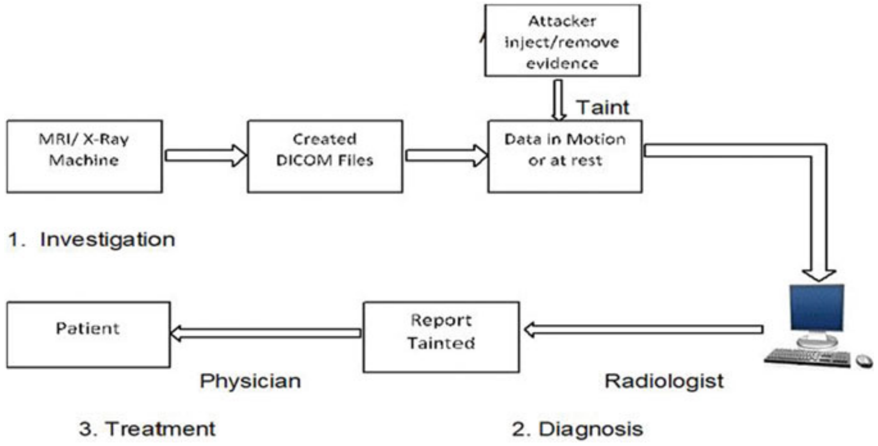


Fig. 4 Medical imagery between the investigation and diagnosis stages, both the radiologist and physician believe the fallacy set by the attacker

Table 4 PACS/RIS server and DICOM file vulnerabilities and its impact

Medical devices	Vulnerability	Severity	Vendor/organization	CVE	Vulnerability impact
PACS workstation 4.0 and 4.0.1	Information disclosure	High	GE Healthcare	CVE-2012-6694 and CVE-2012-6693 [20]	It has a password of 2charGE for the geservice account, which has unspecified impact and attack vectors related to TimbuktuPro
DICOM Part 10 file format	Portable executable (PE) malware	High	NEMA DICOM Standard 1995	CVE-2019-11687 [20]	It can execute a malicious file that is injected in the DICOM Part 10 File Format and manipulate the image stored in the PACS
Medical imaging system	Remote code execution	High	GE Healthcare	CVE-2017-14008 [18]	This may allow an attacker to bypass authentication and gain access

Steps to Mitigate

To prevent the injection of malware at the stage of the data-in-motion, the network administrator should encrypt the data communicated between the PACS network hosts using proper TLS certificate. To secure the data-at-rest, anti-virus software and servers running on end workstations should be regularly updated. Also, the exposure of the PACS server to the Internet must be restricted.

To prevent the spreading of malware embedded in the DICOM files through DICOM viewer, the vendors should test their applications through certified application tools at regular intervals. These application tools automatically update products based on third-party libraries when vulnerabilities become public, and employ, where possible, bitstream validators that identify distorted documents and restrict their processing and display.

To prevent malicious manipulation of medical images [23], digital signatures can be used to assure that any changes of an image cannot remain undetected at any point after image creation.

To protect the HL7 message exchange, TLS can be used to encrypt network traffic between the endpoints and the PACS server. This will thwart an attacker from analyzing the network traffic. Also, an MITM [22] attack can be averted if a bidirectional certificate exchange policy is implemented.

3.3 Compromising the Hospital Network

This can occur via access to a LAN port of the cabled network which is unprotected or misconfigured switches/routers, or if the encryption of the wireless network (WLAN) is compromised. After successfully compromising the network, the attacker intercepts the network traffic and analyzes the traffic through the Wireshark. Also, the attacker can learn about the network structure, available systems on the network, unencrypted user credentials, and the network protocols used. This enables the attacker unauthorized access to the network and gets a patient's sensitive information such as personal data, including personal health records, ID numbers, address, contact number, and much more. The hospital management system vulnerabilities, along with its severity and impact, are shown in Table 5.

Table 5 Hospital management system vulnerabilities and its impact

Management system	Vulnerability	Severity	Vendor/organization	CVE	Vulnerability impact
Monitoring systems, telemetry server, clinical information systems	Open SSH	Critical	GE Healthcare, ApexPro, Carescape	CVE-2020-6962 [18]	It can allow an attacker to obtain access to the SSH private key in configuration files
OpenClinic GA	Authentication bypass using an alternate path or channel	Critical	A product of open-source collaboration on Source Forge	CVE-2020-14485 [20]	It has bypass client-side access controls and may allow execution of admin functions such as SQL queries
Hospital management system in PHP v4.0	SQL injection	High	PHP Gurukul	CVE-2020-5192 [18]	It allows for the application's database and information to be compromised

To prevent the hospital network from cyberattack, we may take the following technical measures:

- Configure the network switches so that only the systems with known MAC address or previously bound MAC (i.e., serial numbers of network interface controller) address can connect [25].
- Switch off all unused ports. If required in the future, the ports may be opened by the administrator.
- Wireless networks should be reviewed and updated regularly. Also, the configuration must be audited periodically.
- Firewalls, routers, and network segmentation should be used to protect the systems that may be more susceptible to attacks.

4 Challenges and Risks Related to the Cybersecurity

- There are several cybersecurity challenges in evolving and expanding healthcare networks, inclusive of medical devices.
- The high cost of medical devices.
- Lack of skills and knowledge about how to use healthcare devices in a wireless network.
- In the market, there are a variety of medical devices and every medical device has its configuration and settings that may be a problem for medical practitioners.
- Lack of universal manufacturing standards and immaturity of existing standards.
- There should be a National level Medical Policy for data security and privacy issues.
- Hospital management should be held responsible for any data leakage as per the provisions of any regulation like the General Data Protection Regulation (GDPR).
- Non-updation of software by healthcare providers and medical practitioners.
- Lack of investment in technology, research, and personnel [26].

Safety risk of Patient

- Device function or performance gets changed that results in misdiagnosis or treatment error of the patient.
- Compromise of sensitive patient data like medical results or device-specific data like heartbeat rate.

Risks related to care delivery

- Hospital operations disruption.
- Reduced ability to properly deliver care.

Risks related to privacy

- Loss of critical information (patient healthcare information, credentials).
- Breach of data.
- Intellectual property (research, design, and trials data).

Table 6 Mitigation matrix for different devices in healthcare systems

Steps to mitigate	IMDs	Medical imaging devices	Data storage server	Hospital management network
Restrict unauthorized access	✓	✓	✓	✓
Pairing protocol between devices	✓	✓		
Cryptographic key exchange	✓	✓		
Disable unused ports			✓	✓
Digital signatures	✓		✓	
Updation of software	✓	✓	✓	✓
Isolation and segmentation of network			✓	✓
Use of security devices such as firewalls, IPS			✓	✓
Risk assessment and threat modeling	✓	✓	✓	✓

Risks related to finance

- Loss of reputation of organization.
- Revenue loss.
- Impact on corporate goodwill and stock value.

In Table 6, we have tabularized the mitigation matrix for different devices in healthcare systems.

5 Conclusion and Future Work

In the healthcare system, the safety of the patient will be a priority over cybersecurity needs. Closing the gap between the two objectives is the primary challenge. Minimizing data compromise and ensuring patient safety while being reactive to the cybersecurity threat environment are today's needs. Healthcare devices, wireless networks, and patient care management systems are now a vital part of healthcare networks. Thus, their security and privacy should be an essential component of cybersecurity defense. More coordination between the network administrative professionals and medical physicists, as well as medical device makers and vendors, are required. Also, input from cybersecurity experts and government agencies at regular intervals are required. Cybersecurity vulnerabilities related to healthcare devices are very similar to any other system connected over the network. The need to mainstream the cybersecurity protection policy of healthcare devices is more visible because of the potential detrimental impact on patient safety after the exploitation of cybersecurity vulnerabilities of healthcare devices. This draws the difference between the importance of securing healthcare devices and other network environments. Given the current lack of governance and national level policy of networked medical devices, amalgamated with risk management, lack of knowledge of the security risks, reliance on medical device regulatory approval, and lack of preparedness by organizations to manage the risks, the need to protect the healthcare cybersecurity system is essential. While jurisdictional regulation has been the drive to enforce increased protection through privacy and security rules for medical data by a concerned government agency, the compliance to the same does not mean adequate security. Data breach regulation laws and compulsory reporting to government agencies have resulted in a proactive approach to secure cyberspace in the healthcare environment. To guarantee the protection of the healthcare system connected in a network, a coordinated, proactive approach including standard cybersecurity control and assessment, along with specific medical device data and workflow considerations, is needed.

References

1. Philips ultrasound authentication bypass vulnerability report published by NHS Digital. (2020)
2. Siemens security advisory by Siemens Product CERT 2019. (2020)
3. https://global.medtronic.com/xg-en/product-security/security-bulletins/conexus.html. Accessed 4 Jun 2020
4. K. Sheridan, A report: severe vulnerabilities discovered in GE medical devices. (2020)
5. Report published by Greenbone Sustainable Resilience: a German cyber security firm. (2018)
6. A report on medical data leak published by Greenbone.: Sustainable Resilience. (2019)
7. A follow report on medical data leak published by Greenbone: Sustainable Resilience (2019)
8. E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, H. Chen, Assessing medical device vulnerabilities on the Internet of Things, in *IEEE International Conference on Intelligence and Security Informatics (ISI)* (2017)
9. D.J. Slotwiner, T.F. Deering, K. Fu, A.M. Russo, M.N. Walsh, G.F. Van Hare, Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians, in *Proceedings of the Heart Rhythm Society's Leadership Summit*
10. E. Marin, On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them, in *ACSAC'16* (Los Angeles, CA, USA, 2016)
11. C. Camara, P. Peris-Lopez, J.E. Tapiadora, Security and privacy issues in implantable medical devices: a comprehensive survey. J. Biomed. Inf. **55**, 272–289 (2015)
12. D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark et al., Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-ower defenses, in *IEEE Symposium on Security and Privacy* (2008)
13. Z. Wang, P. Ma, X. Zou, J. Zhang, T. Yang, Security of medical cyber-physical systems: an empirical study on imaging devices, in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (2020)

14. https://www.softneta.com/wp-content/uploads/2019/02/SendToPACS-converting-files-to-dicom-workflow.png
15. M. Burhan, R.A. Rehman, B. Khan, B.-S. Kim, IoT elements, layered architectures and security issues: a comprehensive survey. Sensors (2018)
16. https://www.medicaldevice-network.com/features/cyberattacks-healthcare-covid-19/. Accessed 13 Sep 2020
17. L. Coventry, D. Branley, Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. 48–52 (2018). Maturitas. ISSN 0378-5122
18. https://nvd.nist.gov/vuln/detail. Accessed 4 Aug 2020
19. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010. Accessed 11 Oct 2017
20. https://cve.mitre.org/. Accessed 4 Sep 2020
21. E. Marin, D. Singelée, B. Yang, V. Volski, G.A.E. Vandenbosch, B. Nuttin, B. Preneel, Securing wireless neurostimulators, in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy—CODASPY'18* (2018)
22. A.I. Newaz, A.K. Sikder, M.A. Rahman, A survey on security and privacy issues in modern healthcare systems, attacks and defenses. ACM Health **1** (2020)
23. M. Eichelberg, K. Kleber, M. Kämmerer, Cybersecurity challenges for PACS and medical imaging. Acad. Radiol. **27**(8), 1126–1139 (2020)
24. L. Pycroft, T.Z. Aziz, Security of implantable medical devices with wireless connections: the dangers of cyber-attacks. Exp. Rev. Med. Devices **15**(6), 403–406, (2018)
25. P. Williams, A. Woodward, Cyber security vulnerabilities in medical devices: a complex environment and multifaceted Problem. Med. Devices Evid. Res. (Auckl) **8**, 305–316 (2015)
26. F. Luh, Y. Yen, Cybersecurity in science and medicine: threats and challenges. TIBTEC **1902** (2020)

Applications of Identity-Based Cryptography in Smart Home and Healthcare: A Recent Review

Soumya Garg, Swagat Nayak, A. B. Bavani Sankar, and Soumyadev Maity

1 Introduction

The basic knowledge that the Internet of Things shares with us is the connection of trillions of custom devices in every corner of this world that have a connection with the Internet and at the same time performing some or the other activity. The Internet of Things is all about the idea to collect different objects and adding different sensors to them, helping in the advancement of the technology and adding up the feature of interaction and the connection with human beings and their needs. Almost any physical object may be converted to an IoT device if it can be linked to the Internet to communicate information and to be controlled by humans. An air conditioner which can be operated via a small software application, a temperature sensor, or a smartwatch everything is sectioned under the Internet of Things. IoT is playing a remarkable role in applications like smart home, transportation, healthcare, industrial automation, etc., improving the quality of our lives and the world economy.

Home automation is one of the major products that has found its place in the world because of IoT. Most homes have been stocked with a number of IoT devices like television, air conditioner, locks, temperature sensors, security cameras, etc. The interconnection of these devices works via HAN, i.e., home area network and interaction of all these devices over this network can be done using an application in the owner's smartphone. However, just as these devices have revolutionized home living, they have also given rise to new complications for home security. Without

S. Garg (✉) · S. Nayak · A. B. Bavani Sankar · S. Maity
Indian Institute of Information Technology Allahabad, Prayagraj, India
e-mail: mit2019083@iiita.ac.in

A. B. Bavani Sankar
e-mail: mit2018015@iiita.ac.in

S. Maity
e-mail: soumyadev@iiita.ac.in

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_18

encrypted message exchange and authentication, an adversary can eavesdrop and analyze the owner's daily routine resulting in the replaying of an attack like unlocking a door.

IoT is a boon for multiple industries. One of the industries among them is the healthcare industry as IoT has a very impactful role in maintaining good health of the patient and in sharing the workload of the medical professionals. When it comes to the human body it becomes very complicated to track down its inner workings, but IoT enables connection and tracking of even the most difficult to observe activities with a few good sensors, preventing many fatal diseases like cardiac arrest. These benefits though come at the cost of security drawbacks. Due to Internet connectivity and resource constraints, there is always a risk of the system being compromised by some adversary which may result in the exposure of patients' health information which might be very harmful. Thus, security is a major concern that must be taken care of.

TLS is one of the protocols that has substantiated secure communication from one end to the other [1]. According to RFC 8446 [2], TLS uses PKI to secure connections over the Internet. In the aforementioned environment, like healthcare and smart homes, TLS would make IoT devices store public key certificates of every other entity with whom it wants to communicate. These certificates are issued by a trusted third party called certification authority or CA which proves the authenticity of the entity. The disadvantages of using PKI in IoT are

- Huge storage overhead due to certificate management in frugal IoT nodes.
- Communication overhead while issuing, updating, and/or revoking certificates.
- Computational cost involved in the processing of certificates as it consumes processor capacity.
- Requirement of online connectivity with certification authority.

This problem can be overcome if one can receive an authentic public key without certificates. Hence, the concept of IBC, i.e., identity-based cryptography is introduced in [3] where the public key is an individual or organization's identity. PKG is a private key generator which is one of the trusted third-party key generators which can be used with this context. When a user registers to a network, it submits its identity to the PKG, and PKG verifies the user. If the user is legitimate, only then, its private key is generated by the PKG and is sent through a secure channel to the user. If A wants to securely communicate to B, then A encrypts the message using B's identity which can only be decrypted by the private key of B. In IoT devices, the public key can be a device's MAC address, and PKG can be any trusted third party like a smart device service provider for a particular hospital or smart home.

The remainder of the survey is organized as follows: literature review is performed in Sect. 2, security challenges and constraints in IoT are described in Sect. 3, some preliminary information is recalled in Sect. 4, followed by the conclusion in Sect. 5.

2 Literature Review

In 1984, Shamir was the first one to introduce the concept of identity-based cryptography [3], he proposed signature and encryption based on RSA algorithm but the security of encryption remained a problem. Then in 2001 Boneh and Franklin gave the solution for the security of ID-based cryptography by introducing pairing in IBC. They proposed IBE scheme using Weil pairing on elliptic curves [4]. But this scheme too have drawback of Key-Escrow problem. There are several schemes which were proposed by different authors to solve this problem which are discussed below.

In 2015, Rune Hylsberg Jacobsen et al. proposed an optimized authentication mechanism for resource-constrained devices by establishing a secure session key between two HAN devices. It optimizes the bootstrapping phase of wireless devices in home area network based on IBC [5]. The proposed scheme uses two private keys and two symmetric keys where symmetric keys are used to encrypt and decrypt the message containing session keys. It uses AES-128-bit symmetric keys. Using this long symmetric key may put high computational cost on IoT devices. According to NIST 128-bit keys should keep data safe until 2030. However, in the performance analysis, it was found that it consumes approximately 48% higher energy than any previous scheme but comparatively it provides high security and a smaller number of steps in key exchange protocol.

In 2016, Sanaah Al Salami et al. gave an idea of a lightweight encryption scheme to provide confidentiality with high-level efficiency to save computational cost, power consumption, and communication and storage overhead for resource-constrained devices in smart homes [6]. This scheme adopts stateful IBE to provide flexibility in public key management and remove the dependency on public key infrastructure. The proposed scheme is based on two sub-algorithms one to encrypt the session key and one to encrypt and decrypt the exchanged messages through the shared symmetric session key. The prime objective of this scheme is to provide confidentiality, but it doesn't provide any authentication between the sender and receiver. The operations performed by the sender and receiver side are a little bit heavy for IoT devices due to the ephemeral exponent of Diffie–Hellman key performed by the sender side. However, the proposed scheme seems feeble because of the use of symmetric session keys for encryption.

In 2016, Shuo Chen et al. proposed a scheme employing identity-based cryptography [7] to secure machine-to-machine (M2M) communication in case the M2M service provider (MSP) is compromised, by only storing partial secrets, unlike previous security solutions, in the MSP. Another goal of their proposal was to save energy and bandwidth.

Also in [8], Sriram Sankaran et al. develop a lightweight security framework for IoTs based on IBC and demonstrate lower overhead than public key cryptography by analyzing and comparing the energy consumed for encryption and decryption in different popular cryptographic techniques.

In 2017, Yosef Ashibani et al. proposed a security technique known as signcryption based on IBC which provides authentication, confidentiality, and integrity combining the signature and encryption scheme in one step which found out to be more efficient than performing encryption and signature separately [9]. Here the protocol is based on a local server (trusted third party) which is responsible for the new devices registration and to provide all required public, private secrets for communication between the smart home devices. This protocol found out to be better in terms of computational cost and ciphertext size as compared to any other scheme. But it doesn't provide any clarity on how to protect local servers if it joins the communication process. Here we have to perform signcryption every time when an end user or any device tries to communicate with each other. As the protocol is realized with bilinear pairing operations which are rarer and significantly slow compared to any other symmetric operation [10], if the number of devices increases then each time performing signcryption and costly map-to-point for communication will put a huge computational and storage overhead to the IoT devices. Nevertheless, the main drawback of the trusted third party is Key-Escrow problem. If TTP is compromised, then the TTP will disclose private keys of all the devices in the smart home which will help the adversary to have full control over the smart home appliances.

In 2017, Bayu Anggorojati et al. gave an idea of security scheme based on identity-based cryptography in federated IoT systems [11]. It solves the Key-Escrow problem of Boneh and Franklin's identity-based encryption [4] by using V-IBE, i.e., variant of identity-based encryption introduced by Zhaohui Cheng et al. [12] with a slight modification. Here is the security proof of this algorithm.

$$\begin{aligned}
g_{ID}^{r} &= e(Q_{ID}, P_{pub} + N_{id})^{r} \\
&= e(Q_{ID}, s.P + t.P)^{r} \\
&= e(Q_{ID}, P)^{((s+t)r)} \\
&= e(s.Q_{ID} + t.Q_{ID}, r.P) \\
&= e(d_{ID} + t.Q_{ID}, U).
\end{aligned}$$

One who knows both d_{ID}(private key) and "t" (sub-private key) can decrypt the message. If PKG is compromised, adversary will only have d_{ID}. With d_{ID} he can't decrypt the message. He also needs "t". But if adversary physically captures IoT node and there is no such method described as to how the sub-private key "t" is stored in the devices. Therefore, if adversary physically captures it, he can get "t" also and the authentication mechanism described in this paper will also fail, because public keys and sub-private key of device are used to encrypt the message and hence he will be able to decrypt any message which is communicated with that physically captured IoT device. Here computational cost also increases due to bilinear operations, modular exponentiation, map-to-point and point multiplication operations. Energy consumption also increases, keeping in mind that increase in computational and communication is an overhead in IoT devices. One more drawback is that PKG needs to be online every time since private key is exchanged via online mode. The practical feasibility and performance of this protocol compared to any other protocol is ill-defined as it isn't implemented in the actual IoT system.

In 2018, Bayu Anggorojati et al. used the same security scheme to secure IoT-based healthcare systems by providing a key management system for mutual authentication and secret key agreement in [13].

In [10, 14, 15], different privacy-preserving schemes based on IBC have been proposed to maintain the privacy and sensitivity of patients exchanged data in E-healthcare systems.

In 2018, Rihab Boussada et al. introduced KE-IBE scheme in healthcare area which relies on Identity-Based Cryptography (IBC). It resolves the Key-Escrow problem by allowing the Key generation center or KGC to generate only a partial private key for a given entity [15]. The procedure of encryption of the health information is same as that in [10]. But here session key is encrypted by KE-IBE scheme rather than simple IBE encryption thus resolving the Key-Escrow problem. In this scheme, communication overhead is comparatively less as compared to the scheme proposed in [11]. Energy consumption is also comparatively low as compared to [11]. However, bilinear map is used twice. And as we know bilinear map is eight times more time-consuming than point multiplication and modular exponentiation. Thus, resulting in increase of the encryption cost. Encryption cost of this scheme is more than Boneh–Franklin IBE scheme but comparatively less than [3] because it uses the implementation presented in [16].

In 2018, Rihab Boussada et al. proposed another PKE-IBE scheme that provided both communication security and information security free off Key-Escrow problem [14]. Earlier in 2017, [10] he proposed a scheme that provided both communication security and information security but vulnerable to Key-Escrow problem. In 2018 only, [15] he proposed a scheme KE-IBE that provided information security without Key-Escrow problem but didn't provide communication security. Therefore, he proposed a scheme that overcome the problems of individual schemes proposed by him earlier.

In 2018, Yandong Xia et al. proposed a novel signcryption scheme to secure patients' healthcare records in [17]. Signcryption is leveraged to achieve identity authentication in the same time as traditional protocols, but with reduced computation and communication cost. In this scheme, biometric key is used as identity to construct public key. Also, the key generation center (KGC) does not generate the full private key corresponding to the identity of the user. Instead, the KGC constructs a partial private key with the received identity, its master private key, and its master public key. The user then constructs their public key and full private key with the received partial key and a random number, after which a fuzzy extraction algorithm generates a biometric key which is sent to the medical center via secret channel. Apart from avoiding the Key-Escrow problem, this paper also tackles non-repudiation by introducing a biological key.

In 2019, M. Mazhar Rathore et al. proposed a scheme which uses all smart devices in a particular area like smart home to generate the private keys in a distributed manner thus preventing the risks associated with the centralized IBC [18]. Even if admin is physically compromised then also all the remaining private keys are unknown to adversary because private share of each device's IBC key is by no means revealed to other party. As a result, even if one or more devices are compromised, the adversary can't compromise the private keys of the honest devices. This scheme solves the problem which might arise in scheme proposed in [11]. Here in some protocols a malicious intruder can send many half key messages to admin pretending that they are from different sources. Admin then needs to calculate full keys which keeps admin so busy that it denies to respond to any legitimate messages, hence resulting in DoS attack.

In 2020, Yudi Zhang et al. tackle the problem of preserving privacy and confidentiality in Wireless Body Area Networks (WBANs) by proposing an efficient obfuscation for identity-based signatures in WBANs [19]. They employ the identity-based signature scheme in the IEEE P1363 standard. Also, instead of using the sensors' computation capabilities, the mobile devices' resources are used to sign and encrypt data received from the sensors.

After analyzing different IBC schemes in smart home and healthcare, we have performed a quantitative comparison between all of them in Table 2.

2.1 Research Gap

After analyzing the above papers, we have listed out some of the major concerns related to use of IBC in IoT that needs to be taken care of.

1. There are some disadvantages of using IBC in IoT like:
   - **Key-Escrow problem**: IBC is fully reliable on the PKG, which if compromised, the adversary gets access to all the private keys. The adversary can then decrypt any message coming from any entity, which is very harmful. In most of the above papers, the researchers have tried to remove this problem.
   - **Key revocation problem**: Suppose one IoT node's private key is compromised. That key corresponds to its MAC address (identity) which has been serving as its public key. Now IoT nodes have to change their MAC address which is difficult to implement in practice.
2. Bilinear pairing is used which is not efficient in terms of cost and computation power if used more than once. As IoT nodes are limited to computational power, battery capacities, and storage resources, pairing operations will put more burden on these resource-constrained devices if used more than once.
3. After all these vulnerabilities also, IoT devices are growing very rapidly and there will be trillions of IoT devices till the end of 2020. In this case, a large number of sensor nodes and devices will continuously generate data, collect data, and will communicate with each other in a complex network.

In this case, we can adopt aggregate signature and edge computing schemes to mitigate the different challenges faced by the IoT devices to improve the performance.

In aggregate signature, instead of using conventional digital signature schemes to ensure data privacy, integrity, and authenticity of received data it combines the digital signatures of different messages into one short digital signature saving energy and improving computational power, beneficial for IoT devices.

Edge computing helps to offload the computational, communication overhead, and storage costs of centralized data centers by distributing the computational stress across the computational nodes deployed at the "edge" near to the end user distributed across the network. Due to this, it significantly reduces the reaction time and transmission cost in message exchange between the nodes and also reduces the computational and communication overhead from nodes with the limited battery life which will improve the lifetime of individual nodes along with the entire IoT system.

3 Security Challenges and Constraints in IoT

3.1 Some Security Challenges in IoT

1. **Confidentiality**: Protecting data from unauthorized users, which ensures that the information is accessible only to authorized users. Only an authorized user should be able to access and read the data.
2. **Authentication**: The assurance that the entity with which communication is taking place is the one that is claimed to be. As many entities are interconnected in IoT every entity needs to be authenticated before sharing information and data.
3. **Integrity**: The changes in information done by the authorized entity through an authorized mechanism. As in IoT devices data is exchanged between many devices it is very important to ensure that no one can tamper the data except the authorized entity during its transmission.
4. **Non-repudiation**: No entity involved in a communication can deny that the message is sent by him.
5. **Availability**: Ensuring that the service provider needed to be available anywhere and anytime for the intended service. IoT devices always need to be ready with all the available data and services whenever any service requested by any user irrespective of any situation.
6. **Privacy**: Protecting private information from malicious agents. Personal data should be protected and only accessible to authorized person to maintain client privacy.

3.2 Resource Constraints

1. **Power**: As most IoT devices are run with batteries it's our responsibility to preserve power for a prolonged battery life. Computational cost should be as little as possible for longer battery life by distributing computational costs among sensor nodes.

2. **Storage**: As most of the devices have limited memory, they are limited to RAM and flash memory compared to the other systems. To minimize it, memory space, key size, and message size should be as small as possible, and different security features must be implemented with fewer software and hardware resources. As traditional security algorithms are not memory efficient, they use large RAM which is not advisable for IoT devices. IoT devices may not have enough space to execute these algorithms. Therefore, it is advised to use lightweight algorithms instead of traditional algorithms.
3. **Computing Capacity**: Many devices are very small and have low processing and computational power. To reduce computation costs, we need to use new and efficient key management protocol with the same level of security and simpler cryptographic algorithms to work efficiently.
4. **Channel Bandwidth**: Power supplies on IoT devices are limited and need to be replaced after some time. Maximum IoT devices are restricted in terms of bandwidth. They are meant to operate with less bandwidth and prefer to operate with low frequency to conserve power and to prolong the battery life for other services.

3.3 Security Threats

IoT devices are always connected to the Internet which is always vulnerable to different kinds of attacks, and these attacks can be an internal attack or external attack, i.e., attacker might reside inside the IoT network where adversary can use malicious code to compromise the network or may use any device to launch an attack. Or the attacker might be an outsider who resides anywhere in the public network, the attacker can try to get unauthorized remote access to the IoT network to compromise the trusted devices. Some of the properties of IoT devices are discussed as follows:

1. **Lack of physical Security** In IoT architecture, different devices may be deployed in different remote areas in a scattered way and left unattended. In such case, an attacker can physically compromise the node and later they can extract sensitive information and cryptographic secrets to manipulate the system. Also by using jammer an attacker can disturb the communication protocol and can physically harm the components of IoT system which will result in DoS/DDoS attack.
2. **Dynamic Nature** An IoT device may join or leave the network, they can move from one network to another network according to their requirements, and nodes can be disconnected due to some connection failure or power failure. These features of temporary devices having to add and exiting characteristics making the network dynamic. Currently available network security models can't cope with this type of unstable network where sudden changes in network topologies take place, which is difficult to maintain.
3. **Heterogeneity** IoT system is a collection of interconnected devices aiming at connecting devices to devices, humans to devices, software to devices, and humans to

humans. The IoT system is a collection of different objects with different capabilities, complexities, and having different behavior; these devices may have different release versions and dates; and they may use different functions, protocols, and technical interfaces. So the designed protocols should be flexible and adaptable to work in a heterogeneous network.

Further attacks can be divided based on active attacks and passive attacks. Active attacks, where an attacker performs illegal activities to damage and disrupt the normal functionality of IoT devices. In passive attacks, the adversary is the authorized node in the network which performs illicit activities against the privacy of the user by eavesdropping the communication channel to gather or gain private information from a trusted IoT device without any authorized access without modifying the system. The possible security threats to smart home and IoT application are discussed as follows:

1. **DoS/DDoS Attack**: In this attack, attacker may access your IoT network and then floods the network by sending messages in bulk to diminish the capacity of the network which prevents legitimate and authorized user to get the benefits of services offered by the network. To perform DDoS, attacker may target some devices which are connected in the network by using malicious code. To avoid this type of attack, it is very important to give access to authenticated users to block and detect unauthorized access.
2. **Replay Attack**: Here attacker will try to mislead or confuse the parties involved in the communication process by sending or re-transmitting the copy of a message which was previously a part of the communication process. This type of attack threatens message freshness. To avoid this we need to verify every transmitted message by timestamp or nonce.
3. **Man-In-The-Middle Attack**: Here attacker intercepts the communication between two users to obtain the keys by making the users think that they are communicating securely with each other while the adversary sits in between them communicating with each of the parties. To prevent parties from this type of attack, they must ensure mutual authentication and the message integrity.
4. **Eavesdropping**: In this type of attack, the attacker threatens message confidentiality. The attacker listens and has access to all the information carried through the communication channel in the network without being noticed. Later the attacker can use that private information, such as node identification numbers, application-sensitive data to carry any type of attack against any node to disrupt the communication protocol. To protect data from this kind of attack, session key needs to be established between the communication parties.
5. **Impersonation Attack**: Here attacker acts as one of the legitimate parties in a communication protocol. Another party is unaware of this attack and it communicates with the attacker assuming it to be a legitimate party. To prevent this attack, authentication must be ensured.

4 Preliminaries

In this section, we briefly revise the concept of bilinear pairing and mapping, Boneh–Franklin identity-based encryption and signature and different complexity assumptions [4]. In Table 1, we have listed the basic notations and their meanings that are to be used throughout this paper.

4.1 Bilinear Pairing

Identity-based cryptography is based on bilinear maps. Given two cyclic groups G1, G2 of the same prime order p, G1 being an additive Abelian group like elliptic curve group and G2 being multiplicative Abelian group. A bilinear map e : $G1 \times G1 \rightarrow G2$.

1. **Bilinearity**: $e(aP, bQ) = e(P, Q)^{ab}; \forall a, b \epsilon F_p \ and \ P, Q \epsilon G1.$

2. **Non-degeneracy**: If $P \neq O$ and $P \epsilon G1$ then $e(P, P) \neq I_{G2}$ where P is a generator point of G1.

3. **Computability**: $e(P, Q) \epsilon G2, \forall P, Q \epsilon G1$ is easy to compute.

Table 1 Notations used in this survey

Symbols	**Meanings**
z	Set of integers
z_q	Set of integers mod q
z_q^*	Set of integers 1 to q-1 having additive and multiplicative inverse
E/F_p	Elliptic curve group over F_p
F_p	Finite field with q elements
e : $G1 \times G1 \rightarrow G2$	Bilinear map between two cyclic groups
P	A generator point
q	A large prime number
C	Cipherspace
M	Message space
P_{pub}	System public key
s	Master secret
$\{0, 1\}^n$	String consisting 0 and 1 of length n
$H(_i)$	Special hash function
d_{ID}	Private key of ID
Q_{ID}	Public key of ID

Table 2 Quantitative comparison among the recent research approaches

Comparison criteria	[5]	[6]	[9]	[11, 13]	[10]	[14, 15]	[18]
Key-Escrow problem	Y	Y	Y	N	Y	N	N
Confidentiality	Y	Y	Y	Y	Y	Y	Y
Integrity	Y	N	Y	Y	Y	Y	Y
Authenticity	Y	N	Y	Y	Y	Y	Y
Eavesdropping attack	N	N	N	N	N	N	N
Replay attack	N	Y	Y	N	N	N	N
Man-in-the-middle attack	N	Y	Y	N	N	N	N
DoS attack	N	Y	Y	N	N	N	Y
Impersonation attack	N	Y	Y	Y	N	N	N
Computational overhead	H	M	H	H	M	H	M
Communication overhead	M	M	H	H	H	M	M
Energy consumption	H	H	H	H	M	M	M

4.2 *Identity-Based Encryption*

Boneh–Franklin's scheme BF-IBE is built upon elliptic curve cryptography (ECC) and bilinear pairings [4]. It includes the following four algorithms:

4.2.1 Setup

Input: security parameter "k".
Output: Master-Secret (s), public params $=< E, p, q, n, P, P_{pub}, e, H1, H2, H3, H4, M, C >$.

1. Initially two cyclic groups G1 and G2 with prime order "p" and a bilinear map e $: G1 \times G1 \rightarrow G2$ should be generated. Then pick a random generator $P \epsilon G1$.
2. Select a random number s in z_q^* as the Master-Secret and compute P_{pub}, i.e., $P_{pub} = s.P$.
3. Define four cryptographic hash functions:
   - $H1 : F_p \rightarrow \{0, 1\}^n$.
   - $H2 : \{0, 1\}^n \times \{0, 1\}^n \rightarrow F_p$.
   - $H3 : \{0, 1\}^* \rightarrow E/F_p$.
   - $H4 : \{0, 1\}^n \rightarrow \{0, 1\}^n$.

The message space is $M = \{0, 1\}^n$ where n is the message size (in no. of bits). The ciphertext space $C = E/F_p \times \{0, 1\}^n \times \{0, 1\}^n$. Setup algorithm is performed by PKG (private key generator) only once at the time of initialization. s (master secret) is only kept by PKG. Public params are public parameters known to all even to adversary.

4.2.2 Extract

Input: $ID\epsilon\{0, 1\}^*$, Master-Secret (s), public params $=< E, p, q, n, P, P_{pub}, e, H1, H2, H3, H4, M, C >$.
Output: Private key of ID (d_{ID}).

1. Compute public key as $Q_{ID} = H3(ID)$.
2. Compute private key as $d_{ID} = s.Q_{ID}$.

Extract algorithm is executed by the PKG. And Q_{ID}, i.e., public key should be published while d_{ID} is sent to the communicating entity through a secure channel.

4.2.3 Encrypt

Input: $m \ \epsilon \ M$, $ID\epsilon\{0, 1\}^*$, public params $= < E, p, q, n, P, P_{pub}, e, H1, H2, H3, H4, M, C >$.
Output: Ciphertext $c \ \epsilon \ C$.

1. Pick a random number $\sigma \leftarrow \{0, 1\}^n$ and compute $r = H2(\sigma, m)$.
2. Compute $Q_{ID} = H3(ID)$ and $g_{ID} = e(Q_{ID}, P_{pub})$.
3. $V = H1(g^r_{ID}) \oplus \sigma$.
4. $U = r.P$.
5. $W = m \oplus H4(\sigma)$.
6. Set the ciphertext to $C =< U, V, W >$.

4.2.4 Decrypt

Input: $C =< U, V, W > \epsilon C, d_{ID}$, public params $=< E, p, q, n, P, P_{pub}, e, H1, H2, H3, H4, M, C >$.
Output: m (message).

1. $W \oplus H4(V \oplus H1(e(d_{ID}, U))) \Rightarrow m$.

4.3 Identity-Based Signature

Shamir was the first one who introduced identity-based cryptography [4]. After that different IBS schemes based on the bilinear pairing were introduced, one of such schemes identity-based signature scheme was proposed in [20]. It includes the following four algorithms:

4.3.1 Setup

Input: k(security parameter).
Output: master secret (s), Public params $=< G1, G2, P, P_{pub}, e, H1, H2 >$.

1. Initially, two cyclic groups, i.e., G1 and G2 should be generated whose order should be prime and select a bilinear map $e : G1 \times G1 \rightarrow G2$. And select a generator P from G1.
2. Generate Master-Secret (s) $[s \epsilon Z_q^*]$. Using the master secret "s" compute P_{pub}, i.e., $P_{pub} = s.P$.
3. Define two special hash functions.

- $H1 : \{0, 1\}^* \rightarrow E/F_p$.
- $H2 : \{0, 1\}^n \times G1 \times \{0, 1\}^n \rightarrow F_p$.

4.3.2 Key Generation

Input: users $ID \ \epsilon \ \{0, 1\}^*$, $d_{ID} = s.Q_{ID}$, and Public params $=< G1, G2, P, P_{pub}, e, H1, H2 >$.
Output: Private key of ID (d_{ID}).

1. Public key as $Q_{ID} = H1(ID)$.
2. Private key as $d_{ID} = s.Q_{ID}$.

Extract algorithm will calculate the public key, private key pair. Q_{ID} which is the public key should be published and d_{ID} should be sent secretly to the communicating entity.

4.3.3 Sign

1. Select a random integer $r \ \epsilon \ Z_q$.
2. $U = r.P$.
3. $H = H2(ID, M, U) \ \epsilon \ G1$.
4. Compute $V = d_{ID} + r.H \ \epsilon \ G1$.
5. The signature on message is the pair $\sigma =< U, V > \epsilon \ G1 \times G1$.

4.3.4 Verify

Input $\sigma =< U, V > \epsilon \ G1 \times G1$.

1. To verify a signature on a message M, the verifier first obtains the signer's Identity ID and compute $Q_{ID} = H1(ID)$.
2. Then verifier recalculates $H = H2(ID, M, U)$.

3. He then accepts the message only if $e(P, V) = e(P_{pub}, Q_{ID}).e(U, H)$, otherwise rejects it. The message is authenticated only if receiver has used signers public key to verify and signer has signed the message using respective private key. Here is the proof:

$$e(P, V) = e(P, d_{ID} + r.H) = e(P, d_{ID}) \cdot e(P, r.H) = e(P_{pub}, Q_{ID}) \cdot e(U, H).$$

Y:-YES N:-NO H:-HIGH M:-MEDIUM

5 Conclusion

In this paper, we have studied and analyzed different research papers based on the applications of identity-based cryptography in smart homes and healthcare. Despite the fact that IBC cryptosystems still show some weaknesses, we must admit that it brings some indisputable advantages for the common user that wishes for a simpler process for setting private, secure communication than classic PKI systems. In many papers, key disadvantage of BF-IBE, i.e., Key-Escrow problem is resolved in a very elegant manner. Therefore, in limited resource devices like IoT, IBC seems, for the time being, a good solution for system security. Holding the belief of this paper, we showcased a quantitative comparison between recently proposed IBC schemes in smart home and healthcare, based on the concept of standard network attacks and different challenges that it would face. Moreover, we have also included the conventional parameters like computation and communication overhead that one needs to keep in mind while choosing the IoT as per their service. We hope this paper can act as a platform for the researchers to get a brief idea about how IBC can be helpful to accomplish the requisite security requirements in application areas of IoT that are limited to resources and vulnerable to a variety of security threats.

References

1. A.K. Ranjan, V. Kumar, M. Hussain, Security analysis of TLS authentication, in *2014 International Conference on Contemporary Computing and Informatics (IC3I).* (IEEE, 2014), pp. 1356–1360
2. E. Rescorla, T. Dierks, The transport layer security (TLS) protocol version 1.3 (2018)
3. A. Shamir, Identity-Based cryptosystems and signature schemes, in *Workshop on the Theory and Application of Cryptographic Techniques* (Springer, Berlin, Heidelberg, 1984), pp. 47–53
4. D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in *Annual International Cryptology Conference* (Springer, Berlin, Heidelberg, 2001), pp. 213–229
5. R.H. Jacobsen, S.A. Mikkelsen, N.H. Rasmussen, Towards the use of pairing-based cryptography for resource-constrained home area networks, in *2015 Euromicro Conference on Digital System Design* (IEEE, 2015), pp. 233–240

6. S. Al Salami, J. Baek, K. Salah, E. Damiani, Lightweight encryption for smart home, in *2016 11th International Conference on Availability, Reliability and Security (ARES)* (IEEE, 2016), pp. 382–388
7. S. Chen, M. Ma, Z. Luo, An authentication scheme with identity-based cryptography for M2M security in cyber-physical systems. Secur. Commun. Netw. **9**(10), 1146–1157 (2016)
8. S. Sankaran, Lightweight security framework for IoTs using Identity-Based cryptography, in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (IEEE, 2016), pp. 880–886
9. Y. Ashibani, Q.H. Mahmoud, An efficient and secure scheme for smart home communication using identity-based signcryption, in *2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC)* (IEEE, 2017), pp. 1–7
10. R. Boussada, M.E. Elhdhili, L.A. Saidane, Privacy preserving solution for internet of things with application to ehealth, in *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)* (IEEE, 2017), pp. 384–391
11. B. Anggorojati, R. Prasad, Securing communication in inter domains Internet of Things using identity-based cryptography, in *2017 International Workshop on Big Data and Information Security (IWBIS)* (IEEE, 2017), pp. 137–142
12. Z. Cheng, R. Comley, L. Vasiu, Remove key escrow from the identity-based encryption system, in *Exploring New Frontiers of Theoretical Informatics* (Springer, Boston, MA, 2004), pp. 37–50
13. B. Anggorojati, R. Prasad, Securing communication in the IoT-based health care systems. Jurnal Ilmu Komputer dan Informasi **11**, 1–9 (2018)
14. R. Boussada, M.E. Elhdhili, L.A. Saidane, A lightweight privacy-preserving solution for IoT: the case of e-health, in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (IEEE, 2018), pp. 555–562
15. R. Boussada, M.E. Elhdhili, L.A. Saidane, Toward privacy preserving in iot e-health systems: a key escrow identity-based encryption scheme, in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (IEEE, 2018), pp. 1–7
16. K.A. Shim, Y.R. Lee, C.M. Park, EIBAS: an efficient identity-based broadcast authentication scheme in wireless sensor networks. Ad Hoc Netw. **11**, 182–189 (2013)
17. Y. Xia, R. Huang, X. Jin, H. Zheng, S. Ji, A novel certificateless signcryption for e-health record system, in *2018 1st International Cognitive Cities Conference (IC3)* (IEEE, 2018), pp. 231–235
18. M.M. Rathore, E. Bentafat, S. Bakiras, Smart home security: a distributed identity-based security protocol for authentication and key exchange, in *2019 28th International Conference on Computer Communication and Networks (ICCCN)* (IEEE, 2019), pp. 1–9
19. Y. Zhang, D. He, Y. Li, M. Zhang, K.K.R. Choo, Efficient obfuscation for encrypted identity-based signatures in wireless body area networks. IEEE Syst. J. (2020)
20. A. Burnett, F. Byrne, T. Dowling, A. Duffy, A biometric identity based signature scheme. IJ Netw. Secur. **5**(3), 317–326 (2007)

Designing of Smart Home: Sustainable Development

Shiva Pujan Jaiswal, Jay Singh, Anjali, Ikul Kamanda Steve, and C. Mohan

1 Introduction

Technology is one of the critical factors for any country, especially for developing countries like India. Starting from the smartphone, internet, online shopping, online working, internet banking, and now to latest young innovations such as home automation, wearable technology, robots, and many more are impacting daily lives of society. A report is saying that the Indian home automation industry is expected to be of $6 billion by 2022 and will increases double from $3 billion expected in 2020 [1]. A home automation can be define in many ways such as a home which is fully automated and contains different types of sensors to automatically control the home appliances, which aims to provide comfortable, reliable, and secure home and improved the quality of life. Home automation means controlling the electronic appliances without physical movement via smartphone or remote with the help of sensors and actuators. Why home automation is required? First of all reduced electricity bills, secondly most of the electricity is produced with the help of non-renewable resources, and earth has limited sources. Nowadays, when the demand of electricity is increasing with increase in population, systems need to follow sustainable development to meet the demand of present without upsetting future [2]. These non-renewable sources are causing pollution also. Home automation can be beneficial for disable and elderly people also. So using electric energy efficiently and effectively society needs home automation.

This paper came up with smart home for the sustainable development of society as an initial step. With the help of smart home, user can turn ON/OFF of light/fan

S. P. Jaiswal · Anjali · I. K. Steve · C. Mohan
Department of Electrical Electronics and Communication Engineering, SET, Sharda University, Greater Noida, India

J. Singh (✉)
G. L. Bajaj Institute of Technology and Management, Greater Noida, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_19

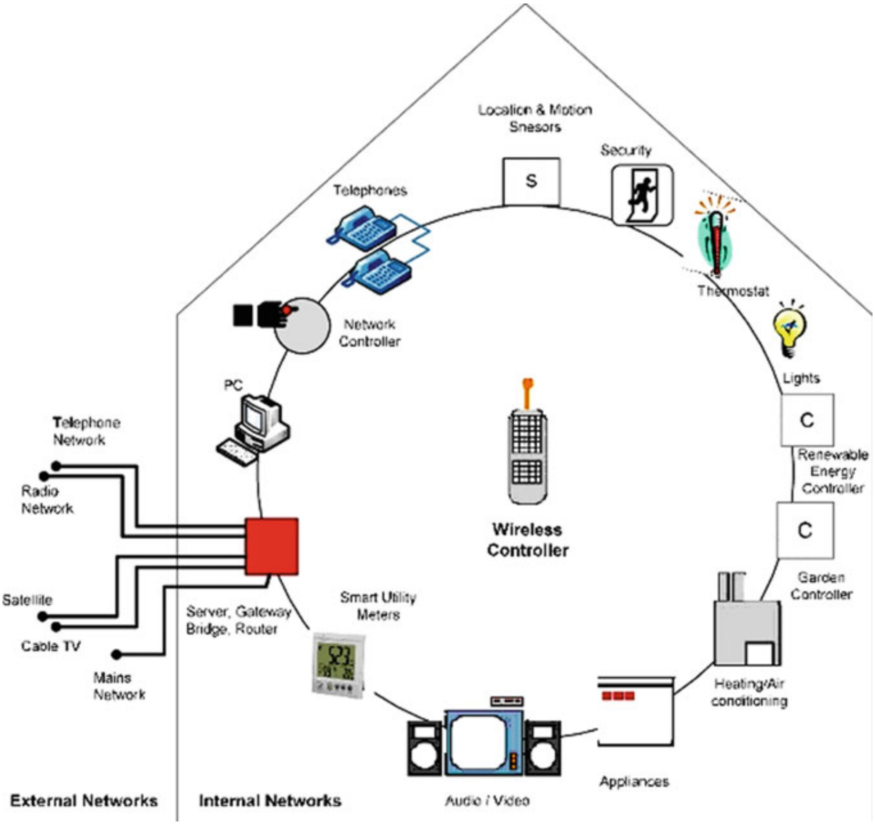


Fig. 1 Smart home architecture

of a room. User can also adjust the luminosity with the help of a remote. Figure 1 is showing architecture of smart home.

1.1 Types of Home Automation Systems

Implementation of home automation depends on the type of controls like wired or wireless. There are mainly three types of home automation systems [3].

(a) Power line-Based Home Automation
(b) Wired or BUS Cable Home Automation
(c) Wireless Home Automation.

Electrical cable Home Automation System: This mechanization is sensibly valued and doesn’t have need of extra wire to ship the data, yet utilize accessible electrical

Fig. 2 Wireless home automation

cables to move the information. In any case, this framework includes an enormous unpredictability and requires extra converter circuits and gadgets.

Wired or BUS Cable Home: Automation in this sort of computerization, all the home hardware is associated with the fundamental regulator (programmable rationale regulator) through a correspondence link. The hardware is appended with actuators to speak with the primary regulator. The whole tasks are unified by the PC that ceaselessly speaks with the primary regulator [3].

Remote Home Automation: This is the extension and headway of wired automation which utilizes remote advancements like IR, Zigbee, Wi-Fi, GSM, Bluetooth, and so forth, for accomplishing far off activity as shown in Fig. 2. For instance, the GSM based home mechanization gives the controlling of home hardware by a SMS to the GSM modem.

1.2 Requirement of Home Automation

Make Tasks More Convenient: Many errands that are dreary in nature can be cultivated consequently or with less advances utilizing home mechanization. Rather than killing or diminishing four unique lights when client need to watch a film, home automation permits him to achieve this assignment with one catch as it were [4].

Get a good deal on Utilities: Utilities can add up to a few hundred dollars for each month. Home automation can off lights or lower the indoor regulator naturally when user aren't utilizing them and effectively bring down his service bills by 10–25% [5].

Expanded Home Safety: Many mishaps occur in the home on account of helpless lighting. Home automation can naturally turn lights on in wardrobes, flights of stairs, and other dull spots whenever user enter and decline the opportunity of coincidentally stumbling or running into things [8].

Home Security: Although home security is a need for everybody, high establishment cost or month to month checking charges make security frameworks cost-restrictive for some mortgage holders [6].

Useful for the Environment: When users are for the most part getting all the more ecologically mindful, home automation gives a decent answer for help save his regular assets. Home mechanization items can lessen power utilization and naturally turn off lights and apparatuses when they aren't being used. The brilliant home diminishes the utilization of electrical vitality which is producing by the consuming of petroleum derivative. The sparing of one unit at customer end is identical to 1.25 units at the age plant; this implies the sparing of discharge is high [9].

True serenity: Never again stress over user's home while he is away. Utilizing home camcorders and a web association, user can mind the status of his home or children from anyplace on the planet utilizing a PC or web-empowered telephone.

Learning Experience for Children: Technology is staying put and the more youngsters find out about forthcoming innovation the more ready they are for what's to come. Transform his home into a study hall, as your home computerization ventures become a learning experience for youngsters [10].

Various paper and articles are available in literature related to home automation system, in which they use different technologies to develop a smart home system. In previous work, they generally use Bluetooth, phone, and personal computer to control the home appliances. The system which uses the smart phone as remote control to control the home appliances is basically connected to the user interface in appliances. One of the modern technologies, which is used as a remote control are Bluetooth, zigbee, GSM, etc., to control the home appliances. There are different kinds of home automation available in the market [11].

Home automation can be divided into two categories. Under first category, user can control their home appliances through their smartphone, Wi-Fi, Bluetooth, Zigbee, or any other wireless system. In second category, user can control the appliances through a remote. However, there are lots of issues comes when designing remote-based home automation, but once it is designed, it will be more reliable compare to the first one. So, this paper developed a remote control-based home automation. Home automation allows user to control, monitor the home appliances easily, safely, and efficiently. It provides a better security to user house. The main aim of this paper is to provide cheap and better home automation system to people so they every individual can buy and use this system. To faster response and provide reliable communication, this paper proposes remotely controlled home automation system using Arduino Uno as well as IoT-based remote control system.

2 Design of Smart Home

The smart home been an automation base project; it works in the principle where a bunch of sensors are placed to give the physical parameters of the environment or the room where smart saving box will be use along with that a remote system is set to give a human control over the automated system [12]. And after the process, the information collected through the sensors will helps us to actuate our output mostly the home appliances connected to it. By this principle, this work is divided in three blocks as presented in Fig. 3.

(a) The Input Unit
(b) The processing unit
(c) The output unit.

The input unit: In the input unit mostly base on sensors. Following are the main sensor which are used to develop a smart home to make life easy, save electricity, and reduce the emission of pollutants while generating power.

Ultrasonic Sensor HC-SR04: The ultrasonic sensor is used here for sensing the presence of a person entering or leaving the room where it is set. Using its measuring function, it will be place in the door and, continually, it will be measuring the distance between the door frames. Once someone crosses the door by entering or leaving, the distance will change and it will be for user information and a counting of number of person [13].

Humidity and Temperature Sensor DHT11: As the name indicates, this sensor is used to sense the temperature and humidity level under the greenhouse environment, where the pyroelectric film is used to sense the temperature and a hygrometer which is resistive in nature is used to sense the humidity. It record the change in resistance with change in humidity and then send the instructions to an ADC which converts the analog signal into digital which is easy for decode. This system used a DHT11 sensor which is a series of DHTXX series. The main advantage of DHT11 sensor is that it can sense the both humidity and temperature. It required less power input and it can sense up to 50 °C temperature and up to 80% RH of humidity value. Figure 4 is showing a DHT11 sensor [14].

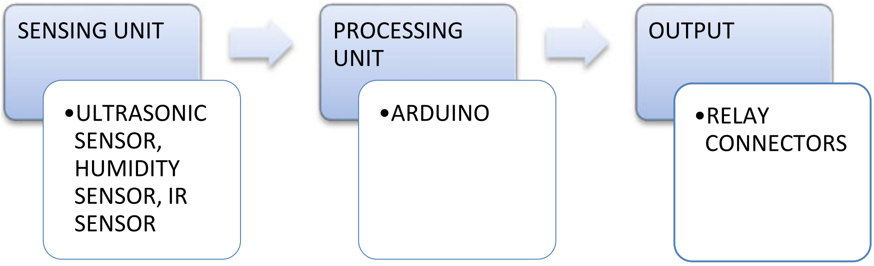
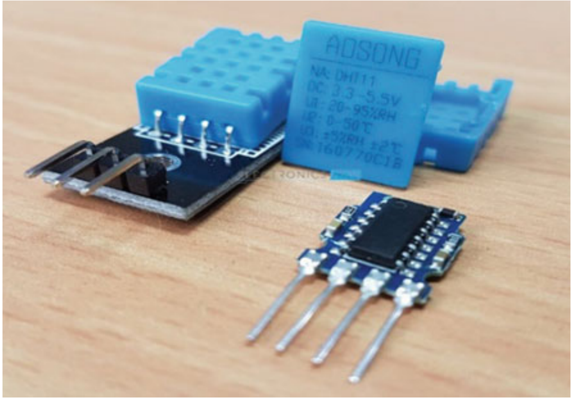


Fig. 3 Block diagram of home automation

Fig. 4 DHT11 sensor



Infrared Receiving Sensor: The infrared here is a channel to communicate directly with the smart saving box by using a remote user can manually turn ON or OFF the light and the fan too and in the same way user can act in the speed control of the fan or brightness of the light.

LDR Sensor: Light-dependent resistor is also called as Photoconductor which works on the principle of photoconductivity. It is basically a photocell in which the resistance is passive element.

The resistance value proportional to the light intensity. When the light intensity decreased, the resistance value is also decreased and sends the output instruction [15]. A most common symbol of LDR and sensor is shown below in Fig. 5.

The processing unit: Processing unit is based on an Arduino microcontroller; it is processing the input information and provides output corresponding to the data received from the input unit. And for the speed control, it to generate the corresponding signal so that user can have a corresponding speed.

Output unit: The output unit consists of different relay-based circuits receiving there signal from the processing unit, they are used as switches to control the appliances. And the speed control circuit also getting a signal from the processing unit acts as an output element and is directly connected with the appliance.

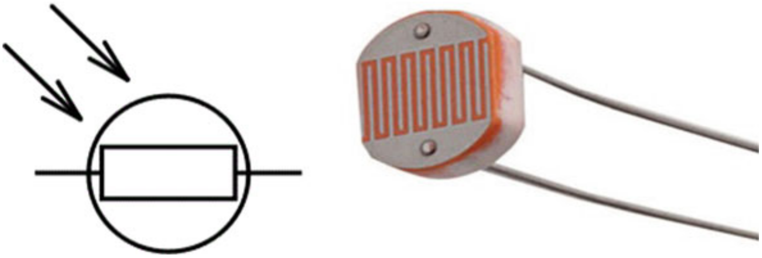


Fig. 5 LDR sensor symbol and sensor

In this work, Arduino software is used. Arduino is the heart of project. It is basically a microcontroller-based board, which consists of 6 analog pins, 14 digital I/O pins, and an Atmega328 microcontroller. It also has serial data communication port "Tx" and "Rx". It is a cost-effective in nature. To work with this, connect this Arduino Uno with computer using USB cable and then install the full program using the Arduino software. Model uses AC or DC adapter to power the board. The Arduino Uno is also connected to the GSM module which is used in this system for communication purpose. The Tx pin of Arduino Uno is connected directly with the GSM Rx pin and the Rx pin of Arduino is directly connected to the GSM Tx pin. Figure 6 is showing an Arduino Uno board. Arduino UNO, Ultrasonic sensor (HR-SR04), IR sensor, Humidity Sensor (DHT11), and Opto-couplers (MOC 3021 & 4N35) in hardware. All the sensors are connected with microcontroller. A sensor is a device that measures and acts according to the reading. There are different sensors for different physical phenomenons, i.e., LM 35 for temperature its output is analog. Output of these sensors can be analog or digital signal. Microcontroller is an Integrated Circuit (IC) in embedded system. It has three parts: processor, memory, and input/output (I/O) peripherals. Arduino Uno is a microcontroller board based on ATmega328P. Ultrasonic sensor is counting the number of person entering and leaving the room.

Along with a remote system is set to allow a manual control and mostly for a speed and brightness control system that can be use for a FAN or a BULB. Figure 6 is showing the different types of sensor which is used in home automation, whereas Fig. 7 is showing the Arduino. In this smart home, ultrasonic sensor is counting the number of person entering and leaving the room. Along with a remote system is set to allow a manual control and mostly for a speed and brightness control system that can be use for a FAN or a BULB. Figure 8 is showing the complete diagram of this system.

The working of the smart home is as one counting system is placed in the door with the help of the ultrasonic sensor that can count the number of persons entering

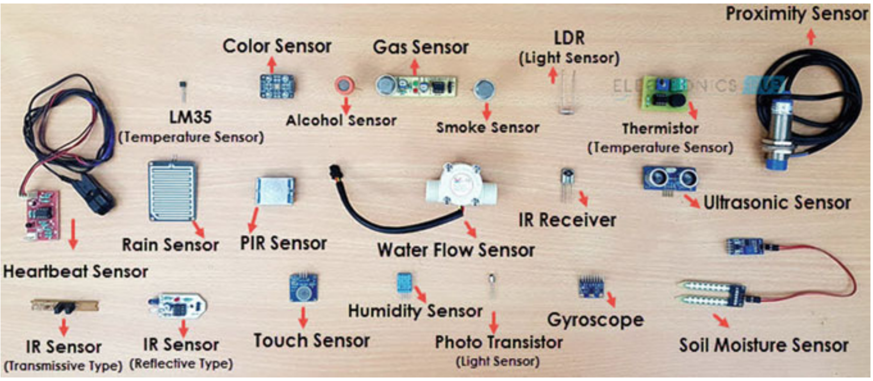


Fig. 6 Types of sensors

Fig. 7 Arduino UNO [7]

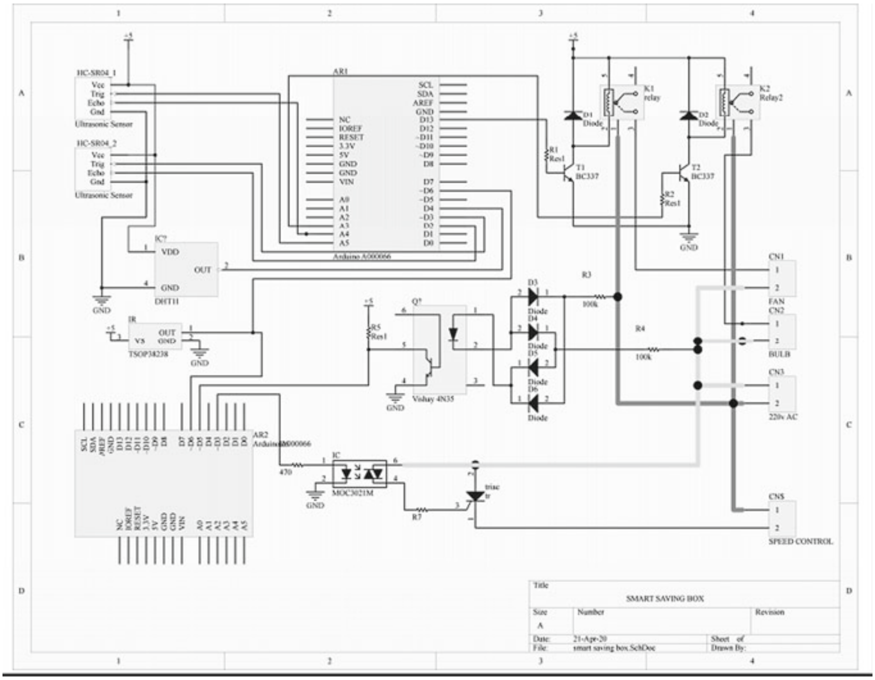


Fig. 8 Circuit diagram

a room as well as those who are leaving. At the same time, humidity sensor will start doing a check at room temperature and compare it with the reference temperature which is set to be 25 °C. If the temperature exceeds than the predefined temperature, then fan will turn on automatically. Further, user can control the brightness of the

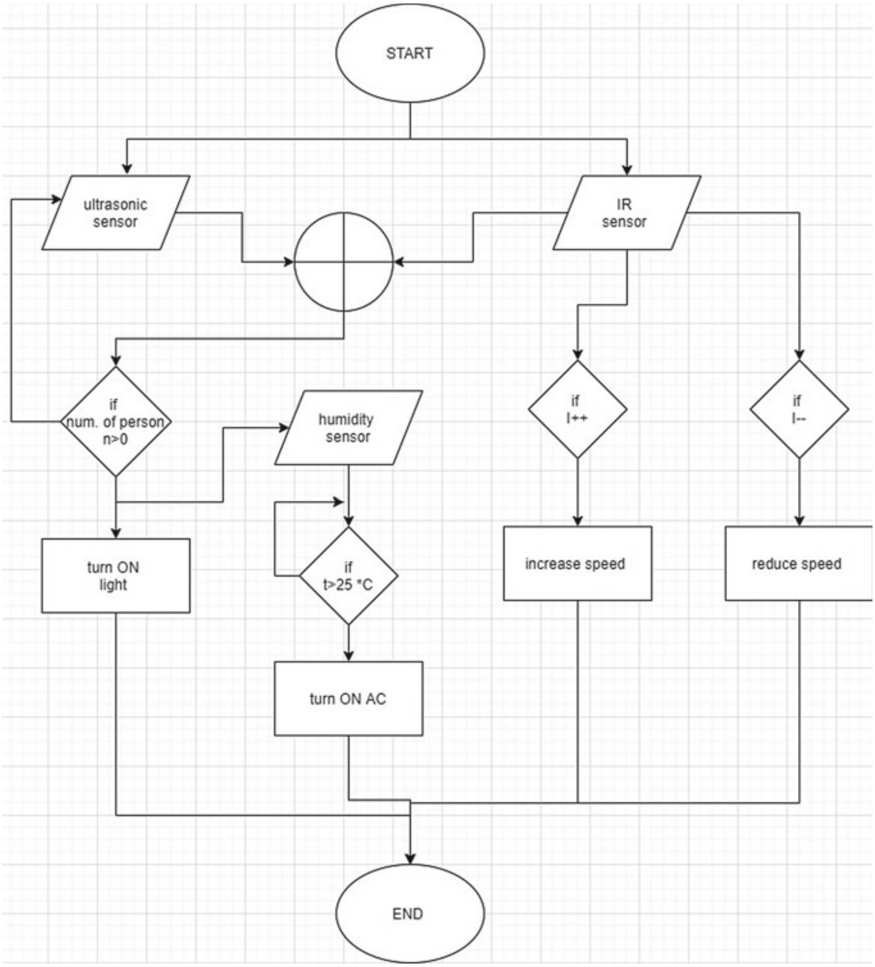


Fig. 9 Flowchart of working of smart home

lamp and speed of the fan with a remote. Figure 9 is showing the flowchart to control appliances.

3 Result and Discussion

The first stage of the design is to automate one room and help to save more in terms of electricity consumption. The circuit utilizes generally accessible segments and, in this manner, a definitive creation cost will be less expensive than different substitutes accessible in the market. The circuit utilizes the entire transmission capacity of distant

IR, and consequently can be constrained by any caring far off. The scope of distant IR is very huge. Subsequently, the controller can be controlled over an enormous room. The circuit utilizes ordinarily accessible parts and in this manner a definitive creation cost will be less expensive than different substitutes accessible in the market. The circuit utilizes the entire data transfer capacity of far off IR, and henceforth can be constrained by any benevolent distant. The scope of distant IR is very enormous. Accordingly, the controller can be controlled over a huge room. The circuit utilizes ordinarily accessible parts and in this manner a definitive creation cost will be less expensive than different substitutes accessible in the market. The circuit utilizes the entire data transmission of far off IR, and henceforth can be constrained by any caring far off. The scope of distant IR is very huge. In this manner, the controller can be controlled over an enormous room. The developed working model is shown in Fig. 10.

4 Conclusion

The system we have designed to automate one small room and help us to save more in terms of money and electricity. It can be further improved in terms of using more sensors. With the use of good quality sensors/upgraded sensors, we can use this system to control micro-industries or bigger spaces. It can also be used at offices, college, school, industry, and say everywhere. Home automation provides smart solutions and high standards of living to the world. This system can smartly control and handle the whole appliances of a room and provides safe and easy way to live life smoothly. “Home Automation is a dream.” However, it is low, but slowly it is going to be a part of our daily lives. A report says that the home automation business will be of $40 billion by 2020.

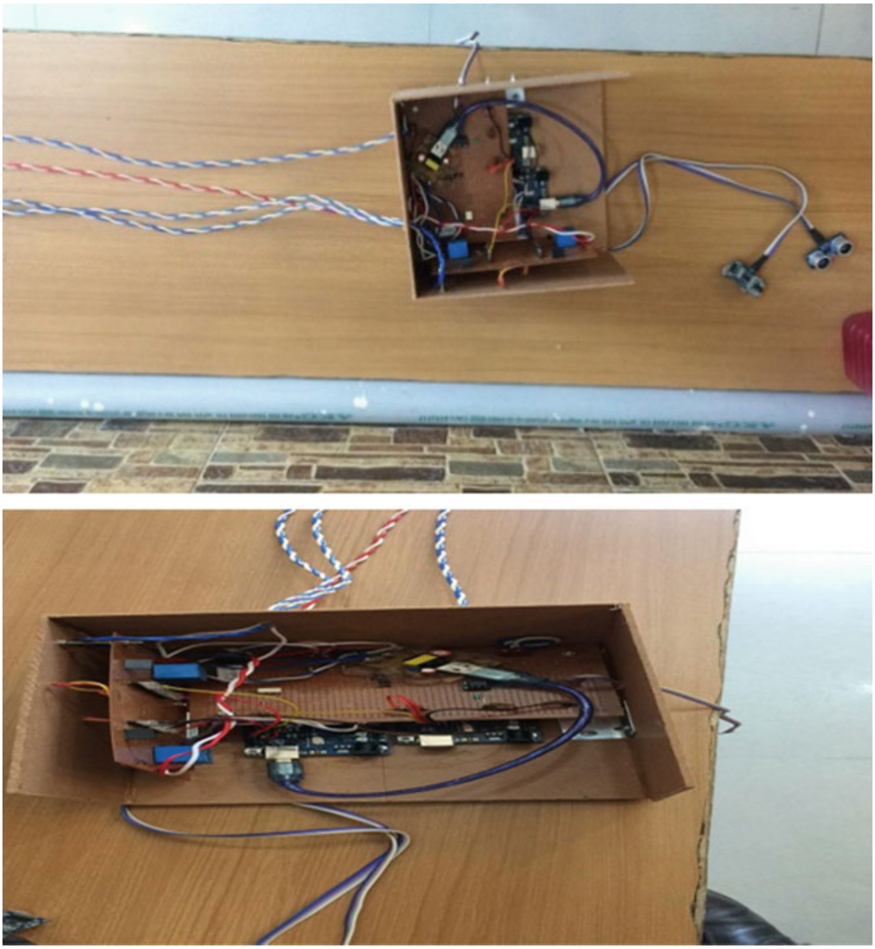


Fig. 10 Working model

References

1. S. Singh, S.P. Jaiswal, Enhancement of ATC of micro grid by optimal placement of TCSC, in *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2020.05.161
2. W.A. Jabbar, M.H. Alsibai, N.S.S. Amran, S.K. Mahayadin, *Design and Implementation of IoT-Based Automation System for Smart Home*. https://doi.org/10.1109/ISNCC.2018.8531006
3. S.P. Jaiswal, V. Shrivastava, D.K. Palwalia, Opportunities and challenges of PV technology in power system, in *Materials Today: Proceedings* (2020). https://doi.org/10.1016/j.matpr.2020.01.269
4. S. Gaidhani, T. Singh, Y. Verma, C. Umayal, IOT-based home automation system: a smart way to conserve energy. IJESRT. https://doi.org/10.5281/zenodo.1312761
5. M.S. Soliman, A. Alahmadi, A. Maash, O. Mohamed, Design and implementation of a real-time smart home automation system based on Arduino microcontroller kit and lab view platform. IJAER **12**(18) (2018)

6. S.P. Jaiswal, V. Shrivastava, S. Singh, Economic viability solar PV power plant in distribution system, in *IOP Conferences Series: Materials Science and Engineering*, vol. 594 (2019). https://doi.org/10.1088/1757-899X/594/1/012010
7. N. Goel, S.R. Ramavt, S.P. Jaiswal, V. Shrivastava, Battery energy storage technology integrated for power system reliability improvement, in *Advances in Energy and Power Systems, Lecture Notes in Electrical Engineering*. https://doi.org/10.1007/978-981-13-0662-4
8. B.M. Al-thobaiti, I.I. Abosolaiman, M.H. Alzahrani, S.H. Almalki, M.S. Soliman, Design and implementation of a reliable wireless real-time home automation system based on Arduino Uno single-board microcontroller. Int. J. Control, Autom. Syst. **3**(3), 11–15 (2014)
9. S.P. Jaiswal, S. Shrivastava, D.K. Palwalia, Impact of semiconductor devices on voltage stability of distribution system, in *Materials Today: Proceedings* vol. 3, issue P3, pp. 581–589. https://doi.org/10.1016/j.matpr.2019.03.101
10. I.M. Iman, A. Sulayman, S.H.A. Almalki, M.S. Soliman, Designing a reliable dual modes real-time home automation system based on very high speed description language. Int. J. Control, Autom. Syst. **5**(3), 19–23 (2016)
11. Official Arduino Website: www.arduino.cc
12. S.P. Jaiswal, V.S. Bhadoria, A. Agrawal, H. Ahuja, Internet of Things (IoT) for smart agriculture and farming in developing nations. Int. J. Sci. Tech. Res. **8**(12), 1049–1058 (2019)
13. S.P. Jaiswal, V.S. Bhadoria, A. Agrawal, J. Singh, Virtual flux and frequency meter, in *2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC)* (2019). https://doi.org/10.1109/PEEIC47157.2019.8976532
14. V.S. Bhadoria, V. Shrivastava, N.S. Pal, S.P. Jaiswal, Reliability improvement of distribution system by optimal sitting and sizing of disperse generation. Int. J. RQSE (2017). https://doi.org/10.1142/S021853931740006X
15. S.R. Ramavt, N. Goel, S.P. Jaiswal, V. Shrivastava, Optimal location and sizing of DG in distribution system and its cost-benefit analysis. Adv. Int. Sys. Comp. https://doi.org/10.1007/978-981-13-1819-1_11

A Case Study on Arduino Mega & Uno Microcontrollers to Estimate On-chip Mismatches for Security Applications

Anil Kumar kurra and Usha Rani Nelakuditi

1 Introduction

The rapid worldwide development of the Internet of Things (IoT), including portable devices, light switches, door locks, communication devices, and a wide range of gadgets are used in our day-to-day life are demanding two issues such as security and power consumption. In recent years, security becomes one of the critical aspects of communicating these devices via the internet and local networks. However, applying the conventional secure algorithms violates basic constraints such as memory. Hence, to attain reliable authenticity, confidentiality, Physical Unclonable Functions (PUFs) emerged as an innovative and widely accepted cryptographic primitive in hardware cryptography over the last decade. It has a wide range of applications, including IP protection, tamper-resistant key storage, authentication (as shown in Fig. 3), ID generation, and cryptographic key generation, which are the main areas where PUFs can address better security solutions also eliminate the need of non-volatile memory (NVM). A PUF is an entity whose response always depends on applied input challenges and randomness of the PUF circuit. A PUF should generate a unique set of responses at each corresponding challenge by utilizing the complex random process variations during IC manufacturing. Therefore, the relation between external challenges and output responses is usually called the challenge–response pair(CRP); mathematically, it can be represented by Ri = F(Ci). The tuples (Ci, Ri) are termed the CRPs of the PUF. Figure 1 depicts the mismatch mechanism of two devices. Miniature and uncontrollable variations occur due to two parameters, such as technology parameters and non-technology parameters (as shown in Fig. 2). Channel length, the geometry of transistors, threshold voltage, oxide thickness, doping concentration are parameters mainly responsible for secret keys, and on the other hand, non-technology

A. K. kurra (✉) · U. R. Nelakuditi
VFSTR (Deemed To Be University), Vadlamudi 522213, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_20

parameters such as temperature, supply voltage, and aging effects the stability of the secret keys.

Depends upon the number of the challenges, PUFs can be broadly distinguished into two types, such as weak PUFs and strong PUFs. Weak PUFs are the PUFs having a limited and fixed number of CRP pairs, which are primarily used for creating digital signatures. Keys generated from weak PUFs cannot be used directly on any authentication system. An adversary can easily replicate the CRPs by applying invasive

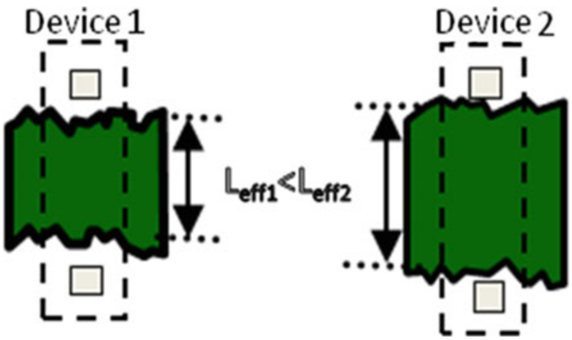


Fig. 1 Mismatch variations in two devices

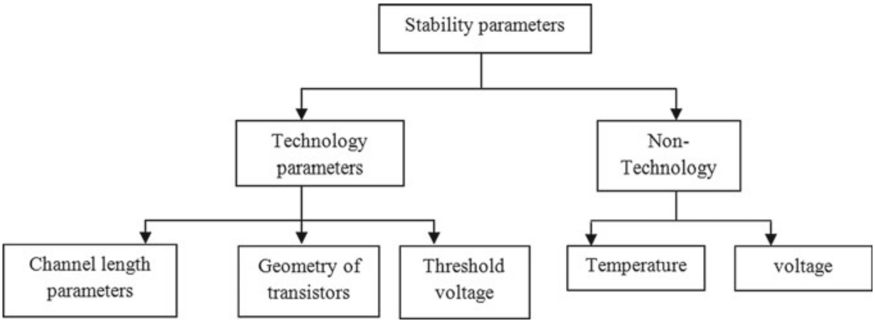
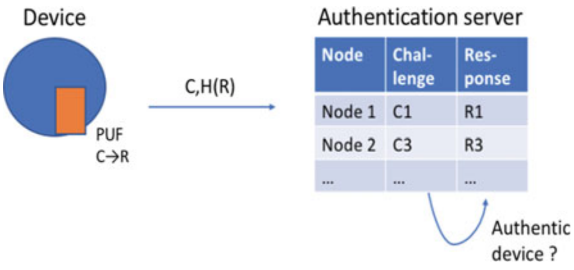


Fig. 2 Variation of parameters due to technology and non-technology parameters

Fig. 3 Device authentication using a PUF-based protocol [3]



Node	Challenge	Response
Node 1	C1	R1
Node 2	C3	R3
...	...	...

and semi-invasive attacks. In contrast to the weak PUFs, strong PUFs having an exponential number of CRPs and a very complex relation is exist between challenges and responses. During this model, the adversary doesn't know about the CRPs and cannot store the complete CRP table. However, over a period of time, its response has been predicted by applying machine learning (ML) techniques to the PUF architecture. The detailed state of the art related to the PUF architectures and corresponding functionalities are discussed in the literature [1–4]. Lofstrom et al. explained the pioneering of the work related to the PUF design and extraction of the on chip-specific data from the manufacturing process variations by comparing the two identical transistors [5]. However, in this paper, we conducted a case study to estimate the process variations in the various types of Arduino mega and Uno-based microcontrollers. The primary goal of this case study is to investigate the amount of mismatches from the microcontrollers and the database of CRPs can be useful for device authentication and identification applications.

The rest of the paper is organized as follows in Sect. 2 elucidates the related work on PUF methodology and existing PUF architectures. Section 3 describes the detailed study of minute process variations on Arduino mega and Uno-based microcontrollers by using statistical approaches, and finally, Sect. 4 concludes the paper.

2 Background and Preliminaries

The concept of the PUF was first suggested by Pappu in the year 2001 [6], by using an optical diffuser, the input can be given through a laser source using a specified wavelength and angle, the generated speckle responses are stored and used for the security applications. It is available in a non-integrated form, and having a set of advantages such as complex output, highly secure against modeling attacks, security against physical cloning attacks. And it is also proven that it cannot be modified and cloned by the adversaries. Figure 4 depicts the basic architecture of optical PUF. Due to its cost, laborious design setup, and tedious mechanical components it is not well suitable for portable design systems. Later, in 2002, Gassend et al. [7] introduced the

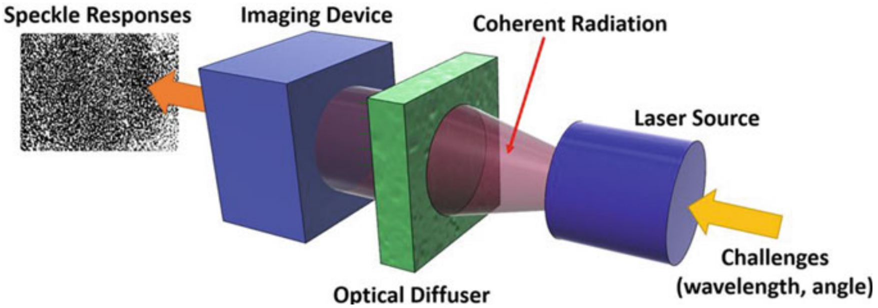


Fig. 4 Optical PUF architecture

concept of the silicon PUFs. He made use of random process variations during the manufacturing process in order to identify the ICs. By using the concept of random process variations in ICs, Lee et al. [8] designed the first silicon-based arbiter PUF architecture in 2004. Based on the input challenges and generated responses from PUFs, it can be broadly classified into two types, such as strong PUFs and weak PUFs. Strong PUFs are PUFs having a large set of CRPs, and difficult to clone these PUFs, which can be widely used for device authentication. Weak PUFs are PUFs having a limited number of challenges and well suitable for device identification. Arbiter PUFs are more generally timing-based PUFs, and it's having an exponential number of challenges. The basic architecture of the arbiter PUF consists of an N number of switching elements which are connected cascaded with each other, the switching block consists of two inputs and two outputs based on applied challenge and internal process variations. The response could be transfer either straight or cross. An arbiter should be connected at the final stage of the delay network, which decides the final response based on the settling time of the input to the arbiter. It was recognized that the response could be estimated by summing up the delays at individual stages using an additive linear delay model. Figure 5 illustrates the basic architecture of arbiter PUF [9]. Even though unclonability and randomness are two prime requirements for any PUF, Ruhimar et al. [10] estimated the entropy of timing delay differences at each stage of the switching element and enclave the mathematical modeling attacks by building a subset of the CRP database. Linear modeling is one of the mathematical modeling attacks that are extensively used to estimate the timing delay difference by using the machine learning tools such as logistic regression (LR). Hence to combat the major drawbacks (attacks) proposed a non-linear feed-forward arbiter PUFs. However, these architectures are vulnerable to evolutionary algorithms [11, 12]. Hence, other advanced modeling attacks include side-channel attacks by collecting the huge set of CRP databases for retrieved the timing information of non-linear PUFs and predicted response of non-linear PUFs. By simulation, it will be slightly harder to construct the CRP database, and approximately requires 50,000 CRPs with a small precession error of 1.3% [13–15].

On the other hand, ring oscillator PUF, is another class of strong PUFs. It can use different approaches to measure the uncontrollable random variations. The architecture mainly consists of three blocks, namely a delay line, edge detector, and counter.

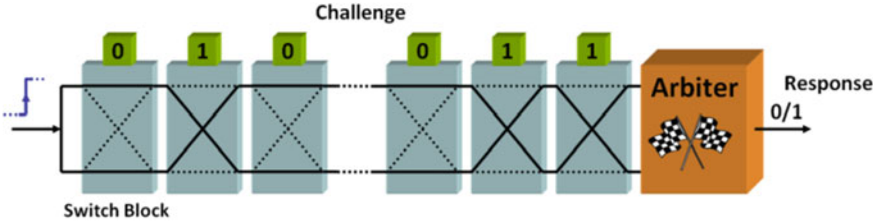


Fig. 5 Basic arbiter PUF architecture

The final response of the delay line is feedback to the input, which creates an asynchronous oscillating loop. The frequency of the oscillator is accurately measured by using the delay line. And the frequency could be altered at each and every iteration due to its random nature even it is sensed by using the edge detector and counter. Edge detectors can be used to detect the edges of the periodic oscillations, and counter can count the total number of oscillations over a period of time, respectively. The final response of the counter will consider being the final digital signatures for the ring oscillator PUFs. Figure 6 depicts the basic architecture of the ring oscillator PUF. Temperature, voltage, and environmental variations heavily affect the timing delay at each and every oscillation stage. As compared to the arbiter PUF, the effect of variations could greatly affect the oscillations on the ring oscillator PUF. In order to compensate for the effect of oscillations due to environmental variations, proposed a set of approaches such as ring oscillator PUF with division compensations and comparator compensation [16–18] as shown in Figs. 7 and 8.

In this section, we briefly discussed the various kinds of weak PUFs such as SRAM PUFs, butterfly PUFs, and latch PUFs. These PUFs are mainly based on digital memory of primitives and a digital memory cell is typical consists of a digital circuit having a single bit of stable logic state. This can be used to store the single bit of binary information in a two possible, stable states, But due to some physical mismatches, the output state tends to oscillate in between '0' and '1'. Moreover, this phenomenon has not explained the implementation of the logic cell. By taking the above pitfalls into consideration, proposed a set of PUF architectures. Out of those SRAM (Static Random Access Memory), PUF is one of the architecture. It is a type of digital memory it can be constructed by using the two cross-coupled inverters, and it having the capability of storing a single bit of binary information in

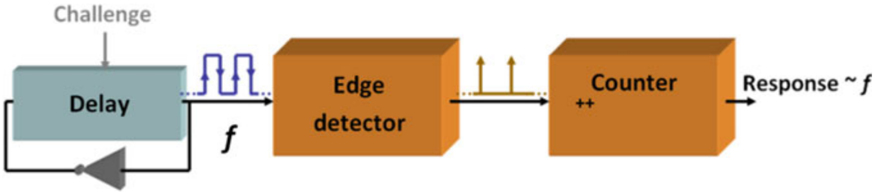


Fig. 6 Ring oscillator PUF architecture

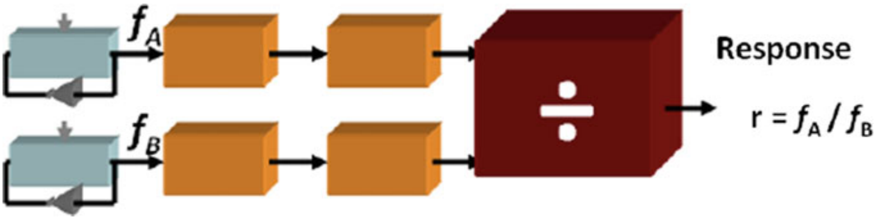


Fig. 7 Ring oscillator with division compensation approach

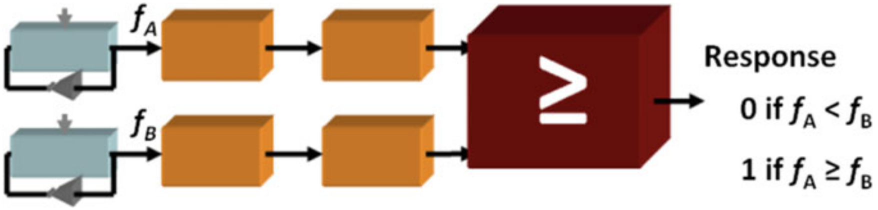


Fig. 8 Ring oscillator with a comparator compensation approach

two states. The basic circuit consists of four transistors for cross-coupled inverters, and two transistors are used to read and write operation. When the supply voltage is applied for the circuit, the cells could be preferably stores the power-up 0 or power-up 1. When the moment it will turn on due to its mismatches, it forces to either '0' or '1'. If the mismatch is very small, it is very difficult to determine the power-up state by using a stochastic approach. Extensive experiments were conducted in SRAMs from different memory blocks on various FPGAs. Over 8190 power-up states were collected. The databases estimated the Interchip Hamming Distance (HDinter) 49.97% and Interchip Hamming Distance (HDintra) 3.57% over different temperature conditions. Similarly, the power-up behavior of eight SRAM cells was measured over two different platforms, its HDinter 49.34% and HDintra is 6.5%, respectively. Figure 9 depicts the basic architecture of the SRAM PUF cell [19, 20].

The SRAM PUFs are mainly facing the two drawbacks, one such as when the power-up is necessary for the response generation, which might not be possible in all scenarios, and when the SRAMs are hard rested to 0, its randomness tends to 0 immediately [21, 22]. Hence, to counter-attack, these two drawbacks proposed a butterfly-based PUF cell. The basic architecture of the butterfly PUF consists of two cross-coupled transparent data latches that were connected. The operation of the butterfly PUF is based on clear and preset inputs of latches. The overall response

Fig. 9 SRAM PUF cell

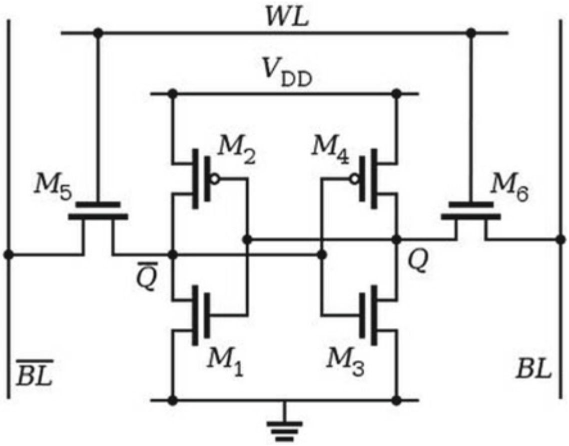
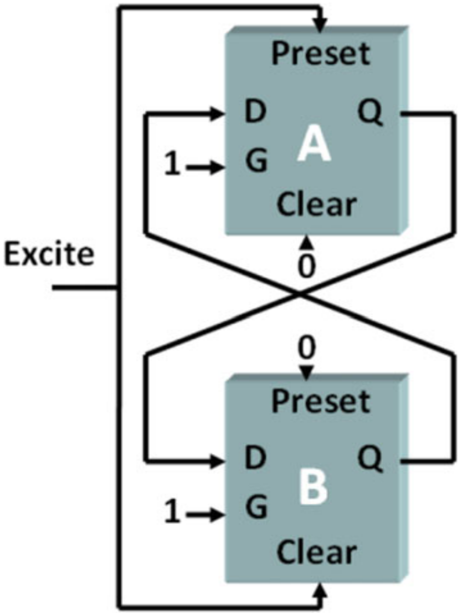


Fig. 10 Butterfly PUF cell



generated from the PUF cell is determined by physical mismatches between latches and interconnect delays, respectively [23–25]. The basic schematic of the butterfly cell, as shown in Fig. 10. Depending upon the nature of the CRPs, architectural design and based on its properties, Table 1 describes an overview of the PUFs.

3 Proposed Work

Extensive research work has been done to extract the characteristics of the PUFs from different architectures. To understand the behavior and its invariability, we conducted a case study on different microcontrollers such as Arduino mega 2560 and Arduino Uno (ATmega328P), estimated its minute voltage variations at different pin configurations using statistical parameters (mean, variance, and standard deviation). Figure 11 depicts the basic setup for analysis of extractions mismatches from Arduino microcontrollers.

3.1 Case1

Figure 12 depicts the design flow for analysis of mismatch variations in Arduino mega 2560. To investigate the amount of process variations that occurred in ICs, we

Table 1 Classifications of different PUF architectures

PUF	Challenge	Response	μinter(%)	μintra(%)	Entropy	Tamper evident
Optical PUF	Laser patterns	Hash of the speckle pattern	49	25.26	0.3 bit/pixel	yes
Basic arbiter PUF	Delay difference	arbiter decision	23	<5	–	yes
Feed-forward arbiter PUF	Delay difference	arbiter decision	38	<5	–	–
Ring oscillator PUF	Delay difference	Division compensated values	36	9.8	–	–
Ring oscillator PUF with the comparator	Loop pair selection	Counter value comparison	46.14	0.01	–	–
SRAM PUF	SRAM address	Power upstate of addressed SRAM cell	49.97	0.48	0.76 bit/pixel	–
Latch PUF	Latch selection	Settling state of destabilized NOR latch	50.55	<12%	–	–
Butterfly PUF	Butterfly cell selection	Settling state of destabilized NOR latch	50	3.04	–	–

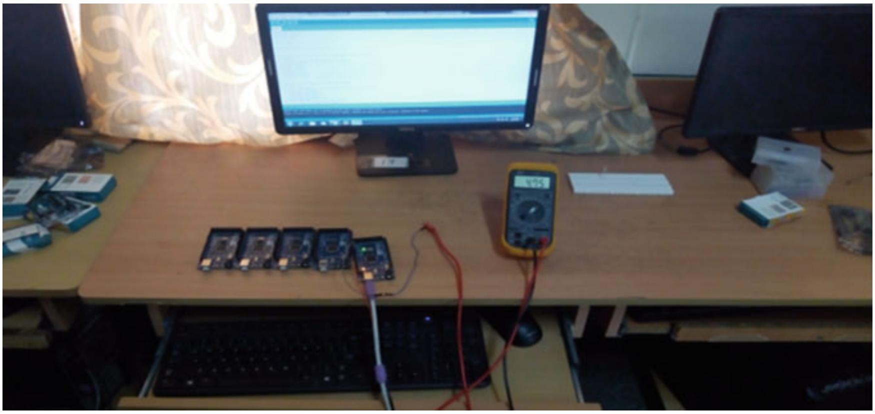


Fig. 11 Case study setup of analysis of random mismatch variations in microcontrollers

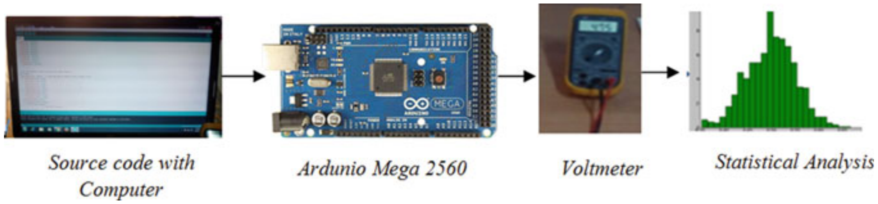


Fig. 12 Design flow for extracting keys from Arduino Mega 2560

Table 2 Technical specifications of the Arduino mega2560 microcontrollers

Microcontroller	ATmega2560
Operating voltage	5 v
Input voltage	7–12 v
Input voltage (limits)	6–20v
Digital I/O pins	54
Analog I/O pins	16
DC current per I/O pin	40 mA
Flash memory	256 KB
SRAM	8 KB
Clock Speed	16 MHz

have chosen a set of five Arduino microcontroller boards from same manufacturer and wrote the source code in embedded C. The generated code was dumped into all the microcontroller boards, and its response was taken at their corresponding pins using the voltmeter. However, to get a better understanding of the percentage of the mismatches, converted into statistical analysis and readings were measured in terms of mean, variance and standard deviation, respectively. Table 2 represents the basic technical specifications of the ATmega2560 and Tables 3 and 4 evaluate the voltmeter readings and statistical parameters of the Arduino mega microcontrollers.

From the above observation, the maximum amount of variations were noticed at board-2, whose mean value is 4.975, a variance is 0.000000038 and standard deviation be 0.055118060, respectively.

3.2 Case 2

In this section, we examine the Arduino Uno-based microcontroller (ATmega328P) in this setup essentially used 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 Analog inputs, with 16 MHz quartz crystal, and a USB connecter. The basic schematic of the Arduino UNO as shown in Fig. 13.

Table 3 Voltmeter readings of Arduino Mega 2560 microcontrollers

Pins	Input voltage	Clk frequency (MHz)	Board-1	Board-2	Board-3	Board-4	Board-5
2	5	16	4.75	4.98	4.72	4.98	4.95
3	5	16	4.78	4.97	4.79	4.98	4.96
4	5	16	4.76	4.98	4.79	4.97	4.69
5	5	16	4.78	4.97	4.79	4.97	4.98
6	5	16	4.76	4.97	4.80	4.98	4.98
7	5	16	4.78	4.97	4.79	4.97	4.89
8	5	16	4.77	4.98	4.80	4.98	4.87
9	5	16	4.76	4.97	4.80	4.97	4.89
10	5	16	4.91	4.98	4.81	4.91	4.96
11	5	16	4.92	4.98	4.80	4.95	4.96
12	5	16	4.79	4.97	4.80	4.98	4.98
13	5	16	4.96	4.98	4.80	4.98	4.89

Table 4 Statistical parameters of different Arduino microcontrollers

Arduino mega 2560	Mean	Variance	Standard deviation
Board-1	4.800	0.00288652	0.052915026
Board-2	4.975	0.00000038	0.055118060
Board-3	4.791	0.00046667	0.021602469
Board-4	4.975	0.00001875	0.043113013
Board-5	4.971	0.00001389	0.032072678

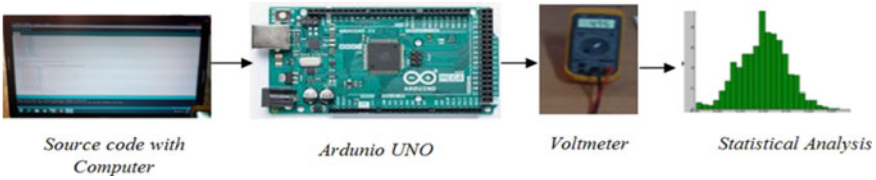


Fig. 13 Design flow for extracting keys from Arduino UNO

Like Arduino mega 2560, we investigated the amount of process variations occurred in Arduino Uno board, for that we have taken five Arduino Uno microcontroller boards from the same manufacturer, dumped in to the code and whose variations were measured by taking the readings using voltmeter by applying input voltage of 5v and clock frequency of 16 MHz, respectively—calculated the statistical parameters mean, variance, and standard deviation, respectively. Tables 5 and 6 represent voltmeter readings and statistical parameters of different Arduino Uno microcontrollers, respectively, and Table 7 represents the technical specifications of

Table 5 Voltmeter readings from Arduino Uno microcontrollers

Pins	Input voltage	Clk frequency (MHz)	Board-1	Board-2	Board-3	Board-4	Board-5
2	5	16	5.04	5.03	4.72	4.98	4.95
3	5	16	5.01	5.03	4.87	4.99	4.89
4	5	16	5.04	5.02	4.88	4.99	4.88
5	5	16	5.04	5.01	4.90	4.98	4.98
6	5	16	5.06	5.03	4.98	4.96	4.88
7	5	16	5.06	5.01	4.87	4.96	4.87
8	5	16	5.08	4.99	4.96	4.98	4.93
9	5	16	5.04	4.97	5.01	5.06	4.98
10	5	16	4.98	4.93	4.89	4.97	4.98
11	5	16	4.98	5.01	4.91	4.98	4.89
12	5	16	4.98	5.01	4.91	4.98	4.89
13	5	16	4.97	4.99	4.90	4.99	4.98

Table 6 Statistical parameters of different Arduino Uno microcontrollers

Arduino Uno	Mean	Variance	Standard deviation
Board-1	5.0066	0.00053889	0.02321398
Board-2	4.8842	0.00034145	0.00018465
Board-3	5.0133	0.00888899	0.06236096
Board-4	4.9825	0.00354265	0.00595119
Board-5	4.9141	0.00220764	0.04698552

Table 7 Technical specifications of the Arduino Uno microcontrollers

Microcontroller	ATmega328P
Operating voltage	5 v
Input voltage	7–12 v
Input voltage (limits)	6-20 v
Digital I/O pins	14
Analog I/O pins	6(A0-A5)
DC current on I/O pins	40 mA
Flash memory	32 KB
Frequency	16 MHz

the Arduino Uno microcontroller.

From the above case study, it is observed that the maximum amount of variations is noticed at board-3, whose mean value is 5.0133, the variance is 0.0088899, and the standard deviation be 0.06236096, respectively.

4 Conclusion

To estimate the mismatches that occurred in microcontrollers (Arduino 2560,uno) and estimated its statistical parameters like mean,variance and standard deviation. From the statistical static timing analysis observed, that same voltage has been applied and getting the different mean and standard deviation, respectively. From the analysis, even if the two ICs coming from the same wafer have different electrical characteristics, which are unavoidable, hence by extracting those information, we can generate the secrete keys which can be used for security applications; these types of phenomenon are commonly termed as PUFs.

References

1. J. Guajardo, S. Kumar, G. Schrijen, et al., FPGA intrinsic PUFs and their use for IP protection, in *Proceedings of CHES* (Vienna, Austria, 2007), pp. 63–80. https://doi.org/10.1007/978-3-540-74735-2_5
2. S. Kumar, J. Guajardo, R. Maes, et al., The butterfly PUF: protecting IP on every FPGA, in *Proceedings of HOST* (Anaheim, USA, 2008), pp. 67–70. https://doi.org/10.1109/HST.2008.4559053
3. R. Maes, D. Schellekens, I. Verbauwhede, A pay-per-use licensing scheme for hardware IP cores in recent SRAMFPGAs. IEEE Trans. Inf. Forensics Secur. **7**(1), 98–108 (2012). https://doi.org/10.1109/TIFS.2011.2169667
4. Y. Alkabani, F. Koushanfar, M. Potkonjak, Remote activation of ICs for piracy prevention and digital right management, in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, ser. ICCAD'07* (2007), pp. 674–677
5. G.E. Suh, C.W. O'Donnell, I. Sachdev, S. Devadas, Design and implementation of the AEGIS single-chip secure processor using physical random functions, in *Proceedings of the International Symposium on Computer Archietcture, ser. ISCA'05* (June 2005), pp. 25–36. https://doi.org/10.1109/ISCA.2005.22
6. U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, J. Schmidhuber, Modeling attacks on physical unclonable functions, in *Proceedings of the ACM Conference on Computer and Communications*. https://doi.org/10.1145/1866307.1866335
7. Y. Hori, T. Yoshida, T. Katashita, A. Satoh, Quantitative Performance Evaluation of Arbiter PUFs onFPGAs, in *IEICE-RECONF2010–37* (2010), pp.115–120. Security, ser. CCS '10 (2010), pp. 237–249. https://doi.org/10.1109/ReConFig.2010.24
8. C. Bösch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi, and P. Tuyls, "Efficient helper data key extractor on FPGAs," in *Cryptographic Hardware and Embedded Systems—CHES 2008* (Springer, Heidelberg, Germany, 2008), pp. 181–197. https://doi.org/10.1007/978-3-540-85053-3_12.
9. R. Maes, P. Tuyls, I. Verbauwhede, Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs, in *Cryptographic Hardware and Embedded Systems—CHES 2009* (Springer, Heidelberg, Germany, 2009), pp. 332–347. https://doi.org/10.1007/978-3-642-04138-9_24
10. S. Shaik, A.K. Kurra, A. Surendar, Statistical analysis of arbiter physical unclonable functions using reliable and secure transmission gates. Int. J. Simul. Syst. Sci. Technol. **19**(4) (2018). https://doi.org/10.5013/IJSSST.a.19.04.06
11. A.V. Herrewege, S. Katzenbeisser, R. Maes, Reverse fuzzy extractors: enabling lightweight mutual authentication for PUF-enabled RFIDs. Financ. Crypt. Data Secur. (FCDS), 374–389 (2012). https://doi.org/10.1007/978-3-642-32946-3_27

12. M. Rostami, M. Majzoobi, F. Koushanfar, D. Wallach, S. Devadas, Robust and reverse-engineering resilient PUF authentication and keyexchange by substring matching. IEEE Trans. Emerg. Top. Comput. (TETC) **2**(1), 37–49 (2014). https://doi.org/10.1109/TETC.2014.2300635
13. A.K. Kurra, U.R. Nelakuditi, A secure arbiter physical unclonable functions (PUFs) for device authentication and identification (2018)
14. U. Ruhrmair, J. Solter, F. Sehnke, X. Xiaolin, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, S. Devadas, PUF modeling attacks on simulated and silicon data. IEEE Trans. Inf. Forensics Secur. (TIFS) **8**(11), 1876–1891 (2013)
15. V.P. Yanambaka, S.P. Mohanty, E. Kougianos, P. Sundaravadivel, J. Singh, Dopingless transistor based hybrid oscillator arbiter physical unclonable function. Proceed. IEEE Comput. Soc. Ann. Symp. VLSI (ISVLSI) (2017). https://doi.org/10.1109/ISVLSI.2017.113
16. A. Kurra, U.R. Nelakuditi, Design of a reliable current starved inverter based arbiter physical unclonable functions (PUFs) for hardware cryptography. Ingénierie des Systèmes d Inf. **24**(4), 445–454 (2019). https://doi.org/10.18280/isi.240413
17. S.R. Sahoo, S. Kumar, K. Mahapatra, A modified configurable RO PUF with improved security metrics, in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems* (2016), pp. 320–324. https://doi.org/10.1109/iNIS.2015.37
18. A. Maiti, J. Casarona, L. McHale, P. Schaumont, A large scale characterization of RO-PUF, in *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 94–99 (2020). https://doi.org/10.1109/HST.2010.5513108
19. L. Bossuet, X.T. Ngo, Z. Cherif, V. Fischer, A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon. IEEE Trans Emerg. Top. Comput. **2**(1):30–36 (2013). https://doi.org/10.1109/TETC.2013.2287182
20. S. Shaik, A.K. Kurra, A. Surendar, High secure buffer based physical unclonable functions (PUF's) for device authentication. Telkomnika **17**(1) (2019). https://doi.org/10.12928/TELKOMNIKA.v17i1.10436
21. S.S. Kumar, J. Guajardo, R. Maes, G.J. Schrijen, P. Tuyls, The butterfly PUF protecting IP on every FPGA, in *IEEE International Workshop Hardware-Oriented Security and Trust (HOST)* (2008), pp. 67–70. https://doi.org/10.1109/HST.2008.4559053
22. A. Maiti, V. Gunreddy, P. Schaumont, A systematic method to evaluate and compare the performance of physical unclonable functions. IACR Cryptol. ePrint Arch. **657** (2011). https://doi.org/10.1007/978-1-4614-1362-2_11
23. A.K. Kurra, U.R. Nelakuditi,A decoder-mux based arbiter physical unclonable functions for low cost security applications, in *2019 International Conference on Communication and Electronics Systems (ICCES)* (IEEE, 2019). https://doi.org/10.1109/ICCES45898.2019.9002187
24. A. Maiti, I. Kim, P. Schaumont (2012) A robust physical unclonable function with enhanced challenge-response set. IEEE Trans. Inf. Forensics Secur. (2012). https://doi.org/10.1109/TIFS.2011.2165540
25. A.K. Kurra, U.R. Nelakuditi, A reliable current starved inverter based arbiter PUF architecture for IoT applications. Int. J. Eng. Adv. Technol. (IJEAT) **9**(1S5). ISSN: 2249 – 8958. https://doi.org/10.35940/ijeat.A1038.1291S52019

Social Distancing and Voice Alerting Using Unmanned Aerial Vehicles

Mayank Jain, Sansar Singh Chauhan, and Sanjeev Kumar Pippal

1 Introduction

During the outburst of the Spanish Flu in 1918s, Philadelphia organized a Liberty Load Parade on 28 September 1918, just 10 days after detecting its first case in which over 200,000 people gathered [1]. Over the next 6 weeks, a quarter of the population of Philadelphia was ill. This scenario outlines the potential severity of how exponentially a contamination can spread if not controlled properly and the need for deploying social distancing protocols during pandemics. Today, as the world is dealing with the global pandemic COVID-19, several measures are being deployed to prevent mass gatherings and maintain social distancing to control the outspread of the virus. The significance for maintaining social distancing can be estimated from the Spanish Flu and COVID-19 crisis. Cyberphysical systems such as Unmanned Aerial Vehicles (UAV) allows us to conduct aerial surveillance with their ability to fly over various places and its mobility offers a vast range of applications and potential use-case in tackling such situations. The model presented in this paper focuses on deploying UAV for maintaining social distancing between people in critical situations such as global pandemics. The model starts off by using an optical camera to capture video from the UAV. This algorithm presented in the paper is a reoccurrence algorithm and is triggered repetitively at a specified time interval. The algorithm is trained using Hierarchical Extreme Learning Machine (HELM) to detect the presence of humans. On detecting the presence of a human being, the number of detected bodies are counted. If the count exceeds more than two people in a range, the geolocation and coordinates for the involved beings are calculated using the drones telemetry and calculations [2]. Upon observation, if two people are in closer proximity than the

M. Jain (🖂)
Galgotias University, Greater Noida 201306, Uttar Pradesh, India

S. S. Chauhan · S. K. Pippal
G.L. Bajaj Institute of Technology & Management, Greater Noida 201306, Uttar Pradesh, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_21

minimum distance, an alert is notified to the involved persons using an integrated speaker on the UAV which plays a prerecorded audio clip. Furthermore, upon aerial surveillance using the UAV if the number of persons detected is found to be more than a specific count, a notification is issued to the local authorities notifying them about a possible mass gathering taking place at a region allowing them to deploy personnel to handle the situation and regulate gatherings ensuring safety and crowd control. The algorithm is set to reset and trigger itself again at a set time interval to ensure efficiency.

2 Related Work

Computer vision provides various methodologies to detect and identify humans. Several researchers and studies in this field have demonstrated the implementation of such systems and algorithms. Dalal and Triggs used HOG (Histogram of Oriented Gradients) feature descriptors with linear SVM model for detecting humans in an image [3].

However, with the advancement in technology, detecting humans using UAVs is also reaping momentum. Various sensors and algorithms have been used for detecting humans through UAVs.

Rudol and Doherty have used an integration of Optical and Thermal camera for detecting humans [4]. The thermal camera helped in limiting the search space while the optical camera helped in detect humans. Furthermore, humans in the frame were geo-localized using on-board GPS and telemetry data. However, each payload carries a weight. Due to the size constraints on a UAV, it can carry minimal weights due to which poor performance sensors must be used which decreases the precision of localizing targets.

UAVs have also been used for search and rescue missions. However, they are mainly effective for bodies lying on the ground or static.

A. Shobika and N. Thenkuzhali proposed a drone that hovers in disaster-hit area and helps identify the injured and performs rescue operations using PIR Sensors [5]. However, this solution is applicable for bodies at rest.

Estrada and Mario proposed deployment of UAVs in case of Pandemics [6]. However, the model proposed by them doesn't incorporate monitoring and ensuring social distancing measures.

Asanka G Perera and Ali Al-Naji1 proposed a model for detecting humans which employed R-CNN method for training. It combined region proposals with CNN [7].

Nouar AlDahoul and Aznul Qalid Md Sabri used automatic feature learning methods that combines opticals and different deep models (i.e., pretrained CNN feature extractor, supervised convolutional neural network (S-CNN), and HELM) for detecting humans in videos captured by the aerial optical camera [8].

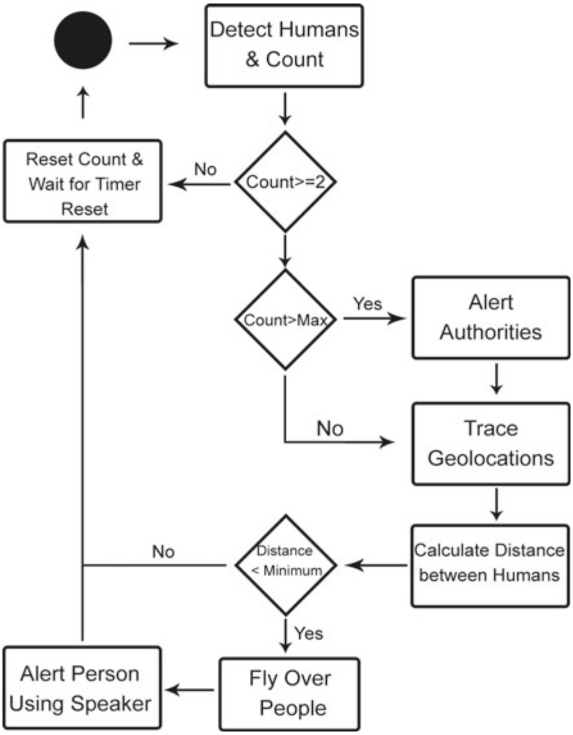
The HELM model is used in this study to detect humans using an optical camera attached to an UAV. Nemi Bhattarai and Tai Nakamura proposed a system capable of detecting humans from UAV camera in real time with the help of on-board telemetry data and further visualize the results in a GIS platform has been used in this paper for geo-localization of humans and calculating their coordinates [9].

3 Methodology

This section of the study proposes a system to help in regulating social distancing norms with the help of UAVs resulting in minimal human intervention and elaborates the workflow of the model (see Fig. 1).

An UAV equipped with an optical camera is deployed into the environment which captures and relays real-time footage. The camera detects the presence of human beings in the frame using HELM [10] which applies deep learning models to identify and detect humans. Furthermore, the number of people detected in the frame are stored in a variable. If more than one person is detected, the geolocation of the involved people is traced using the UAVs telemetry data, GPS, and Compass present on the UAV [11]. If the distance between any two persons is less than the minimum set distance, the UAV navigates to the persons coordinates and fires an alert using

Fig. 1 Workflow diagram of proposed model



speakers installed on the drone to notify the person and ensure social distancing is maintained. This section provides details on the functionality aspects and role of each component of the model.

3.1 Human Detection and Counting

For detecting humans in a region, an optical camera is used on an UAV which captures the video. The video frames serve as an input for stabilization by optical flow model which helps deal with fuzziness due to constantly moving frames. The computation from the optical flow model results in image patches for the human as well as non-human objects which are then utilized as inputs by the HELM. The model yields the type of representation of the object as the output.

3.1.1 Optical Flow Model for Stabilizing Background

The optical flow model plays a vital part for stabilizing the background since the optical camera is mounted on an UAV which is constantly in motion and hence tackles the video movement problem. It reckons the direction and speed of the motion vector amongst consecutive frames. Blob analysis is run for locating mobile objects in each binary feature images which can be produced upon performing morphological operations on motion vectors held by a threshold [3]. Finally, the detected objects are enclosed within boxes marked off by green boundaries.

3.1.2 Hierarchical Extreme Learning Machine (HELM)

HELM is an extension of Extreme Learning Machine (ELM) which was proposed by Guang-Bin Huang [10] which follows layer-wise learning. It is a fast and efficient unsupervised learning deep model which is capable of learning features automatically.

HELM randomizes the input weights and output weights and calculated analytically by closed form solutions. HELM outpaces the latest advancements in training speed since it learns without iteratively fine-tuning hidden neurons. In this deep model, the hidden layer parameters and input weights are initialized randomly, while output weights are analytically calculated. The output function fL(x) of the model can be given as

$$f_L(x) = \sum_{i=1}^{L} \beta_i G(a_i b_i x), \tag{1}$$

L = Number of hidden layer nodes
a_i b_i = Output function of ith hidden node
β_i = Output weight vector
HELM is a highly efficient model and gives a testing accuracy of 99.14%.

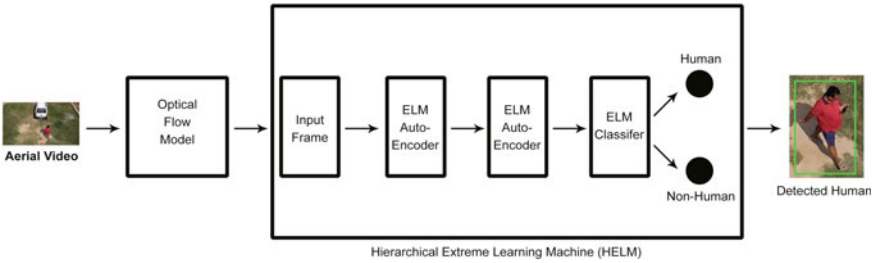


Fig. 2 Human detection workflow model

3.1.3 Detecting Humans Using HELM

In this study, HELM deep model has been utilized for detecting humans in video captured using the UAV-mounted optical camera in real time. After background stabilization has completed, HELM model is used for classifying objects into human and non-human classes. HELM makes use of ELM AutoEncoders to achieve feature learning in an unsupervised environment. The Deep nature of the model is incorporated by deploying multiple encoders which forms an ELM-AutoEncoder-based multi-layer HELM which doesn't require any iteration for fine-tuning the whole environment. Hence, it decreases the learning and time significantly by reducing the count of active neural nodes (see Fig. 2).

According to an experiment conducted by [8], the input layer comprised of a gray image having 100 * 100 pixels. This input is forwarded to the first ELM-AE having 1000 neurons. The AutoEncoder helps in dimensionality reduction. The first hidden layers output serves as the input for the second Autoencoder which has 1000 neurons too. Finally, the output transmits through an ELM-based classifier containing 12,000 nodes which is connected to the 2 output nodes within the last output layer that determines the class of the detected object that is human or non-human. It was found that using HELM which runs on CPU, the training time was 445 s while the testing time for one sample was 0.1 s.

The number of objects classified as human bodies are stored in a variable to count the presence of humans in a region.

3.2 Geolocalization and Coordinate Projection

This section determines the calculations and procedures for estimating the positioning and co-ordinates of the detected human in the world frame and units. Since the frames are captured from aerial perspective in digital image format, therefore each point on the image is a pixel.

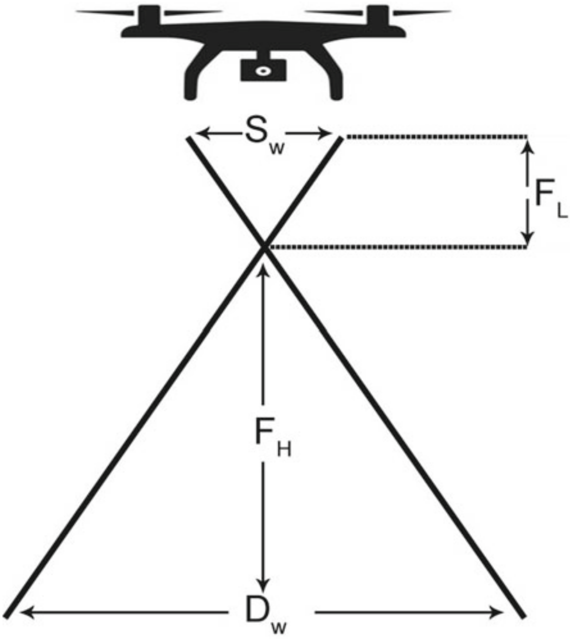


Fig. 3 Optical camera angled towards ground

Hence, for calculating the distance or the coordinates of a person, it's vital to know how much distance each pixel on the frame covers for which we calculate the Ground Sampling Distance (GSD) of the drone which can be calculated as (see Fig. 3):

$$\text{GSD} = \frac{F_H \times S_W}{F_L \times I_W}, \tag{2}$$

where GSD= Ground Sampling Distance

F_H= Flight Height, S_w= Sensor Width

F_L= Focal Length, I_w = Image width (Pixels)

As the camera is inclined downwards, it follows a different co-ordinate system than the world. Right direction marks the positive x axis, while the downwards direction arks the positive y axis.

The center of the image in Image coordinate system is given by Ci = $(C_i x, C_i y)$, while in the World coordinate system it is given as Cw = (Cwx, Cwy). Cw can be directly inferred using the GPS mounted on the UAV. The Human coordinates detected by the UAV is given as H = $(H_i x, H_i y)$ (see Fig. 4).

The calculations and equations in [4] have been used to calculate the human coordinates. The vector from the center of Image to the Humans location can be determined cf. Eq. 3:

$$\overrightarrow{CH} = (H_x^i - C_x^i)\overrightarrow{i} + (H_y^i - C_y^i)\overrightarrow{j}\,. \tag{3}$$

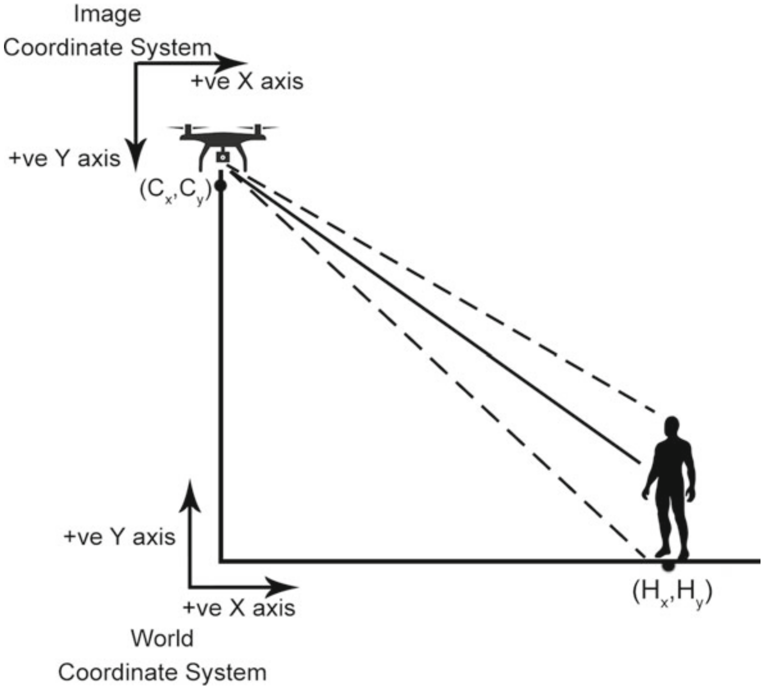


Fig. 4 World and image coordinate systems

The length of vector (world units) can be given as [2]

$$||\overrightarrow{CH}||^{W} = \sqrt{((H_x^i - C_x^i) \times GSD)^2 + ((H_y^i - C_y^i) \times GSD)^2}. \qquad (4)$$

Angle θ measures the deviation of True North to the vertical. The image frame is rotated by θ degrees such that the North gets aligned at the top according to the world coordinates.

$$\varphi = \begin{cases} -\theta, x < 0 \\ \theta, \ x \geq 0 \end{cases} \qquad (5)$$

Using trigonometric functions, the new Human Coordinates H' as per the image plane can be determined using:

$$\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} H_x^i - C_x^i \\ H_y^i - C_y^i \end{bmatrix} = \begin{bmatrix} H_x^{'i} \\ H_y^{'i} \end{bmatrix}. \qquad (6)$$

Table 1 Coordinates calculation for a human in world frame

	$H_x^{'w}$	$H_y^{'w}$
Quadrant 1	$C_x^w + \|\|\overrightarrow{CH}\|\|^w \cos\varphi$	$C_y^w + \|\|\overrightarrow{CH}\|\|^w \sin\varphi$
Quadrant 2	$C_x^w - \|\|\overrightarrow{CH}\|\|^w \cos\varphi$	$C_y^w + \|\|\overrightarrow{CH}\|\|^w \sin\varphi$
Quadrant 3	$C_x^w - \|\|\overrightarrow{CH}\|\|^w \cos\varphi$	$C_y^w - \|\|\overrightarrow{CH}\|\|^w \sin\varphi$
Quadrant 4	$C_x^w + \|\|\overrightarrow{CH}\|\|^w \cos\varphi$	$C_y^w - \|\|\overrightarrow{CH}\|\|^w \sin\varphi$

Based on the quadrant in which the rotated vector settles four cases can be drawn, a new angle φ is used to make the vector angle positive and acute [4] such that: Finally, the coordinates of the detected human being can be found using cf. Table 1.

Using Table 1, the coordinates of human in world frame can be obtained.

3.3 Distance Calculation Between Humans

Using the UAVs telemetry data, we get information about the UAVs flight height, longitude, latitude, and the compass heading. And the calculations and equations given above gives the human coordinates (longitude and latitude) and the angle THETA which can be plotted on a Geographical Information System. The above information is stored in a structured format for each detected human patch. Now, for all the detected humans in a frame, T number of pairs between total detected humans can be made (see Fig. 5).

For the first person in N humans, the first persons distance can be calculated with $(N-1)$ humans. Similarly, the second person can be paired with $(N-2)$ humans. Therefore, the total number of possible pairs for calculating the distance amongst can be given by

$$T = (N-1) + (N-2) + \ldots\ldots + (N-(N-1)). \tag{7}$$

Alternatively, the formula for combinations can be used for finding the total number of possible pairs of 2 humans from N people:

$$^{N}C_2 = \frac{N!}{2! \times (N-2)!}. \tag{8}$$

The equation can be furthered expanded to

$$^{N}C_2 = \frac{N \times (N-1) \times (N-2)!}{2! \times (N-2)!}. \tag{9}$$

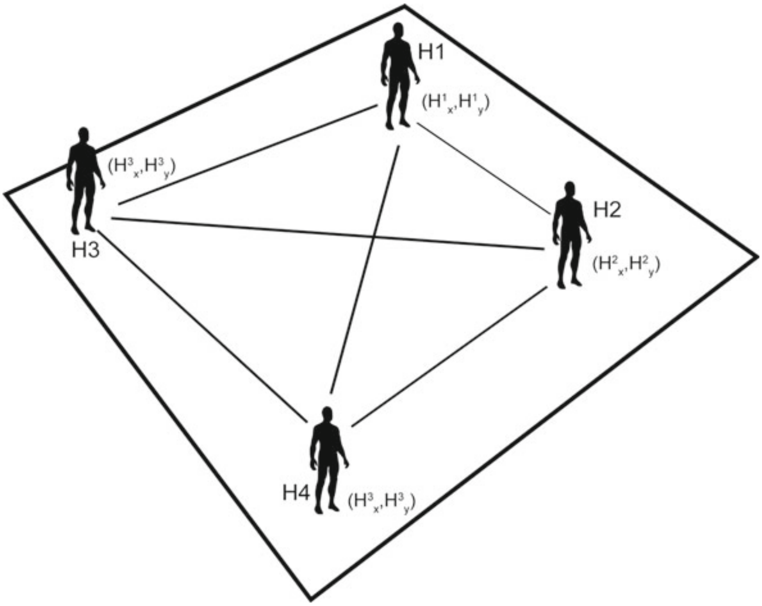


Fig. 5 Number of possible pairs between 4 humans

On simplifying and solving Eq. 8, the total number of pairs (T) which can be formed between N detected humans can be given as

$$T = \frac{N(N-1)}{2}. \tag{10}$$

The set of T pairs containing each possible pair of two humans can be given as Let the set be defined by symbol X.

$$X = \{(H_i, H_j) : i, j \in N \; \forall \; i \not\equiv j, \; i < j\}, \tag{11}$$

where N = Total number of detected humans in a frame.

For each pair of human in the set X, the distance Dij between Human Hi and and Human Hj can be calculated using cf. Eq. 12.

$$D_{ij} = \sqrt{|((H^i_x - H^j_x)^2 - (H^i_y - H^j_y)^2)|}, \tag{12}$$

where (Hi, Hj) represents one element out of all possible elements in the set of T possible pairs of two human beings.

3.4 Alert Triggering and Crowd Control

Once the distance between every possible pair of human detected in a frame is calculated, each value is checked against a minimum set criteria value which determines if two humans are in close proximity or not maintaining social distancing norms.

If any of the distance values is found to be less than the minimum distance to be maintained, the UAVs navigation system is set to fly over to the humans' co-ordinates by setting a Navigation Waypoint for the UAV using the on-board GPS system and play a prerecorded audio clip using an on-board speaker to alert the human and ask it to maintain required social distance. Once every person disobeying the social distancing norms is alerted in case the detected number of humans is low and all the alerts can be issued within the set algorithm reset time interval, humans count is reset to zero.

The UAV is also set to re-activate human sensing and resetting the detection count and to zero and restarting the algorithm automatically at a fixed interval of time to avoid navigating to a humans' position well after he has moved on due to the time delay in case of navigating the drone to multiple locations in case the count of humans exceeds a specific count.

This approach refrains the UAV from:

- Alerting a specific human after it has moved far away from his position in case the human was in motion.
- Issuing multiple alerts at clear coordinates making the system inefficient and causing chaos.
- Buffer overflow and high time delays in case many people are gathered and detected in an area.

Additionally, the proposed system helps in crowd detection and control measures. If the human detection count exceeds a pre-defined set number of humans, a notification is issued to the local authorities notifying them about a possible crowd gathering in real time to which personnel can be deployed to handle the situation and regulate the crowd. The UAV coordinates (latitude, longitude) which can be obtained using the mounted GPS and UAVs telemetry data are relayed with the notification message to communicate the point of gathering.

Henceforth, local authorities can take required actions to control mass-gatherings and ensure social distancing, safety and crowd control without the necessity to keep patrolling and be omnipresent for ensuring social distancing measures also allowing them to monitor situations from a central point of observation by using UAVs for aerial surveillance.

4 Algorithm

```
$count \Leftarrow 0$
Start Time Countdown
Trigger Human Detection Algorithm using HELM
**if** Human(s) are Detected **then**
    Count Humans and set count variable.
    **if** $Count$ >Allowed Crowd Gathering **then**
        Alert Local Authorities
    **end if**
    Track geolocation for every human.
    Make T pairs for humans.
    **for** each element in set X **do**
        Calculate distance between Hi and Hj
        **if** Time remaining> 0 **then**

            **if** $Distance$ <Minimum Distance **then**
                Navigate UAV to Humans coordinates
                Alert Human through a Prerecorded Audio Clip using on-board Speaker
            **end if**
        **else**
            Goto Start
        **end if**
    **end for**
**end if**
**while** $Timer > 0$ **do**
    Wait
**end while**
Goto Start
```

5 Conclusion and Future Works

In this study, we have proposed a model which can be used to ensure social distancing between humans and keep a minimum distance between every two humans in a region. It leverages technological advancements to tackle global pandemic like COVID-19 and ensure safety and control the spread of contamination.

The model first uses HELM model to detect the presence of humans in the region where the UAV is hovering over.

The total number of detected humans is stored in a count variable. On discovering two or more persons in a region, the geolocation of each human is found using the GPS system, telemetry data of the UAV, and given calculations and equations.

The distance between each pair of human is then calculated using calculations. If the distance between two humans is found to be less than the minimum distance the UAV is set to navigate over the specific human using his coordinates.

A prerecorded audio clip alert is played to the respective human using an on-board speaker to defer to the set social distancing norms and reposition itself.

This model hence minimizes needed human intervention for maintaining social distancing and helps in covering larger regions without the need for deploying mass personnel for regulating crowds. Furthermore, it can help the authorities in responding to emergency situations or large crowd gatherings.

References

1. C.M. Stetler, The 1918 Spanish influenza: three months of horror in Philadelphia. Pa. Hist. A J. Mid-Atl. Stud. **84**(4), 462–487 (2017). JSTOR. www.jstor.org/stable/10.5325/pennhistory.84.4.0462
2. C. Luo, W. Miao, H. Ullah, S. McClean, G. Parr, G. Min, *Unmanned Aerial Vehicles for Disaster Management* (2019). https://doi.org/10.1007/978-981-13-0992-2_7
3. N. Dalal, B. Triggs, Histograms of oriented gradients for human detection, in *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, vol. 1 (San Diego, CA, USA, 2005), pp. 886–893. https://doi.org/10.1109/CVPR.2005.177
4. P. Rudol, P. Doherty, Human body detection and geolocalization for UAV search and rescue missions using color and thermal imagery, in *IEEE Aerospace Conference. Big Sky, MT*, pp. 1–8 (2008). https://doi.org/10.1109/AERO.2008.4526559
5. A. Shobika, N., Thenkuzhali, S. Suganya, G.R. Nivedha, R. Hiemaja, Human detection system using drone for earthquake rescue operation, in *2018 International Journal of Advanced Research in Computer and Communication Engineering*, vol. 7, Issue 4 (2018)
6. A. Ruiz Estrada, *Mario: The Uses of Drones in Case of Massive Epidemics Contagious Diseases Relief Humanitarian Aid: Wuhan-COVID-19 Crisis* (2020). https://doi.org/10.13140/RG.2.2.25794.94402
7. A.G. Perera, A. Al-Naji, Y.W. Law, J. Chahl, Human detection and motion analysis from a quadrotor UAV, in *2018, IOP Conference Series: Materials Science and Engineering 405* (2018) https://doi.org/10.1088/1757-899X/405/1/012003
8. N. AlDahoul, A.Q. Md Sabri, A.M. Mansoor, Real-time human detection for aerial captured video sequences via deep models, in *2018, Computational Intelligence and Neuroscience* (2018), 14 pp. Article ID 1639561. https://doi.org/10.1155/2018/1639561
9. N. Bhattarai, T. Nakamura, C. Mozumder, Real Time Human Detection and Localization Using Consumer Grade Camera and Commercial UAV. Preprints 2018, 2018110156. https://doi.org/10.20944/preprints201811.0156.v1
10. G.-B. Huang, Q.-Y. Zhu, C.-K. Siew, Extreme learning machine: theory and applications. Neurocomputing **70**(1), 489–501 (2006)
11. H. Hosseinpoor, F. Samadzadegan, F. Dadrass Javan, Pricise target geolocation and tracking based on UAV video imagery, in *ISPRS—International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. XLI-B6*, pp. 243–249 (2016). https://doi.org/10.5194/isprs-archives-XLI-B6-243-2016

Plant Leaf Disease Identification Using Unsupervised Fuzzy C-Means Clustering and Supervised Classifiers

Priya Kohli, Indrajeet Kumar, and Vrince Vimal

1 Introduction

Plants are very crucial for mankind and are thus used in many sectors in the form of raw material in various industries, or the medical field. It also helps in maintaining environmental conditions well. Thus, it is very much important to protect plants from extinction through human, natural disasters, and various diseases. There are various plant disease which can affect plant from growing like Anthracnose are spots of different sizes and colors on the leaf, leaf blights are very tiny spots with a large number on the leaf, rust pustules are yellow, orangish-red, brown, black on the leaf. Leaves die quickly with such a disease. Powdery mildew is a very common problem in vegetables and grains. Downy mildew is pale yellow on the surface of the leaf [1].

Many techniques and tools were adopted in past years to protect plants. But the results were not very much efficient. Therefore, it is very crucial to identify and characterize them into proper class plants with accuracy. Though it is not easy to identify and classify every plant species through naked eyes. Laboratory testing sounds good but is quite expensive. A combination of mathematics and computation can provide us with the best and accurate results [15].

Automated plant leaf identification and classification majorly include image procurement, pre-processing of an image, extraction of features, and classification based on of length, width, height, color, texture, etc. This work proposes a mechanism to identify and characterized diseased plant leaf using digital images as input. Apart from all four leaf identification steps, this study also includes image segmentation using FCM clustering for better and optimized results. In image segmentation, for selecting a segment ROI is being used. For the classification of diseased images,

P. Kohli (✉) · I. Kumar · V. Vimal
Graphic Era Hill University, Dehradun, Uttarakhand, India

I. Kumar
e-mail: ikumar@gehu.ac.in

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_22

three experiments are done using machine learning algorithms, SVM, PNN, and KNN. Based on those experiments, overall classification accuracy is calculated in all the cases [2].

Machine learning is a marvelous tool to read the pattern and to predict based on that learning. Machine learning has a wider scope in real time whether to predict the weather, credit card fraud, online transaction frauds, Data stealing, etc. If the accurate and large number of datasets are provided while training and testing, the machine can learn from the past patterns of cyber frauds and can predict it with much more accuracy. It can even respond or can take suitable actions while predicting any fraud. They learn from previous computations to produce reliable, and repeatable decisions. It can be used to prevent cybercrimes as well. Machine learning focuses on learning the pattern and thus can prevent any threat or attack and can help the cybersecurity team to prevent any loss using the pattern learning concept [22].

Apart from preventing cyberattacks [22], machine learning is widely used in image recognition for easily identifying various objects present in the digital image or facial recognition, product recommendation based on the searches or viewed products, health care for predicting various diseases like a tumor, cancer, etc. Machine learning became very popular after the development of virtual assistants like Siri, Google Assistant, Alexa, etc., which can respond to humans based on experience and training. Machine learning is also helpful in predicting traffic while finding the best and shortest way to the destination like maps.

The remainder of the manuscript is being ordered as Sect. 2 presents the review of literature related to plant disease detection and classification using various mathematical models. Section 3 gives a summing-up and detailed description of the used materials and methodology. Next, Sect. 4 describes the experiments and result from the analysis of the proposed work. In the final section, Sect. 5 concludes the work.

2 Literature Review

In the area of plant leaf disease identification and classification, so much work has been already done in the past. A brief description of previously published work has been discussed here. Firstly, Kaur et al. present plant categorization using multiclass-SVM. 1125 images of 15 different species were used from Swedish datasets. The accuracy after applying the algorithm is 93.26% [2]. Pankaja et al. proposed a plant leaf classification using the SVM classifier. The datasets were taken from Flavia and the testing was applied on 250 images and accuracy obtained was 96.29% [3]. While Mahapatra et al. showcase plant leaf classification and recognition of diseased leaf using SVM. The accuracy rate achieved for classifying and recognition of plants was 91% [4]. Ahmed et al. presented the classification of plant species using SVM. The datasets were taken from Flavia with 32 different species of 1800 images. Training and testing were done in 1800 and 100 images. The accuracy rate obtained was 87.40% which is less [5]. Another study proposed by Turkoglu et al. for leaf-based classification using SVM. A Multi-class SVM (MCSVM) was used for classification.

90.7% of accuracy was obtained during training and testing [6]. Lukic et al. proposed an approach for plant leaf classification and recognition using the SVM classifier. Datasets were used from Flavia and classification was done based on surface, color, and the shape of the plant leaf. An accuracy of 94.13 was achieved [7]. Kumar et al. presented an approach for classifying plant leaf using an SVM classifier. Testing was done in three phases using different plant leaf features. Training and testing were done on 80% and 20%, respectively. Datasets were taken from Flavia. The overall accuracy of 97.64 was obtained [8]. Wang et al. proposed a review to identify plant using image processing. The SVM classifier was concluded to get the best and accurate results [9]. Another approach was proposed by Ali et al. for plant leaf recognition and classification using an SVM classifier. The classification was done on Bag-of-features (BOF) and Local binary patterns (LBP). The accuracy of 99.4% was achieved during training and testing [10]. Sahay et al. proposed an algorithm for plant leaf recognition using the KNN classifier. The testing phase was divided into three phases. After every testing phase, 15% of the improvements were there [11]. Zhang et al. proposed an approach for plant leaf recognition based on CCD and LDCCA. The classification was done using KNN.1000 images of 20 different species that were taken for training and testing [12]. Another approach proposed by Codizar et al. for plant leaf recognition using ANN. The leaf classification was done using the shape and venation of the leaf image in the dataset. After applying ANN for classification, an accuracy of 95% was obtained [13]. De Luna et al. showed cases an approach for the Philippine herbal medicinal plant using ANN classifier. After performing, the accuracy of 98.61% was achieved [14]. Turkoglu et al. presented another approach to classifying a plant leaf by splitting leaf images into two and four parts. Datasets were taken from Flavia with a 1907 leaf of 32 different species. The proposed technique uses the ELM method as a classifier and GLCM method for feature extraction. The accuracy after non-splitting was 97.68%, while the accuracy after applying the bisection method was 99.10% [15]. Yang et al. proposed plant recognition using TDR (Triangle Distance Recognition). The datasets were taken from Swedish, Flavia, ImageCLEF2012, and Smithsonian. The decision of the system was based according to geometrical feature of the leaf and texture was neglected throughout [16]. Zheng et al. presented an infected plant leaf detecting using a capsule neural network. ICL leaf datasets were used. The proposal on the capsule neural network shows better results as compared to CNN [17]. Pankaja et al. presented mango leaf recognition using MFO based on the DPN method. The accuracy rate was 98.5% when applied on five different sets of mango [18].

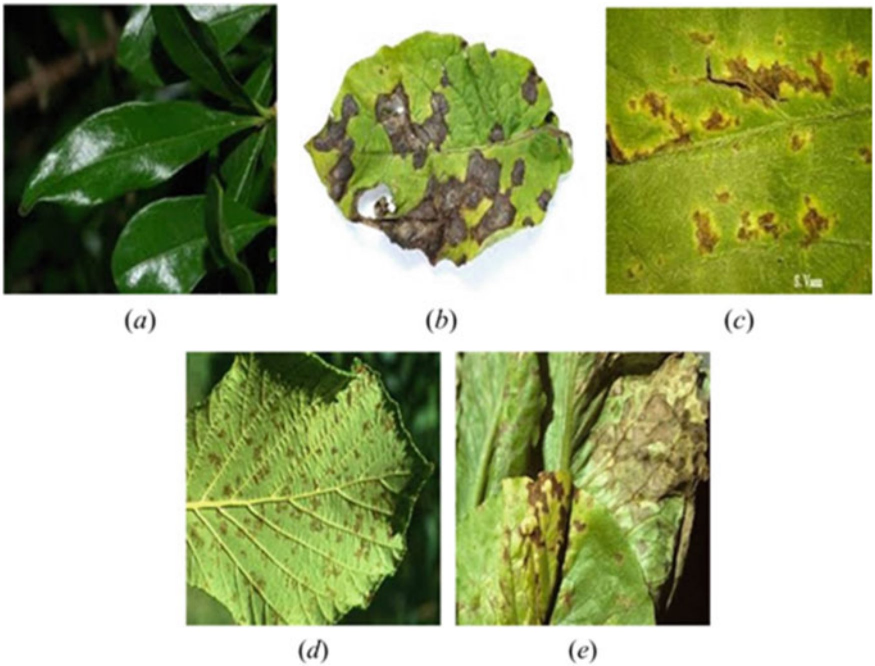


Fig. 1 Sample images are taken from the used dataset. *Note* **a** Healthy class image, **b** alternari-aalternata class image, **c** anthracnose class image, **d** bacterial blight class image, and **e** Cercospora leaf spot class image

3 Material and Methodology

3.1 Dataset Preparation

In this work, a total set of 250 images of plant leaves is considered. Among 250 images 50 images of healthy class, 50 images of AlternariaAlternata, 50 images of Anthracnose, 50 images of Bacterial Blight, and 50 images of Cercospora Leaf Spot are used. All images are stored in the system having configuration 512 GB SSD, Intel@i7 processor, 2.3 GHz with 8 GB RAM. The sample image of each class is shown in Fig. 1.

3.2 Proposed Work

The experimental workflow diagram of the proposed work for plant leaf disease identification using unsupervised fuzzy c-means clustering and supervised classifiers is shown in Fig. 2. The proposed work is consisting of a preprocessing unit,

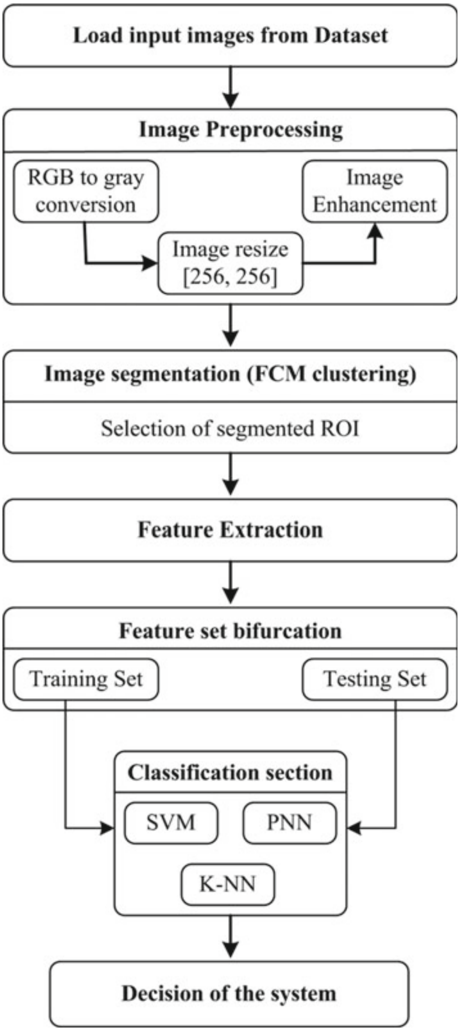


Fig. 2 Experimental workflow diagram of the proposed work for plant leaf diseases identification using unsupervised fuzzy c-means clustering and supervised classifiers

segmentation unit, feature extraction, and bifurcation unit and classification unit. A brief illustration of each segment is given in succession here.

Image Preprocessing Unit

The main purpose of this segment is to have all the input images of similar properties and equal size so that the proposed system can work accurately. Therefore, the complete set of input images is initially converted into grayscale, and then further converted image is resized to 256 × 256 pixels and then performs denoising and histogram linearization for image enhancement. The histogram linearization is mathematically expressed as

$$s_k = T(r_k) = \frac{(L-1)}{M \times N} \sum_{j=0}^{k} n_j \tag{1}$$

$$\text{Here } k = 0, 1, 2, 3, \ldots, (L-1)$$

Segmentation Unit

In this work, Fuzzy C-Mean (FCM) is used for infected portion segmentation. The FCM was proposed by Dunn in 1974 study [19] and later was extended as study in [20]. The calculation of FCM is a petitious approach that delivers an exemplar c parcel by specifying the weighted inside bunch $\{x_k\}_{k=1}^{N}$ whole of squared mistake target work J_{FCM}.

$$J_{FCM} = (A, B) = \sum_{i=1}^{c} \sum_{k=1}^{N} \mu_{ik}^{p} \|x_k - b_i\|^2 \tag{2}$$

where $B = \{b_i\}_{i=1}^{c}$ is the example of cluster and array $A = \{\mu_{ik}\}$ represents the partition array, c is cluster count centroid, N used for the data point numbers, x_k is the kth pixel, and b_i is the centroid of the ith cluster.

In this work, segmented image is divided into three clusters. For feature extraction, one cluster is selected known as segmented ROI passed to the next module called feature extraction. The output of the segmentation section is demonstrated in Fig. 3.

Feature Extraction and Feature Set Bifurcation Unit

The segmented ROI is passed to a feature extraction unit where statistical models are used for feature extraction. A set of 13 attributes is an excerpt for each input image. The feature vector of length 13 is further divided into two feature sets named training feature set and validating feature set. The training feature set is used for classifier building and the validating set is used for trained model evaluation. The description of the training and validating feature set is demonstrated in Table 1.

From Table 1, it has been scrutinized that 250 digital images are used for the research. Among the 250 images, 50 instances of each category are considered. The training and validating attribute set is created using a balanced bifurcation of the total dataset. Therefore, 125 instances are considered as a training set and the remaining 125 instances are considered for the validating set.

Classification Unit

The classification task of the urged system for plant leaf disease identification using unsupervised fuzzy c-means clustering and supervised classifiers is performed by SVM, PNN, and KNN classifiers. The description of each model is given here one by one.

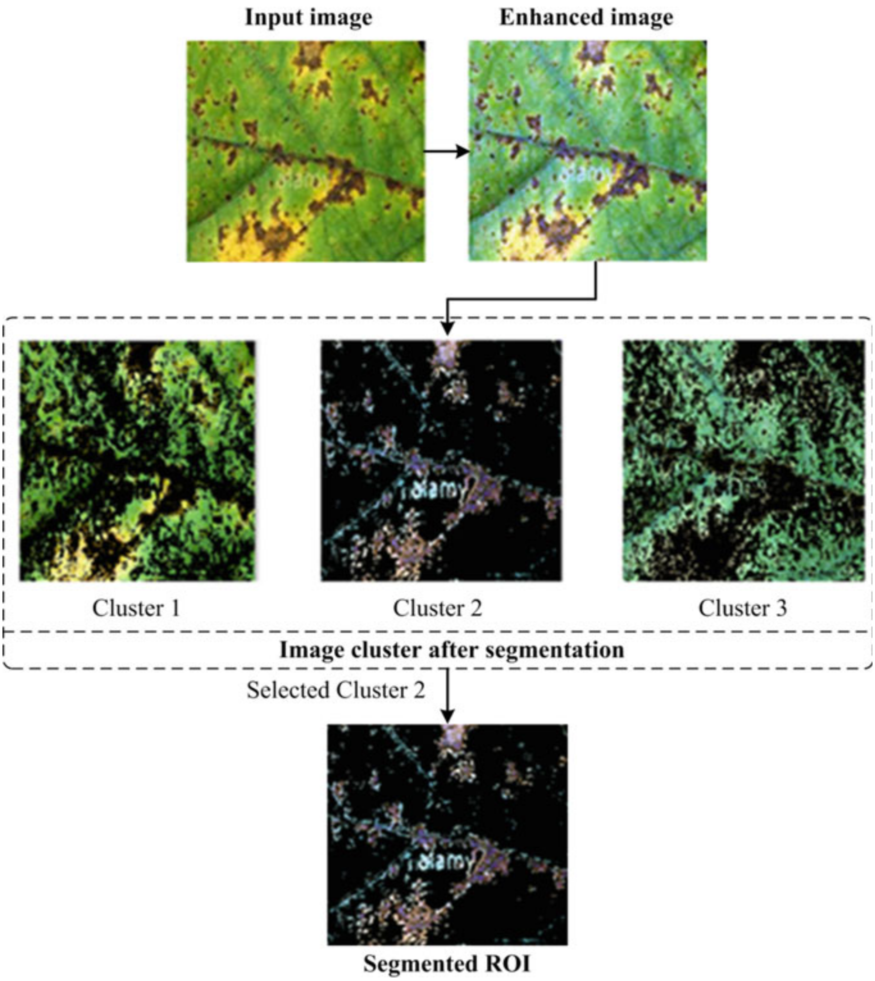


Fig. 3 Result of the segmentation section

Table 1 Characterization of training and validating feature set

Class name	Total sample	Number of samples in training feature set	Number of samples in validating feature set
Healthy	50	25	25
Alternariaalternate	50	25	25
Anthracnose	50	25	25
Bacterial blight	50	25	25
Cercospora leaf spot	50	25	25
Total	250	125	125

SVM Classifier

SVM stands for the support vector machine. In the coeval work, the design of IDS is done with the support of RBF (Radial Basis Kernel), also known as Gaussian kernel, which is based on SVM classifier (accessible in LibSVM library) [21]. The RBF kernel is used in assorted disparate learning of kernels that engage absolute amplitude attribute space and filigree search with cross-validation on two instances a and a', illustrate trait vectors in some input space, is exemplified as

$$KER(a, a^{'}) = \exp\left(-\frac{\left\|a - a^{'}\right\|^{2}}{2\sigma^{2}}\right) \tag{3}$$

where $\left\|a - a^{'}\right\|^{2}$ is identified as the squared Euclidean distance (SED) among the two feature vectors and σ is a free parameter.

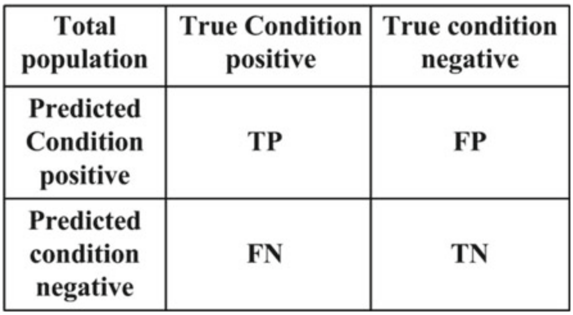
PNN Classifier

The PNN classifier dwells four important layers. Those are the input layer in which every neuron serves a predictor value, the pattern layer which consists of one neuron for each case while training datasets, the summation layer which contains one pattern neuron for each category, and the output layer which analyzes the weighted votes for each target category and uses largest vote to forecast the targeted category. The used classification algorithm caters to an anticipation density function and enhanced the width value of kernel for all categories accessible in the training dataset. The RBF kernel function is used and the width of the RBF is computed by the spread parameter symbolizes as S_p. In the ongoing study, the optimal value of S_p is culled by imitated experiment for classifier blueprint by treading through diversified values of $S_p$inclining from 1 to 10. After the PNN (Probabilistic Neural Network) classifier is schooled with the optimal value of S_p,it is then tested with a decreased occurrence of the testing dataset.

KNN Classifier

In the K-Nearest Neighbor classifier Euclidean separation is used for selection of closest neighbors [22]. It attempts to bunch the cases of highlight features into put out of articulation classes with a presumption that the occurrences of highlight features lying near one another in include space that speaks to occasion having a place with an identical class. The label of an obscure testing sample is chosen to be the label of lion's share of cases along with its k-closest neighbors in the preparation set. The benefit of the KNN classifier is its capacity to manage different class issues and is powerful to loud information as it midpoints the k-closest neighbors. The characterization execution is influenced by differing boundary k. In this task, the estimation of k is improved by rehashed experiment for model configuration by venturing through by 1 fluctuating from 1 to 15, and if the similar attainment is accomplished for more than one value of k the minimal value of k is contemplated.

Fig. 4 Structure of the confusion matrix



Total population	True Condition positive	True condition negative
Predicted Condition positive	TP	FP
Predicted condition negative	FN	TN

Staging Analysis Parameters

The performance parameters PPV, TPR, OCA, and MCA [24] are computing using the following mathematical expressions:

$$\mathrm{PPV} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \times 100\% \tag{4}$$

$$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \times 100\% \tag{5}$$

$$\mathrm{OCA} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \times 100\% \tag{6}$$

$$MCA = \frac{FP + FN}{TP + TN + FP + FN} \times 100\% \tag{7}$$

The structure of the confusion matrix is given in Fig. 4.

4 Experiment and Results

In this work, extensive work has been carried out through the entire experiments. Initially, input images are passed to the image preprocessing unit and the segmentation unit. After the segmentation, selected ROI is passed to the feature extraction unit, where a set of 13 features are extracted for each input image. The extracted character set is further split into training set and testing feature set. The training feature set is adopted to train the SVM, PNN, and KNN classifier, and the trained classifier model is validated on the testing set. Throughout the work, three important experiments have been carried out. The detail of the experiments drifted out for the work is showcased in Table 2.

Table 2 Detail of the experimentation

Experiment no. #	Depiction
Experiment no. 1	An experiment carried out for plant leaf disease characterization using unsupervised FCM clustering and SVM classifier
Experiment no. 2	An experiment carried out for plant leaf disease characterization using unsupervised FCM clustering and PNN classifier
Experiment no. 3	An experiment carried out for plant leaf disease characterization using unsupervised FCM clustering and KNN classifier

Experiment 1: In this experiment SVM classifier is used and 125 samples are practiced training the SVM model and the trained model is tested on 125 samples. The obtained results for the experiment are injured in Table 3.

Experiment 2: The same feature set of training and testing is used for this experiment on the PNN classifier. The achieved outcomes are reported in Table 4.

Table 3 Results obtained for experiment 1

	Confusion matrix					PPV (%)	TPR (%)	OCA (%)	MCA (%)
	HC	AAC	AC	BBC	CLSC				
HC	25	0	0	0	0	100	100	98.4	1.6
AAC	0	24	0	1	0	96.0	96.0		
AC	0	1	24	0	0	96.0	100		
BBC	0	0	0	25	0	100	100		
CLSC	0	0	0	0	25	100	100		

Note HC: Healthy Class; AAC: Alternariaalternata Class; AC: Anthracnose Class; BBC: Bacterial Blight Class; CLSC: Cercospora Leaf Spot Class; PPV: Positive Predictive Value; TPR: True Positive Rate; OCA: Overall Classification Accuracy; MCA: Mis-Classification Accuracy

Table 4 Results obtained for experiment 2

	Confusion matrix					PPV (%)	TPR (%)	OCA (%)	MCA (%)
	HC	AAC	AC	BBC	CLSC				
HC	24	0	0	0	1	96.0	100	94.4	5.6
AAC	0	24	1	0	0	96.0	92.3		
AC	0	1	24	0	0	96.0	92.3		
BBC	0	0	1	23	1	92.0	95.8		
CLSC	0	1	0	1	23	92.0	92.0		

Note HC: Healthy Class; AAC: Alternariaalternata Class; AC: Anthracnose Class; BBC: Bacterial Blight Class; CLSC: Cercospora Leaf Spot Class; PPV: Positive Predictive Value; TPR: True Positive Rate; OCA: Overall Classification Accuracy; MCA: Mis-Classification Accuracy

Table 5 Results obtained for experiment 3

	Confusion matrix					PPV (%)	TPR (%)	OCA (%)	MCA (%)
	HC	AAC	AC	BBC	CLSC				
HC	25	0	0	0	0	100	100	95.2	4.8
AAC	0	24	1	0	0	96.0	92.3		
AC	0	1	24	0	0	96.0	92.3		
BBC	0	1	1	22	1	88.0	95.6		
CLSC	0	0	0	1	24	96.0	96.0		

Note HC: Healthy Class; AAC: Alternariaalternata Class; AC: Anthracnose Class; BBC: Bacterial Blight Class; CLSC: Cercospora Leaf Spot Class; PPV: Positive Predictive Value; TPR: True Positive Rate; OCA: Overall Classification Accuracy; MCA: Mis-Classification Accuracy

Experiment 3: In this experiment, the KNN classifier is used and the same training and testing feature set as Experiment 1 and Experiment 2 is used for KNN classifier training and testing. The obtained outcomes are reported in Table 5.

Comparative Analysis

The contingent scrutiny of Experiment 1, Experiment 2, and Experiment 3 is demonstrated in Table 6.

5 Conclusion

The proposed study for automatic plant leaf identification shows a comparative study using SVM, PNN, and KNN classifiers. Different experiments were carried out for different classifiers to obtain the best accuracy with minimum error. Thus, in every experiment, OCA and MCA are calculated using the confusion matrix. With SVM classifier, OCA was the maximum among all other classifiers with 98.4% and MCA is minimum with 1.6%. Furthermore, experiments were carried out taking PNN and KNN classifiers. While using the PNN classifier, the OCA was 94.4%, and MCA obtained was 5.6% which is maximum among all. When the KNN classifier was used to classify and identify plant leaf using digital images, the OCA obtained was 95.2% which is least among all and MCA obtained was 4.8%. While comparing the results, the accuracy is maximum when the SVM classifier is deployed.

Table 6 Contingent scrutiny of Experiment 1, Experiment 2, and Experiment 3

Experiment no. #	Total testing samples	Correctly detected samples	Incorrectly detected samples	Misclassification Analysis
Experiment no. 1	125	124	1	Out of 125 samples, 1 sample of AAC class is predicted as BBC
Experiment no. 2	125	118	7	Out of 125 samples, 1 sample of HC is predicted as CLSC, 1 sample of AAC is detected as AC, 1 sample of AC is detected as AAC, 1 sample of BBC is detected as AAC, 1 sample is detected as AC, and 1 is detected as CLSC, 1 sample of CLSC is predicted as BBC
Experiment no. 3	125	119	6	Out of 125 samples, 1 sample of AAC is detected as AC, 1 sample of AC is detected as AAC, 1 sample of BBC is detected as AC, and 1 is detected as CLSC, 1 sample of CLSC is detected as AAC, and 1 sample of CLSC is predicted as BBC

References

1. Available at: http://www.uky.edu/Ag/PAT/cat1/leafdis.htm. Last accessed 8 July 2020
2. S. Kaur, P. Kaur, Plant species identification based on plant leaf using computer vision and machine learning techniques. J. Multimedia Inform. Syst. **6.2**, 49–60 (2019). https://doi.org/10.33851/JMIS.2019.6.2.49
3. K. Pankaja, V. Suma,*Leaf recognition and classification using chebyshev moments. Smart intelligent computing and applications* (Springer, Singapore, 2019), pp. 667–678. https://doi.org/10.1007/978-981-13-1927-3_70
4. S. Mahapatra, S. Kannoth, R. Chiliveri, R. Dhannawat, Plant leaf classification and disease recognition using SVM, a machine learning approach. Sustain. Humanosphere **16**(1), 1817–1825 (2020)

5. N. Ahmed, U.G. Khan, S. Asif, An automatic leaf based plant identification system. Sci. Int. **28**(1), 427–430 (2016)
6. M. Turkoglu, D. Hanbay, Classification of the grape varieties based on leaf recognition by using SVM classifier, in *proceeding of Signal Processing and Communications Applications Conference (SIU)* (IEEE, 2015), pp. 2674–2677. https://doi.org/10.1109/SIU.2015.7130439
7. M. Lukic, E. Tuba, M. Tuba, Leaf recognition algorithm using support vector machine with Hu moments and local binary patterns, in *2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)* (IEEE, 2017), pp. 000485–000490. https://doi.org/10.1109/SAMI.2017.7880358
8. T.P. Kumar, M.V. Reddy, P.K. Bora, Leaf identification using shape and texture features, in Proceedings of International Conference on Computer Vision and Image Processing (Springer, Singapore), pp. 531–541. https://doi.org/10.1007/978-981-10-2107-7_48
9. Z. Wang, H. Li, Y. Zhu, T. Xu, Review of plant identification based on image processing. Arch. Comput. Methods Eng. **24**(3), 637–654 (2017). https://doi.org/10.1007/s11831-016-9181-4
10. R. Ali, R. Hardie, A. Essa, A leaf recognition approach to plant classification using machine learning, in *National Aerospace and Electronics Conference* (IEEE, 2018), pp. 431–434. https://doi.org/10.1109/NAECON.2018.8556785
11. A. Sahay, M. Chen, Leaf analysis for plant recognition, in *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)* (IEEE, 2016), pp. 914–917. https://doi.org/10.1109/ICSESS.2016.7883214
12. S. Zhang, Z. Wang, Y. Shi, Multi-modal plant leaf recognition based on centroid-contour distance and local discriminant canonical correlation analysis, in *International Conference on Intelligent Computing* (Springer, Cham, 2018), pp. 61–66. https://doi.org/10.1007/978-3-319-95933-7_8
13. A.L. Codizar, G. Solano, Plant leaf recognition by venation and shape using artificial neural networks, in *2016 7th International Conference on Information, Intelligence, Systems & Applications (IISA)* (IEEE, 2016), pp. 1–4. https://doi.org/10.1109/IISA.2016.7785361
14. R.G. Luna, R.G. Baldovino, E.A. Cotoco, A.L. de Ocampo, I.C. Valenzuela, A.B. Culaba, E.P. Gokongwei, Identification of Philippine herbal medicine plant leaf using artificial neural network, in *2017IEEE 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM)* (IEEE, 2017), pp. 1–8. https://doi.org/10.1109/HNICEM.2017.8269470
15. M. Turkoglu, D. Hanbay, Recognition of plant leaves: An approach with hybrid features produced by dividing leaf images into two and four parts. Appl. Math. Comput. **352**, 1–14 (2019). https://doi.org/10.1016/j.amc.2019.01.054
16. C. Yang, H. Wei, Plant species recognition using triangle-distance representation. IEEE Access **7**, 178108–178120 (2019). https://doi.org/10.1109/ACCESS.2019.2958416
17. Y. Zheng, C.A. Yuan, L. Shang, Z.K. Huang, Leaf recognition based on capsule network, in *International Conference on Intelligent Computing* (Springer, Cham, 2019), pp. 320–325. https://doi.org/10.1007/978-3-030-26763-6_31
18. K. Pankaja, V. Suma, Mango leaves recognition using deep belief network with 'MFO and multi-feature fusion, in *Smart Intelligent Computing and Applications* (Springer, Singapore, 2020), pp. 557–565. https://doi.org/10.1007/978-981-32-9690-9_61
19. J. C. Dunn, A fuzzy relative of the ISODATA process and its use in detecting compact well-separated clusters. 32–57 (1973). https://doi.org/10.1080/01969727308546046
20. J.C. Bezdek, A convergence theorem for the fuzzy ISODATA clustering algorithms. IEEE Trans. Pattern Anal. Mach. Intelligence **1**, 1–8 (1980). https://doi.org/10.1109/TPAMI.1980.4766964
21. C. Chih-Chung, L. Chih-Jen, LIBSVM: a library for support vector machines. ACM Trans. Intell. Syst. Technol. (TIST) **2.3**, 1–27 (2011). https://doi.org/10.1145/1961189.1961199
22. I. Kumar, N. Mohd, C. Bhatt, S.K. Sharma, Development of IDS using supervised machine learning, in *Soft Computing: Theories and Applications* (Springer, Singapore, 2020), pp. 565–577. https://doi.org/10.1007/978-981-15-4032-5_52

An Automated Recognition System of Sign Languages Using Deep Learning Approach

Ganesh Prasad Pal, Archana Das, Saswat Kumar Das, and Mayank Raj

1 Introduction

Sign Language is the only way of communication between deaf people and the hearing community. It is very useful for huge groups of people in society, which can be used as a different form of communication language. We can find various forms of signs such as dimensions of hands, motion profile, hand shapes, face, body parts, etc., for representing each sign in Sign Language. So, recognition of Sign Language is a very complicated area of research in computer vision. Around 70 million speech-impaired people have employed about 300 Sign Languages throughout the world [1]. Doing proper communication of hearing people with deaf people is the biggest challenge. This communication gap is noticed very clearly. For encouraging them, 23 September is celebrated as an "International Day of Sign Languages (IDSL)" every year. To overcome this, Sign language uses gestures as an interface of communication as shown in Fig. 1.

Through the different types of Sign Languages, deaf people can share their feelings to others as shown in Fig. 2.

Throughout all around the world, we can find various types of Sign Languages such as American Sign Language (ASL), British Sign Language (BSL), Indian Sign Language (ISL), Australian Sign Language (Auslan), etc., which are in the form of

G. P. Pal (✉)
Department of Computer Science & Engineering, G.L. Bajaj Institute of Technology & Management, Greater Noida, U.P., India

A. Das
Department of Computer Science & Engineering, Accurate Institute of Management & Technology, Greater Noida, U.P., India

S. K. Das · M. Raj
Department of Mechanical Engineering, IIMT College of Engineering, Greater Noida, U.P., India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_23

Fig. 1 Communication using sign language. *Source* https://www.shutterstock.com/editor/design/14602623

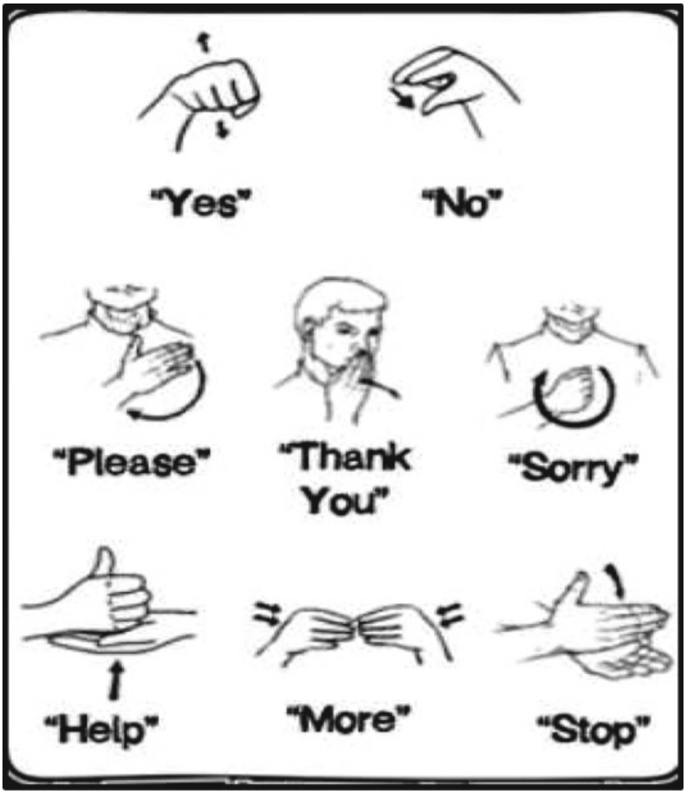


Fig. 2 Representation of different types of emotions. *Source* https://www.teacherspayteachers.com/Product/Sign-Language-842981

gestures. So, understanding human gestures can be presented or assumed as recognizing the problems of patterns. If these gesture patterns are detected and distinguished by the computers, then the reconstruction of the expected language can be possible. Our research on Sign Language translation contributes to a variety of statistical computer vision used to identify all types of letters and numbers. It is specially used for the automatic recognition of Sign Languages more effectively.

Here, we used the Convolutional Neural Network (CNN) to recognize ASL gestures. ASL is the most widely used Sign Language in more than 20 nations all over the world. This form of communication is most favorable to a large number of people. These global impacts of the sign recognitions are quite surprising and eye-catching. American Manual Alphabets of 26 static signs are provided by ASL which used for creating so many English words. Nineteen various hand shapes can make the 26 American Manual Alphabets of ASL. "K" and "P" alphabets provide identical gestures of hands with multiple directions. It also uses the sign gestures of numeric values from "0" to "9". It additionally includes built-in ASL equivalent signs for nouns and technical terms.

To recognize the static signs of ASL more effectively and further conversion to the corresponding text are the major aim of this automated recognition system. For gathering data, we can use a vision-based approach such as a web camera which is available even offline, to obtain the data from the signer. The angle between the hands is strict when it comes to ASL. So, the purpose of this recognition system is to serve as the most efficient way of communication for people who communicate using Sign Language.

2 Related Works

A fuzzy Min–Max Neural Network with X, Y, Z coordinates was proposed by Grobel et al. [2]. They have used the angles of the hand gestures as the inputs. The proposed model recognizes 25 distinct hand gestures with 85% accuracy. In Chung et al. [3], one HMM model one sign was used. From each video frame, the feature vectors were extracted for both the training and the recognition of signs, and these features were also used as input to the HMM model. They used cotton gloves with various types of color makings wore by the signer provide the trajectory and hand shape features effortlessly. Sandjaja et al. [4] proposed the Hidden Markov Models (HMMS) for the recognition of Sign Languages most popularly. To recognize ASL signs, Pugeault et al. [5] proposed a Gabor Filter-based method, which has only 75% mean accuracy. With the similar types of letters like "r" and "u", it gives very high confusion rates (17% Confusion Rate). Dardas et al. [6] developed a model using SIFT-based bag-of-features and a Support Vector Machine (SVM) classifier for recognizing six custom signs with an accuracy of 96.3%. But, when this method comes across with ASL signs, it is unable to attain the desired accuracy, since ASL signs are very complex and large in number.

Shotton et al. [7] proposed a method based on depth contrast features and a Random Decision Forest (RDF) classifier, which were segmented the human body pixel by pixel into many parts. It was developed to recognize various poses of the human body in the Kinect system. Qin et al. [8] developed a model by applying convex shape decomposition the method which is based on the Radius Morse function for the recognition of eight direction pointing signs. This method, as a result, provided 91.2% accuracy. Deora et al. [9] used Principal Component Analysis (PCA) to recognize sign symbols. They also use neural networks for the recognition of Sign Languages. They use a 3-megapixel camera for getting data which gave the images of very poor qualities due to the small dataset. They took around 15 images for each and every sign and kept them in their database. They had segmented and segregated RGB into components and then performed a boundary pixel Analysis. They were not giving satisfactory results due to the small dataset. Yeo et al. [10] implemented a model to recognize nine custom hand signs, where they used a contour shape analysis method. This model had given an accuracy level of 86.66%. Ren et al. [11] implemented a model based on a part-based hand sign recognition method which was parsed fingers according to the contour shape of the hand. There were 14 hand signs (10 digits and 4 arithmetic symbols) used for the recognition with 93.2% accuracy. Dominio et al. [12] proposed a model to recognize 12 static ASL signs which are based on combined multiple depth-based descriptors for hand signs. They used an SVM classifier for the classification of signs with 93.8% accuracy.

Cao Dong [13] proposed a model using a depth contrast feature-based classification algorithm to recognize 24 ASL signs. After this, a hierarchical mode finding approach was applied to localize hand joint positions. Then, a Random Decision Forest (RDF) classifier was applied for the recognition of ASL gestures by using joint angles. By using this method, the system can achieve 92% of mean accuracy. Balbin et al. [14] used a different approach by using Kohonen Self-Organizing Maps. This is a type of neural network which can use to classify patterns and batch of datasets in an unsupervised manner. After testing, the accuracy level of 97.6% was achieved by the given system. For making hand gesture identification more easily, Ong et al. [15] use color-coded gloves. While the comparison with the data gloves, these are more reasonable and very less restricting. The main weakness of the given approach is the very high consumption of computing power and less accuracy in comparison to others. Lean Karlo et al. [16] developed a model using a skin color modeling technique for hand detection in sign language. It can find the range of the skin color by extracting the pixels (hand) from the non-pixels (background). They used CNN for the classification of images. This system has 97.52% of static word recognition, 90.04% for ASL alphabets recognition, 93.44% attributed to the recognition of numbers, and 93.67% of average testing accuracy.

3 Technical Background

In the following sections, we will give description about the recent technologies.

3.1 Deep Learning

In the current years, deep learning techniques outplayed previous state-of-the-art Machine Learning (ML) techniques [17] in almost all the fields such as in Computer Vision and Natural Language Processing (NLP) [18]. It uses deep layers to extract features from the given input data. The main aim of deep learning is to perform automatic feature extraction without the need for human intervention. It can also create new features. It can give an end-to-end problem solution. Many important deep learning models are used in Computer Vision problems such as Convolutional Neural Network (CNN) [19], Recurrent Neural Network (RNN) [20], Deep Belief Network (DBN) [21], Generative Adversarial Network (GAN) [22], Auto Encoder (AE) [23], Variational Auto Encoder (VAE) [24], etc.

3.2 Convolutional Neural Network

In vision-based applications, CNN can be performed as mostly used ML techniques. Due to some capabilities like feature generation and discrimination ability, it is basically used for feature generation and classification [25]. Below in Fig. 3, we represent a typical CNN Learning strategy.

CNN architecture consists of the convolution layer and pooling layer alternately with one or more fully connected layers at the end of the network. With this, various types of mapping functions, regulatory units like batch normalization, and dropout are used for the optimization of the performance of CNN [26]. CNN has various types of loss functions and optimizers as shown in Table 1.

For designing new architecture and enhancing the performance, the components of CNN can be used. For improving the capabilities of CNN, further developments

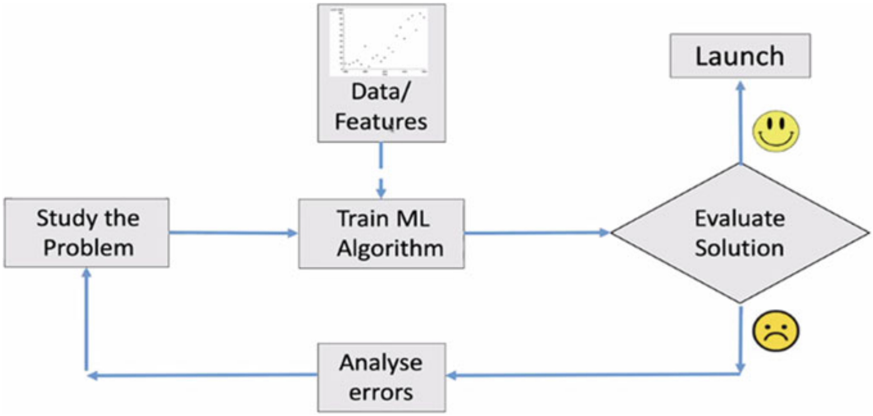


Fig. 3 Representation of CNN learning strategy

Table 1 Representation of various loss functions and optimizers occur in CNN

Loss functions	Optimizers
Cross-entropy loss/negative log likelihood	Stochastic gradient descent (SGD)
Mean square error/quadratic loss/L2 loss	SGD with Momentum
Mean absolute error/L1 loss	RMSProp
Etc.	Adam
	Etc.

are going on especially after 2015. The emerging area of research [27] was mainly developed to enhance the convergence rate of deep CNN. Many deep architectures like VGG, ResNet, LeNet, etc., also very useful for recognition and localization challenges. Then after many popular object detection and segmentation algorithms like Single-Shot Multibox Detector (SSD), Region-based CNN (R-CNN), Faster R-CNN, and Mask R-CNN [25] were built. In this way, various detection algorithms are developed to enhance performance by modifying the previously occurred architectures. Those algorithms are like Libra R-CNN, Feature Pyramid Networks, Cascade R-CNN, etc. [28–30].

4 Taxonomy

In American Sign Language (ASL), 24 alphabets except J and Z have been considered out of 26 static signs, since J and Z require more motion to represent as shown in Fig. 4.

In the current years, more hand pose features are used for the recognition of sign languages [31–33]. From the input data, the extraction of hand features has to be performed by using various types of deep learning approaches like CNN, RNN, GAN, AE, VAE, and many more [17, 32, 34–38]. So, in this form, detecting hand and extracting features effectively is very challenging. To work with the still images as an input, CNN is very efficient, but it does not perform the operation with the sequence information. It can be associated with the other deep learning model like RNN, Long-short Term Memory (LSTM) [39], and Gated Recurrent Units (GRU) to perform the functions of extracting sequence features from the visualized form of the data.

5 Proposed Methodology

This section provides a comprehensive description of the proposed Sign Language Recognition Model.

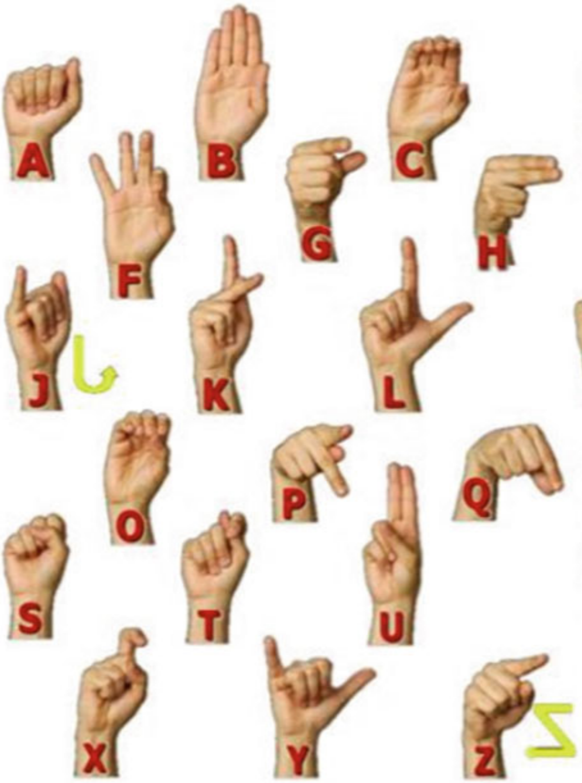


Fig. 4 Representation of ASL Alphabets. *Source* https://www.researchgate.net/figure/Signs-of-the-ASL-sign-language-1-some-signs-are-very-difficult-to-differentiate-for_fig1_261860712

5.1 Dataset Preprocessing

The MNIST Dataset, consisting of a total of 34,627 28 × 28 images, used here after splitting into a training set of 25055 images, a validation set of 7172 images, and a testing set of 2400 images. The dataset is present as a CSV with 784 columns, one is the label and 784 pixels (28 × 28), and each row has a label of the image and then pixel values in order. The pixel values are normalized between the scales 0 and 255 by dividing each pixel value with 255. Images reshaped from one dimension to three dimensions of (28 × 28 × 1) are used for CNN.

5.2 Data Augmentation

During the training of the neural network, augmentation is an important step. There may be some features of images in the test data which are unavailable in the training data, so our model will be a failure to capture the patterns. To avoid such type of problems, augmentation is a very useful method to apply for the training dataset. This approach can increase the size of the dataset by flipping, zooming, cropping, rotation, normalization, etc.

The augmentation of data can be performed on the training dataset to prevent overfitting and the size of the dataset increase artificially by making small transformations or reproducing variations in the existing training dataset. An ImageDataGenerator function provided by Tensorflow can able to perform augmentation on data in memory without modifying the local data. For our model, the images are augmented by rotating some random training images by 10 degrees, randomly shifting images horizontally or vertically by 10% of their width or height, respectively, zooming random images by 10%. Vertical or horizontal flips must not be applied; otherwise, it might change the sign completely.

5.3 Model Architecture

The model consists of three different 2D Convolutional Keras Layers. Each of these layers followed by a 2D max pooling layer. A flatten layer is applied before this passes to a dense layer. A dropout layer here makes the model more flexible. The proposed model uses another dense layer at the end. Adam optimizer compiles this sequence to form the proposed model (Fig. 5).

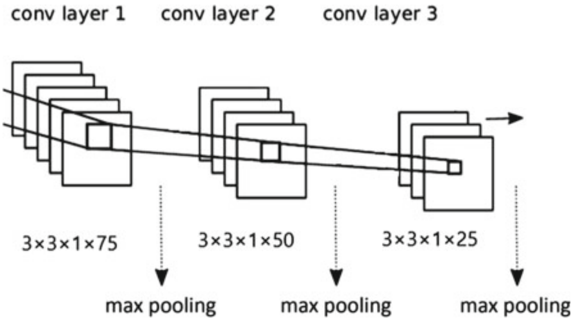


Fig. 5 The convolutional layers of 3 × 3 × 1 each followed by a max pooling layer

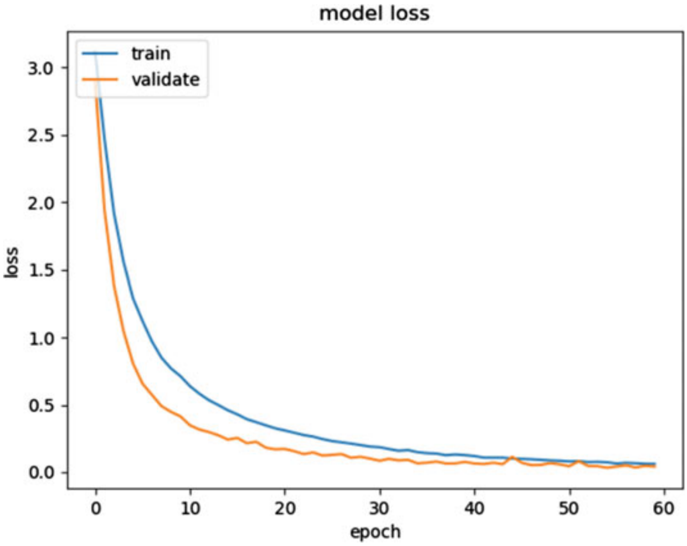


Fig. 6 The graph loss of the model for 60 epochs at a learning rate of 0.0001

5.4 Model Parameters

All convolutional layers and mean filters used are 2D 3 × 3 filters, using the same padding as the input with default stride and Relu as the activation function. All max pooling layers have a 2 × 2 filter using the same padding as inputs with strides equal to 2.

The first convolutional layer consists of 75 activation layers followed by a max pooling layer, with 28 × 28 × 1 images of the training dataset. The second convolutional layer consists of 50 activation layers, followed by the same max pooling layer. The last convolutional layer has 25 activation layers.

The flatten layer has default parameters. The first dense layer uses ReLu as its activation function, has a unit of 512, and a probability of 0.2 uses for dropout. The last layer, the dense layer has 24 units of activation layers, and Softmax used as an activation function.

During compiling, it uses a learning rate of 0.0001. For the optimization purpose, we are using Adam optimizer and categorical cross-entropy as its loss function. The batch size as 128 compiles the model for 60 epochs using the 7172 validation data for validation of the model (Fig. 6).

5.5 Use Case Diagram for the Proposed Model

Following is a use case diagram for our proposed model (Fig. 7).

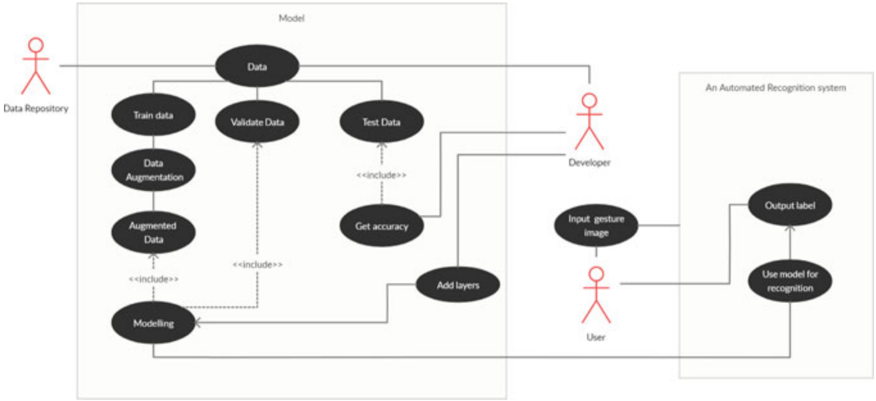


Fig. 7 The use case diagram for the proposed model

6 Experimental Results

6.1 Datasets

The dataset used to build the model is MNIST Dataset from Kaggle [40], which has about 27455 images worth of pixel data for training and over 7172 for validation. A dataset can be split into the ratio of 90:10 for the training and the testing set, respectively. The dataset is modified, as mentioned in proposed methodology. The augmentation of training data almost doubles or even triples the training set. Remember not to flip or rotate images as they might lead to misclassification (See Fig. 8).

6.2 Implementation

Setting an environment

The environment required for the implementation has to set up before building the model, i.e., installing all necessary packages and libraries such as Keras, Matplotlib, Numpy, Pandas, Pillow, Seaborn, Sklearn, and TensorFlow.

Model

A model is trained using the proposed methodology and saved for further use. The Keras model saved locally can be loaded for use anytime and anywhere.

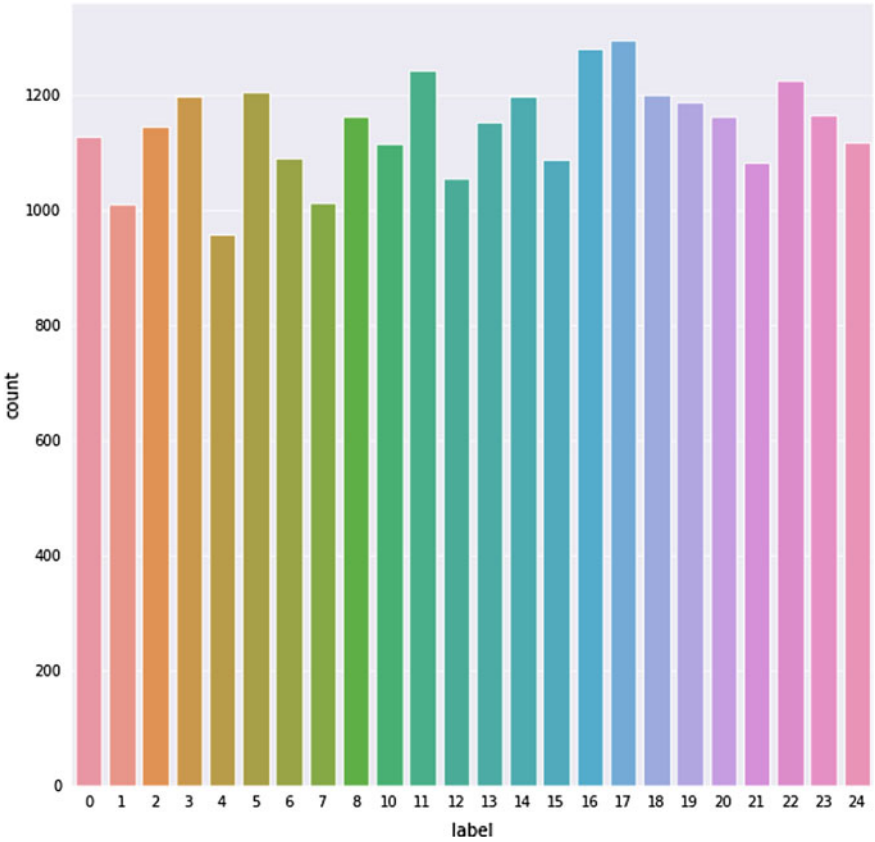


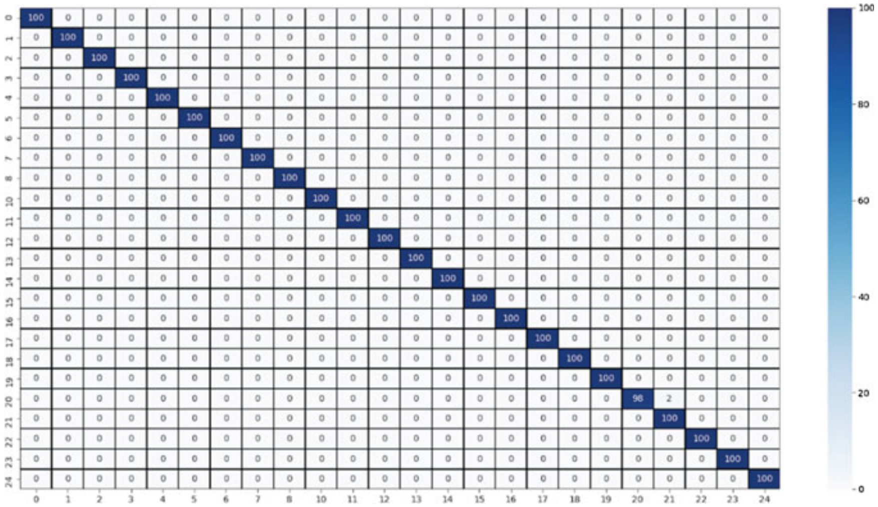
Fig. 8 Complete data visualization for each sign alphabet

Use of the Model

The model will predict the letters for any sign image inserted in it after processing the image as described in the proposed methodology.

6.3 Result

The model gives an accuracy of 99.1% of test data and an accuracy of 98.56% on validation data (See Fig. 2). This model becomes over-fitted if trained further. Each class test data has 100 test images shown in the confusion matrix after outputting its prediction. The results correctly predict 100 images for each of the classes (See Fig. 9).



	0	1	2	3	4	5	6	7	8	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	98	2	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100

Fig. 9 Confusion matrix for the proposed model

6.4 Comparison with Other Models

We are comparing accuracy of our model with various models developed by different authors, as shown in Table 2.

7 Conclusion

The signs for the alphabets, except J and Z, because they are not static gestures, are recognized using the combinatorial neural network architecture. The model gives real-time results, making it usable for practical purposes. The proposed model was successful in surpassing state-of-the-art testing. The highest generalized testing accuracy achieved is 98.56% of validation data and 99.91% of test data. This proposed method converts the gestures to text, but not speech format. Adding NLP to the model will help make words and sentences out of the letters it recognizes. For future work, we can use NLP so that the letters can be converted to some meaningful words or even sentences. Grammar checking functionality can also be applied in sentences.

Table 2 Comparison of accuracies with other models

Year	Author's reference	Method	Accuracy (%)
2011	Pugeault et al. [5]	Gabor Filter-Based method	75.0
2011	Dardas et al. [6]	SVM	96.3
2012	Qin et al. [8]	Convex Shape Decomposition method	91.2
2013	Yeo et al. [10]	Contour Shape Analysis method	86.66
2013	Ren et al. [11]	Part-Based hand sign recognition method	93.2
2014	Dominio et al. [12]	SVM	93.8
2014	Neverova et al. [41]	CNN	82.0
2014	Toshev & Szegedy [42]	DNN	96.0
2015	Cao Dong [13]	RDF Classifier	92.0
2015	Kang et al. [43]	CNN	99.0
2016	Han et al. [44]	CNN	93.80
2016	Duan et al. [45]	CNN	96.74
2016	Balbin et al., [14]	Kohonen Self-Organizing Maps	97.6
2017	Dibia [46]	CNN	96.86
2018	Dadashzadeh et al. [47]	CNN	86.46
2018	Rao et al. [48]	CNN	92.88
2019	Karlo et al. [16]	CNN	93.67
2019	Kopuklu et al. [49]	CNN	94.04
2019	Ferreria et al. [50]	CNN	97.27
2020	Elboushaki et al. [51]	CNN	99.72

References

1. Murray, J. (2018). World Federation of the deaf. Rome, Italy. http://wfdeaf.org/ourwork/%20Accessed%202020-01-30
2. K. Grobel, M. Assan, Isolated sign language recognition using hidden markov models, in *Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation. IEEE International Conference on 1997*, vol. 1 (IEEE, 1997), pp. 162–167
3. C.-L. Huang, W.-Y. Huang, Sign language recognition using model-based tracking and a 3D hop field neural network. Mach. Vis. Appl. **10**(5–6), 292–307 (1998)
4. I. N. Sandjaja, N. Marcos, Sign language number recognition, in *Proceedings of 2009 Fifth International Joint Conference on INC, IMS and IDC* (2009), pp. 1503–1508
5. N. Pugeault, R. Bowden, Spelling it out: real-time ASL fingerspelling recognition, in *IEEE Workshop on Consumer Depth Cameras for Computer Vision* (2011)
6. N.H. Dardas, N.D. Georganas, Real-time hand gesture detection and recognition using bag-of-features and support vector machine techniques. Instrument. Measur. **60**, 3592–3607 (2011)
7. J. Shotton, A. Fitzgibbon, M. Cook, T. Sharp, M. Finocchio, R. Moore, A. Kipman, A. Blake, Real-time human pose recognition in parts from single depth image, Commun. ACM (CACM) (2011)
8. S. Qin, X. Zhu, H. Yu, S. Ge, Y. Yang, Y. Jiang, Real-time markerless hand gesture recognition with depth camera, in *Advances in Multimedia Information Processing* (2012), pp. 186–197

9. D. Deora, N. Bajaj, Indian sign language recognition, in *IEEE Xplore, Conference* 19–21 Dec 2012. https://doi.org/10.1109/ET2ECN.2012.6470093
10. H.S. Yeo, B.G. Lee, H. Lim, Hand tracking and gesture recognition system for human-computer interaction using low-cost hardware. Multimedia Tools Appl. (2013)
11. Z. Ren, J. Yuan, J. Meng, Z. Zhang, Robust part-based hand gesture recognition using Kinect sensor. IEEE Trans. Multimedia 15(5), (2013)
12. F. Dominio, M. Donadeo, P. Zanuttigh, Combining multiple depth-based descriptors for hand gesture recognition. Pattern Recogn. Lett. 101–111 (2014)
13. C. Dong, American sign language alphabet recognition using Microsoft Kinect, Thesis (2015)
14. J.R. Balbin, D.A. Padilla, F.S. Caluyo, J.C. Fausto, C.C. Hortinela, C.O. Manlises, C.K.S. Bernardino, E.G. Finones, L.T. Ventura, Sign language word translator using neural networks for the aurally impaired as a tool for communication, in *Proceedings of the 2016 6th IEEE International Conference on Control System, Computing and Engineering (ICCSCE)* (2016), pp. 425–442
15. C. Ong, I. Lim, J. Lu, C. Ng, T. Ong, Sign-language recognition through gesture & movement analysis (SIGMA). Mechatron. Mach. Vis. Pract. **3**, 232–245 (2018)
16. L.K.S. Tolentino, R.O. Serfa Juan, A.C. Thio-ac, M.A.B. Pamahoy, J.R.R. Forteza, X.J.O. Garcia, Static sign language recognition using deep learning. Int. J. Mach. Learn. Comput. **9**(6) (2019)
17. R. Rastgoo, K. Kiani, S. Escalera, Sign language recognition: a deep survey. Published by Elsevier Ltd (July 2020). https://doi.org/10.1016/j.eswa.2020.113794
18. A. Voulodimos, N. Doulamis, A. Doulamis, E. Protopapadakis, Deep learning for computer vision: a brief review. Hindawi Comput. Intell. Neurosci. 1–13 (2018). https://doi.org/10.1155/2018/7068349
19. J. Wu, Convolutional neural networks. *LAMDA Group, National Key Lab for Novel Software Technology Nanjing University, China* (2019). https://cs.nju.edu.cn/wujx/teaching/15%7B%5C_%7DCNN.pdf
20. T. Wang, Recurrent neural network. Machine Learning Group, University of Toronto, for CSC2541, Sport Analytics (2016). https://www.cs.toronto.edu/%7B~%7Dtingwuwang/rnn%7B%5C_%7Dtutorial.pdf
21. G. Hinton, *Deep Belief Nets* (NIPS, Vancouver, B.C., Canada, 2007)
22. I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, *Generative Adversarial Nets* (NIPS, Monteral, Canada, 2014)
23. R. Grosse, *CSC321 Lecture 20: Autoencoders* (Toronto University, 2017). http://www.cs.toronto.edu/%7B~%7Drgrosse/courses/csc321%7B%5C_%7D2017/slides/lec20.pdf
24. C. Doersch, *Tutorial on Variational Autoencoders* (2016). arXiv:1606.05908
25. A. Khan, A. Sohail, U. Zahoora, A.S. Qureshi, A survey of the recent architectures of deep convolutional neural networks. Artif. Intell. Rev. (2020). https://doi.org/10.1007/s10462-020-09825-6
26. J. Bouvrie, *1 Introduction Notes on Convolutional Neural Networks* (2006). https://doi.org/10.1016/j.protcy.2014.09.007
27. C. Szegedy, W. Liu, Y. Jia, et al., Going deeper with convolutions, in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (IEEE, 2015), pp. 1–9
28. J. Pang, K. Chen, J. Shi, et al., Libra R-CNN: towards balanced learning for object detection (2020)
29. T.Y. Lin, P. Dollár, R. Girshick, et al., Feature pyramid networks for object detection, in *Proceedings—30th IEEE Conference on Computer Vision and Pattern Recognition* (CVPR, 2017)
30. Z. Cai, N. Vasconcelos, Cascade R-CNN: high quality object detection and instance segmentation. IEEE Trans. Pattern Anal. Mach. Intell. (2019). https://doi.org/10.1109/tpami.2019.2956516
31. X. Chen, G. Wanga, H. Guoa, C. Zhanga, Pose guided structured region ensemble network for cascaded hand pose estimation. Neurocomputing (2018). https://doi.org/10.1016/j.neucom.2018.06.097

32. E. Dibra, T. Wolf, C. Oztireli, M. Gross, How to refine 3D hand pose estimation from unlabelled depth data? in *International Conference on 3D Vision (3DV)* (Qingdao, China, 2017)
33. B. Doosti, *Hand Pose Estimation: A Survey* (2019). arXiv: 1903.01013
34. E. Escobedo-Cardenas, G. Camara-Chavez, Multi-modal hand gesture recognition combining temporal and pose information based on cnn descriptors and histogram of cumulative magnitudes. J. Vis. Commun. Image Represent. (2020)
35. F. Gomez-Donoso, S. Orts-Escolano, M. Cazorla, Accurate and efficient 3D hand pose regression for robot hand tele-operation using a monocular RGB camera. Expert Syst. Appl. **136**, 327–337 (2019)
36. L. Zheng, B. Liang, A. Jiang, Recent advances of deep learning for sign language recognition, in *2017 International Conference on Digital Image Computing: Techniques and Applications (DICTA)* (Sydney, NSW, Australia, 2017)
37. H. Guo, G. Wang, X. Chen, *Towards Good Practices for Deep 3D Hand Pose Estimation* (2017). arXiv:1707.07248
38. J. Supancic, G. Rogez, Y. Yang, J. Shotton, D. Ramana, Depth-based hand pose estimation: methods, data, and challenges. Int. J. Comput. Vis. 1180–1198 (2018)
39. K.Y. Huang, C.H. Wu, Q.B. Hong, et al., Speech emotion recognition using deep neural network considering verbal and nonverbal speech sounds, in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing—Proceedings* (2019)
40. Kaggle Dataset. https://www.kaggle.com/datamunge/sign-language-mnist
41. N. Neverova, C. Wolf, G. Taylor, F. Nebout, Hand segmentation with structured convolutional learning, in *Asian Conference on Computer Vision (ACCV) 2014: Computer Vision, Singapore* (2014), pp 687–702
42. A. Toshev, C. Szegedy, *DeepPose: Human Pose Estimation via Deep Neural Network* (2014). arXiv:1312.4659
43. B. Kang, S. Tripathi, T. Nguyen, Real-time sign language finger-spelling recognition using convolutional neural networks from depth map, in *3rd IAPR Asian Conference on Pattern Recognition (ACPR)* (Kuala Lumpur, Malaysia, 2015)
44. M. Han, J. Chen, L. Li, Y. Chang, Visual hand gesture recognition with convolution neural network, in *17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), China* (2016)
45. J. Duan, S. Zhou, J. Wany, X. Guo, S. Li, Multi-modality fusion based on consensus-voting and 3D convolution for isolated gesture recognition (2016). arXiv:1611.06689
46. V. Dibia, HandTrack: *A Library for Prototyping Real-time Hand Tracking Interfaces using Convolutional Neural Networks* (GitHub Repository, 2017). https://github.com/victordibia/handtracking/tree/master/docs/handtrack.pdf
47. A. Dadashzadeh, A. Tavakoli Targhi, M. Tahmasbi, *HGR-Net: A Two-stage Convolutional Neural Network for Hand Gesture Segmentation and Recognition* (2018). arXiv:1806.05653
48. G. Anantha Rao, K. Syamala, P.V.V. Kishore, A.S.C.S. Sastry, Deep Convolutional Neural Networks for Sign Language Recognition (SPACES, IEEE Xplore, 2018). https://doi.org/10.1109/SPACES.2018.8316344
49. O. Kopuklu, A. Gunduz, N. Kose, G. Rigoll, Real-time hand gesture detection and classification using convolutional neural networks, in *2019 14th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2019)*. https://doi.org/10.1109/fg.2019.8756576
50. P.M. Ferreira, D. Pernes, A. Rebelo, J.S. Cardoso, DeSIRe: deep signer-invariant representations for sign language recognition. IEEE Trans. Syst. Man Cybern. Syst. 1–16 (2019). https://doi.org/10.1109/tsmc.2019.2957347
51. A. Elboushaki, R. Hannane, K. Afdel, L. Koutti, MultiD-CNN: a multidimensional feature learning approach based on deep convolutional networks for gesture recognition in RGB-D image sequences. Expert Syst. Appl. **139** (2020)

Natural Language Processing for Small Businesses and Future Trends in Healthcare

Saurav Jha, Priyesh Tiwari, Shiv Narain Gupta, and Vivek Gupta

1 Introduction

You Natural Language Processing (NLP) is the mix of Artificial Intelligence (AI) and linguistics. It powers the computers to finally able to understand human and talk to them in their own language, this bridges the gap between people who are not very well equipped with machine-specific language. It can help people who don't have time to get well versed with any specific language. Language is the way to exchange information between entities. The ongoing research in the field of linguistics is dealing with how language is shaped, what it means and in what context it was used. All these tasks are achieved by running python tools and models like Spyder, nltk, and py Audio Analysis which helps us in manipulating text data as well as speech data.

The work in the field of NLP is carried out by computer scientists as well as a mix bag of linguists and psychologist. The task of the linguistics and psychologists is to make sure the applied model is able to understand and comprehend the words spoken by humans. The various task and block diagram of NLP are shown in Fig. 1.

The NLP is classified further into two categories [1], i.e. Natural Language Understanding and Natural Language Generation.

S. Jha (✉) · P. Tiwari · S. N. Gupta · V. Gupta
Department of Electronics and Communication Engineering, Greater Noida Institute of Technology, Greater Noida, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_24

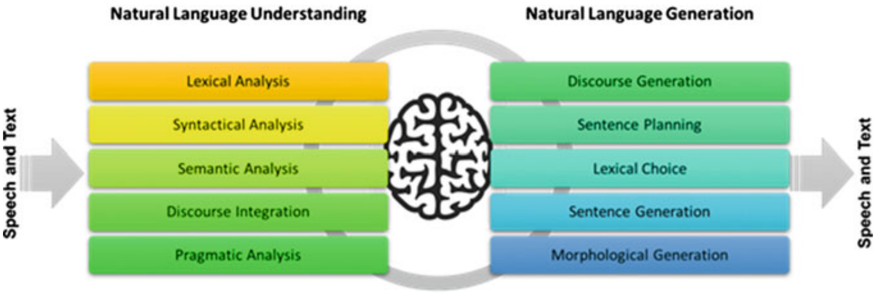


Fig. 1 Natural language processing

1.1 Natural Language Understanding

Natural language understanding (NLU) is a branch of artificial intelligence (AI) that uses computer software to understand input made in the form of sentences in text or speech format [2].

Lexical Analysis. It is used to interpret the meaning of individual words for machines as well as humans. A word which can have different meaning need to be understood with the reference in which it was stated. Let's take an example: (A) *Sachin got out for a duck* (B) *Duck is an amphibian.*

Morphological Analysis. Different parts of a word can be separated and those words can represent the smallest meaning of the word know as Morphemes. This analysis is used to reach the core meaning of a word or you can say the root of a word. Any word can have a prefix, root word, and suffix. Here, we remove those prefix and suffix to get to the root of word as the prefix or suffix doesn't add much value and only make the dataset larger. For example, root words which are taken in consideration in following words are: *"Work"ed*, *"Love"ed*, *"Small"est*, etc.

Syntactic Analysis. In this level of analysis, our main goal is to uncover the grammatical structure of a sentence. A sentence which does not make much sense grammatically might be rejected as they are in violation of the rules of language. For example, "*Man the mall the go to*".

Semantic Analysis. Most of the time, we assume that this section deals with determining the meaning of the sentence. However, it does more than that. Semantic processing determines the meaning of sentence by checking on the interaction of every word present in the sentence as it determines what could be meant by a particular word in that sentence. A particular word can mean multiple things when it is in a sentence. For example, sentence with no meanings are rejected here, "*Colourless red thoughts*".

Discourse Analysis. While syntax and semantic deals with a particular sentence, the discourse analysis deals with the whole units of texts. It doesn't work in a multi sentence text just taking sentence as a segment request instead; it takes the properties of sentences as a whole to make sense out of the data. For example, "I *wanted it very badly*", the word it here depends on the reference given in text earlier or later.

Pragmatic Analysis. Pragmatic deals with the language using knowledge from external common sense information. It analyzes the sentence intentions, goals, and plans. For example, "*Do you mind opening the door?*" should be interpreted as a request.

1.2 Natunal Language Generation

This is one of the fastest evolving technologies which convert data into a plain-English text for humans to understand. The models of NLG are fed with data in either files or through web scraping mode. Then NLG model reads out the data to provide us with a comprehensive English worded output. It is been in major use since 2014 as the best visible example of it is robojournalism. Here, an article can be written by content generation algorithm. This can be done within minutes and get uploaded on website soon after any certain major event occurs to give information to public. Also, online platforms such as Netflix has been toying with the idea of AI backed with NLG writing stories on its own when fed with popular movie plot. It will be rise of new way of storytelling and how our entertainment world will evolve will be decided on basis of this.

2 Current Trends

As stated earlier, the data consumption rate is at all time high in past decade so is the working of deep learning. The deep learning models were applied on everything from object detection to chatbot. As deep earning model have been successful in the field of pattern recognition and computer vision, NLP also started studying and applying how to best use new deep learning models. Previously, we were only working with SVM and logistic regression models to obtain result of NLP problems but now the deep Recurrent Neural Network (RNN) is slowly but steadily making its place in the field of text analysis. RNN are used as they are designed in such a way that they can recognize patterns in the sequence of data, such as text, spoken words, handwriting, numerical time series data, etc. It uses back propagation algorithm for training [15]. Let's take an example of movie, Avengers: Endgame, if you have seen the movie then you know that to make sense out of it you need to watch previous movies and same goes for the RNN models, as they tend to predict the next word in paragraph by training themselves. In RNN, every input is considered connected to each other unlike other neural networks where every input is independent of each other [3].

Traditional machine learning-based NLP systems were time consuming as they tend to be dependent on hand-made features.

3 Applications of NLP

NLP powers the computers to able to understand human and talk to them in their own language or its aims to make channel between human to machine, where it is easy to talking to a machine as compare to the talking to a human. NLP still collecting unstructured data and make it meaningful to a machine.

3.1 Text Analysis (Sales and Marketing)

Let's say that we have very big dataset of reviews of restaurant and we need to know how many of them liked it or hated it and if they hated it then what they hated? This kind of questions can be solved by text analysis [16].

3.2 Marketing Intelligence (Sales and Marketing)

The output found by text analysis of aforementioned restaurant review can be used as a marketing tactics or to find the weak points and then work on it.

3.3 Automatic Answering (Sales and Marketing)

The systems can easily answer questions posed by humans. Every machine categorized in this can answers question and also has few NLP functions. They can understand the speech or text or clicking an option (first half) and answer it as well (second half) [17].

3.4 Speech Recognition (IT and Security)

As the trends are trying to get the technology more suitable for everyday use, typing or clicking is the more traditional way and now we have Google Assistant, Siri, etc., which works on speech recognition technique as we just have to speak our command and tasks are performed. However, it is still not perfect, so with the help of NLP and neural networks, we can possibly make them better in every language not just in English. The applications mentioned in above list are not exhaustive and they are also evolving and work is being done to make them better as you are reading this [18].

3.5 Cybersecurity (IT and Security)

The interactions between human and machines are increasingly based on natural language through the use of chatbots, virtual assistants, etc. The NLP models can be effective against cyber threats as they can read the content and analyze it and alert the user when the person-sensitive information is present or being misused. Also, through NLP the cyber police can differentiate between threats and normal texts and find the culprit which can help in curbing the effect of cyberbullying. NLP can help in detecting phishing mail by reading the content of the mail beforehand and blocking it as 76% of companies in 2017 had their troubles with phishing emails.

4 Our Motivation

We have used a dataset and obtained results by testing on it and, through the output, we will be able to help business in solving their problem in allocation of capital and approaches to make while taking decision [19]. There is already work going on in the field of finding the best suitable research classification model for NLP. Our paper, however, focuses more on finding the applications of NLP in the field of healthcare and to make it easier to use and derive results for individuals and small firms with limited exposure to NLP. In the next segment, we dwelled on the aforementioned dataset and the step-by-step approach taken by us in obtaining final prediction.

4.1 Step-by-Step Working of NPL

The dataset taken by computer scientists, student, or researchers could be different, but there is a basic framework on which NLP works [4]. Researchers and scholars have their own way of approaching the data and steps as there is no static way to deal with the dataset. Methods or development step could vary person to person and change the output corresponding to the method taken. Some steps might even overlap or be part of one another.

There have been various developments in past few years and maybe in upcoming years this framework could be obsolete too.

Importing Libraries to dataset. These are the libraries essential in any machine learning algorithm and might vary on need to need basis in different classifications or regression or reinforcement or NLP model. The libraries are Numpy, Pandas, Matplot lib, sklearn, etc.

Importing the dataset in required form. The dataset could be in a text form or speech or inputs through click and user needs to analyze if the data could be imported in csv or tsv form if it is a text dataset. Python models can get confused while reading it; therefore, a file with delimiter and quoting and more functions corresponding to the need of user can be added and the dataset imported could be then error free and categorized accordingly for python (Fig. 2).

Clean dataset through nltk libraries (Pre-processing). In this study we used nltk (natural language tool kit) library with re (regular expression) library. re is essentially a string matching function which can amend the dataset according to user requirement. Our text cleaning was is in several stages are Lowercasing, Splitting, Removing common Stop Words present in dataset, and Stemming to get the original core word. Initially, only English characters from A to Z were taken from the dataset and everything apart from characters are discarded. It is achieved through re library.

Lowercasing deals with making all the words be in lowercase which are present in the dataset after re library implementation and taking only English alphabets for the lowercase application.

Splitting deals with making every word as an individual object. Before implementation of split, the words were in string and now it will be in list. The individuality of every word helps the user in removing each word on its own as an item of list and makes the cleaning process easier.

Removing stop words is necessary as there could be multiple words which are now an object in list who aren't of any value to the dataset. These words just make the data provided to us bigger and so we need to eradicate them and make our data more

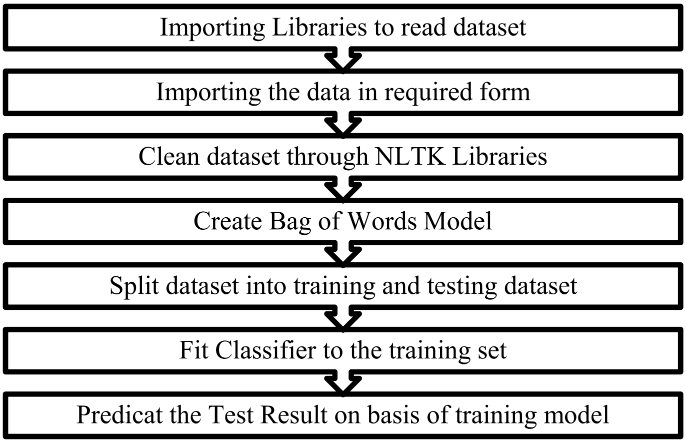

Importing Libraries to read dataset
Importing the data in required form
Clean dataset through NLTK Libraries
Create Bag of Words Model
Split dataset into training and testing dataset
Fit Classifier to the training set
Predicat the Test Result on basis of training model

Fig. 2 Step-by-step flow of NLP application development

optimized and fast functioning. The nltk library package stop word is the tool used to perform this function.

Stemming is one the functions we have discussed above and it deals with obtaining core word and removing all the prefix and suffix to make sure our list is as exclusive as it needs to be. The extra alphabets were dead weight as they weren't important to the original or core meaning of word. In our testing, we used PorterStemmer for stemming function.

Although, there is always a debate going on between researchers about which one is better: Stemming or Lemmatization? We can safely say that lemmatization is a notch better than stemming in few aspects and also, provides us with better precision. Although, the reason to use stemming in our research was due to the reason it gave a better recall value than lemmatization.

The next step is to join our list again and bring all individual elements of list back into a string to form a meaningful sentence with lesser and important words only. Thus, completing the data cleaning portion for our dataset.

Bag of Words Model. Bag of Words Model is essentially a way of depiction of texts when modeling text with algorithms of ML [6]. In our corpus, we essentially had a lot of words which were then through data cleaning steps were removed but still even important core words can be same in the remaining corpus, so we need bag of words model as they only contain unique words rather than having all previous individual words who are same in different sentences in list. It gives us again a fixed model of unique characters which can be analyzed better than before. The main goal of this step in our research was to make the sparse matrix through the use of fit-transform method. The countvectorizer function of sklearn (Scikit-learn) library is used in our code. It is also very often used by most of NLP users as it gives the easiness in setting standards for their text as well as cleaning it in one line of code. However, we didn't use it much in our code as we wanted to be more flexible with our data cleaning procedure.

Split dataset into training and testing set. Split dataset into training and testing set is the step where splitting of cleaned dataset begins. We set our test dataset size to 20% or 0.2 as lower test size and higher training size is most optimum way of getting a good prediction.

Fitting classifier to the training model. Fitting classifier to the training model is a task which needs to be carried with precision and in-depth analysis of how your data functions. There are multiple classifiers which can be used in our NLP dataset but we went ahead with Naïve Bayes [7]. We can see the Naïve Bayes formula below:

$$P(A/B) = \frac{P(B/A)P(B)}{P(A)}$$

where $P(A/B)$ is Probability of "A" being true given that "B" is true; $P(B/A)$ is Probability of "B" being true given that "A" is true; $P(A)$ is Probability of "A"

Table 1 Analyzing prediction output and classification models

Classifier	Accuracy	Precision	Recall	F1 score
Logistic Regression	71	78.35	67.25	72.38
SVM	72	76.28	69.15	72.54
Naïve Bayes	73	56.70	82.08	67.07
Random Forest	72.5	90.72	65.67	76.19
K-Nearest Neighbors	61	76.28	57.36	65.48
Kernel SVM	72.5	92.78	66.17	77.25

being true; and $P(B)$ is Probability of “B” being true. It is called Naïve as it makes assumption that the occurrence of a certain feature is independent of occurrence of other features. The class we imported from naïve bayes classifier was Gaussian NB. Gaussian Naïve Bayes (NB) is based on continuous data. When dealing with continuous data, a typical assumption is that the continuous values associated with each class are distributed according to normal (or Gaussian) distribution.

The prediction. This is our final output after training our dataset and we can set it side by side with the original test data and see how efficiently our model is working. The confusion matrix is 2 × 2 matrixes and an essential part in knowing efficiency of our model as it gives us True Positive, False Positive, True Negative, and False Negative. On the output provided to us by confusion matrix, we can determine the Accuracy, Precision, Recall, and F1 score (Table 1).

4.2 Classifier Selection Criteria

Logistic Regression. Logistic Regression can be very used when we want to describe a relation between a dependent binary data variable and an independent variable. This classifier is suitable for business analysis applications.

Support Vector Machine (SVM). SVM is a supervised machine algorithm which can be used for both regression as well as classification. It comprises of a technique known as kernel which can be defined by user to transform the data and then based on these transformations it searches for an optimal boundary among all the possible outputs of the dataset. We used linear kernel while training our model for this classifier and you can see through above values that it gave us better result than logistic regression.

Naïve Bayes. A Naïve Bayes classifier is a probabilistic machine learning model which is used for classification task, it essentially means that it predicts on the basis of the probability of an object. The reason to use it was our focus on obtaining high precision and recall value as we have used Stemming too instead of Lemmatization.

The above result indicates that Recall value and Accuracy of Naïve Bayes is among the highest in all the classifier used on the dataset used by us for research.

Random Forest. Here in this research, we initially ran different output numbers from the minimum value to 1000 times of minimum value. We first started with a forest of five decision trees and then gradually increased number of decision trees. The forest with highest number of decision tree was 50,000. Although, neither of them gave us the most optimum result and the forest with 275 decision trees is included in our research output table above. It can be observed that Random Forest is better than Naïve Bayes in some area but still lacks in few areas important for the research standards set prior to conducting analysis.

K-Nearest Neighbors. This algorithm is one of the easiest one to implement and this supervised algorithm is widely used in both regression and classification models. This model usually works on the belief of assuming similar things exist close to each other. The K-NN model is one of the most underperforming models in our research with the lowest accuracy and F1 Score. The outcome from using K-NN model makes it pretty evident that this algorithm is not well suited for NLP problems.

Kernel SVM. We had already taken SVM as one of the classification models, however, that was with a linear function. In this particular model, we have changed the kernel to Radial Basis Function (RBF). The outcome obtained from it was mostly positive as we obtained the highest Precision and F1 Score. While other models focus more on differences in the dataset, SVM focuses more on finding the similarities.

5 Changes in Scope of NLP

In 2010, researchers were trying to use NLP only for very basic tasks such as text reading and malware identification [11]. However, the tasks were knowledge acquisition, classifying text into categories, etc. In India, since the launch of Reliance Jio, the availability as well as use of internet grew exponentially [20]. This sudden outburst of data gave researchers to work on many things which weren't possible without the data generated from all nooks and cranny of India. As the country have a large population and vivid cultures, the task of NLP becomes much tough. Now, the speech to text in Google is available in regional languages too. The application is very useful for people who are suffering from some sort of disability as it can help in interpretation of sign language in context of India and its regional language. Although, the work is still going on and is expected to be completed soon to accommodate a better understanding among people who use sign languages and who doesn't even know them [5]. The papers a decade ago [12] were only dealing with the theoretical aspect of the use of NLP in India and that too only in major cities as internet were slower and costlier. However, as seen in the research papers of now [14], these theories are now all backed by substantial research and data. The results are optimistic and we can now apply them to saving and digitization of ancient Indian manuscripts [8].

This also boosted the scope of Digital Humanities in India as researchers are trying to understand the ancient texts and try to understand the symbols present in caves and match the texture and deduced meanings with other symbols present all over India. The research opportunities and scope are ever changing as the reach of internet is expanding and in next decade we will be taking and studying data from the smart appliances as well as humans to put the use of text and language analysis to its optimum use.

6 Future Trends of NLP

As the world is right now fighting with COVID-19 without any possible solution in sight. The most pressing concern right now is our healthcare system. So, we are going to focus majorly on healthcare applications of NLP in this section.

6.1 Clinical Trials (Healthcare)

NLP can help the doctors to help the enrolled patients in dire need of medical care as it can isolate the clinical method which proved the best for patients. Currently, this is done by keeping records by doctors who track improvement on their own. It would be very easy for them to now work on treatment knowing it is going to be best for their patients.

6.2 Clinical Documentation (Healthcare)

Right now, the documentation in healthcare system is done by human scribes. Once, speech recognition and recording is implemented on a large scale than the error in documentation will be down by very high percentage.

6.3 Depression Predictor (Healthcare)

As stated above in text analysis, we can monitor the posts or comments publicly made or shared on social media and analyze them. In recent events, a bollywood star took drastic step of ending his life, if we can predict from earlier behavior and text patterns that a person is in need of psychologist help then medical professionals can be alerted and they can help those people and might save their life.

6.4 Payment Authorization (Healthcare)

A lot of time hospitals start treatment and patients continue in it until their health insurance comes in and there might be some issues or uncertainty over payment or particular treatment covered this causes an extreme uncomfortable situation for both parties involved. To overcome this, big hospitals can make predictions seeing the past trends of the patient's expenditure and will they be able to go through with the procedure or not. IBM Watson and Anthem are currently working on to develop similar kind of NLP model to predict a prior authorization from patient side by analyzing patient/payer's network.

6.5 Population Monitoring (Healthcare)

China has began the use of facial recognition software in their country for law and order purpose. However, NLP models can be used widely to determine health issues faced by citizens over any part of country. It can also be beneficial in analyzing if the health problems are associated with any particular region or ethnic or racial group. It could also help in government taking effective measures as the problem is discovered early and can be contained.

6.6 Marketing Strategies (Sales and Marketing)

The impact of NLP is on the business world as well. As more and more people are spending time online and writing reviews or about themselves, all of this data can be computed and analyzed by companies in knowing what will a person like or dislike and according to that they can make Ads specifically tailored for an individual. It helps companies save money by not spending hefty amount on marketing products online which the other person doesn't want.

6.7 Virtual Assistant (Sales and Marketing)

This is the most usable application of NLP in every field from business to healthcare to feedbacks to grievance. A virtual assistant also helps website owners maintain customer engagement by solving all their queries. Let's take an example of RedBus virtual assistant RedBuddy. It is used to solve most of customer queries as when someone sign in it reads all the data of theirs like when was last booking, which bus they boarded, etc. it helps in customer lodging their grievance and getting help very quickly. The reason for virtual assistant popularity is it makes the other person comfortable and the hassle to call and connect to call centre is not required anymore.

6.8 Digital Humanities

The integration of words and symbols throughout history can help us in analyzing their meaning better as NLP models are trained to find similarities and then give us the most optimum output [10].

7 Limitations

There are still some challenges and problems left for NLP to tackle and to become more suitable in upcoming time. These challenges have been reduced greatly since 1950s when Alan Turing first published their article titled "Computing Machinery and Intelligence" [9].

7.1 Lack of Emotions

Computer programmers with help of psychologist are trying to train the models to recognize emotions like stress, fear, happy, etc. However, analyses through word and through speech recognition are two different things. The models currently are training in understanding the difference in these emotions to help the humans better. It would also positively impact human–machine interaction.

7.2 Data Security

The security of individual personal data is at stake always. Not everyone will be on board with the idea of foreign companies monitoring their country citizen. A mutual agreement on data usage is also need of the hour. International bodies need to make a division solely dedicated to apply regulation in data monitoring practices too.

8 Conclusions

Our focus was to find the best accuracy for the classification model used on our dataset. The reason to focus on Accuracy rather than F1 score was taken because both false positives and false negatives had similar cost. Also, our data was not consisting highly of an uneven class distribution. If we have a data with uneven class distribution then it is better to use F1 Score rather than Accuracy. We had a restaurant review dataset which was a symmetric dataset. The model which performed best among all other classifiers in term of Accuracy (73%) and Recall (82.08%) was Naïve Bayes. The Kemel SVM (RBF) is also a close competition or could be a substitute of Naïve Bayes model as it too has a slight less accuracy but a very high Precision (92.78%) as well as better F1 score (77.25%). However, the sensitivity or recall value was lowest among all the classifiers models which were taken as case study for this research. RNN could be better than all the classifiers as deep learning neural networks are performing better with even big dataset [9]. However, their limitation is that they cannot be trained very easily due to gradient vanishing and exploding problems and need a sophisticated device to run. These reasons are a big concern for small level entrepreneur and that is why they can use classification model stated in our research for expansion of their enterprise. Businesses which are trying to make a better strategy for their businesses to grow and need to know what will the most optimum way to allot capital and on which segments they need to improve can use this text classification model after obtaining restaurant reviews and then plan ahead. This result will help even small hospitality chains as well and it could be achieved without any hassle and results would be the best way to move forward for those chain owners. Our research paper will also help individuals and small business firm with lack of exposure towards NLP to utilize and have the benefit of using the proper algorithm in lieu of their goals with low resources on their end.

Healthcare industry, on the other hand, can be benefited with all the future applications like clinical trials, clinical documentation, depression predictor, etc., and future development stated in our paper as they have bigger capital at their disposal and use of the optimum neural network model will increase their efficiency by large [13]. The use of deep learning models and classifiers both will be needed for the smooth functioning of future applications.

References

1. D. Khurana, A. Koli, K. Khatter, S. Singh, Natural language processing: state of the art, current trends and challenges (2017). arXiv preprint arXiv:1708.05148
2. T. Wolf, L. Debut, V. Sanh, J. Chaumond, C. Delangue, A. Moi, P. Cistac, T. Rault, R. Louf, M. Funtowicz, J. Brew, HuggingFace's transformers: state-of-the-art natural language processing. ArXiv, arXiv-1910 (2019)
3. A. Sherstinsky, Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. Phys. D: Nonlinear Phenomena 404–132306 (2020)

4. A. Romanov, K. Lomotin, E. Kozlova, Application of natural language processing algorithms to the task of automatic classification of Russian scientific texts. Data Sci. J. **18**(37), 1–17 (2019)
5. I. Bornkessel-Schlesewsky, D. Roehm, R. Mailhammer, M. Schlesewsky, Language processing as a precursor to language change: evidence from Icelandic. Front. Psychol. **10**, 3013 (2020)
6. Y. Zhang, R. Jin, Z.H. Zhou, Understanding bag-of-words model: a statistical framework. Int. J. Mach. Learn. Cybern. **1**, 43–52 (2010)
7. H.M. Kubade, The overview of Bayes classification methods. Int. J. Trend Sci. Res. Develop. (IJTSRD) **2**(4), 2801–2802 (2018)
8. N. Singh, *NLP for Indian Languages* (2020)
9. A.M. Turing, Computing machinery and intelligence. Mind, New Series **59**(236), 433–460 (1950)
10. M. Piotrowski, Natural language processing for historical texts. Synth. Lect. Human Lang. Technol. **5**(2), 1–157 (2012)
11. P. Teufl, U. Payer, G. Lackner, NLP (Natural Language Processing) to MLP (Machine Learning Processing), in *5th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security* (MMM-ACNS 2010, St. Petersburg, Russia, 2010), pp. 256–269
12. M.C. Surabhi, Natural language processing future, in *2013 International Conference on Optical Imaging Sensor and Security (ICOSS)* (IEEE, Singapore, 2013), pp. 1–3
13. T. Young, D. Hazarika, S. Poria, E. Cambria, Recent trends in deep learning based natural language processing. IEEE Comput. Intell. Mag. **13**(3), 55–75 (2018)
14. A. Fadhil, S. Gabrielli, Addressing challenges in promoting healthy lifestyles: the aI-chatbot approach, in *Proceedings of the 11th EAI International Conference on Pervasive Computing Technologies for Healthcare* (Barcelona, Spain, 2017), pp. 261–265
15. Datahack Summit 2019 Homepage, Power Talk: The current state and limitations of Natural Language Processing, Data Hack Summit (2019). https://www.analyticsvidhya.com/datahack-summit-2019/schedule/the-current-state-and-limitations-of-natural-language-processing-nlp/. Published 13 Nov 2019
16. Towards Data Science Homepage, https://towardsdatascience.com/natural-language-processing-nlp-top-10-applications-to-know-b2c80bd428cb. Last updated 19 Dec 2019
17. Maruti Techlabs Homepage, https://marutitech.com/use-cases-of-natural-language-processing-in-healthcare/. Last updated 05 June 2020
18. R. Madhavan, Natural language processing- current applications and future possibilities. https://emerj.com/partner-content/nlp-current-applications-and-future-possibilities/. Last updated 13 Dec 2019
19. Super Data Science Homepage, https://www.superdatascience.com/pages/machine-learning. Last accessed 04 Dec 2018
20. Economic Times Homepage, https://economictimes.indiatimes.com/tech/internet/india-has-the-cheapest-mobile-data-in-world-study/articleshow/68285820.cms. Last updated 06 March 2019

A Review on AI-Based Techniques for Tackling COVID-19

Taranjeet Singh, Rijwan Khan, and Sandeep Srivastava

1 Introduction

Corona virus 2 has affected 213 countries and territories all over the world with more than nine million cases and 400,000 deaths (fatality rate of 9%) as of 22 June 2020 [1]. It has become a challenge for WHO (World Health Organization), governments, companies, researchers, and other health organizations for reducing the effects of the virus and developing its cure as soon as possible. The transmission rate of the virus is very high as it can be easily transmitted through discharge from the nose or mouth of a diseased person when he/she sneezes or coughs. Over six months have passed since the virus was detected in China, but its transmission seems to have no end, especially in countries where the density of population is high. Latest technologies, especially artificial intelligence (AI), seem to be quite helpful in this pandemic as it is being used for disease identification, prediction, diagnosis, drug discovery, and spreading awareness about the disease [2].

As the name suggests, artificial intelligence is non-natural intelligence acquired by machines to perform the tasks that human intelligence can. With AI applications symptoms of the corona virus can be identified and tests can be conducted with high accuracy. AI has shown active participation in COVID-19 by improving planning, spreading awareness, diagnosing patients, and many more. Thus in reducing the harmful effects of the pandemic AI plays an important role. This paper aims to review the role of artificial intelligence-based systems in the COVID-19 outbreak. Sections are detailed as follows: Sect. 2 presents literature survey while Sect. 3

T. Singh
Mangalmay Institute of Engineering and Technology, Greater Noida, India

R. Khan
ABES Institute of Technology, Ghaziabad, India

S. Srivastava (✉)
GL Bajaj Institute of Technology & Management, Greater Noida, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_25

focuses on applications of AI in minimizing the effects of the Corona 2 outbreak. Sect. 4 discusses several approaches for diagnosing COVID-19 patients and Sect. 5 provides discussions and outcomes.

2 Related Works

Vaishya et al. [3] reviewed the role of AI in analyzing, preparing, and fighting against corona virus or any other pandemics. In this paper, several applications of AI for COVID-19 were identified and the difference between traditional and AI-based techniques for diagnosing COVID-19 patients was also discussed. The author concluded that AI can not only help in the treatment of COVID-19 patients but also in monitoring their health too. Iyengar et al. [4] presented the role and applications of smartphone technology in telemedicine for dealing with the COVID-19 pandemic. Several applications of smartphone technology such as radio diagnosis, monitoring patients, education, counseling, consultation, training, and monitoring patients were discussed briefly. Along with advantages the author also presented the side effects and limitations of this technology.

Shi et al. [5] presented a review on AI techniques in diagnosing COVID-19 patients using CT and X-ray images. This would ease the work of radiologists and help them in decision-making. This review discusses the accuracy, efficiency, and safety that AI incorporates in applications of COVID-19. The author concluded that AI has a natural capability in acquiring data from multiple sources and can perform diagnoses of COVID-19 patients accurately and efficiently. Tang et al. [6] proposed a model for severity assessment of COVID-19 patients using chest CT images. The model used the random forest algorithm for classifying the severity of the virus in COVID-19 patients. The flowchart of the model is shown below. Firstly, 176 images of COVID-19 patients were gathered from 7 hospitals, then 63 quantitative features were extracted using a deep learning tool named uAI-Discover-NCP and finally severity was assessed using the random forest algorithm. The author concluded that this model is very promising and has high accuracy. Xiaowei et al. [7] proposed a model using deep learning techniques for distinguishing COVID-19 pneumonia from viral pneumonia and healthy images using CT samples. In total, 618 samples were collected, to which the deep learning model was implemented by the ResNet-18 network of convolution neural network. The author concluded that the prediction rate of the model was 86.7% and can be used as a promising tool for providing automatic detection of COVID-19. Wang et al. [8] used CT images for identifying radio graphical variance, based on deep learning algorithms' graphical features.

Based on X-ray images Wang et al. [10] proposed a convolution neural network model named COVID-Net, which is the first open-source neural network for identifying COVID-19 from X-ray image samples. The proposed COVID-Net predicts COVID-19 cases based on COVIDx which is an open-source dataset of around 14,000 CXR images and can provide help clinicians in improving the diagnosis process. The author concluded that this model has higher accuracy than other models of convolution neural networks and can provide aid in accelerating the treatment process of COVID-19. Shi et al. [11] used 1658 image samples of people affected with COVID-19 and 1027 other samples of CT for extracting segments; later these segments were fed to iSARF (infection Size Aware Random Forest) model for automatically clustered into groups and finally random forest technique was used for classification. Using the fivefold cross-validation method, the model was trained, and the overall accuracy of the proposed model was 87.9%. The author concluded that the model has high accuracy and can serve as an efficient technique for screening COVID-19 patients by assisting in the clinical decision-making process. Tuli et al. [15] applied an improved machine learning-based mathematical model for analyzing and predicting the growth of COVID-19. For real-time prediction and analysis of the epidemic, the model used a cloud computing platform for deployment. Case studies were illustrated which show country-wise predictions were made using the mode and research opportunities were presented. The author concluded that mathematical modeling, ML, and cloud computing were used by the model for predicting the growth of COVID-19. The next section presents applications of artificial intelligent techniques in facing an epidemic. Table 1 displays various AI models proposed by researchers for diagnosing COVID-19 patients using CT or X-ray images. Zixin et al. [16] proposed

Table 1 Methods proposed for COVID-19 detection

References	Technique	Method used	No. of samples	Accuracy (%)
[6]	CT	Random Forest	COVID-19—179	87.5
[7]	CT	Convolution Neural Network	COVID-19—219 Influenza A—224 Normal—175	86.5
[8]	CT	Convolution Neural Network	COVID-19—44 Viral pneumonia—55	82.9
[9]	CT	UNet++	COVID-19—51 Others—55	95.2
[10]	X-ray	Convolution Neural Networks	COVID-19—45 Bacterial pneumonia—931 Viral pneumonia—660 Normal—1203	83.5
[11]	X-ray	ResNet-50	COVID-19—50 Normal—50	98
[12]	X-ray	Convolution Neural Networks	COVID-19—70	92.9
[13]	CT	Random Forest	COVID-19—1658 Others—1027	87.9
[14]	CT	ResNet-50	Bacterial pneumonia—100 Normal—86	86

nature-inspired techniques for forecasting COVID-19 in China. This COVID-19 forecasting was real time as size, length, and ending time were predicted. Jamshidi et al. [17] surveyed several DL techniques for diagnosis and treatment of COVID-19. The major goal of this research was to propose user-friendly techniques for the treatment. Lin and Hou [18] presented several methods for combating COVID-19, and these methods were based on Bigdata and AI. Thompson and Crayton [19] recommended a low-cost, self-tested, and tracking system based on blockchain and AI techniques for self-testing of COVID-19. Arni and Jose [20] proposed an ML-based system for the identification of COVID-19 patients using a mobile-based survey. According to the author, this method can limit the spread of COVID-19 and appropriate measures could be taken after identification. Salman et al. [21] proposed an AI-based method for the identification and detection of COVID-19 patients. Dataset was collected from Kaggle and GitHub which consists of 260 images. Then these were fed to the DL model for classification. Lessmann et al. [22] implemented an AI-based system by using three DL models for assessing suspects of the corona virus. Jiang et al. [23] proposed an AI-based system that would identify patients with risk of COVID-19 using data from two hospitals. Pham et al. [24] tend to use Big data and AI techniques for providing a survey for improving and stopping corona virus. Bellomarini et al. [25] presented a report on AI technology for demonstrating the impact of COVID-19 on several Italian company's networks.

Zhang et al. [26] presented a system named Covidex, which was a search engine to help experts in the COVID-19 outbreak. Ahsan et al. [27] proposed a DL-based model for identifying COVID-19 patients using both X-ray and CT scan images. The model used several architectures of DL but NasNetMobile architecture provides the best results. Shaoping et al. [28] presented a supervised DL technique for predicting COVID-19 patients using CT images. The author concluded that the model achieved good results and can be deployed worldwide. Imran et al. [29] proposed a technique for sentiment analysis of people from different locations all over the world. The system used DL's LSTM (long short-term memory) for estimating the sentiments and emotions from tweets on Twitter.

3 Applications of Artificial Intelligence in COVID-19

Few applications of AI are robotic vehicles, speech recognition, autonomous planning and scheduling, game playing, spam fighting, logistic planning, robotics, machine translation, etc. AI can be applied to multiple areas of medical and healthcare. Earlier in the past decade also, intelligent systems based on artificial intelligence were used in the diagnosis of disease (DENDRAL, MYCIN), and their performance was very high [30]. Doctors can be assisted by AI systems as these systems can provide a huge amount of information to them which could result in a reduced number of errors during the treatment of patients. Past information of patients which can be fed to systems by activities such as diagnosis, screening, treatment, etc. can be extracted and health risks can be predicted. Researchers mainly concentrate on diseases, namely cancer, cardiovascular, and nervous system diseases where AI-based systems play an important role. AI techniques such as machine learning (ML), deep learning (DL), and natural language processing (NLP) are found to be very useful in medical applications. ML is a subset of AI in which the system learns itself using examples and the system is not explicitly programmed. ML has been used for diagnosing cancer, Parkinson's disease, predicting breast cancer, stroke diagnosis, identifying Alzheimer's disease, and predicting neurological and psychiatric disease. DL is a subfield of AL, which uses artificial neural networks [31]. A DL algorithm such as CNN has been used for detecting skin cancer using clinical images, identifying referable diabetic retinopathy, etc. However, NLP is being used in reading chest X-ray reports, monitoring adverse effects of laboratory, and detecting several diseases with the help of clinical notes [32]. Apart from these applications, AI and its techniques are actively being used by several nations for fighting against COVID-19. A Canadian company Blue Dot was the first to reveal the outbreak of corona in December 2019 and have developed an AI-based application that could recognize the location of the next outbreak of this virus. A drug that can reduce the effect of the virus was developed by Imperial College London and Benevolent using AI algorithms. For halting virus replication, six molecules are designed using AI algorithms by Insilico Medicine [33]. Several applications of AI in COVID-19 are displayed in Fig. 1 and are discussed below [2–4, 34].

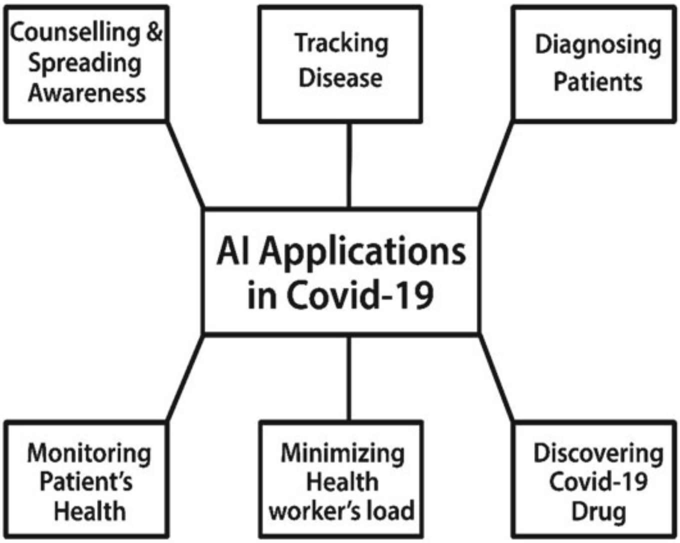


Fig. 1 Applications of artificial intelligence in COVID-19

3.1 Diagnosis

It has been seen that AI models can diagnose COVID-19 patients very quickly which gives radiologists more time to perform their tasks more effectively in a much cheaper way. Using radiology images COVID-19 can be detected. In a very short span of time, deep learning techniques can easily detect and predict whether a person is suffering from Coivd-19 or is healthy by simply using CT or X-ray images with high accuracy. Using deep learning an AI tool was developed for predicting and quantifying symptoms of COVID-19 in the lungs. Using this tool doctors can monitor health detecting the growth and the reaction of the virus during curing.

3.2 Tracking Disease

By tracking the spread of pandemic, significant information is generated which provides aid to health authorities and governments in planning and dealing with it. AI-based models are capable of monitoring and predicting the spread of this pandemic, as COVID-19 symptoms are little different from the regular cold or seasonal influenza. The person suffering from COVID-19 has a respiratory illness and displays fast breathing (tachypnea). Day-to-day updates of patients can be taken with the aid of a smartphone. Several applications are being deployed using smartphones by which a person can take self-assessment tests for COVID-19 and awareness is also spread amongst people. The location of the infected people is being tracked by the governments using GPS and Bluetooth features present in smartphones. As a result, the spread can be minimized. During the tracking process clusters and hotspots of the virus can be easily identified using AI and future spread can be predicted.

3.3 Monitoring Patient's Health

Visual features (blood tests, clinical data, etc.) of this disease are very helpful for proper monitoring of patient health conditions. These features are fed to various ML and DL models and the burden of health workers is being reduced. Moreover, these models are capable of providing updates to patients on a regular basis. High-risk patients can be identified early. This will reduce the mortality rate. A forecast model based on XGBoost calculation was proposed for forecasting the mortality risk and clinical features for predicting the probability of patient's mortality.

3.4 Discovering COVID-19 Drug

With a very high transmission rate and no signs of reducing mortality rate, it becomes a high priority to invent anti-viral drugs and medicine for curing patients. By incorporating AI for drug discovery, the development process of vaccines is shortened by several years. In 2019, based on AI, the first US clinical trial on flu vaccine was conducted by the National Institute of Allergy and Infectious Diseases. Using the AI program Flinders University created a synthetic chemist which can generate trillions of synthetic compounds. SAM (search algorithm for ligands), which is another AI program for searching compounds among trillions of compounds for identifying those which can be used in COVID-19. AI can help in accelerating the development process of vaccines by searching through the available dataset of available drugs and vaccines. MIT researchers are using AI models for obstructing corona virus by developing a type of protein that can be taken as medicine of COVID-19, as this virus binds the body's ACE2 receptors and causes sickness.

3.5 Spreading Awareness and Counseling

AI-based techniques are very much helpful in this battle. These techniques are being used for training, counseling, and spreading awareness among people. Multiple social media platforms are utilized by governments and health organizations for spreading awareness and for counseling people remotely. World Health Organization is tackling this pandemic by its information portal EPI-WIN (Information network for Epidemics). Facebook uses phrases such as "corona virus" and "COVID-19" for scanning all the content using its Ad Library and gathered 923 results from 34 countries. For battling against the spread of corona virus, the Indian government deployed a mobile application named "Arogya Setu" which tracks contamination by using Bluetooth and GPS. Using this application one can track cases around and recent updates are also available. Due to self-isolation and quarantine, various cases have come forward in this COVID-19 that people are suffering from depression and mental health issues. AI-based mobile applications can help in advising and counseling patients. In various cases, AI-enabled drones are being used for sanitizing contaminated areas, identifying people who are not putting on masks, and broadcasting information related to the pandemic and its precautions to the crowd. Small-Muti-Copter is a drone that is being used for supplying clinical and quarantine material through drones. AI models are being trained using the data from social media, smartphones, clinical data, and other sources so that they can detect contaminated areas, early detection of cases, and spread awareness among helpless people.

3.6 Minimizing Healthcare Worker's Load

Due to rapid rise in the number of cases of COVID-19, health workers have a very busy workload but due to AI their workload was reduced. Not only AI helps in early detection and treatment of COVID-19 but also helpful in providing training to doctors about novel diseases. AI-based chatbots have already shown success in clinical conditions for advising and helping multiple people. These chatbots can be deployed in this pandemic too for providing aid to people which could reduce more workload of health workers.

Multiple techniques are developed and are under development process for tackling COVID-19. Several countries have implemented strict lockdowns, thus reducing the transmission rate of the virus. Using technological enhancements various procedures have come into effect for diagnosing patients and predicting whether a person is affected by it or not. The next section describes various approaches in diagnosing COVID-19.

4 Approaches in Diagnosing COVID-19

Several AI techniques have been developed for automatic diagnosing and estimation of the severity of COVID-19. These AI techniques are showing great promise and are replacing traditional approaches for diagnosing COVID-19 patients. Figure 2 displays procedures (AI and non-AI) adopted by health workers for diagnosing COVID-19 patients. For diagnosing COVID-19 patients, first image acquisition needs to be done where images of the chest are captured using medical imaging equipment's like chest X-ray (X-radiation), thoracic CT (computer tomography), etc. which provides aid to doctors. In traditional techniques, there is contact between imaging technical persons and patients, as patients' positions are manually adjusted by the technicians for CT or X-ray. This may result in the spread of virus from patients to technicians. Conventional techniques lack accuracy, so they are inefficient and less reliable in comparison to AI-based techniques. AI-based sensors define the scan range of CT by defining the start and endpoints of the scan. After the image acquisition, the second step is image segmentation, where the region of interest is separated from the captured images for analyzing and quantification of COVID-19. For segmentation from CT images, several AI algorithms are used, namely U-Net, U-Net++, VB-Net etc., and from X-ray images it is very complex to segment the region of interest.

Several AI models have been proposed which are helpful for screening purposes based on X-ray or CT images of patients. In AI-based techniques, CT or X-ray systems are embedded with cameras for monitoring patients. In this pandemic, these systems provide contactless scanning processes and technicians can sit in the control room to monitor patients through video camera. CT or X-ray should not be performed for screening of asymptomatic patients if there are no or very less symptoms, so the performance of the AI model degrades sharply [35]. AI techniques are effective and

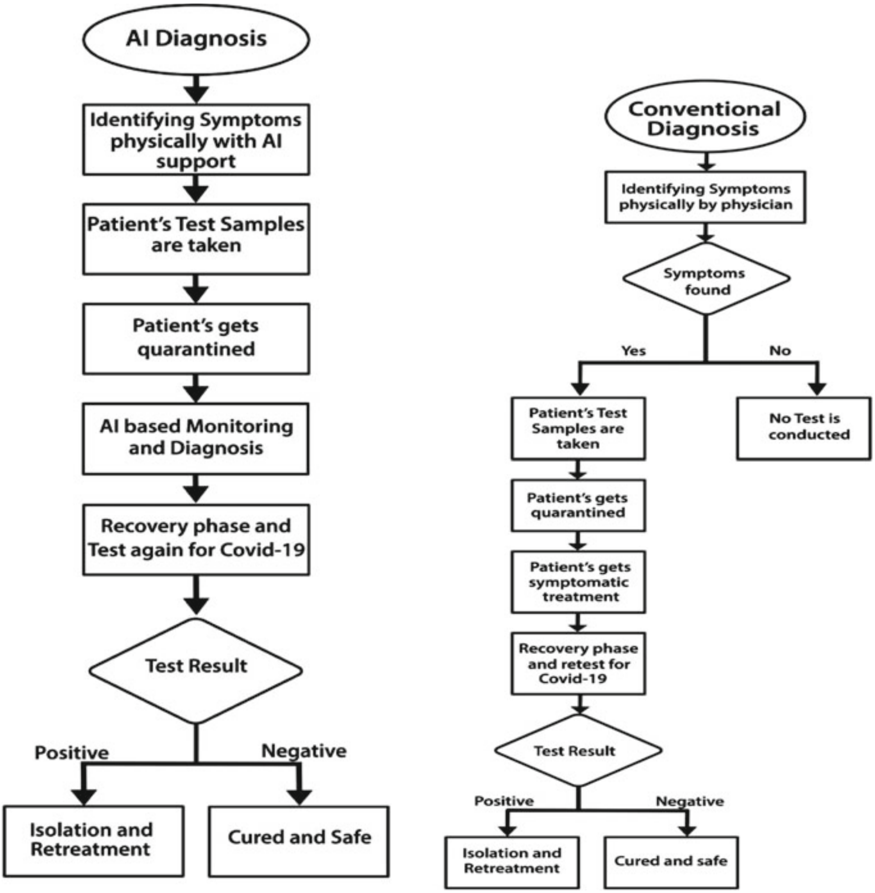

AI Diagnosis
Identifying Symptoms physically with AI support
Patient's Test Samples are taken
Patient's gets quarantined
AI based Monitoring and Diagnosis
Recovery phase and Test again for Covid-19
Test Result
Positive
Negative
Isolation and Retreatment
Cured and Safe
Conventional Diagnosis
Identifying Symptoms physically by physician
Symptoms found
Yes
No
Patient's Test Samples are taken
No Test is conducted
Patient's gets quarantined
Patient's gets symptomatic treatment
Recovery phase and retest for Covid-19
Test Result
Positive
Negative
Isolation and Retreatment
Cured and safe

Fig. 2 AI approach (left) and conventional approach (right) in COVID-19 diagnosis [3]

reliable only for the prediction of symptomatic patients. To the authors' best knowledge, till date no AI-based model is proposed which could recognize asymptomatic patients with high reliability and accuracy, so still a lot of work is to be done for the detection of asymptomatic patients. AI techniques have been playing a vital role in the healthcare sector, thus we can hope that they would play an important role in the eradication of COVID-19 from this world. The major advantage of diagnosing a patient with AI techniques is that the chain of virus is broken using these techniques. There are only minute chances of the virus to spread as tests are conducted without any physical interface between the patient and the COVID worker. But while using conventional techniques the virus can be transmitted very easily. There is no method for segmenting lesions from X-ray images. The third step after segmentation is screening where the patient is classified as positive or negative.

5 Discussion and Future Work

AI-based techniques are being actively used by several nations for fighting against COVID-19. AI has shown active participation in COVID-19 by improving planning, spreading awareness, diagnosing patients, and many more, thus in reducing the harmful effects of pandemic AI plays an important role. Multiple models have been already proposed for efficient detection of COVID-19 patients based on X-ray and CT images. It can be clearly assumed from Table 1 that multiple models have already been trained and tested on images but the accuracy level of detection through X-ray images is higher than that of CT images but these accuracies may differ when the model will be used in a real-time environment. In Fig. 2 multiple applications of AI techniques have been depicted in tackling COVID-19 and it has been observed that AI techniques had not only saved time for COVID workers but also the lives of patients. Manual detection techniques are prone to transmission, but AI techniques are automated and have prevented further transmission of virus from patients to technicians and other COVID workers. The objective of this research was to identify AI applications in this pandemic and several research papers were surveyed for the same. Furthermore, based on X-ray or CT scan images several classification techniques are identified for predicting whether a person is suffering from COVID-19 or not. These classification techniques are convolution neural networks, random forest, and other deep learning models. But the major issue is that these models can only detect symptomatic patients, not asymptomatic ones. This problem is yet to be solved by researchers and scientists. CT or X-ray should not be performed for screening of asymptomatic patients if they have no or very less symptoms, so the performance of the AI model degrades sharply [35]. AI techniques are effective and reliable only for the prediction of symptomatic patients. To our best knowledge to date, no AI-based model is proposed which could recognize asymptomatic patients with high reliability and accuracy, so still a lot of work is to be done for the detection of asymptomatic patients. The future direction of research would be diagnosing asymptomatic patients using AI algorithms. The next section concludes the paper.

6 Conclusion

COVID-19 has become quite a challenge for governments, companies, researchers, and other health organizations for developing policies to reduce the effects of corona virus and developing its cure as soon as possible. Technologies, particularly artificial intelligence (AI) is playing a vital role in managing COVID-19 as it is capable of rapidly processing a large amount of data and analyzing it in no time. Artificial intelligence (AI) is playing a vital role in managing COVID-19 as it is capable of rapidly processing a large amount of data and analyzing it in no time. AI-based techniques are being actively used by several nations for fighting against COVID-19. AI has shown active participation in COVID-19 by improving planning, spreading awareness, diagnosing patients, and many more. Thus reducing the harmful effects of pandemic AI plays an important role. This study discussed several applications of AI techniques for tackling COVID-19 and approaches used in diagnosing patients based on CT and X-ray images. This paper would provide aid to researchers for surveying applications of AI in COVID-19.

References

1. www.worldometers.info/coronavirus/
2. A. Kumar, P.K. Gupta, A. Srivastava, A review of modern technologies for tackling COVID-19 pandemic. Diabetes Metab. Syndr. Clin. Res. Rev. (2020)
3. R. Vaishya, M. Javaid, I.H. Khan, A. Haleem, Artificial Intelligence (AI) applications for COVID-19 pandemic. Diabetes Metab. Syndr. Clin. Res. Rev. (2020)
4. K. Iyengar, G.K. Upadhyaya, R. Vaishya, V. Jain, COVID-19 and applications of smartphone technology in the current pandemic. Diabetes Metab. Syndr. Clin. Res. Rev. (2020)
5. S. Kumar, M.S. Gaur, Call admission control in mobile multimedia network using grey wolf optimization, in *Intelligent Computing in Engineering. Advances in Intelligent Systems and Computing*, ed. by V. Solanki, M. Hoang, Z. Lu, P. Pattnaik, vol. 1125 (Springer, Singapore, 2020)
6. Z. Tang, W. Zhao, X. Xie, Z. Zhong, F. Shi, J. Liu, D. Shen, Severity assessment of coronavirus disease 2019 (COVID-19) using quantitative features from chest CT images. arXiv preprint arXiv:2003.11988 (2020)
7. C. Butt, J. Gill, D. Chun, B.A. Babu, Deep learning system to screen coronavirus disease 2019 pneumonia. Appl. Intell. (2020)
8. S. Wang, B. Kang, J. Ma, X. Zeng, M. Xiao, J. Guo, M. Cai, A deep learning algorithm using CT images to screen for Corona Virus Disease (COVID-19). MedRxiv (2020)
9. J. Chen, L. Wu, J. Zhang, L. Zhang, D. Gong, Y. Zhao, S. Hu, Deep learning-based model for detecting 2019 novel coronavirus pneumonia on high-resolution computed tomography: a prospective study. MedRxiv (2020)
10. L. Wang, A. Wong,COVID-Net: a tailored deep convolutional neural network design for detection of COVID-19 cases from chest X-Ray images. arXiv preprint arXiv:2003.09871 (2020)
11. A. Narin, C. Kaya, Z. Pamuk, Automatic detection of coronavirus disease (Covid-19) using x-ray images and deep convolutional neural networks. arXiv preprint arXiv:2003.10849 (2020)
12. B. Ghoshal, A. Tucker, Estimating uncertainty and interpretability in deep learning for coronavirus (COVID-19) detection. arXiv preprint arXiv:2003.10769 (2020)
13. F. Shi, L. Xia, F. Shan, D. Wu, Y. Wei, H. Yuan, H. Jiang, Y. Gao, H. Sui, D. Shen, Large-scale screening of covid-19 from community acquired pneumonia using infection size-aware classification. arXiv preprint arXiv:2003.09860 (2020)
14. Y. Song, S. Zheng, L. Li, X. Zhang, X. Zhang, Z. Huang, J. Chen, Deep learning enables accurate diagnosis of novel coronavirus (COVID-19) with CT images medRxiv (2020)
15. S. Tuli, S. Tuli, R. Tuli, S.S. Gill, Predicting the growth and trend of COVID-19 pandemic using machine learning and cloud computing. Internet Things (2020)
16. Z. Hu, Q. Ge, L. Jin, M. Xiong, Artificial intelligence forecasting of Covid-19 in china. arXiv preprint arXiv:2002.07112 (2020)
17. M. Jamshidi, A. Lalbakhsh, J. Talla, Z. Peroutka, F. Hadjilooei, P. Lalbakhsh, M. Jamshidi et al., Artificial intelligence and COVID-19: deep learning approaches for diagnosis and treatment. IEEE Access **8**, 109581–109595 (2020)
18. L. Lin, Z. Hou, Combat COVID-19 with artificial intelligence and big data. J. Travel Med. **27**(5) (2020)

19. T.P. Mashamba-Thompson, E.D. Crayton, Blockchain and artificial intelligence technology for novel coronavirus disease-19 self-testing. (2020)
20. A.S.R.S. Rao, J.A. Vazquez, Identification of COVID-19 can be quicker through artificial intelligence framework using a mobile phone–based survey when cities and towns are under quarantine. Infect. Control Hosp. Epidemiol. **41**(7) (2020)
21. F.M. Salman, S.S. Abu-Naser, E. Alajrami, B.S. Abu-Nasser, B.A.M. Alashqar, Covid-19 detection using artificial intelligence. (2020)
22. N. Lessmann, C.I. Sánchez, L. Beenen, L.H. Boulogne, M. Brink, E. Calli, J.-P. Charbonnier et al., Automated assessment of CO-RADS and chest CT severity scores in patients with suspected COVID-19 using artificial intelligence. Radiology (2020)
23. X. Jiang, M. Coffee, A. Bari, J. Wang, X. Jiang, J. Huang, J. Shi et al., Towards an artificial intelligence framework for data-driven prediction of coronavirus clinical severity. CMC Comput. Mater. Continua **63** (2020)
24. Q.-V. Pham, D.C. Nguyen, W.-J. Hwang, P.N. Pathirana, Artificial Intelligence (AI) and big data for coronavirus (COVID-19) pandemic: a survey on the state-of-the-arts. (2020)
25. L. Bellomarini, M. Benedetti, A. Gentili, R. Laurendi, D. Magnanimi, A. Muci, E. Sallinger, Covid-19 and company knowledge graphs: assessing golden powers and economic impact of selective lockdown via ai reasoning. arXiv preprint arXiv:2004.10119 (2020)
26. E. Zhang, N. Gupta, R. Tang, X. Han, R. Pradeep, K. Lu, Y. Zhang et al., Covidex: neural ranking models and keyword search infrastructure for the Covid-19 open research dataset. arXiv preprint arXiv:2007.07846 (2020)
27. Md M. Ahsan, K.D. Gupta, M.M. Islam, S. Sen, Md Rahman, M.S. Hossain. Study of different deep learning approach with explainable AI for screening patients with COVID-19 symptoms: using CT scan and chest x-ray image dataset. arXiv preprint arXiv:2007.12525 (2020)
28. S. Hu, Y. Gao, Z. Niu, Y. Jiang, L. Li, X. Xiao, M. Wang et al., Weakly supervised deep learning for covid-19 infection detection and classification from CT images. IEEE Access **8** (2020)
29. A.S. Imran, S.M. Daudpota, Z. Kastrati, R. Batra, Cross-cultural polarity and emotion detection using sentiment analysis and deep learning on covid-19 related tweets. IEEE Access **8** (2020)
30. S.J. Russell, P. Norvig, Artificial intelligence—a modern approach, 3rd International edn. (2010), pp. I–XVIII
31. S. Kumar, M.S. Gaur, Handoff prioritization to manage call admission control in mobile multimedia networks for healthcare, in *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (Kanpur, India, 2019), pp. 1–7
32. F. Jiang, Y. Jiang, H. Zhi, Y. Dong, H. Li, S. Ma, Y. Wang, Q. Dong, H. Shen, Y. Wang, Artificial intelligence in healthcare: past, present and future. Stroke Vasc. Neurol. **2**(4), 230–243 (2017)
33. B. McCall, COVID-19 and artificial intelligence: protecting health-care workers and curbing the spread. Lancet Digit. Health **2**(4), e166–e167 (2020)
34. A.S. Ahuja, V.P. Reddy, O. Marques, Artificial intelligence and COVID-19: a multidisciplinary approach. **100434** (2020)
35. C. Jalaber, T. Lapotre, T. Morcet-Delattre, F. Ribet, S. Jouneau, M. Lederlin, Chest CT in COVID-19 pneumonia: a review of current knowledge. Diagn. Interv. Imaging (2020)

Role of ICT in Imparting Quality Education and Curbing Cyber Security Risks During COVID-19 Pandemic

Nidhi Agarwal, Ruchika Gupta, and Puneet Kumar

1 Introduction

Education upholds the basic values that lead to the well-being of people and communities. This offers the foundation for meaningful learning and encourages trust despite the obstacles encountered. It gives the ability to people to turn out to be progressively independent and mindful of chances and rights. It likewise upgrades the capacity of people to oversee medical issues, improve sustenance and childcare, and plan for what's to come. Education does not just affect human turn of events and financial development, yet in addition, it is the central necessity for democracy. Through education individuals become progressively dependable and educated residents and have a voice in governmental issues and society, which is fundamental for sustaining democracy. This is important to eliminate deprivation and helps people to be more successful, to perform greater roles in economic life, and to make a better living. It suggests that the concept and scope of education are very wide and it is a continuous process in human life. Every student in the classroom situation gets knowledge from the teacher and the textbooks. It is a formal education, whereas family society mass media are the sources of giving formal education, and teacher plays a very important role in it. In any case, the procedure of education doesn't possibly begin when a child initially goes to school.

Education starts at home. One doesn't just obtain information from an instructor; one can take in and get information from a parent, relative, and even a colleague. In practically all social orders, going to school and accepting an education is very

N. Agarwal
Integrated School of Education, Ghaziabad, India

R. Gupta (✉)
Amity University Uttar Pradesh, Greater Noida Campus, Greater Noida, India

P. Kumar
Kalinga University, Chhattisgarh, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_26

imperative and fundamental in the event that one needs to make progress. Be that as it may, shockingly we have put on the planet where not every person has a chance to get this proper sort of education. The open doors that are offered are significantly constrained. Now and then there are insufficient assets to give schooling. Besides in light of the fact that guardians need their children to assist them with working in industrial facilities, have unspecialized temp jobs, or simply accomplish ranch work [1].

Since it isn't customary, in certain spots, to get a conventional education, the person who gets an education is normally begrudged, adulated, and even appreciated by individuals from the network. Children once in a while take a gander at other children with wonderment. Simply a similar path as one child would begrudge another in light of the fact that he got another pair of tennis shoes, and wishes he could have as well. There is a feeling of adoration and yet there is a feeling of desire too. Seeing your friend shows improvement over yourself, causes some pressure and envy on account of the scant open doors accessible. As a child, it is difficult to comprehend why there is a distinction.

Learning subjects in school isn't sufficient. One can learn history, math, science in school, and be "book-shrewd". Moreover, one can figure out how to live by realizing what to state when acting a specific path in specific circumstances and be "road shrewd". These two sorts of knowledge are very basic to be effective throughout everyday life. For instance, you can have all the "book" knowledge on the planet about a specific calling, yet in the event that you don't have the foggiest idea how to carry on with your collaborators or potentially your bosses, having "book" knowledge won't get you excessively far. Be that as it may, regardless, education is the key that permits individuals to climb on the planet, look for better occupations, and at last succeed completely throughout everyday life. Education is significant, and nobody ought to be denied of it. Education is the procedure of guidance focused on the inside and out improvement of people, giving the vital apparatuses and knowledge to comprehend and take an interest in everyday exercises of the present world. It scatters numbness and lifts the virtues of the people. It is the main riches that can't be looted. It manufactures character, gives the quality of brain, and builds knowledge.

Now the world is being confronted with the explosion of information and knowledge in every discipline. For their dissemination advanced communication technology is felt essential for both developing and developed countries. Moreover, since the time and space could be effectively cut down by the media, it will be easily possible to capture the events and relay them as it happens. Hence an effect of direct experience could have been made possible by the effective utilization of media.

ICT is another way to say "Information and Communication Technologies". It is like IT (information technology), yet concentrates more on telecommunications mediums, for example, the web, wireless systems, and satellite innovation. The present-day types of ICT have made it feasible for clients over the world to speak with one another progressively all the time. Models incorporate texting, media tools, video-conferencing, online multiplayer gaming, and long-range interpersonal communication sites.

Information and communication technologies (ICT) have become ordinary elements in all parts of life. Over the previous 20 years, the utilization of ICT has on a very basic level changed the practices and strategies of almost all types of try inside business and administration. Education is a socially arranged action and quality education has customarily been related with solid educators having high degrees of individual contact with students. The utilization of ICT in education fits more understudy-focused learning settings. However, with the world moving quickly into advanced media and information, the job of ICT in education is turning out to be increasingly significant and this significance will proceed to develop and create in the twenty-first century.

Furthermore, the current global pandemic COVID-19 has brought transformation in all spheres of life and has totally reshaped the way we used to work earlier. Education has tirelessly clung to conventional methods for getting things done. There was also strong development and penetration of education technologies well before COVID-19, with global revenues of edutech hitting US$ 18.66 billion in 2019 and the total online education industry expected to hit $350 billion by 2025. Regardless of whether it is language applications, virtual coaching, video conferencing instruments, or internet learning programming, there has been a critical flood in use since COVID-19 [2].

Also, it needs to be mentioned that online learning was launched in a hurry in institutions around the nation because of the rapid disruption of common in-classroom practices due to virus outbreak, leaving networks on campus fully accessible to security issues.

2 Objectives of the Study

With this unexpected move away from the homeroom in numerous pieces of the globe, some are pondering whether the reception of web-based learning will keep on persevering post-pandemic, and how such a move would affect the overall education sector. Therefore, the objectives of this paper are:

- To study the role of ICT in improving the quality of education.
- To study the impact on quality education using ICT under COVID-19.
- To study the role of ICT in curbing cyber security risks.
- To suggest remedial measures for the successful imparting of quality online education.

3 Hypothesis

The null hypothesis based on the objectives of the paper is as follows:

1. There is no impact of COVID-19 on quality education for using ICT in online teaching.

4 Previous Background of the Study

Jhurree (2005) states that much have been said and announced about the effect of innovation, particularly PCs, in education. At first, PCs were utilized to encourage PC programming yet the improvement of the microchip in the mid-1970s saw the presentation of reasonable microcomputers into schools at a quick rate. PCs and utilizations of innovation turned out to be increasingly inescapable in the public eye which prompted a worry about the requirement for figuring aptitudes in regular existence [3].

Dodzi Amemado (2020) states that with this abrupt and sudden surge, online education worldwide has come one considerable above and beyond. Since the late 1990s, when the web began assuming a job in course conveyance, advanced education foundations (HEIs) have been step by step utilizing this development and changing their key headings. Online guidance ends up being advantageous for working grown-ups. This urged colleges to utilize online guidance to advance course content and draw in understudies. As new needs arise among target gatherings, the authenticity of online education continues expanding and its raison gets irreversible. For example, through flipped study halls, making course materials accessible online is the best educational strategy to show some scholastic subjects. The advantages are instructive, yet in addition social and monetary. For computerized locals, online is a favored mechanism for social connections, and their desires around multimodality and online devices continue expanding. For working grown-ups, taking on the web rather than face-to-face courses has a financial advantage. Online education additionally cultivates a worldwide knowledge society, global associations, and substance sharing and local coordinated effort among colleges. It connects with outcasts and detainees, expanding the administration of crucial colleges. In nations where advanced education is overloaded by massification, online education might be a piece of the answer for expanding access. And now, online education is being utilized to go around face-to-face gatherings out of fear of sullying from the coronavirus [4].

4.1 Cyber Security and Crime

Cybercrime which is otherwise called "web wrongdoings" or "PC violations" is any crime that uses a PC either as an instrument, target, or a method for propagating further wrongdoings or offenses or negations under any law. Cybercrime is by and large viewed as any criminal behavior directed through a PC. The stress is cybercrime as a noteworthy worry to the worldwide network [5, 6].

The presentation, development, and use of data and correspondence advances (ICTs) have been joined by an expansion in crimes. There are four noteworthy classifications of digital violations such as digital wrongdoing against people, digital wrongdoing against property, digital wrongdoing against association, and digital wrongdoing against society. Digital violations against people are hacking, email satirizing, spamming, digital criticism and provocation, digital stalking, and digital harassment. “Hacking in layman terms implies an unlawful interruption into a PC framework” [7, 8].

Parthasarathi (2003) obviously expressed that cybercrime against the association is such unapproved getting to of PC, refusal of administration, infection assault, email besieging, salami assault, rationale bomb, Trojan pony, and information diddling. Malaysian cyber security likewise recognizes that digital wrongdoing against society such as imitation in money notes, income stamps, mark sheets additionally can be manufactured utilizing PCs and amazing scanners and printers. “Digital fear based oppression is the utilization of PC assets to threaten or constrain others” and “web jacking is programmers’ obtain entrance and authority over the site of another, even they change the substance of the site for satisfying political target or for cash” [9].

The present computerized age is quickly getting to be consistent with practically all parts of current social orders. While reliance on data frameworks develops, so does the utilization of such frameworks range out to arrive at the most disengaged places the world over. Multiplication of PCs and dependence on these frameworks turns into a worldwide wonder, augmenting the data foundation connecting these various frameworks together, winding up increasingly mind-boggling and progressively hard to oversee at a concentrated level without obstructing on speed and quality.

5 Methodology

The scientific investigations of some problems are included in the process of research. The process of investigation is the acknowledgment of this fact and thus the problem can be seen from a very interactive process. It is to be required and then the knowledge belonging to the problem can be known accordingly. In this study, we try to study researches and educational researches and the utility relating to educational aspects. Besides this, more effective light will be thrown on the knowledge and inquiry. The most important aim of the research is to search specific answer to the specific question to seek the solution to problems on the basis of collected data through scientific methods. To achieve these answers and solutions, the main methods are developed by which more possibility of the subjects increases as well. It is very obvious to note that due to solutions we observe that the questions asked related to information are not only connected with the subject but also are more reliable [10, 11].

Methodology of the research paper mentioned here that we have applied random purposive technique to find out the data collection with the sample of 50 teachers residing in National Capital Region of India (Delhi-NCR) using media tools and ICT for their teaching-learning process during COVID-19 pandemic [12].

6 Analysis of Data

First of all, we asked the questions to 50 randomly selected teachers of any region. We asked them whether they prefer online teaching using media tools or any other ICT rather than face-to-face during COVID-19. In this regard, all the respondents were not similarly responsive; therefore, the overall response is given in the table and chart (Table 1; Fig. 1).

We further asked the respondents whether they agree that they stick to media information and knowledge for the result while talking or writing about ideas during online teaching in lockdown. In this regard all the respondents were not similarly

Table 1 Response for question number 1

S. no.	Parameters	Number of respondents	Observed mean
1	Not at all well	2	**3.50**
2	Not very well	2	
3	Slightly well	25	
4	Somewhat well	11	
5	Well	10	
6	Very well	0	
7	Extremely well	0	

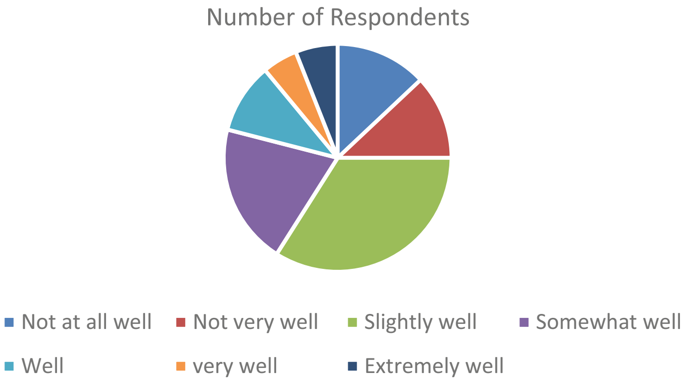


Fig. 1 Response for question number 1

Table 2 Response for question number 2

S. no.	Parameters	Number of respondents	Observed mean
1	Not at all well	2	**3.72**
2	Not very well	10	
3	Slightly well	18	
4	Somewhat well	2	
5	Well	8	
6	Very well	8	
7	Extremely well	2	

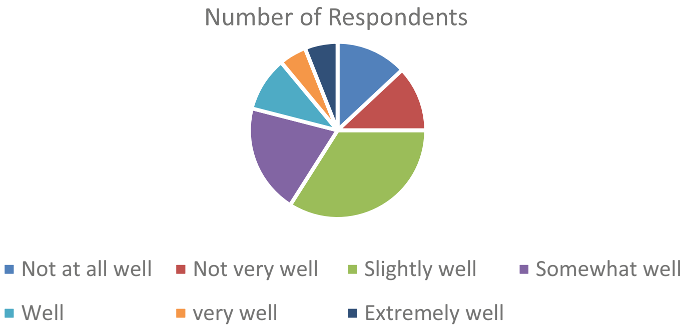


Fig. 2 Response for question number 2

responsive; therefore, the overall response is given in the table and chart (Table 2; Fig. 2).

There are various factors that are considered during the start of any task. Hence, we asked the respondents whether they like to use ICT face-to-face better than online teaching during COVID-19. In this regard, all respondents were not similarly responsive. Therefore, the overall response for this question is given in the table and chart (Table 3; Fig. 3).

Table 3 Response for question number 3

S. no.	Parameters	Number of respondents	Observed mean
1	Not at all well	1	**4.64**
2	Not very well	4	
3	Slightly well	4	
4	Somewhat well	12	
5	Well	19	
6	Very well	2	
7	Extremely well	8	

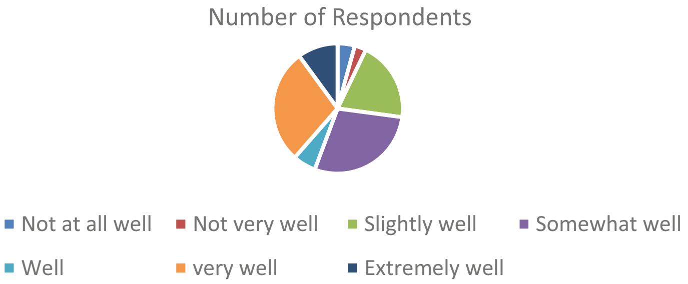


Fig. 3 Response for question number 3

Table 4 Response for question number 4

S. no.	Parameters	Number of respondents	Observed mean
1	Not at all well	3	**4.06**
2	Not very well	5	
3	Slightly well	18	
4	Somewhat well	4	
5	Well	7	
6	Very well	6	
7	Extremely well	7	

We further asked the respondents whether they agree that they always set priorities before starting, to prepare set up for the online task is always beneficial due to COVID-19 pandemic. In this regard, all respondents were not similarly responsive. Therefore, the overall response for this question is given in the table and chart (Table 4; Fig. 4).

As per the questionnaire survey, we further asked the respondents, whenever you face any problem, you seek help from media and online tools during the lockdown.

Fig. 4 Response for question number 4

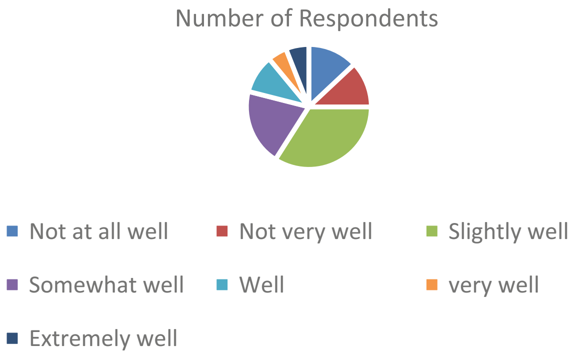
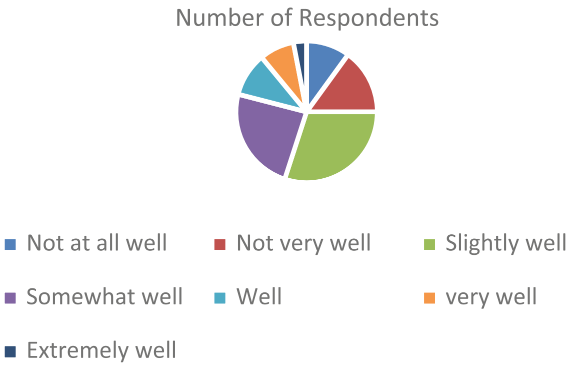


Table 5 Response for question number 5

S. no.	Parameters	Number of respondents	Observed mean
1	Not at all well	1	**3.46**
2	Not very well	5	
3	Slightly well	30	
4	Somewhat well	4	
5	Well	6	
6	Very well	2	
7	Extremely well	2	

Fig. 5 Response for question number 5



In this regard, all respondents were not similarly responsive. Therefore, the overall response for this question is given in the table and chart (Table 5; Fig. 5).

It was also asked to the respondents whether they are aware of cyber risks associated with online teaching during COVID-19. In this regard, all respondents were not similarly responsive. Therefore, the overall response for this question is given in the table and chart (Table 6; Fig. 6).

Table 6 Response for question number 6

S. no.	Parameters	Number of respondents	Observed mean
1	Not at all well	7	**3.94**
2	Not very well	6	
3	Slightly well	14	
4	Somewhat well	3	
5	Well	5	
6	Very well	6	
7	Extremely well	9	

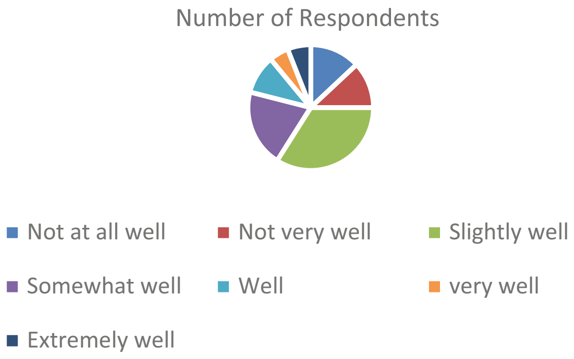


Fig. 6 Response for question number 6

Table 7 Response for question number 7

S. no.	Parameters	Number of respondents	Observed mean
1	Not at all well	10	**4.04**
2	Not very well	4	
3	Slightly well	6	
4	Somewhat well	6	
5	Well	8	
6	Very well	10	
7	Extremely well	6	

Whenever we are given any task to do we need to consider each and every task. While keeping this fact in mind, we asked the respondents whether they agree that they pay less attention to the online teaching during COVID-19 in detail. In this regard, all respondents were not similarly responsive. Therefore, the overall response for this question is given in the table and chart (Table 7; Fig. 7).

We further asked the respondents whether they agree that they figure out the solution for the problem facing how to use ICT equipment during teaching facing

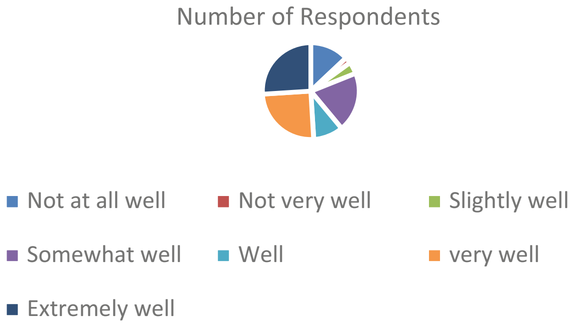


Fig. 7 Response for question number 7

Table 8 Response for question number 8

S. no.	Parameters	Number of respondents	Observed mean
1	Not at all well	4	**4.36**
2	Not very well	2	
3	Slightly well	14	
4	Somewhat well	6	
5	Well	8	
6	Very well	8	
7	Extremely well	8	

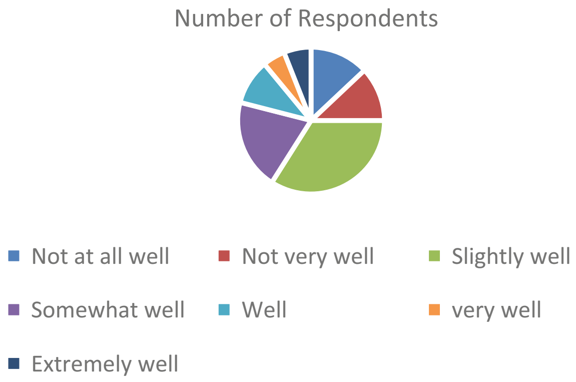


Fig. 8 Response for question number 8

COVID-19. In this regard, all respondents were not similarly responsive. Therefore, the overall response for this question is given in the table and chart (Table 8; Fig. 8).

To know any type of help is needed to deal with the task in different situations, hence we asked the respondents whether they agree that they do not need any help from others while controlling class online during COVID-19. In this regard, all respondents were not similarly responsive. Therefore, the overall response for this question is given in the table and chart (Table 9; Fig. 9).

Table 9 Response for question number 9

S. no.	Parameters	Number of respondents	Observed mean
1	Not at all well	7	**3.96**
2	Not very well	5	
3	Slightly well	14	
4	Somewhat well	4	
5	Well	6	
6	Very well	5	
7	Extremely well	9	

Fig. 9 Response for question number 9

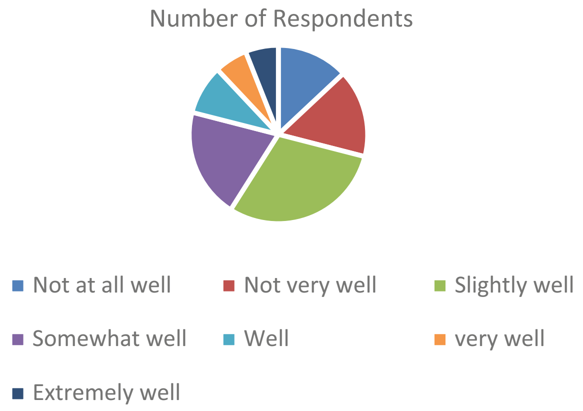


Table 10 Response for question number 10

S. no.	Parameters	Number of respondents	Observed mean
1	Not at all well	8	**3.54**
2	Not very well	6	
3	Slightly well	16	
4	Somewhat well	5	
5	Well	6	
6	Very well	4	
7	Extremely well	5	

Whenever we do any task we should also notice its implementation. Hence, we asked the respondents whether they follow the media information and also observe them online with interest during COVID-19. In this regard all respondents were not similarly responsive. Therefore, the overall response for this question is given in the table and chart (Table 10; Fig. 10).

Fig. 10 Response for question number 10

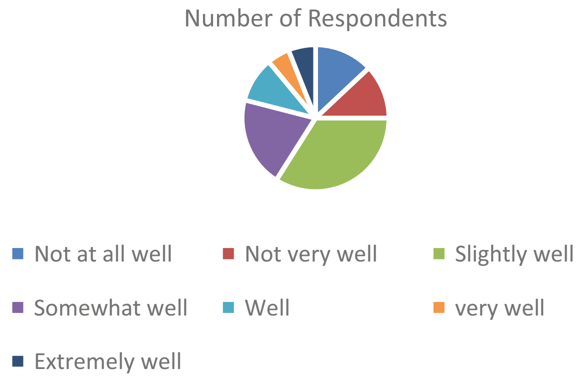


Table 11 Impact of COVID-19 on online teaching for quality education

Q. no.	Observed mean	Expected mean	Chi-square value
1	3.5	4.0	**0.03453**
2	3.72	4.0	
3	4.64	4.0	
4	4.06	4.0	
5	3.46	4.0	
6	3.94	4.0	
7	4.04	4.0	
8	4.36	4.0	
9	3.96	4.0	
10	3.54	4.0	

The perusal of Table 11 shows that the chi-square value has come out to be 0.03453 which is below the table value of chi-square at any level of significance.

7 Motivation for Undertaking the Study

During the pandemic COVID-19 situation, it was very difficult to attend classes face-to-face during the lockdown, and to take precautions from COVID the education system should have to use media tools and ICT to improve the online teaching-learning process. The education system always seeks the role of ICT in education to improve it, but during COVID-19 the situation became mandatory and necessary to add an online system in the education system to maintain its quality. The challenges faced by teachers to do online teaching among others are poor usage and management of learning management system to facilitate courses online, poor internet connection, poor computer usage among students and lecturers at the university, small lecture rooms as a result of an ever-increasing number of students' admission at the university [13].

8 Conclusion and Suggestions

The quality in higher education using ICT under COVID-19 is affected. Conveying education online has been received by practically all colleges and schools around the world at various paces, going from the disconnected, drop-and-go model to exceptionally serious, all-around organized, and completely online projects. However, a few difficulties are as yet hindering e-learning in advanced education. Media used in online teaching sometimes lack facts and information which misguide the education system and affect it vigorously. The ICT equipment is used in online teaching for effective teaching and maintaining the quality of higher education, but due to lack of connectivity and technology, effective results could not be achieved.

In India the most genuine difficulties are monetary costs, guidelines, the advanced hole, and the social jump for instructors. The primary hindrances are understudies' self-inspiration and self-association abilities in completely online educational settings. And there is a typical misperception that educating or taking courses online may be less demanding than eye-to-eye courses. Staying aware of the innovation and getting staff to adjust to the social change are viewed as the fundamental troubles.

Legitimate measures absolutely assume an indispensable job in combatting cybercrime and should address various zones, going from substantive to procedural criminal law, just as incorporating jurisdictional issues. At any rate, far-reaching arrangement systems ought to likewise be set up. The following areas will concentrate on three explicit classes of approach methodology that could help the battle against cybercrime: counteractive action through risk appraisals, effort, and mindfulness raising.

The study suggests certain common tasks that need to be implemented in order to make sure that both students and teachers enjoy a safe experience with the online education system during the COVID-19 pandemic:

- Holding cybersecurity awareness programs for the users so as to enable them to understand the dark side of technology and also to guide them on how to stay safe during online education.
- It is also recommended that a security manual be prepared and retained at all stages. When adhering to a published/prepared protection rule, a checklist or an enforcement plan should be there with regard to the use of the online mode of education.
- Using a protected system to ensure optimization of the computer or system being used to launch the new app.
- It should always be ensured to log in to an online service with maximum encryption turned on.
- Generally, it is recommended to use the learning platform or application to launch a session with the camera, and the microphone was put on Off mode after joining the session.

Appendix

Q1. Do you prefer to deal with online teaching using any ICT rather than with face-to-face during COVID-19?

(a) Not at all well
(b) Not very well
(c) Slightly well

(d) Somewhat well
(e) Well
(f) Very well
(g) Extremely well

Q2. Do you agree that you stick to media information and knowledge for the result while doing online teaching during COVID-19?

(a) Not at all well
(b) Not very well
(c) Slightly well
(d) Somewhat well
(e) Well
(f) Very well
(g) Extremely well

Q3. Do you think the students like to use ICT equipment face-to-face better than online teaching during COVID-19?

(a) Not at all well
(b) Not very well
(c) Slightly well
(d) Somewhat well
(e) Well
(f) Very well
(g) Extremely well

Q4. Do you agree that you always set priorities before starting the task online during COVID-19?

(a) Not at all well
(b) Not very well
(c) Slightly well
(d) Somewhat well
(e) Well
(f) Very well
(g) Extremely well

Q5. Whenever you face any problem, you seek help from media and online tools during lockdown COVID-19?

(a) Not at all well
(b) Not very well
(c) Slightly well
(d) Somewhat well
(e) Well
(f) Very well
(g) Extremely well

Q6. Are you aware of the cyber risks associated with online teaching?

(a) Not at all well
(b) Not very well
(c) Slightly well
(d) Somewhat well
(e) Well
(f) Very well
(g) Extremely well

Q7. Do you agree that you pay less attention to the online teaching during COVID-19?

(a) Not at all well
(b) Not very well
(c) Slightly well
(d) Somewhat well
(e) Well
(f) Very well
(g) Extremely well

Q8. Do you agree that you figure out the solution for the problem facing how to use ICT equipment safely for preventing cyber security risk during online teaching?

(a) Not at all well
(b) Not very well
(c) Slightly well
(d) Somewhat well
(e) Well
(f) Very well
(g) Extremely well

Q9. Do you agree that you do not need help from others while controlling class online during COVID-19?

(a) Not at all well
(b) Not very well
(c) Slightly well
(d) Somewhat well
(e) Well
(f) Very well
(g) Extremely well

Q10. Do you follow the media information and also observe them online with interest during COVID-19?

(a) Not at all well
(b) Not very well
(c) Slightly well
(d) Somewhat well

(e) Well
(f) Very well
(g) Extremely well.

References

1. N. Agarwal, N. Pundir, A comparative study of personality traits and thinking styles of ICT users and non users. Int. J. Dyn. Educ. Res. Soc. **1**(1), 74–83 (2019)
2. http://www.who.int/docs/default-source/coronaviruse/key-massages-and-actions-for-COVID-19-prevention-and-control-in-schools-march-2020.pdf
3. Jhurree, Impact of technology, especially computers. Educ. JIER **8**(2), 23–34 (2005)
4. A. Dodzi, COVID-19 an unexpected and unusual driver to online education. Glob. Pict. Int. High. Educ. **102**, 12–14 (2020)
5. G. Chandra, R. Gupta, N. Agarwal, Role of artificial intelligence in transforming the justice delivery system in COVID 19 pandemic. Int. J. Emerg. Technol. **11**(3), 344–350 (2020). ISSN: 0975-8364
6. N. Agarwal, P. Kumar, Role of Information Technology in Education, in *AICTE Sponsored National conference on Information Integrity & Supply chain Management Abstracts Proceeding* (Book World Publisher, Dehradun, 2009), p. 18
7. S Varma, R Gupta, Customer perception and behavioral intention to adopt biometric enabled e-banking services in India, in *Business Analytics and Cyber Security Management in Organizations* (IGI Global Publications, 2016), pp. 137–146
8. R. Gupta, S Agarwal, A comparative study of cyber threats in emerging economies. Glob. Int. J. Manag. IT, **8**(2), 24–28 (2017)
9. P. Pati. Cyber-crime, The Indian Law Institute (2003), http://naavi.org/pati/
10. N. Agarwal, P. Kumar, S. Mishra, Need to acquire democratic competency by teacher educator in global scenario. Maa Omwati J. Educ. Res. Dev. **1**(1). https://doi.org/10.5281/zenodo.3837657. ISSN: 0976-1365
11. N. Agarwal, M. Sharma, A matter of styles in education. Asian J. Psychol. Educ. **69**(5), 2–6 (2007). https://doi.org/10.5281/zenodo.3813617
12. E. Agarwal, A review of test prioritization regression testing based on time. Glob. Int. J. Manag. IT **11**(1), 35–38 (2019). ISSN: 0975–721X
13. A. Goel, E. Agarwal, Assessing innovation in teacher education. Glob. J. Prog. Educ. **9**(2), 50–52 (2019). ISSN: 2231-1335

Detect and Track the Motion of Any Moving Object Using OpenCV

Harikesh Pandey, Pushpa Choudhary, and Arjun Singh

1 Introduction

In computer vision using OpenCV library, i.e., the open-source library enables computers to visualize objects like humans. It is the image processing library [1] created by Intel and later supported by willow garage and maintained by Itseez. OpenCV library is the python library used for machine learning applications like image detection, motion detection, etc. It gives a machine a vision, which is basically known as computer vision through which a machine is able to visualize things. The command to install OpenCV is "!pip install OpenCV."

- OpenCV is available on different operating systems such as Linux, Windows
- Works in C, C++, and Python
- Open Source and free
- Easy to use and install
- Used in machine learning
- Used in image processing, motion tracking, etc.

Tracks the motion of an object when placed in front of camera uses contours around the object to detect the motion while this process can be done by MATLAB also, but we are using OpenCV. Why we use OpenCV not MATLAB is because:

a. OpenCV is an open-source means free for the user that is of no cost, while in the case of MATLAB it is not free, meaning MATLAB is expensive than OpenCV.
b. OpenCV is fast compared to MATLAB because OpenCV converts an image directly to machine language code.
c. As OpenCV runs on C and MATLAB on Java, so any system uses C language then OpenCV runs on any operating system while Windows or Linux.

H. Pandey (✉) · P. Choudhary · A. Singh
Department of Information Technology, GL Bajaj Institute of Technology and Management, Greater Noida, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_27

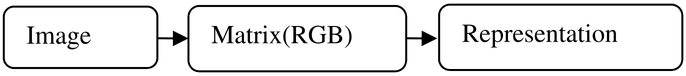


Fig. 1 Recognition system

2 Related Work

The paper is based on the OpenCV library of python in machine learning which is used to provide vision to computers:

- A machine visualizes an image as follows:
- Machine interprets any image [2] as a matrix with rows, columns, and an RBG channel.
- This matrix actually represents the pixels count at every inch of the image.
- OpenCV uses this image processing technique to see objects.

As mentioned above that image detection can be done in three phases, the first one is to visualize the image; the second is to visualize image interpreted as a matrix in RGB color, and the last third is a representation of the image. In image detection camera or video takes an object image as an input and produces output in the form of matrix color that is segmented in combined part of cells (Fig. 1).

Object detection [3] focuses on the foreground and does not focus on the background side of an object, meaning the detection technique eliminates the background [4] and focused on the foreground pixel of the object. But object detection faces problems during overlapping of the object and is unable to detect the object [5]. Image overlapping is then reduced with the help of object framing phenomena. Object movement is found by using a threshold with the comparison of the observed image.

3 Proposed Work

In this paper, we use contours to detect and track the motion of any moving object. Contours are nothing but imaginary points on the boundaries of a moving object that help us track the motion of the object.

Here we observe this paper in two parts:

1. Object detection
2. Tracking the object

3.1 Object Detection

Fig. 2 first defines the image. The image should be saved in a specific frame. After saving the image in a frame using Gaussian methods take some not clear image

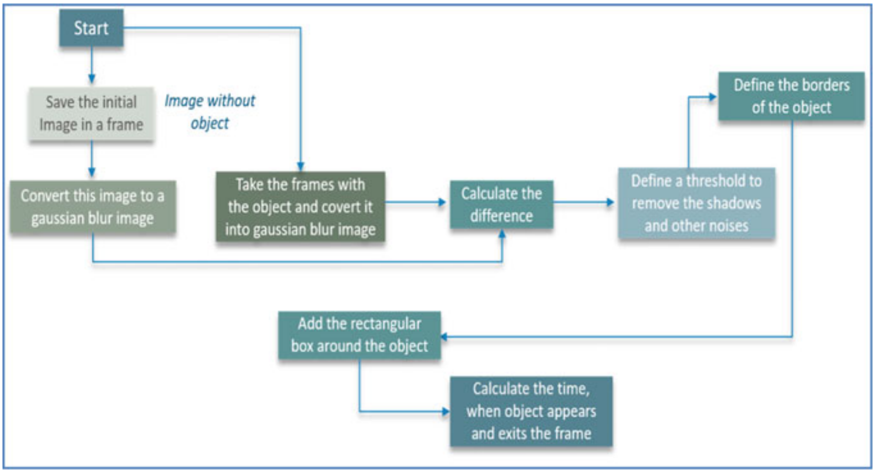

Start
Save the initial Image in a frame
Image without object
Convert this image to a gaussian blur image
Take the frames with the object and covert it into gaussian blur image
Calculate the difference
Define a threshold to remove the shadows and other noises
Define the borders of the object
Add the rectangular box around the object
Calculate the time, when object appears and exits the frame

Fig. 2 The process of converting the image in a frame

and the real image and find out the differences between both pixel gaps. This is not confirming the final object of the image that implemented threshold to remove some noise and distortion of image points. We do not confuse detection and recognition [6]. Let us see that both are different and their concept is different. In the case of object detection [7, 8], we detect the object among given multiple objects while in the recognition, the system identifies the object. Here in this paper, we focus on detecting the object.

3.1.1 Segmentation

Segmentation is a technique that divides the images (binary form images are called digital images) into multiple areas or regions that contain pixels. The main aim of segmentation [9–11] is to make it user-friendly to view, impactful, and analyze the set of pixels. The output of segmentation is a conation group of segments; the segment contains the collection of each image or picture that represents the clip of contours that gain from the picture.

Each pixel has some characteristics and each group of pixels maintains a similar property of each pixel that is put together to form a meaningful area that has similar characteristics such as color, power, and features (Fig. 3).

That kinds of pixels are put together in a contour that forms a segment and that contour is looked at in a computer vision, which is more important to distinguish the different characteristics that adjoin the areas of similar types of pixels with identical characteristics.

Detecting [12] non-static object in a picture in computer vision is a very tough task because their sequences are not in the same manner, so sequencing the image processing pixels with the background of an image is discarded and points out those

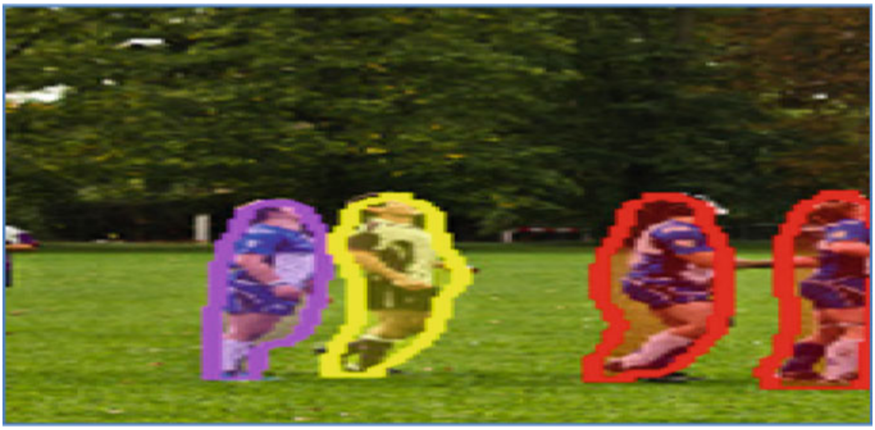


Fig. 3 Image segmentation process

points that are moving. So focus on those points that are changing their location point and those points are moving points, and some other points or pixels that do not change their location are static points or pixels. So by using these location points discard the static point that are background points effectively.

3.1.2 Gaussian Model

In this Gaussian model [13], we find a foreground image in four steps:

Step 1. In this step, we find the mean of input pixels and compare this mean pixel and consider those points that are near enough to this mean pixel. By using this mean pixel discard the pixels in a contour and maintain a segment. So after segmenting compare with the standard deviation that differences should be less than the standard deviation.

Step 2. After getting the pixels, update the content that affects the obtained new pixels, that is, weight, mean, and standard deviation or variance. So in comparison let standard deviation and mean remain the same. Then new pixels' weight value decreases and points out in the non-matched category.

Step 3. After identifying the new pixels, in this step we find out the background image pixels. Now for getting a background image set a comparison value that is a threshold value. This threshold value compares with the component's weight value.

Step 4. In this step we identify the pixels that are in front, meaning find foreground pixels. This foreground pixel is compared with background pixels and no matching is found between foregrounds and background pixels.

The Gaussian mixture model is calculated from each pixel and that calculated part is placed in the frame. Let x be the value of a pixel point that represents a randomly generated pixel in a time. In the Gaussian mixture model the probability density function $p(x)$, i.e., is defined by

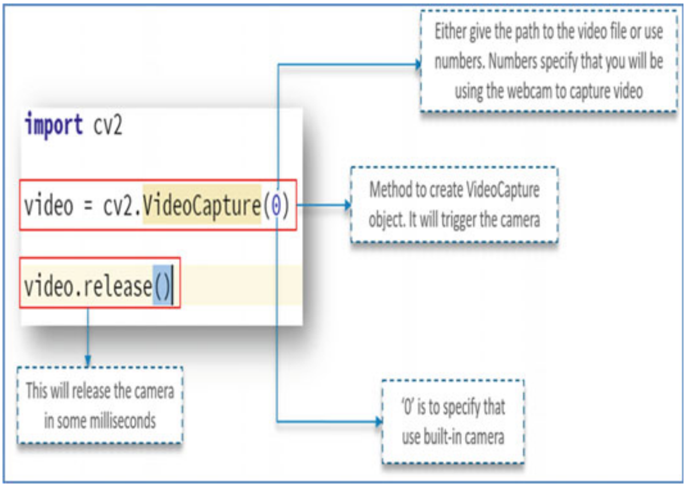
$$\sum w_i ND(x : m_i,\ \sigma_i), \quad i = 1 \text{ to } n \tag{1}$$

where i component densities, w_i weight, and ND (x:μ_k, σ_k) normal density of mean mi and covariance matrix $\Sigma i = \sigma_i I$ (I denotes identity matrix). Detection works on the classifier. Classifier is an algorithm that decides this object, and this classifier is already in use in OpenCV. OpenCV uses two types of classifiers: LBP (Local Binary Pattern) and Haar Cascades [14].

At the very first stage we take or input two images from the camera, hence two frames are read by the camera at once. We use cv2.imread() function to do so. After capturing the two images from the camera we take the difference between these two frames using cv2.absdiff() function. Now it's time to find contours on the real frame obtained by the difference between the two frames. After finding the contours we use draw contours () to draw the contours over the boundaries of the frame.

According to Fig. 4, we found that these are completed using some steps as follows:

1. When using this concept first we needed library of OpenCV.
2. By using the library implement video capture methods. This method is called for generating video object; start the camera. While find the object and that is check out inbuilt or not in user machine, for checking camera on user machine this is generate 0 or 1. If the method generates 0 it means the camera is integrated into the machine, otherwise not integrated.



```
import cv2

video = cv2.VideoCapture(0)

video.release()
```

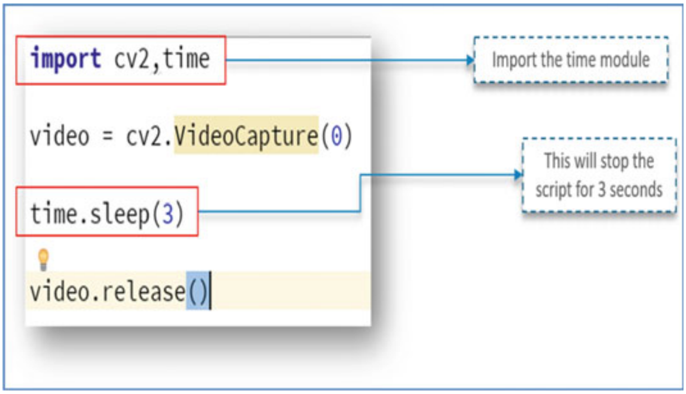
Either give the path to the video file or use numbers. Numbers specify that you will be using the webcam to capture video

Method to create VideoCapture object. It will trigger the camera

This will release the camera in some milliseconds

'0' is to specify that use built-in camera

Fig. 4 Process of image capture



```
import cv2,time

video = cv2.VideoCapture(0)

time.sleep(3)

video.release()
```

Fig. 5 Process of finding a gap between two frames

3. In the library using a release method terminates the video capture machine for a very short duration of more than microseconds. By observing the camera light on and off duration make some differences that are switched on in second but off later. This occurred because between on/off no delay, so keep some delay between on/off.
4. For making a gap between them use a library function, that is the sleep method. By using this method stop script for sleep duration time, as it is shown here above 3 s, the camera will be working for 3 s.

In case of finding a gap between the frames, use a different library function that is absolutely different. Absolute difference function finds a gap between first and other frames (Fig. 5).

3.2 Object Tracking

Simply, tracking is locating an object in frames of video [15]. After tracking the object, detection of the object is done. The link between the frames is facing problem; that problem arises when setting the object in frames. So avoid these problems by assigning an identification number of every object. Because it is necessary that after tracking object further activity identity will be more important. So achieve that activity using the filtration technique.

The filtration technique works on iteration at the iterative stage and is divided into two steps: one is forecast and the next renewal step in this filtration technique is called Kalman filtering [16]. In forecast steps observe the current location of the moving object based on the previous point or location. So let any object that is moving but their movement is in fixed means same speed, then we can forecast the current location and renew again the location of the object and this phenomenon will continue until all pixels will be filtered.

4 Result Analysis

Through computer vision many article works are going on using OpenCV. Machines do work on detecting object through pixels of objects and classify object according object location and movement of object. So while detecting real-time object images, use frames that contain images pixels and that frames make the connection between successive frames, every frame is checked by independently, and then co-relate to each other.

For example, let us track the movement of the object as cars and then frames evaluate its current movement or velocity and forecast its location in the upcoming frame. Like here we find in Fig. 6 when the object is placed in front of webcam. Then frames capture the image pixels and forecast the image that shows moving object or not. When the object is placed find not only the foreground object while some pixels of the background also show in the frame.

In Fig. 7 we saw that when the object is placed in front of webcam, the frames capture the image pixels and forecast the image that shows that moving object or not. When the object is placed find the foreground object that is focused and some background pixels [17] also. But when the object is moving here to there then find the exact object and track this object from their previous location to current location and fit it to in a frame and detect the object.

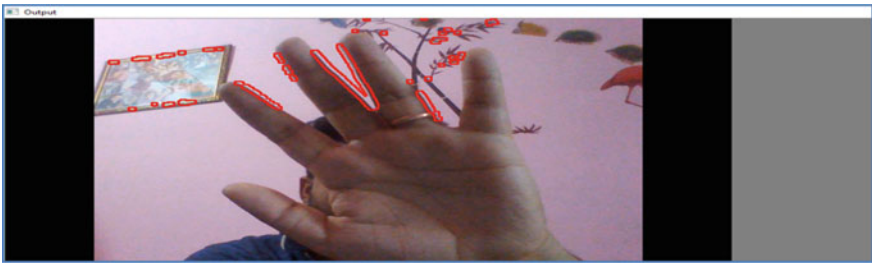


Fig. 6 Foreground background image frame

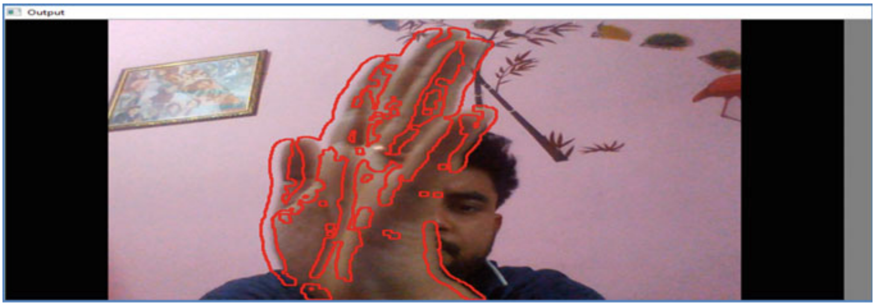


Fig. 7 Foreground image frame

4.1 Security and Video Image

In OpenCV we can use video image in different areas for different purposes, as a security point of view using OpenCV makes vision-based real-time application for indoor security as home security and outdoor security as street security from a suspected object. Let an accident occur in street by vehicle and the scenario is captured in street surveillance video camera. We want to see that incident and then detect and track the person with the vehicle in real time except looking at all videos. Capture a prominent or important portion of video automatically, which is called video summarization, using OpenCV with deep learning. In this video summarization approach one works for vision and the other works for automatic training of the system. So by this the motion detection and security system are improved. Many systems use sensors for detecting motion but the detection rate is low compared to vision-based system. So we use this vision-based system to improve the performance and security of video image, where security image prospects focus on the suspected object.

5 Conclusion

This paper is based on the image processing library of python used in machine learning. The future scope of AI and machine learning is going to be very tremendous in IT sector. Image processing is still used in applications like Facebook, Twitter, cab driver blinks eyes more than 3 s [18], and when we tag someone. Giving a vision to the machines is one of the great achievements in machine learning field.

OpenCV can also be used to detect and track the path in self-driving cars, which is the greatest advancement in AI. Machine learning is nothing but teaching intelligence to machines so that they can learn on their own without being explicitly programmed. The advancement in machine learning is as such that 80% of development in IT sectors depends on AI and machine learning.

References

1. M. Kirby, L. Sirovich, Application of the Karhunen-Loeve procedure for the characterization of human faces. IEEE Trans. Pattern Anal. Mach. Intell. **12**(1), 103–108 (1990)
2. L.J. Latecki, V. Rajagopal, A. Gross, *Image retrieval and reversible illumination normalization. Internet Imaging VI*, vol. 5670 (International Society for Optics and Photonics, 2005)
3. K. Goyal, A. Kartikey, K. Rishi, Face detection and tracking: using OpenCV, in *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, vol. 1 (IEEE, 2017)
4. G. Bradski, A. Kaehler, *Learning OpenCV computer vision with the OpenCV library.* (O'Reilly Media, Inc., 2008).

5. N. Saini, S. Kaur, H. Singh, A review: face detection methods and algorithms. Int. J. Eng. Res. Technol. (IJERT) **2**(Issue 6) (2013). ISSN: 2278-0181. www.ijert.org
6. D.J. Robertson, R.S.S. Kramer, A. Mike Burton, Face averages enhance user recognition for smartphone security. Plos One **10.3**, e0119460 (2015)
7. S. Tripathi, V. Sharma, S. Sharma, Face detection using combined skin color detector and template matching method. Int. J. Comput. Appl. **26**(7) (2011)
8. H. Makwana, T. Singh, Comparison of different algorithm for face recognition. Glob. J. Comput. Sci. Technol. (2014)
9. N. Rani et al., Analyzing the performance of image segmentation using its efficient architecture. (2007)
10. P. Spagnolo, M. Leo, A. Distante, Moving object segmentation by background subtraction and temporal analysis. Image Vis. Comput. **24**(5), 411–423 (2006)
11. P.W. Power, J.A. Schoonees, Understanding background mixture models for foreground segmentation, in *Proceedings Image and Vision Computing New Zealand*. (2002)
12. P. Viola, M.J. Jones, Robust real-time face detection. Int. J. Comput. Vis. **57**(2), 137–154 (2004)
13. A.K. Chauhan, P. Krishan, Moving object tracking using gaussian mixture model and optical flow. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **3**(4), 243–246 (2013)
14. D.-S. Chen, Z.-K. Liu, Generalized Haar-like features for fast face detection, in *2007 International Conference on Machine Learning and Cybernetics*, vol. 4 (IEEE, 2007)
15. K. Meenatchi, P. Subhashini, Multiple object tracking and segmentation in video sequences. Int. J. **2**(5), 71–79 (2014)
16. V. Naidu, J. Raol, Object tracking using image registration and Kalman filter, in *International Conference on Avionics Systems*. (2008)
17. A. Tiwari, J. Verma, Scene understanding using back propagation by neural network. (2011)
18. M.S. Kalas, Real time face detection and tracking using OpenCV. Int. J. Soft Comput. Artif. Intell. **2**(1), 41–44 (2014)