CRITERIA III: RESEARCH, INNOVATION AND EXTENSION

3.2.1: NUMBER OF PAPERS PUBLISHED PER TEACHER IN THE JOURNALS NOTIFIED ON UGC WEBSITE

DATA COLLECTION YEAR FOR ASSESSMENT

2020-21

Emotional Intelligence as a mediating variable in the impact of Leadership on Organizational Commitment

Ms Suchitra Srivastava,
Faculty, Jagannath International Management School,
Vasant Kunj, New Delhi
suchitra.srivastava@yahoo.co.in

Dr Sandhya Sinha,
Faculty, Maharishi University of Information and Technology,
IIM Road, Lucknow
sandhyasinha.mgmt@gmail.com

Abstract:

The role and impact of leaders has intrigued scholars since time immemorial. Different leadership theories have been proposed since the early twentieth century with the behavioral theory, trait theory, contingency theory etc. The construct emotional intelligence that gained popularity with the works of Goleman during the 1990s provides a sound basis of effective social interactions both at work and otherwise. In the organizational setup, a higher level of emotional intelligence is believed to facilitate social interactions in the work environment, thereby providing a higher motivation to perform the duties at the job willingly and with utmost dedication. This is turn is bound to result in higher productivity and efficiency which would benefit both the individual and the organization. This would lead to higher levels of identification of the employees with the organization and thereby higher organizational commitment.

Numerous studies have been carried out to study the relationship between leadership and constructs such as organizational culture, behaviour, performance, change and commitment. Leaders who possess high EI may be expected to steer the employees towards the achievement of organizational goals more effectively. The present study examines the mediating role of emotional intelligence in analyzing the impact of leadership on organizational commitment. It is an empirical work and attempts to construct a conceptual model for further testing and validation. Additionally the paper reviews different leadership theories, theories of emotional intelligence and also highlights the elements of organizational commitment.

Key words: emotional intelligence, leadership, organizational commitment, satisfaction, productivity

AI INITIATIVES BY INDIAN GOVERNMENT: JOURNEY TOWARDS BECOMING GLOBAL TECHNOLOGY LEADER

Poonam Malik[1], Dr. kavita[2], Dr. Kusum Singal[3]

[1]Jagannath International Management School, VasantKunj, New Delhi, India
[2]Jyoti Vidyapeeth University, Jaipur, India
[3]AIIMS, New Delhi, India

Email id- [1]poonamdhillon_444@yahoo.co.in, [2]kavita.yogen@gmail.com, [3]kusumsingal731@gmail.com

Received: May 2020 Revised and Accepted: August 2020

ABSTRACT: India has realized the importance of AI for its economic growth and is moving towards its way to become the Global leader in the new emerging technologies of AI. In June 2020, India launched an AI portal “indiaai.in” where Government, startups, academic learners can come together and synchronize their effort for the growth of AI in India. The government has also framed an architecture to develop a cloud computing infrastructure to support facilities for AI named as AIRAWAT. Both the initiatives are great efforts of Indian Government towards establishing India as an AI enabled country in the world. With the latest AI initiatives being taken by the Indian government, now India has the biggest opportunity to fully reap the benefits of AI as a problem solver for its Healthcare, industry, education, infrastructure, public dealing, policy and regulation making, transportation and technology development sectors. This research paper discuss the latest trends in AI, role of AI Chatbots, which come as helping tool for Public Service Delivery in different areas, AI Startups in India, National AI Strategy, AI Portal of India, AIRAWAT-AI Cloud Infrastructure , AI initiatives by Central and State Government of India. “Ethics in AI” is also being discussed in this paper as it is a major issue of concern since the technology is going to be utilized in every field and it is on the way to be implemented across the world.

KEYWORDS: Artificial Intelligence, National AI Strategy, AI Startups, Indian AI portal, AIRAWAT, AI initiatives by central and state Government of India, upcoming trends in AI, Ethics in AI

I. INTRODUCTION

AI is the field where human intelligence is simulated through digital technology/machines by developing algorithms to make machines learn, imitate, act, interpret, analyze, recognize to work towards problem solving. Robotics, ML, deep learning, NLP, NLG, visual recognition, OCR are the subsystems which are working together to represent the broad term of AI [1].

With focus on AI research, India must work to solve the Indian specific problems like Indian language character recognition, multilingual text use in one sentence, proper image recognition of roads, soil and weather data from agriculture perspective etc. Along with that, India also faces other challenges like less number of students in the AI/ML research area, limited infrastructure and resources compatible with emerging technologies, approach towards research in India, non-availability of organized data sets [2]. The AI solutions developed specifically for Indian problems may also be beneficial for other countries because these solutions would be used and tested for more critical conditions in a highly populated, multilingual, monetary diverse country like India. AI technology would be adopted by India in the field of healthcare, education, cyber security, law, finance, transport, virtual assistance, e-commerce, customer care, energy, business strategy and many more.

If India wants its position among the AI global leaders of the world, then it must think of ways to capitalize upon its large internet savvy population which can act as an asset. It needs to be ensured that the AI technologies complement and augment this large workforce rather than making it jobless. Also, India has a huge amount of data with a lot of variety due to its diverse population, which need to be qualitative and correct for its AI infrastructure to be robust [3].
The union budget 2020 of government has tried to give required impetus to the emerging technologies including ML, IOT, AI, and Big Data. To enhance the level of digital penetration, a drive has been launched to digitize

Dimensions and Consequences of Cause Related Marketing: A Conceptual Framework

Marketer these days are expected to satisfy all stakeholder and the most important stakeholder is general public, that exist in the society. Companies across the world are engaging in philanthropic strategies like Cause Related Marketing (CRM) in which company agrees to contribute fixed amount towards selected social cause for each unit sold. This paper undertakes methodical analysis of prevailing work for better understanding and recording of the dimensions impacting CRM strategy and it possible consequences. This researcher deliberate on variables, that have not be studied together before. For better understanding and execution, dimensions of CRM, have been categorized into Consumer specific and Company specific. This study aims to propose an integrated conceptual framework of interrelationships of variables that have potential to mitigate the impending problems of organization. Finally, it suggests that relationship exists amid the dimensions and consequences of CRM. This study will have social, managerial and academic implications.

Keywords: *Corporate Social Responsibility, Cause Related Marketing, Consumer Behavior, Consumer Attitude, Brand Credibility.*

Anu Bhardwaj
Assistant Professor,
Jagannath International
Management School, Vasant Kunj.

Bilal Mustafa Khan
Professor,
Aligarh Muslim University (AMU).

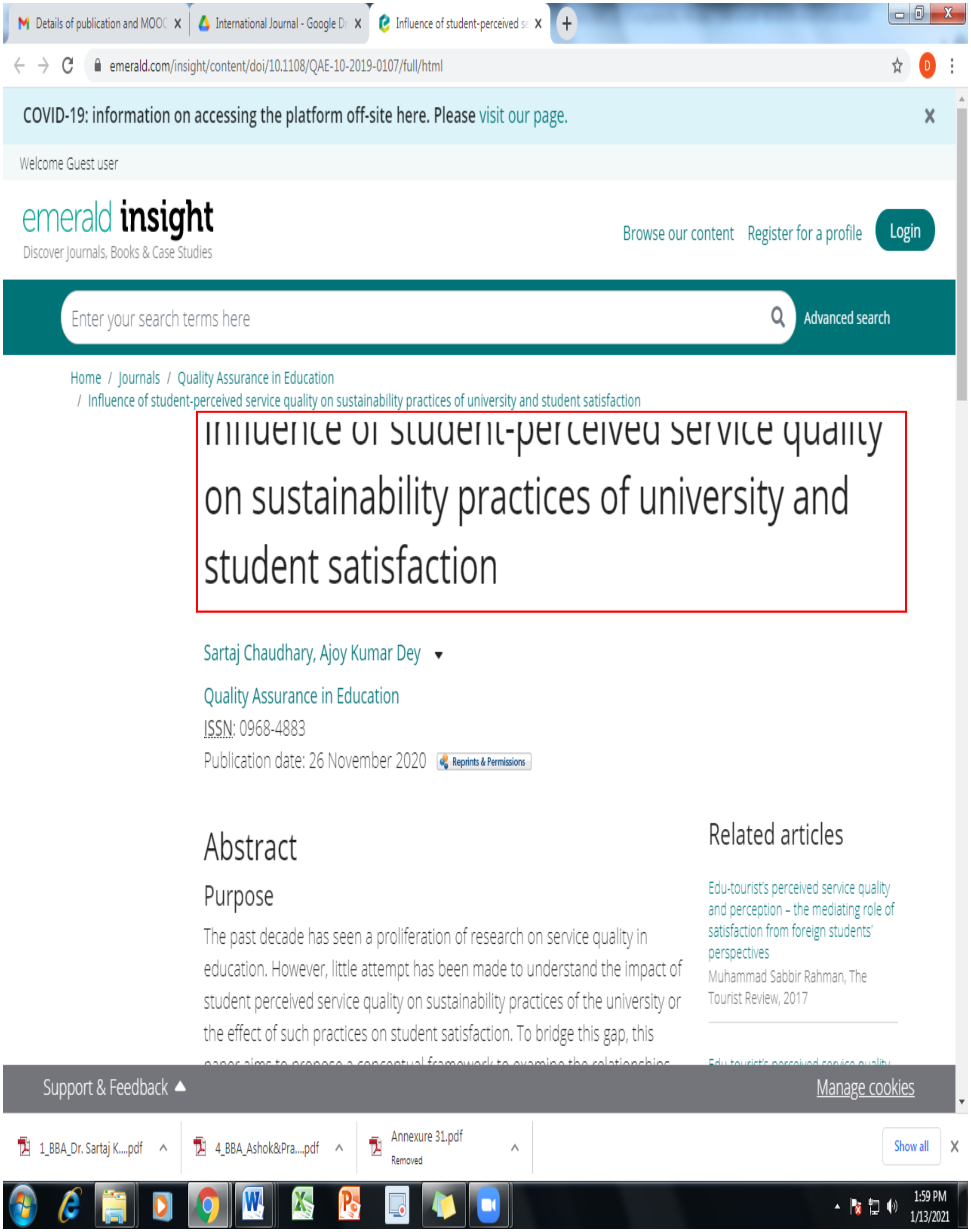
Vikas Nath
Director,
Bharati Vidyapeeth Institute of
Management and Research,
New Delhi.

Introduction

In today's competitive scenario sustainability is a subject of concern. Organisations should make their offering different as basic attributes of marketing are not enough. Connecting the brand with philanthropy is effective differentiation strategy (Carringer, 1994). Cause Related Marketing (CRM), is manifestation of CSR, where organizations corroborate with non-profit organizations for mutually beneficial relationships and predefined share of every purchase is contributed to social cause. This relationship between company and cause and attaching the sales with contribution for charity, is known as Cause Related Marketing (CRM). Companies in India are implementing CRM strategy that benefits both parties (Aggarwal and Singh, 2019) and is an impressive way through which it conveys a message that is distinctive and well-targeted (Carringer, 1994).

Recent studies have emphasized the influence of CRM strategy in improving awareness of a brand (Varadarajan & Menon, 1988), enhancing attitude (Barone, et.al., 2007), refining image and increasing purchase intentions (Chaudhary, 2018). CRM influences attitude, improves brand reputation, creates differentiation, improves credibility and create brand attractiveness. CRM is an upcoming marketing strategy and the research in this area is scant especially in developing country like India. Literature

Paper received on July 9, 2019 Revised paper received on September 7, 2019 Paper accepted on October 11, 2019


Details of publication and MOOC
International Journal - Google Dr
Influence of student-perceived se
emerald.com/insight/content/doi/10.1108/QAE-10-2019-0107/full/html
D
Welcome Guest user
emerald insight
Discover Journals, Books & Case Studies
Browse our content
Register for a profile
Login
Enter your search terms here
Advanced search
Reprints & Permissions
Support & Feedback
Manage cookies
1_BBA_Dr. Sartaj K....pdf
4_BBA_Ashok&Pra....pdf
Annexure 31.pdf
Removed
Show all
1:59 PM
1/13/2021

COVID-19: information on accessing the platform off-site here. Please visit our page.

Home / Journals / Quality Assurance in Education / Influence of student-perceived service quality on sustainability practices of university and student satisfaction

Influence of student-perceived service quality on sustainability practices of university and student satisfaction

Sartaj Chaudhary, Ajoy Kumar Dey

Quality Assurance in Education

ISSN: 0968-4883

Publication date: 26 November 2020

Abstract

Purpose

The past decade has seen a proliferation of research on service quality in education. However, little attempt has been made to understand the impact of student perceived service quality on sustainability practices of the university or the effect of such practices on student satisfaction. To bridge this gap, this paper aims to propose a conceptual framework to examine the relationships

Related articles

Edu-tourist's perceived service quality and perception – the mediating role of satisfaction from foreign students' perspectives

Muhammad Sabbir Rahman, The Tourist Review, 2017

Edu-tourist's perceived service quality

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:07:2021
DOI 10.17605/OSF.IO/EKSG8

AN INVESTIGATION INTO THE RELATIONSHIP BETWEEN MULTIDIMENSIONAL SELF CONCEPT AND INTERPERSONAL RELATIONSHIP: A CASE OF BUDDING MANAGERS IN DELHI AND NCR

Anju Shukla,
Assistant Professor, Jagannath International Management School, Kalkaji, New Delhi.
Brijesh Singh,
Research scholar from VTU, Belagavi & Associate Professor, Department of MBA, SJB Institute of Technology, Bangalore.
Meenakshi Chopra,
Assistant Professor, Jagannath International Management School, Vasant Kunj, New Delhi.

Abstract

The research aims at finding out the relationship between Self Concept from multidimensional perspective and Interpersonal relationship amongst a selected group of management students from Delhi and NCR. The relationship also aimed at a wholesome exploration taking into consideration the gender differences, age dimension , family type and educational background. An empirical investigation was carried out involving 720 management students from private B - Schools . Data was obtained with the help of standardized questionnaires, and analyzed through SPSS. The results showed that there is a significant association between Multidimensional Self Concept and Interpersonal Relationship of participants, also there is a significant association between Multidimensional Self Concept and Interpersonal Relation Orientation of various demographic factors into consideration.

Keywords: Self Concept, Interpersonal Relations, Management students, Delhi

Introduction

Never think that you're not good enough yourself. A man should never think that. People will take you very much at your own reckoning. *Anthony Trollope*****

A study published in 1918 by Carnegie Foundation, now more than 100 years old, which was authored by Charles Riborg had the mention of the importance of soft skills. From then till now in 2021, various organizations like Harvard, Stanford Research Center and Carnegie Foundation have time and again proved from their research the importance of soft skills. In fact the researchers have stated that its importance is so much so that 85% of the success for an individual comes from good soft skills and people skills.

The Self Concept of an individual has been seen from different perspectives, but one view which all theorists and practitioners agree upon is that it is the view one has for

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
E-Publication: Online Open Access
Vol:54 Issue:07:2021
DOI 10.17605/OSF.IO/WTBY9

WOMEN ENTREPRENEURS:

SOFT SKILLS AND STRESS MANAGEMENT AT THE WORKPLACE

Brijesh Singh
Research Scholar, VTU, Belagavi & Associate Professor, Department of MBA, SJB Institute of Technology, Bangalore.
Anju Shukla
Assistant Professor, Jagannath International Management School, Kalkaji, New Delhi.
Meenakshi Chopra
Assistant Professor, Jagannath International Management School, Vasant Kunj, New Delhi.
Rekha Gupta
Assistant Professor, Department of Commerce, Government General Zorawar Singh Memorial Degree College, Reasi.

Abstract- In the current situation where technology is dominating the current market and making the things more convenient and easy for most of the people. By considering the current scenario with the help of technology and globalization on par with women empowerment has made the global business highly challenging and competitive. Women have evolved in to potential leaders and proved to be strong competitors not only at the home front but also at the international front. In this highly competitive and challenging working ambience, developing soft skills is vital in curbing stress and other issues related to the impact of stress. As such, most of the organizations are opting for a stress free ambience as Human Resource is a vital vein breathing productivity and profits for the business enterprises. This is not just for the economic empowerment of the enterprise alone but also to that of individuals working in that and also to the benefit of the society and Nation. Women constitute major workforce contributing to the economic empowerment of the business enterprise, family, society and Nation to a larger extent. Women entrepreneurs are prone to stress as they have the obligation to manage both household decisions and workplace decisions. Soft skills training and development at the work place aids in maintaining congenial and stress free working environment. This helps women in boosting their confidence and also to handle various situations not only at the home front and at the workplace but in any given situation. Thus, the paper is an attempt to study the profile of 50 women entrepreneurs in relation to soft skills training and stress management at the workplace, its issues and challenges. Convenience sampling method is taken in to consideration.

Keywords: Women Entrepreneurs, Soft skills, Stress Management, Issues and Challenges.

COVID -19 Pandemic Outbreak and its Impact on Bombay Stock Exchange Indices: An Empirical Analysis

Himani Gupta

Jagannath International Management School, Vasant Kunj, New Delhi

Email: himanigupta8476@gmail.com

Manisha Gupta

School of Business Studies, Sharda University, Greater Noida

Anu Bhardwaj

Jagannath International Management School, Vasant Kunj, New Delhi

Trupti Rakesh Bhosale

Symbiosis School of Banking and Finance
Symbosis International (Deemed University)

Mohd Athar

Research Scholar, University of Hyderabad

Abstract: This COVID 19 pandemic has affected the world's economies, and India; nonetheless, little endeavour has been had to comprehend the impact of COVID 19 pandemic on the Bombay Stock Exchange (BSE) indices. This paper analyses the impact of this pandemic on returns of selected BSE indices in pre-pandemic and during pandemic. Data were collected from selected five sector indices through official website of Bombay Stock Exchange and the study adopted Kolmogorov-Smirnov Test and Student paired t-test. Kolmogorov-Smirnov test is adopted to check the normality of the selected sample and t-test is adopted to verify the effect of COVID on the returns of selected sampled BSE indices. Results revealed that COVID 19 had no impact on the sampled BSE indices. The price of BSE indices is moving at its own pace. If we look at today's scenario BSE indices are doing quite well. Result may guide the key decision-makers such as investors and speculators in the financial market to invest in the stock indices. It would also help the policy makers to understand fluctuations in financial market and take necessary decisions. This study is the first of its sort to inspect the effect of this deadly coronavirus pandemic on Bombay Stock Exchange indices.

Keywords: India, Bombay Stock Exchange, Global Crisis, COVID -19 Pandemic, Kolmogorov-Smirnov Test, Student paired t-test

1. Introduction

The present reality is seeing a worldwide pandemic because of the Coronavirus episode. Each living being is taking a stab at its own level to adapt up to the present circumstance,

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Circular route to the management of solid waste: A case study of EcoSage Enviro

Hari Shankar Shyam [a], Manisha Gupta [a,*], Himani Gupta [b]

[a] *School of Business Studies, Sharda University, India*
[b] *Jagannath International management School, Vasant Kunj, India*

ARTICLE INFO

Article history:
Received 7 August 2021
Accepted 26 August 2021
Available online xxxx

Keywords:
Circular supply chain
Waste management
Sustainable Development
EcoSage Enviro

ABSTRACT

These days, circular supply chain management has taken on a new level of meaning as environmental practises are incorporated into diverse supply chains. Environmental issues have gained increased importance within supply chain management, and it is necessary that each step in the supply chain management process be integrated with environmental consciousness. Solid waste management firms like EcoSage Enviro and others that include circularity in their services are inspiring interest, adoption, and replication of circular supply chain in waste management. ECOSAGE ENVIRO Waste Initiative's circular supply chain concept and its services related to waste management are good models for private–pub lic-partnerships to follow when it comes to waste management in Himalayan region of country India.

Selection and peer-review under responsibility of the scientific committee of the National Conference on Functional Materials: Emerging Technologies and Applications in Materials Science

1. Introduction

As the emphasis society places on greenhouse gas (GHG) emission reduction and better environmental stewardship grows, the number of consumers choosing to purchase climate-friendly products and manufacturing methods has also risen. In addition, a higher understanding of the consequences of climate change and environmental sustainability has emerged in the world. Awareness of personal and public health in relation to things that we consume is also influenced by society's consciousness of personal and public health. Furthermore, SDG 12 – sustainable consumption and production increases awareness. People are more concerned about environmental issues, which makes them want to know about the integrity of the things they buy. Additionally, we query the carbon footprints of producers, the ways in which they recycle, and their overall environmental impact. An impact on the environment can be found in several supply activities. Packaging and other recyclable materials end up in landfills or go into the environment when they are disposed. All of these discarded materials increase carbon monoxide emissions and pollution levels [1]. If you're manufacturing or ecological service has nothing to do with the protection of the earth's resources along their supply chain, you will not be able to exist in either worldwide or local markets. Companies are likely to transform their environmental and supply chain models as a result of rising environmental issues owing to products. Thus, circular supply chain management could not exist without extending companies' environmental operations to embrace the complete supply chain. While extending firms' environmental actions to embrace the entire supply chain has pushed for the creation of the circular supply chain idea, it is acceptable to argue that the requirement is the main driver of this [2].

Circular supply chain management is a fancy way of saying supply chain management with an environmental outlook. It can be considered an environmental innovation (in the broader sense) [3]. The main objective of the ultimate initiative is to cut costs by reducing all types of waste, including hazardous chemical, emissions, energy, and solid waste, in the supply chain, including the development of new products, the sourcing of materials, the manufacturing process, the delivery of final products, and the disposal of the products at the end of their useful life [4]. Moreover, because environmental management practises have become a multi-disciplinary concept by establishing supply chain environmental practises in many contexts, whether they provide environmental services or not. Also, circular supply chain is important in helping companies affect the whole environmental effect of their supply chain activities, with this resulting in an improvement in

* Corresponding author at: School of Business Studies, Sharda University, Greater Noida

E-mail address: guptaamanisha@gmail.com (M. Gupta).

https://doi.org/10.1016/j.matpr.2021.08.259
2214-7853/
Selection and peer-review under responsibility of the scientific committee of the National Conference on Functional Materials: Emerging Technologies and Applications in Materials Science

Journal of Information & Optimization Sciences

Taylor & Francis
Taylor & Francis Group

Journal of Information and Optimization Sciences

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tios20

Comparative study on web-based and cloud-based application

Anisha Tandon , Mamta Madan & Meenu Dave

To cite this article: Anisha Tandon , Mamta Madan & Meenu Dave (2020): Comparative study on web-based and cloud-based application, Journal of Information and Optimization Sciences, DOI: 10.1080/02522667.2020.1802127

To link to this article: https://doi.org/10.1080/02522667.2020.1802127

Published online: 14 Aug 2020.

Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
DOI : 10.1080/02522667.2020.1802127

Comparative study on web-based and cloud-based application

Anisha Tandon *
Department of Engineering and Technology
Jagannath University
Jaipur 302022
Rajasthan
India

and

Department of Information Technology
Jagannath International Management School
Vasant Kunj 10070
Delhi
India

Mamta Madan [†]
Department of Engineering & Technology
Vivekananda Institute of Professional Studies
Pitampura
New Delhi 110034
India

Meenu Dave [§]
Department of Engineering and Technology
Jagannath University
Jaipur 302022
Rajasthan
India

*E-mail: 84.anisha@gmail.com (Corresponding Author)
[†]E-mail: mamta.vips@gmail.com
[§]E-mail: meenu.s.dave@gmail.com

Abstract

Software Testing is a demanding activity for several software engineering projects and is one of the prime technical part of the software engineering cycle that still contains considerable challenges. Testing software requires enough resources and budget to complete it successfully. This paper proposed a Traceability Matrix for Web-based and Cloud-based Applications. This research introduced a new matrix that contains features of both Traceability and Test Coverage Matrix and after the development of that Matrix, the same is first implemented in the web-based application and then further enhancement of the same is implemented in a cloud-based application. This research paper also presented a comparative study on Web-based and Cloud-based Applications.

Subject Classification: *68U01.*

Keywords: *RTM, WPS, EDP, HSM, Test Case, Test Coverage.*

1. Introduction

RTM stands for Requirement Traceability Matrix. RTM assemble [1] all necessities through users or market research at the beginning of any project development [2]. It is used to associate and track requirements against TCs generally with the requirement as well as test IDs [3] [4]. The prime goal is to inspect the test cases so that no functionality should be missed while testing [5]. This research paper having the following divisions: Section 1 discussed about RTM. Section 2 presents an RTM for Web-based Application. Section 3 proposed an RTM for Cloud-based Application. Section 4 contains a comparative view of Web and Cloud-based Application.

2. Research Questions

To fulfil this research, the following questions must be answered:

RQ1 : How to present an RTM for Web as well as Cloud-based Application

RQ2 : How to implement RTM for Web and Cloud Application as there is no predefined template and set of rules for creating the same

RQ3 : How to calculate the test coverage and defect leakage of Web and Cloud Matrix

RQ4 : How to perform a comparison study on Web and Cloud.

The research questions deliverables are:

D1 : Introduction of RTM based on Web and Cloud-based Application

D2 : Implementation of RTM for Web and Cloud-based Application

D3 : Calculation of the test coverage and defect leakage of Web-based and Cloud-based RTM

D4 : The comparison results of Web and Cloud-based Application

3. Related Work

The literature study shows that there was no standardized format is followed to design RTM. This section demonstrates the fundamentals of the research done by numerous researchers for creating RTM in the domain of Web-based Applications as well as Cloud-based Applications. The following provides an overview of some related studies that have challenged while creating RTM and for calculating the test coverage of the same.

Anupama Saswihalli, Shilpa Kongi [6] discussed the usage of RTM, which is required for the higher quality of any web-based project. This paper discussed the importance of Requirement Traceability Matrix (RTM) which is most essential and required to check opposed the SRS by the client or end-user. They also discussed the types of Traceability Test Matrix and the benefits of using the same. However, in this paper, they have not defined how to calculate the test coverage. Even, the RTM defined by them was not standardized.

Falak and Mohammad Suaib [7] described the related terms, techniques, problem associated with traceability. In this paper, various research papers are discussed based on the effectiveness of traceability and with much research and detailed analysis of some techniques. While most of the ideas mentioned followed the manual approach but it was realized that some realistic approach can provide some better solution and can be further enhanced.

Muhammad Shahid *et.al.* [8] provided a study on recent test coverage researches done by various researchers to find the test coverage. The paper has shown various areas of research to calculate the Test Coverage. In this paper, other important factors like defect leakage, execution coverage is not calculated.

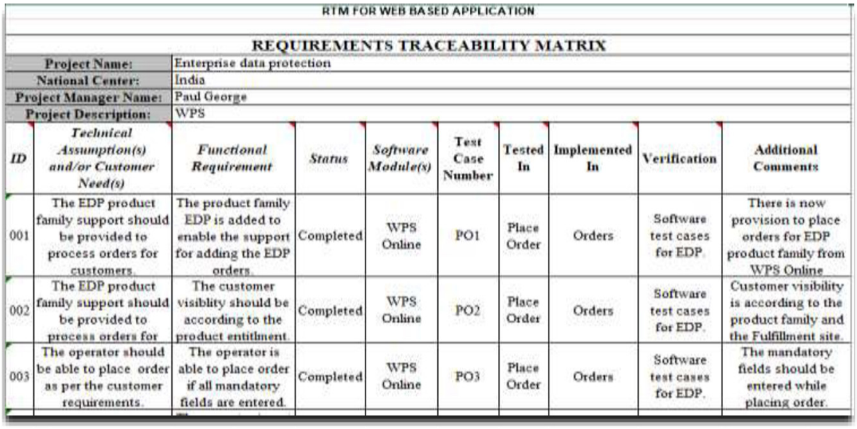
Vijay Pratap Katiyar [9] explores and reanalysis the process of bug LC and debated the process of how to remove the bug. He proposed the bug report template that must be created by QA engineer and elucidated the numerous steps to evade the same. He also discussed the test case template. This paper does not contain any technique or method for finding Test Coverage in software testing.

Richard Torkar *et.al.* [10] analyzed requirements traceability challenges, techniques and tools. They proposed a number of common definitions, available tools, challenges, and techniques while complementing the results and analysis.

Almost all papers implemented RTM for any legacy application. The study included the implementation of the matrix proposed for Web and Cloud Application and to discuss the comparative results between both of them.

4. RTM for Web-based Application

RTM include [11] all requirement at the beginning and end of each stage and assures that each requirement will be delivered to the end-users [12] [13]. In this paper, we have proposed a matrix for the web application, called Worldwide Programming System (WPS). The WPS maintains the EDP boxes license, cluster, features and all other customers relevant information with them. The EDP devices (Popularly known as HSM boxes) encrypt the important end-user information in the banking domain and provide the key encoding/Encryption for the critical card info and other banking-related transactions are done by the end-users on a banking site or ATM's. Hardware Security Module (HSM) is the hardware devices used by various financial institutions such as banks to safeguard customer sensitive data. The RTM [14] contains all the requirements that are must to be a part new application and must be included in the WPS application [15] so that WPS can support all the current and upcoming support of



RTM FOR WEB BASED APPLICATION

REQUIREMENTS TRACEABILITY MATRIX

Project Name:	Enterprise data protection
National Center:	India
Project Manager Name:	Paul George
Project Description:	WPS

ID	*Technical Assumption(s) and/or Customer Need(s)*	*Functional Requirement*	*Status*	*Software Module(s)*	**Test Case Number**	**Tested In**	**Implemented In**	**Verification**	**Additional Comments**
001	The EDP product family support should be provided to process orders for customers.	The product family EDP is added to enable the support for adding the EDP orders.	Completed	WPS Online	PO1	Place Order	Orders	Software test cases for EDP.	There is now provision to place orders for EDP product family from WPS Online
002	The EDP product family support should be provided to process orders for	The customer visiblity should be according to the product entitlment.	Completed	WPS Online	PO2	Place Order	Orders	Software test cases for EDP.	Customer visibility is according to the product family and the Fulfillment site.
003	The operator should be able to place order as per the customer requirements.	The operator is able to place order if all mandatory fields are entered.	Completed	WPS Online	PO3	Place Order	Orders	Software test cases for EDP.	The mandatory fields should be entered while placing order.

Figure 1

Screenshot of WPS Matrix

EDP [16] [20]. The following figure 1 depicts the screenshot of the RTM for Worldwide Programming System i.e. "WPS", a web-based Application.

Calculation of Test Coverage of the RTM for WPS are as follows:

Table 1 shows the Test coverage of the WPS matrix, which is as follows:

Table 1

Test Coverage of RTM for Web Application, WPS

Actual "executed" Test cases	Actual "planned" Test cases	Results of Test coverage
54	60	90 %

So, Test coverage [17] of the matrix is calculated here to find the actual test coverage [18] of the matrix [8]. The pie chart of Table 1 is depicted in Figure 2, which is as follows:

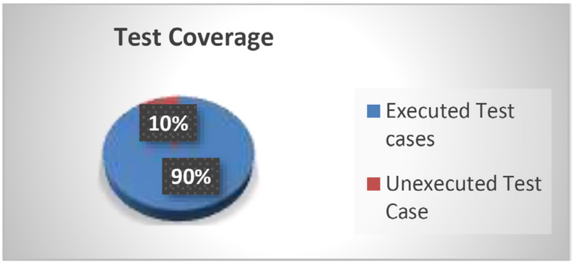


Figure 2

Test Coverage of Web-based Application

Calculation of Passed and Failed Test Case Coverage of WPS RTM as follows:

Passed Test Case Coverage= (Actual no. of passed Test/Actual Test case executed) * 100

Failed Test Case Coverage= (Actual no. of Failed Test/Actual Test case executed) * 100

The Passed and Failed Test Coverage of the WPS RTM are calculated in Table 2 and Table 3. Table 2 depicts Passed Test Coverage, which is as follows:

Table 2

Calculation of Passed Test Case Coverage of WPS RTM

Actual no. of Passed Test	Actual "executed" Test case	Passed Test Case Coverage
50	54	92.5%

Table 3 depicts Failed Test Coverage, which is as follows:

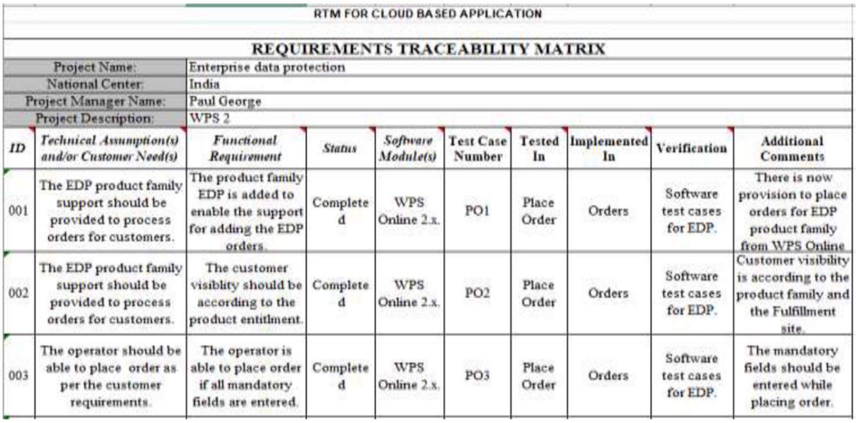
Table 3

Calculation of Failed Test Case Coverage of WPS RTM

Actual no. of Failed Test	**Actual "executed" Test case**	**Failed Test Case Coverage**
4	54	7.4%

5. RTM for Cloud-based Application

Our proposed Matrix is based on Cloud-based Application [19]. As there were very fewer features in the WPS, a Web Application [20] [21], the new Application is created in the Cloud [22] and its look and feel are better than the Web-based Application [23] [24]. This paper proposed an RTM for WPS 2, a Cloud-based Application [25] [26]. The screenshot of the RTM for WPS 2, a cloud-based Application is depicted in Figure 3. WPS 2 is the version of WPS that support HSM and migrated to cloud [27].



RTM FOR CLOUD BASED APPLICATION

REQUIREMENTS TRACEABILITY MATRIX

Project Name:	Enterprise data protection
National Center:	India
Project Manager Name:	Paul George
Project Description:	WPS 2

ID	*Technical Assumption(s) and/or Customer Need(s)*	*Functional Requirement*	*Status*	*Software Module(s)*	Test Case Number	Tested In	Implemented In	Verification	Additional Comments
001	The EDP product family support should be provided to process orders for customers.	The product family EDP is added to enable the support for adding the EDP orders.	Complete d	WPS Online 2.x.	PO1	Place Order	Orders	Software test cases for EDP.	There is now provision to place orders for EDP product family from WPS Online
002	The EDP product family support should be provided to process orders for customers.	The customer visiblity should be according to the product entitlment.	Complete d	WPS Online 2.x.	PO2	Place Order	Orders	Software test cases for EDP.	Customer visibility is according to the product family and the Fulfillment site.
003	The operator should be able to place order as per the customer requirements.	The operator is able to place order if all mandatory fields are entered.	Complete d	WPS Online 2.x.	PO3	Place Order	Orders	Software test cases for EDP.	The mandatory fields should be entered while placing order.

Figure 3

Screenshot of the Cloud-based Application Matrix

Table 4 depicted the Test Coverage of WPS 2 RTM.

Table 4

Test Coverage of RTM for Cloud-based Application, WPS 2

Executed TCs	Planned TCs	Test coverage (Results)
97	100	97

The pie chart of the Table 4 is depicted in Figure 4, which is as follows:

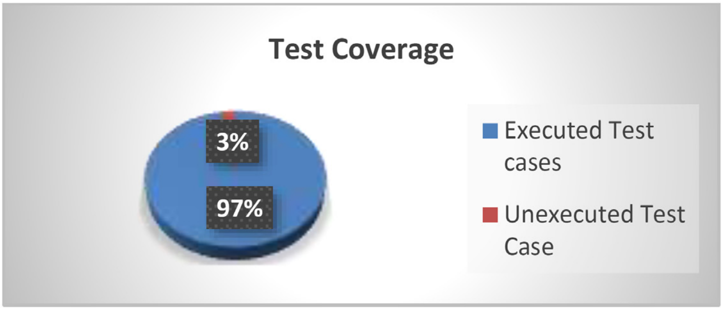


Figure 4

Test Coverage of Cloud-based Application

Table 5

Test Coverage of Passed TCs.

Actual no. of Passed Test Case	Actual "executed" Test case	Passed Test Case Coverage
90	97	92.7%

Calculation of Passed and Failed Test Case Coverage of WPS 2 RTM as follows:

Table 6

Test Coverage of Failed TCs

Actual no. of Failed Test	Actual "executed" Test case	Failed Test Case Coverage
7	97	7.2%

The Passed as well as Failed Test Coverage of the WPS 2 RTM is calculated in Table 5 and Table 6.

6. Comparison between Web and Cloud Application

Table 7 shows the comparison [28] results of Web as well as Cloud Application [29] [30], which is as follows:

Table 7

Comparison between Web and Cloud based Application

Parameters	Web-based	Cloud-based
Data Integrity	Less	High(improved table scheme)
Security	Less Secure	Highly Secure (due to cloud environment)
Availability	Dependency on resources \ project on various factors.	24*7 availability
Users Accessibility	Limited users can access	Unlimited users can access
Scalability	Non-Scalable	Scalable (expandable)
Cost	The high cost (hardware box required)	Low cost (no hardware device is required)
Text Coverage	Results of Test coverage is 90%	Results of Test coverage is 97%

Conclusion

The eventual aim of the paper is to propose the RTM for the web and cloud based application and primarily to elucidate comparison between them. The proposed RTM is applied and validated on Web and Cloud-based Application. The Test Coverage results are found to be adequate. To get the highest test coverage, Passed and Failed Test Case Coverage of RTM for Web and Cloud Application were calculated. It has been analyzed that the proposed RTM for Cloud-based Application as compared to Web-based Application having highest Test Coverage (97%). The comparison results of web-based and cloud-based applications has also been discussed.

References

[1] A. Tandon, "Usage of Traceability Matrix and Test Coverage Matrix from Testing Perspective," in *National Conference in ITBT*, 2011.

[2] D. Cuddeback, A. Dekhtyar and J. H. Hayes, "Automated Requirements Traceability: the Study of Human Analysts," in *18th IEEE International Requirements Engineering Conference*, 2010.

[3] M. Hassnain, "A Comparative Study on Traceability Approaches in Software development," *ITEE Journal,* vol. 4, no. 2, pp. 1-4, 2015.

[4] A. Ghazarian, "Traceability Patterns: An Approach to Requirement-Component Traceability in Agile Software Development," in *International Conference on Applied Computer Science*, 2008.

[5] A-Jaleel, N. Al-Saati and Raghda, "Requirement Tracing using Term Extraction," *International Journal of Computer Science and Information Security,* vol. 13, no. 5, pp. 1-6, 2015.

[6] A. Saswihalli and S. Kongi, "Project Quality Assurance using Traceability Matrix," *International Journal of Scientific & Engineering Research,* vol. 8, no. 5, pp. 5-7, 2017.

[7] Falak and M. Suaib, "A Survey on Importance of Requirement Traceability in Software Engineering," *International Journal of Engineering and Innovative Technology,* vol. 5, no. 4, pp. 109-112, 2015.

[8] M. Shahid, S. Ibrahim and M. N. Mahrin, "A Study on Test Coverage in Software Testing," *International Conference on Telecommunication Technology and Applications,* vol. 5, pp. 207-215, 2011.

[9] V. P. Katiyar, "Technique of Finding the Defect in Software Testing," *International Research Journal of Engineering and Technology,* vol. 5, no. 12, pp. 833-840, 2018.

[10] R. Torkar,T. Gorschek, R. Feldt, M. Svahnberg, U. A. Raja and K. Kamran, "Requirements Traceability: A Systematic Review and Industry Case Study," *International Journal of Software Engineering and Knowledge Engineering,* vol. 22, no. 3, pp. 1-49, 2012.

[11] M. Madan,M. Dave and A. Tandon, "Need and Usage of Traceability Matrix for Managing Requirements," *International Journal of Engineering Research,* pp. 666-668, 2016.

[12] R. Watkins and M. Neal, "Why and How of Requirement Tracing," in *5th International Conference on Application of Software Management*, 1994.

[13] M. Madan and A. Tandon, "Testing Application on the Web," *International Journal of Advanced Research in Computer Science and Software Engineering*, 2013.

[14] M. Madan, M. Dave and A. Tandon, "RTM and Testing Challenges in Cloud Based Application," in *Proceedings of 4th International Conference on Computers and Management*, Delhi, 2018.

[15] Neha Gupta, "Hybrid cryptographic technique to secure data in web application & Cryptography," *Journal of Discrete Mathematical Sciences*, 2020.

[16] M. Madan, M. Dave and A. Tandon, "Importance of RTM for Testing a Web-based Project," in *IEEE*, 2018.

[17] Nisha Rathee and Rajender Singh Chillar, "Gravitational search algorithm: A novel approach for structural test path optimization," *Journal of Interdisciplinary Mathematics*, 2020.

[18] A. Ehsani & F. H. Ghane, "Iterated Function Systems with the Weak Average Contraction Conditions," *Journal of Dynamical Systems and Geometric Theories*, vol. 17, no. 2, 2019.

[19] J. Cai and Q. Hu, "Analysis for Cloud Testing of Web Application," in *International Conference on Systems and Informatics*, 2014.

[20] I. A. Khan and R. Singh, "Quality Assurance and Integration Testing Aspects in Web based Applications," *International Journal of Computer Science, Engineering and Applications*, pp. 109-116, 2012.

[21] B. Kalyani, "Challenges in the Cloud Application Development," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 2, no. 1, pp. 310-313, 2013.

[22] A. Tandon and M. Madan, "Cloud Computing Security & Its Challenges," *International Journal of Electrical Electronics & Computer Science Engineering*, pp. 68-71, 2015.

[23] M. S. Das, A Govardhan and D.V. Lakshmi, "A Classification Approach for Web and Cloud Based Applications," in *International Conference on Engineering & MIS (ICEMIS)*, 2016.

[24] S. Sharmila and E. Ramadevi, "Analysis of Performance Testing on Web Applications," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 3, pp. 5258 - 5260, 2014.

[25] M. Madan,M. Dave and A. Tandon, "Challenges in Testing of Cloud Based Application," *International Journal of Advanced Research in Computer Science and Electronics Engineering*, pp. 28-31, 2016.

[26] M. Madan and M. Mathur, "A Satiated Method for Cloud Traffic Classification in Software," *International Journal of Cloud Applications and Computing,* vol. 6, no. 2, pp. 64-79, 2016.

[27] A. Tandon, "Implementing & Developing Cloud Computing on Web Application," *International Journal of Computer Science and Mobile Computing,* vol. 3, no. 2, pp. 153-157, 2014.

[28] Mohamed Majeed Mashroofa, Mazuki Jusoh & Karuthan Chinna, "Research trend on the application of "E-learning adoption theory" : A scientometric study during 2000-2019, based on Web of Science and SCOPUS," *COLLNET Journal of Scientometrics and Information Mangement,* vol. 13, no. 2, 2020.

[29] A. Tandon and M. Madan, "Challenges in Testing of Web Applications," *International Journal Of Engineering And Computer Science,* vol. 3, no. 5, pp. 5980-5984, 2014.

[30] M. Madan and M. Mathur, "Cloud Network Management Mode: A Novel Approach to Manage," *International Journal on Cloud Computing: Services and Architecture,* 2014.

[31] S. Delgado, "Next-Generation Techniques for Tracking Design Requirements Coverage in Automatic Test Software Development," in *Santiago Delgado*, Austin, 2006.

[32] E. Bernard and B. Legeard, *Requirements Traceability in the Model-Based Testing Process,* Software Engineering (Workshops), 2007.

[33] S. T. Dakshinamurthy and M. Z. Kurian, "Impact Analysis Based on Change Requirement Traceability in Object Oriented Software Systems," *International Journal of Computer and Information Engineering,* vol. 11, no. 1, pp. 43-47, 2017.

[34] F. Khursheed and M. Suaib, "A Survey on Importance of Requirement Traceability in Software Engineering," *International Journal of Engineering and Innovative Technology (IJEIT),* vol. 5, no. 4, pp. 109-112, 2015.

COVID19 – TRANSMISSION OF CORONA VIRUS AND IT'S MATHEMATICAL MODEL TO ANALYZE

Dr. Nripendra Narayan Das*[1], Dr. Naresh Kumar[2], Deepak Sharma[3], Sonakshi Rao[4]

[1]Associate Professor, Department of Information Technology
Manipal University Jaipur, Rajasthan, India-303007

[2]Associate Professor, Dept. Of Computer Science & Engineering
Maharaja Surajmal Institute of Technology, Janakpuri, New Delhi, India.

[3]Assistant Professor,
Jagannath International Management School, Vasant Kunj, New Delhi

[4]Regn No – 169108143(Final year Student) , Department of Information Technology
Manipal University Jaipur

Emails: [1]nripendradas@gmail.com, [2]narsumsaini@gmail.com,[3]deepaktech@hotmail.com,
[4]sonakshi.169108143@muj.manipal.edu

Received: 14 April 2020 Revised and Accepted: 8 August 2020

ABSTRACT: It was accounted for that the vast majority of the contaminated cases in INDIA have visited some neighborhood refers to before positive affirming their sickness (i.e., seclusion medical clinic, air terminal, eatery, advertise, bistro, clinic, organization, Movie Hall, and so forth.).
Obviously, a few likely explanations behind spreading coronavirus in INDIA are summed up by numerous scientists in the field. Several researches were led to locate the plausible reasons of spreading the coronavirus in INDIA as opposed to different nations. Research Scientist have begun to extricate data about the contaminated cases and examined the biomedical data and their clinical narratives to separate the principle parameters that could cause coronavirus spreading. Scientists proposed that the spreading of coronavirus could be associated with sex, birth year, or the district they originate from.
KEYWORDS : Corona Virus, parameters, biomedical.

I. INTRODUCTION

The objective of this paper is to consider the impact of a few traits on the spreading of coronavirus CoVID-19 in INDIA dependent on genuine gathered information and reports published in various sources. The primary objective is to examine the impact of sex, birth year, the district they originate from, and the spot they visited on the quantity of expired and recouped cases in INDIA. The investigation would give a review about the present circumstance in INDIA, moreover, it might show the primary parameters that can be utilized to design a predicting models.

(a) In order to comprehend the profundity of disturbance, following signs may need to be checked:

- Time to execute social distancing after network transmission is affirmed –

Since this pandemic is spreading through network and nearby transmission, it is extremely vital to screen the time taken to execute social separating which can be achieved by utilizing time series analysis. The reason for Time Series Forecasting is commonly twofold-to comprehend or display the
stochastic mechanism offering ascend to an observed series and to anticipate the future assessments of a sequence dependent on the chronological personal history of that series.

- Number of cases-absolute: Classification calculations can be utilized for checking the quantity of outright dynamic COVID19 cases.

  Geographic dissemination of cases comparative with financial commitment Clustering algorithm can help in observing this indicator as it permits congregation a lot of objects so that items in a alike congregation (called a cluster) are increasingly similar (in some sense) to one another than to those in different congregations (clusters). For instance, Maharashtra State contributes impressive bit to the Indian media outlet and economy which has most extreme number of COVID-19 cases.

- Extent of movement decrease
  Post COVID19 circumstance should be examined regarding the degree of movement decrease with the assistance of time series analysis algorithm and deep learning models. It will affect both vacationer and business trip because of at least one autonomous factors, for example, work steadiness, travel choices, direness of movement and travel cost.

(b) In order to understand the length of disruption, the following indicators may need to be monitored:

- Rate of change of cases- The following factors will allow the chain to break
  (i) lack of community and local transmission
  (ii) self-quarantine and self-isolation
  Rate of change of COVID19 cases could be understood using an algorithm i.e. time series analysis.
- Evidence of virus seasonality–Predictions of COVID19 can be provided by Time Series Analysis in a linear or nonlinear pattern that repeats at regular or irregular intervals. It is also stated in various articles when temperature will increase, the impact and spread of this virus will decrease which is not proved by any scientist yet. Seasonality data can be obtained by using time series analysis algorithm and later on patterns can be identified, if observed.
- % of cases treated at home- In this case all data will be consisted of structured data classification and can be derived by classification algorithms.
- % utilization of hospital beds- Linear Regression Models can be used to find utilization forecasting to anticipate and make predictions based on existing data. This will help in reducing the curve to let the dynamic cases stay beneath the limit of emergency hospitals to treat the contaminated individuals.
- Availability of therapies- Binary Classification Algorithms can also be used for therapies treatment based on infection severity and spread and It will allow prediction of future cases with such types of medical diagnosis details

II. TENTATIVE MODEL

As clarified before, this examination considers the impact of sex, age, district, and transportation on sensitivity to CoVID-19 in INDIA. The data received contains many information about 2771 contaminated cases (where the remainder of information is missing and not revealed) in INDIA specifically, sex, birth year, the first nation they originate from, the area that they live in, regardless of whether they conveying any sort of ailment previously, disease reason and request, affirmed date, expired or discharged date. The information contain several missed factors that barred from the investigation to give a reasonable summary about coronavirus pestilence in INDIA.

The transmission of CORONA virus can be understood by the following flow chart.

Fig 1. Flow diagram of Corona virus patient

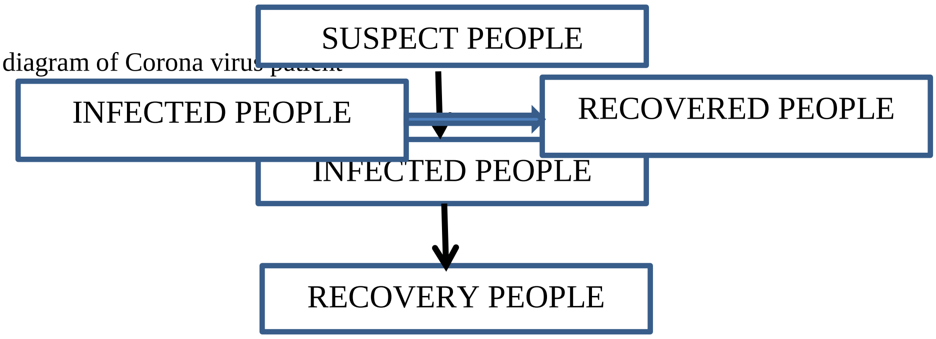


Fig 2. : Infected people to Recovered people

(On average, how long does it take one infected person to recover?)

$$\text{Recoveries} = \text{Infected Population} \times \frac{1 \text{ Recovery / person}}{\text{Duration of Infection}}$$

People Recoveries per person per day

Total Number of Contacts each day

Total Number of Contacts each day = Contacts each day for every infected person * Contaminated population

Infections per day = Total contacts per day * Infectivity

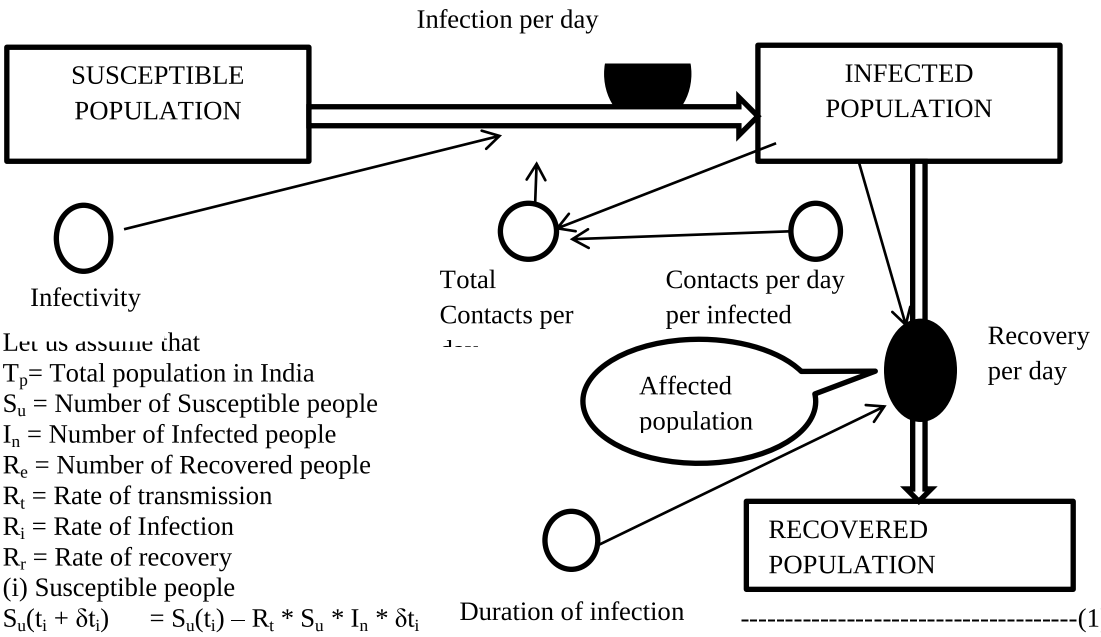
In the proposed model the population is divided into 3 categories for example susceptible person at time t_i, denoted by $S_u(t)$, enter the Infected class. The infectious class at time t_i, denoted by $I_n(t_i)$, represent the person who are contaminated with the virus and are experiencing the symptoms of Corona, then the recuperated class at time t_i is represented by $R_e(t)$.

The mathematical model has been formulated on the basis of the following assumption :

i. Population is fixed(no entries / births or departure / deaths)
ii. Latent period is zero
iii. Infectious period = disease duration
iv. After recovery, individuals are immune

People can be on of the three states

i. Susceptible to the infection
ii. Infected and Infectious
iii. Recovered/immune/removed



Let us assume that

T_p= Total population in India
S_u = Number of Susceptible people
I_n = Number of Infected people
R_e = Number of Recovered people
R_t = Rate of transmission
R_i = Rate of Infection
R_r = Rate of recovery

(i) Susceptible people

$S_u(t_i + \delta t_i) = S_u(t_i) - R_t * S_u * I_n * \delta t_i$ --------------------------------------(1)

(ii) Infected People

$I_n(t_i + \delta t_i) = I_n(t_i) + R_t * S_u$ ------------------------(2)

Fig 3: Steps of Corona Virus

(iii) Recovered people

$R_e(t_i + \delta t_i) = R_t + \gamma * I_n * \delta t_i$ --- (3)

3. SAMPLE DATA COLLECTED FROM GOVT. AGENCY [28] AS ON DATE(29/06/20).

The data have been taken from government agency, Ministry of Home Affairs(https://www.mohfw.gov.in/) and its graphical representation is shown below.

3.1 GRAPHICAL REPRESENTATION OF DATA

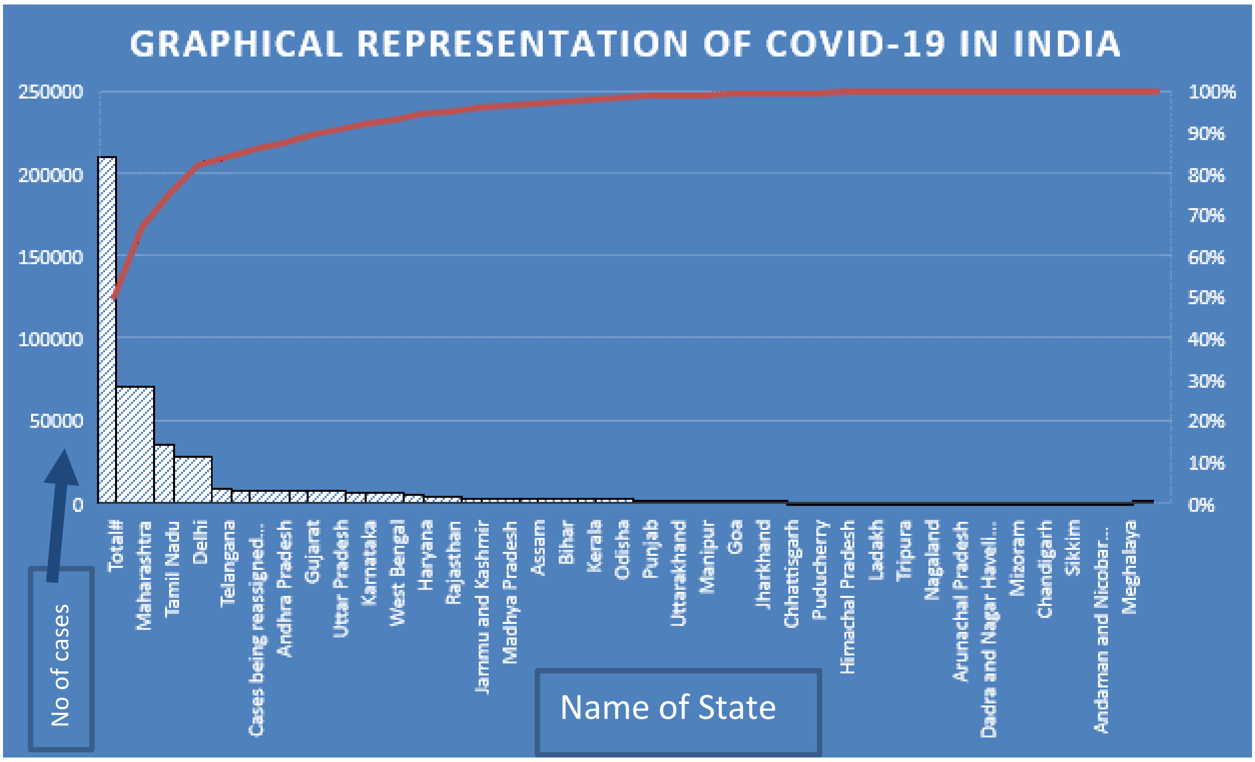


Figure -4 Graphical representation of Covid-19 cases in India

III. CONCLUSION

We are observing Corona Virus from since last 6 months and one thing is common in every patient who have become infected is sequence of events. Either they have come in contact with any person or he/she has touched the infected object any where i.e. Office, Shopping Mall, City Bus, Metro, Flight etc…

We all peoples in the world have been suffering from one the most deadliest diseases which is known in the name of COVID-19 and all health agencies, researchers are working 24×7 to control its spreading. Researcher are also working day and night to find the medicine of this deadly virus which is not yet discovered. As long as antidote or medicine etc. are not found, there is only one solution to defeat the corona virus which is the instructions given by Govt agencies, Hospitals, Doctors etc..

In addition, the procedures of testing individuals against coronavirus ought to be quicker. Keeping INDIA clean from coronavirus would influence on every close by nation.

5. FUTURE SCOPE

There are many scopes of research not in the field of medical science but also in every areas. My future work will be on implementing of Machine Algorithm related to future prediction using actual dataset.

IV. REFERENCES

[1] J. Alton. The Ebola Survival Handbook. Skyhorse Publishing, New York, 2014.

[2] A. Atangana, E. F. Doungmo Goufo. On the mathematical analysis of Ebola hemorrhagic fever: deathly infection disease in West African countries, BioMed Research International 2014 (2014), Art. ID 261383, 7 pp.

[3] I. Area, H. Batarfi, J. Losada, J. J. Nieto, W. Shammakh, A. Torres. On a fractional order Ebola epidemic model, Adv. Difference Equ. 2015 (2015), Art. ID 278, 12 pp.

[4] D. Ariens, B. Houska, H. J. Ferreau. ACADO Toolkit User's Manual, Toolkit for Automatic Control and Dynamic Optimization, 2010. http://www.acadotoolkit.org.

[5] M. Barry, F. A. Traor´e, F. B. Sako, D. O. Kpamy, E. I. Bah, M. Poncin, C. Keita, M. Cisse, A. Tour´e. Ebola outbreak in Conakry, Guinea: Epidemiological, clinical, and outcome features. M´edecine et Maladies Infectieuses 44 (2014), no. 11–12, 491–494.

[6] J. Bartlett, J. DeVinney, E. Pudlowski. Mathematical modeling of the 2014/2015 Ebola epidemic in West Africa, SIAM Undergraduate Research Online 9 (2016), 87–102.

[7] H. G. Bock, K. J. Pitt. A multiple shooting algorithm for direct solution of optimal control problems. Proc. 9th IFAC World Congress, Budapest, Pergamon Press, 1984, 243–247.

[8] L. Borio et al. [Working Group on Civilian Biodefense; Corporate Author]. Hemorrhagic fever viruses as biological weapons: medical and public health management. Journal of the American Medical Association 287 (2002), no. 18, 2391–2405.

[9] H. Boujakjian. Modeling the spread of Ebola with SEIR and optimal control, SIAM Under-graduate Research Online 9 (2016), 299–310.

[10] F. Brauer, P. D. V. Driessche, J. Wu. Mathematical Epidemiology. Lectures Notes in Math-ematics 1945, Mathematical Biosciences Subseries,

[11] 2008.E. K. Chapnick. Ebola Myths & Facts. Wiley & Sons, 2015.

[12] O. Diekmann, H. Heesterbeek, T. Britton. Mathematical tools for understanding infectious disease dynamics, Princeton Series in Theoretical and Computational Biology, Princeton Univ. Press, Princeton, NJ, 2013.

[13] O. Diekmann, J. A. P. Heesterbeek, J. A. J. Metz. On the definition and the computation ofthe basic reproduction ratio R0 in models for infectious diseases in heterogeneous populations.J. Math. Biol. 28 (1990), no. 4, 365–382.

[14] S. F. Dowell, R. Mukunu, T. G. Ksiazek, A. S. Khan, P. E. Rollin, C. J. Peters. transmissionof Ebola hemorrhagic fever: a study of risk factors in family members, Kikwit, Democratic Republic of the Congo, 1995. Commission de Lutte contre les Epid´emies `a Kikwit. J. Infect. Dis. 179 (1999), Suppl. 1, S87–S91.

[15] Embaixada da Rep´ublica Popular da China no Brasil. China ter´aprodu¸c˜ao em massa de vacina contra v´ırus Ebola, 14/Oct/2015. http://br.china-embassy.org/por/szxw/t1305911.htm

[16] H. Gaff, E. Schaefer. Optimal control applied to vaccination and treatment strategies for various epidemiological models. Math. Biosci. Eng. 6 (2009), no. 3, 469–492.

[17] J. M. Heffernan, R. J. Smith, L. M. Wahl. Perspectives on the basic reproductive ratio. J.
R. Soc. Interface 2 (2005), 281–293.

[18] IndexMundi. http://www.indexmundi.com.

[19] W. O. Kermack, A. G. McKendrick. Contributions to the mathematical theory of pidemics–I. 1927. Bull Math Biol. 53 (1991), 33–55.

[20] W. O. Kermack, A. G. McKendrick. Contributions to the mathematical theory of pidemics–II. The problem of endemicity. 1932. Bull Math Biol. 53 (1991), 57–87.

[21] M. Kretzschmar. Ring Vaccination and Smallpox Control. Emerging Infectious Diseases 10(2004), no. 5, 832–841.

[22] J. Legrand, R. F. Grais, P. Y. Boelle, A. J. Valleron, A. Flahault. Understanding the dynamics of Ebola epidemics. Epidemiol. Infect. 135 (2007), no. 4, 610–621.

[23] Jr. I. M. Longini, E. Ackerman. An optimization model for influenza A epidemics. Mathe-matical Biosciences 38 (1978), no. 1-2, 141–157.

[24] D. K. Mamo, P. R. Koya. Mathematical modeling and simulation study of SEIR disease and data fitting of Ebola epidemic spreading in West Africa, Journal of Multidisciplinary Engineering Science and Technology 2 (2015), no. 1, 106–114.

[25] C. J. Peters, J. W. LeDuc. An introduction to Ebola: the virus and the disease. Journal of Infectious Diseases 179 (1999), Suppl. 1, ix–xvi.

[26] A. Rachah, D. F. M. Torres. Mathematical modelling, simulation and optimal control of the 2014 Ebola outbreak in West Africa. Discrete Dyn. Nat. Soc. 2015 (2015), Art. ID 842792, 9 pp. arXiv:1503.07396

[27] A. Rachah, D. F. M. Torres. Optimal control strategies for the spread of Ebola in West Africa. J. Math. Anal. 7 (2016), no. 1, 102–114. arXiv:1512.03395

[28] https://www.mohfw.gov.in/

[29] A. Rachah, D. F. M. Torres. Modeling, dynamics and optimal control of Ebola virus spread. Pure and Applied Functional Analysis 1 (2016), no. 2, 277–289. arXiv:1 603.05794

[30] A. Rachah, D. F. M. Torres. Dynamics and optimal control of Ebola transmission. Math. Comput. Sci. 10 (2016), no. 3, 331–342. arXiv:1603.03265

[31] A. Rachah, D. F. M. Torres. Predicting and controlling the Ebola infection. Math. Methods Appl. Sci., in press. DOI:10.1002/mma.3841 arXiv:1511.06323

[32] Report of an International Commission. Ebola haemorrhagic fever in Zaire, 1976. Bull. World Health Organ. 56 (1978), no. 2, 271–293.

[33] Reuters. Two new trials of Ebola vaccines begin in Africa and Europe,http://voicesofafrica.co.za/two-new-trials-ebola-vaccines-begin-africa-europe

[34] H. S. Rodrigues, M. T. T. Monteiro, D. F. M. Torres. Dynamics of dengue epidemics when using optimal control. Math. Comput. Modelling 52 (2010), no. 9-10, 1667–1673. arXiv:1006.4392

[35] H. S. Rodrigues, M. T. T. Monteiro, D. F. M. Torres. Vaccination models and optimal control strategies to dengue. Math. Biosci. 247 (2014), no. 1, 1–12. arXiv:1310.4387

[36] T. C. Smith. Ebola. Deadly Diseases and Epidemics, Chelsea House Publisher, 2006.

[37] T. C. Smith. Heymann Ebola and Marburg Virus. Second Edition. Deadly diseases and epidemics, Chelsea House Publisher, 2010.

[38] Uganda Ministry of Health. An outbreak of Ebola in Uganda. Trop. Med. Int. Health. 7 (2002), no. 12, 1068–1075.

[39] X.-S. Wang, L. Zhong. Ebola outbreak in West Africa: real-time estimation and ultiplewave prediction. Math. Biosci. Eng. 12 (2015), no. 5, 1055–1063.

[40] WHO, World Health Organization. Report of an International Study Team. Ebola aemorrhagic fever in Sudan 1976. Bull. World Health Organ. 56 (1978), no. 2, 247–270.

[41] WHO, World Health Organization. Ebola Situation Reports.http://apps.who.int/ebola/ebola-situation-reports

[42] WHO, World Health Organization. Ebola Data and Statistics. http://apps.who.int/gho/data/view.ebola-sitrep.ebola-country-LBR.

DECLARATIONS

CONFLICT OF INTEREST

The paper of authors declare that there is no conflict of interest in any capacity.

AUTHOR’S CONTRIBUTION

The authors has contributed their original work in this paper.

FUNDING

None.

COLLECTION OF DATA

Dataset taken from Ministry of Home Affairs (https://www.mohfw.gov.in/[28])

SpringerLink Search Log in

Research Article | Published: 29 May 2021

Improved Change Detection in Remote Sensed Images by Artificial Intelligence Techniques

Snehlata Sheoran, Neetu Mittal & Alexander Gelbukh

Journal of the Indian Society of Remote Sensing (2021)

51 Accesses | Metrics

Abstract

The remote sensed images carry large amount of crucial information. Image processing, a field of signal processing, helps in analysis of remote sensed data. One of the major processing areas is image segmentation with edge detection, which helps in segmenting an image into various sub regions. These regions identified from images, captured over long span of time can help in identification of change detection. This paper presents an application of nature-inspired algorithms viz.: Ant Colony Algorithm, Particle Swarm Optimization and Genetic Algorithm to optimize edge detection procedure. These methods have been implemented on a set of 15 satellite images and further enhancement is done by application of adaptive thresholding using Python. For qualitative analysis, entropy of each output image is computed. The comparison of computer results revealed that particle swarm optimization outperforms conventional methods, i.e., Sobel, Canny and Prewitt as well as ACO and GA. The PSO-based method is able to find more edges and presents far superior quality output images for further analysis with respect to change detection.

Data Availability

Images available on Google Earth.

Code Availability

Yes.

References

1. Abualigah, L. M., Khader, A. T., & Hanandeh, E. S. (2018). A new feature selection method to improve the document clustering using particle swarm optimization algorithm. *Journal of Computational Science, 25*, 456–466

2. Ahmadi, Maliheh, Kazemi, Kamran, Aarabi, Ardalan, Niknam, Taher, & Helfroush, Mohammad Sadegh. (2019). Image segmentation using multilevel thresholding based on modified bird mating optimization. *Multimedia Tools and Applications, 78*(16), 23003–23027

3. Amanpreet, K., & Singh, M. D. (2012). An overview of pso-based approaches in image segmentation. *International Journal of Engineering and Technology, 2*(8), 1349–1357

4. Anju, A., & Anitha, J. (2019). Change detection techniques for remote sensing applications: A survey. *Earth Science Informatics, 12*(2), 143–160

5. Attri, P., Chaudhry, S., & Sharma, S. (2015). Remote sensing & GIS based approaches for LULC change detection–a review. *International Journal of Current Engineering and Technology, 5*(5), 3126–3137

6. Deng, Wu., Junjie, Xu., & Zhao, H. (2019). An improved ant colony optimization algorithm based on hybrid strategies for scheduling problem. *IEEE Access, 7*, 20281–20292

7. Goldberg, David E. (1989) "Genetic algorithms in search." Optimization, and Machine Learning.

8. Holland, J. H. (1975). *Adaptation in natural & artificial systems*. Ann Arbor: University of Michigan Press.

9. Jones, K. O. (2006) Comparison of genetic algorithms and particle swarm optimization for fermentation feed profile determination. In Proceedings of the CompSysTech, (pp. 15–16).

10. Kennedy, J., and Eberhart, R. (1995) "Particle swarm optimization." In Proceedings of ICNN'95-International Conference on Neural Networks, vol. 4, pp. 1942–1948. IEEE.

11. Krishna Satya, V. M., & Kameswara Roa, N. K. (2017). Satellite image classification using genetic algorithm based on SVM classifier. *International Journal of Control Theory & Applications, 10*(26), 13–20

12. Li, H., He, H., & Wen, Y. (2015). Dynamic particle swarm optimization and K-means clustering algorithm for image segmentation. *Optik, 126*(24), 4817–4822

13. Liu, Yi., Caihong, Mu., Kou, W., & Liu, J. (2015). Modified particle swarm optimization-based multilevel thresholding for image segmentation. *Soft Computing, 19*(5), 1311–1327

14. Marco, D., & Gambardella, L. M. (1997). Ant colony system: a cooperative learning approach to the traveling salesman problem. *IEEE Transactions on evolutionary computation, 1*(1), 53–66

15. Marco, D., and Birattari, M. (2010) "Ant colony optimization. Encyclopaedia of machine learning." 39.

16. Matheson, R. (2020) Using artificial intelligence to enrich digital maps, Massachusetts Institute of Technology News Office, January, 2020, https://news.mit.edu/2020/artificial-intelligence-digital-maps-0123.

17. Mehdi, M., Amini, J., Hahn, M., & Saati, M. (2017). Object-based road extraction from satellite images using ant colony optimization. *International Journal of Remote Sensing, 38*(1), 179–198

18. Nandan, P. B., and Rana, A. (2018) "A Literature Survey of Optimization Techniques for Satellite Image Segmentation." In 2018 International Conference on Advanced Computation and Telecommunication (ICACAT), pp. 1–5. IEEE.

19. Neetu, M., Tanwar, S., and Khatri, S. K. (2017) "Identification & enhancement of different skin lesion images by segmentation techniques." In 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 609–614. IEEE.

20. Nezamabadi-Pour, H., Saryazdi, S., & Rashedi, E. (2006). Edge detection using ant algorithms. *Soft Computing, 10*(7), 623–628

21. Nipotepat, M., Sunat, K., and Chiewchanwattana, S. (2016) "Multilevel thresholding for satellite image segmentation with moth-flame based optimization." In 2016 13th International Joint Conference on

Computer Science and Software Engineering (JCSSE), pp. 1–6. IEEE.

22. Pedram, G., Couceiro, M. S., Martins, F. M. L., & Benediktsson, J. A. (2013). Multilevel image segmentation based on fractional-order Darwinian particle swarm optimization. *IEEE Transactions on Geoscience and Remote sensing, 52*(5), 2382–2394

23. Poorti, S., & Mittal, N. (2019). *Breast cancer detection using image processing techniques*. *Advances in interdisciplinary engineering*. (pp. 813–823). Singapore: Springer.

24. Qingwu, F., Chen, G., Zhou, X., and Li, L. (2019) "Image threshold segmentation based on auxiliary individual oriented crossover genetic algorithm." In 2019 IEEE International Conference on Industrial Internet (ICII), pp. 411–416. IEEE.

25. Radke, Richard J., Andra, Srinivas, Al-Kofahi, Omar, & Roysam, Badrinath. (2005). Image change detection, algorithms: a systematic survey. *IEEE Transactions on Image Processing, 14*(3), 294–307

26. Ruiguo, Yu., Fu, X., Jiang, H., Wang, C., Li, X., Zhao, M., Ying, X., and Shen, H. (2018) "Remote Sensing Image Segmentation by Combining

Feature Enhanced with Fully Convolutional Network." In International Conference on Neural Information Processing, pp. 406–415. Springer, Cham.

27. Safaa, Y. Z., Mohamad, D., Saba, T., Alkawaz, M. H., Rehman, A., Al-Rodhaan, M., & Al-Dhelaan, A. (2015). Content-based image retrieval using PSO and k-means clustering algorithm. *Arabian Journal of Geosciences, 8*(8), 6211–6224

28. Sengupta, S., Mittal, N., & Modi, M. (2019). Improved skin lesion edge detection method using Ant Colony Optimization. *Skin Research and Technology, 25*(6), 846–856

29. Shakti, S., & Buddhiraju, K. M. (2018). Spatial–spectral ant colony optimization for hyperspectral image classification. *International Journal of Remote Sensing, 39*(9), 2702–2717

30. Shubham, K., Zeya, I., Singhal, C., & Nanda, S. J. (2017). A grey wolf optimizer based automatic clustering algorithm for satellite image segmentation. *Procedia Computer Science, 115*, 415–422

31. Simranpreet, K., and Kaur, P. (2016) "An edge detection technique with image segmentation using ant colony optimization: A review."

In 2016 Online International Conference on Green Engineering and Technologies (IC-GET), pp. 1–5. IEEE.

32. Singh, P. P., & Garg, R. D. (2013). A Hybrid approach for Information Extraction from High Resolution Satellite Imagery. *International Journal of Image and Graphics, 13*(2), 1340007

33. Singh, P. A. (2017) "Satellite image segmentation based on differential evolution." In 2017 International Conference on Intelligent Sustainable Systems (ICISS), pp. 621–624. IEEE.

34. Singh, P. P. and Garg, R. D. (2011). Land Use And Land Cover Classification Using Satellite Imagery: A Hybrid Classifier And Neural Network Approach. proceedings of International Conference on Advances in Modeling, Optimization and Computing, Dec. 5–7.

35. Singh, V., and Misra, A. K. (2015) "Detection of unhealthy region of plant leaves using image processing and genetic algorithm." In 2015 International Conference on Advances in Computer Engineering and Applications, pp. 1028–1032. IEEE.

36. Sudhriti, S., and Mittal, N. (2017) "Analysis of various techniques of feature extraction on skin

lesion images." In 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), pp. 651–656. IEEE.

37. Suresh, S., & Lal, S. (2017). Multilevel thresholding based on Chaotic Darwinian particle swarm optimization for segmentation of satellite images. *Applied Soft Computing, 55*, 503–522

38. Vito, D. G., and Bosco, G. L. (2005) "Image segmentation based on genetic algorithms combination." In International Conference on Image Analysis and Processing, pp. 352–359. Springer, Berlin, Heidelberg.

Funding

No funding from any source.

Author information

Affiliations

1. Amity University Uttar Pradesh, Noida, Uttar Pradesh, India

   Snehlata Sheoran & Neetu Mittal

2. Instituto Politécnico Nacional [IPN], Mexico City, Mexico

Alexander Gelbukh

Corresponding author

Correspondence to Snehlata Sheoran.

Ethics declarations

Conflict of interest

No conflict of interest between the authors.

Additional information

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Supplementary Information

Below is the link to the electronic supplementary material.

Supplementary file1 (DOCX 5505 kb)

About this article

Cite this article

Sheoran, S., Mittal, N. & Gelbukh, A. Improved Change Detection in Remote Sensed Images by Artificial Intelligence Techniques. *J Indian Soc Remote Sens* (2021). https://doi.org/10.1007/s12524-021-01374-x

- Received29 September 2020
- Accepted16 April 2021
- Published29 May 2021
- DOIhttps://doi.org/10.1007/s12524-021-01374-x

Keywords

- Satellite images
- Swarm intelligence
- Artificial intelligence
- Change detection
- Particle swarm optimization

International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 /doi:10.14445/22312803/IJCTT-V69I3P109

Volume 69 Issue 3, 46-51, March, 2021
© 2021 Seventh Sense Research Group®

Analysis of Optimization Technique of Same Program Written in Two Different Interfaces i.e. CUI and GUI Using Java and Calculate Their Differences

Dr. Arpana Chaturvedi[#1], Dr. Deepti Khanna[*2], Deepit Aggarwal [#3,] Ayush Prasad [#4]

[#1] Associate Professor, Jagannath International Management School, New Delhi, India
[#2]Associate Professor, JIMS, New Delhi, India
[#3]Student, JIMS New Delhi, India
[#4]Student, JIMS New Delhi, India

Received Date: 01 February 2021
Revised Date: 11 March 2021
Accepted Date: 16 March 2021

Abstract — *Java is one of the most stable programming languages and form time to time Oracle Corporation frequently updates the language , it is also platform independent and supports common programming paradigms has got rich set of APIs , loads of frameworks, Libraries, IDEs and development tools ,simplify Development of real-time software , facilitates embedded computing and is robust and secure ,so a vast majority of applications use JAVA Programming Language .Here in our research work we have developed a program named inventory control management system. It's a CUI program which is created in core java. A GUI application is also created of the same program with the help of JFrame using event driven programming. in our research work we have used different optimization techniques such as CPU utilization, Heap Count and Threads, etc. to study performance on CUI and GUI, based upon the result we tried to find out which interface is better in terms of memory utilization and CPU utilization.*

Keywords — *Java program, optimization techniques, GUI, CUI, JFrame.*

.

I. INTRODUCTION

Java is a simple object-oriented, robust, secure, architecture-neutral, portable, high performance, interpreted, threaded, platform independent programming language. it is used to develop applications for the various fields such as banking , retail , information technology , android etc. here for our research paper we have developed a program which is an inventory management system of a company to watch the products requirements of the company and which item needs to be re-ordered accordingly from time to time .this will help the companies in managing the warehouses and keeping a proper track of the items available that can be further used in the calculations of the gross production cost evaluated we have developed the program in Command Line Interface as well as in Graphical User Interface and using both the interfaces we studied the utilization and performance of the program and with the help of the results obtained we have further tried to optimize the program for better performance for the industrial purpose . we have prepared graph to study the performance and memory utilization by both the interfaces and also conducted statistical test based upon the data collected and further studied the test results for the better optimization of the program.

.

II. OBJECTIVE

A. To create same program in Core Java and JFrame using event driven programming, the program is created in both CUI and GUI: -

To objective of the research paper is to create a program in Core Java and JFrame using event driven programming, the program is created in both CUI and GUI.

B. To find the optimization techniques which include Memory optimization, CPU performance, Heap memory utilization and Disk utilization: -

To study the optimization techniques which include Memory optimization, CPU performance, Heap memory utilization and Disk utilization to study the performance of the program in CUI and GUI interface for the purpose of finding out which interface is better suitable for the industrial use.

C. To find out which interface is better suitable for the performance of the program: -

Based upon the study conducted, compare the results of the optimization techniques and study its performance and coming to a conclusion.

III. TOOLS USED

We used following software and hardware for our research: -

Operating System:-	
Edition	Windows 10 Home Single Language
Version	1909

Table 1. Operating System Details

Hardware Requirements: -	
Processor	Intel® Core™ i5-8250U CPU @ 1.60GHz
Installed RAM	8.00 GB (7.87 GB usable)
Hard disk	1TB
System type	64-bit OS *64-based processor

Table 2. Hardware Requirement Details

Software Requirements: -	
IDE	Eclipse
Web serer	Xampp
Connector	mysql-connector-java-5.0.8-bin
Analysis Tool	Your Kit-JAVA Profiler

Table 3. Software Requirement Details

Additional Software: -	
Additional IDE Software	Window Builder
Connectors: -	rs2xml
	jgoodies-forms-1.8.0-sources
	javax.mail-1.6.2

Table 4. Additional Requirement Details

IV. INTRODUCTION TO THE PROGRAM TO PERFORM RESEARCH

For our research paper we have a written a program in core java, core java is a collection of libraries rather than just the simple programming language. We developed a code for inventory management system which is made for the purpose of keeping the track of the available stock in the warehouses; it is a multiple user system which will help in saving the time of the organization while keeping a record. The program has got a login system which is of multiple user login and is robust and secure, the program contains mainly three functions i.e. item , supplier and reorder each function have sub functions such as insert, update, display and delete .The program is easy to use and is secure as well.

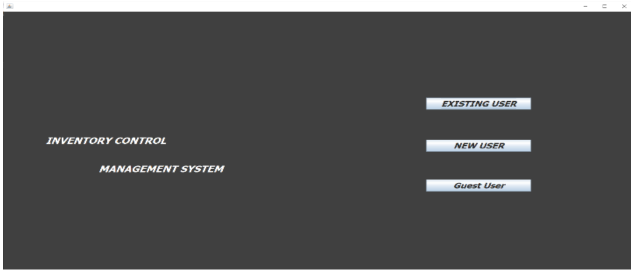


Fig. 1. Main Frame of the GUI Application

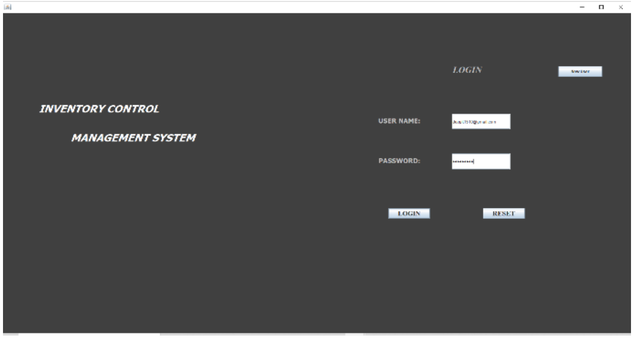


Fig. 2. Login Frame of the GUI Application

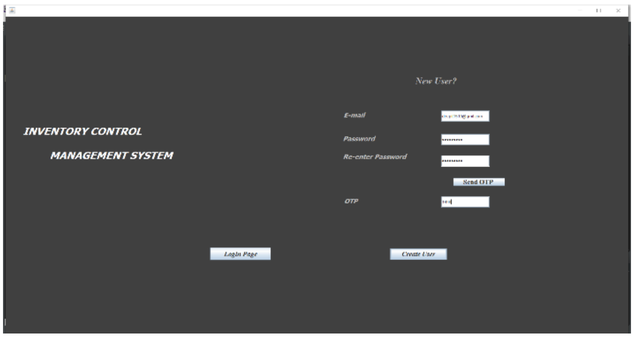


Fig. 3. New User Login Creation Frame of the GUI Application

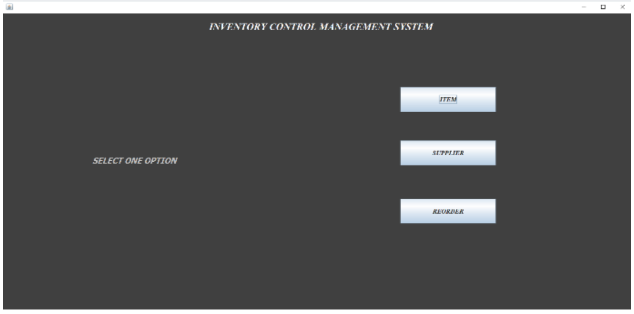
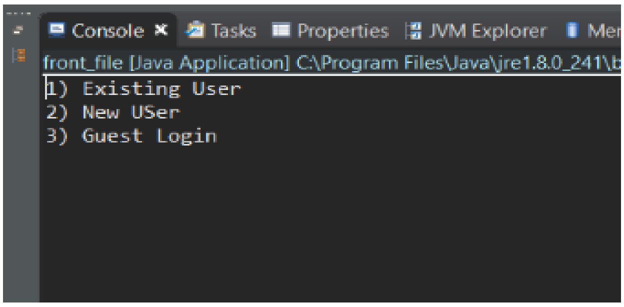
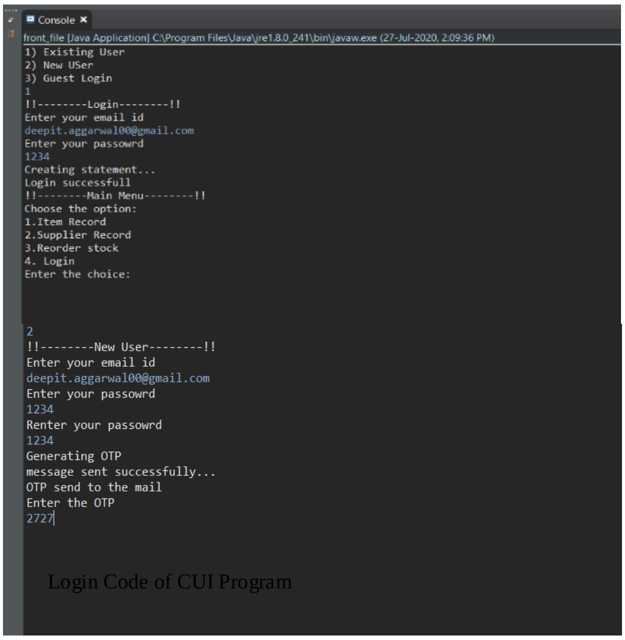


Fig. 4. First Frame After Login Frame of the GUI Application



```
front_file [Java Application] C:\Program Files\Java\jre1.8.0_241\b
1) Existing User
2) New USer
3) Guest Login
```

Fig. 5. Login and the main menu after Login of the CUI Program



```
front_file [Java Application] C:\Program Files\Java\jre1.8.0_241\bin\javaw.exe (27-Jul-2020, 2:09:36 PM)
1) Existing User
2) New USer
3) Guest Login
1
!!--------Login--------!!
Enter your email id
deepit.aggarwal00@gmail.com
Enter your passowrd
1234
Creating statement...
Login successfull
!!--------Main Menu--------!!
Choose the option:
1.Item Record
2.Supplier Record
3.Reorder stock
4. Login
Enter the choice:


2
!!--------New User--------!!
Enter your email id
deepit.aggarwal00@gmail.com
Enter your passowrd
1234
Renter your passowrd
1234
Generating OTP
message sent successfully...
OTP send to the mail
Enter the OTP
2727
```

Login Code of CUI Program

Fig. 6. Login and the main menu after Login of the CUI Program

V. CHARACTER USER INTERFACE

Character user interface or command –line user interface (CUI) is a method in which the user interacts with computer programs. The interface allows the users to issue commands in one or more lines to a program. It is difficult in navigation has got high precision, computing speed is high, is difficult to operate and require expertise, requires low memory, is less flexible and the appearance cannot be changed. One of the best examples of the CUI interface is MS-DOS and Windows command Prompt. The CUI interface of the inventory management system is easy to understand and use.

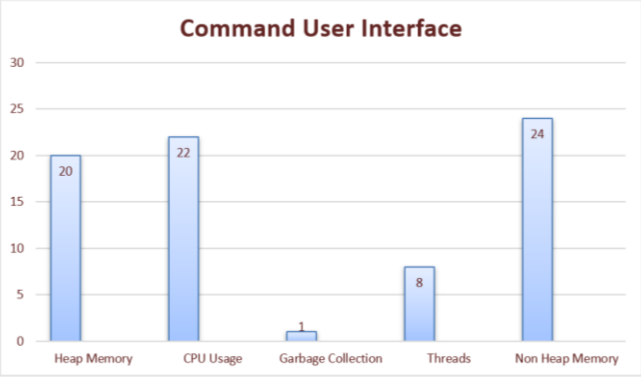
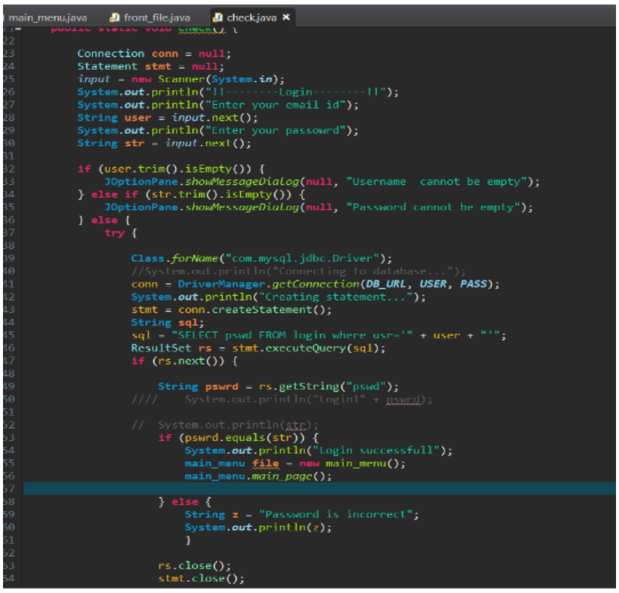
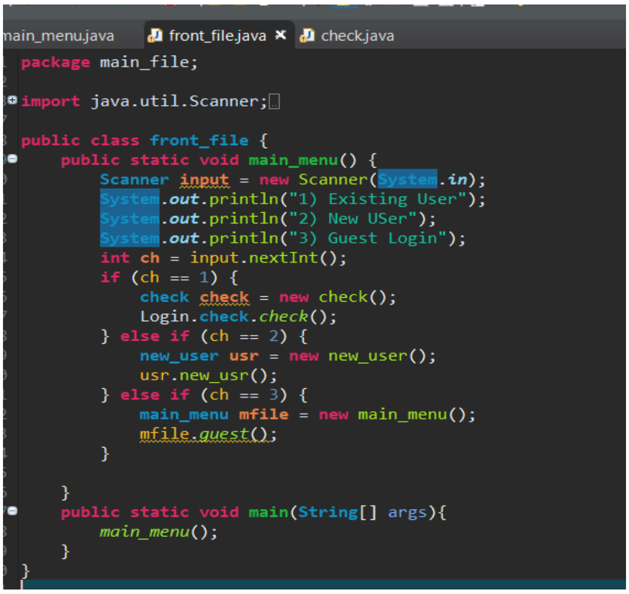


Fig. 7. The Memory, CPU, Threads Utilization and Displaying the Garbage Collection in CUI



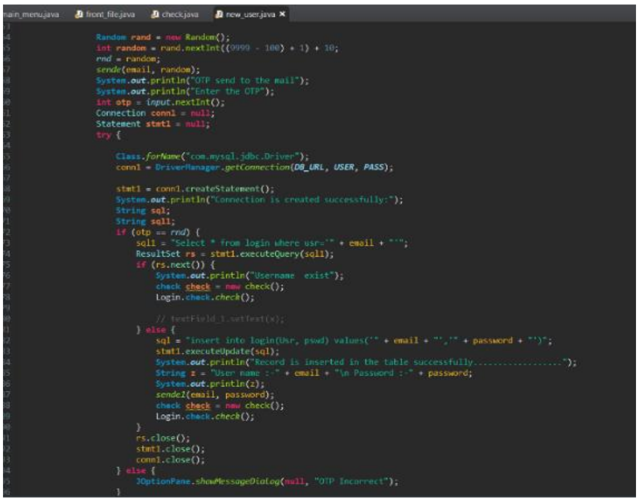
```java
    public static void check() {

        Connection conn = null;
        Statement stmt = null;
        input = new Scanner(System.in);
        System.out.println("!!--------Login--------!!");
        System.out.println("Enter your email id");
        String user = input.next();
        System.out.println("Enter your passowrd");
        String str = input.next();

        if (user.trim().isEmpty()) {
            JOptionPane.showMessageDialog(null, "Username  cannot be empty");
        } else if (str.trim().isEmpty()) {
            JOptionPane.showMessageDialog(null, "Password cannot be empty");
        } else {
            try {

                Class.forName("com.mysql.jdbc.Driver");
                //System.out.println("Connecting to database...");
                conn = DriverManager.getConnection(DB_URL, USER, PASS);
                System.out.println("Creating statement...");
                stmt = conn.createStatement();
                String sql;
                sql = "SELECT pswd FROM login where usr='" + user + "'";
                ResultSet rs = stmt.executeQuery(sql);
                if (rs.next()) {

                    String pswrd = rs.getString("pswd");
                ////    System.out.println("login1" + pswrd);

                //  System.out.println(str);
                    if (pswrd.equals(str)) {
                        System.out.println("Login successfull");
                        main_menu file = new main_menu();
                        main_menu.main_page();

                    } else {
                        String z = "Password is incorrect";
                        System.out.println(z);
                        }

                    rs.close();
                    stmt.close();
```

Fig.8. Main Menu Code of the CUI Program



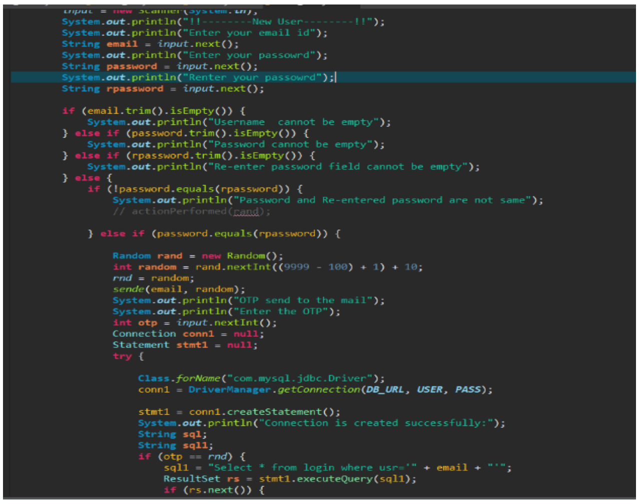
```java
package main_file;

import java.util.Scanner;

public class front_file {
    public static void main_menu() {
        Scanner input = new Scanner(System.in);
        System.out.println("1) Existing User");
        System.out.println("2) New USer");
        System.out.println("3) Guest Login");
        int ch = input.nextInt();
        if (ch == 1) {
            check check = new check();
            Login.check.check();
        } else if (ch == 2) {
            new_user usr = new new_user();
            usr.new_usr();
        } else if (ch == 3) {
            main_menu mfile = new main_menu();
            mfile.guest();
        }

    }
    public static void main(String[] args){
        main_menu();
    }
}
```

Fig. 9. New User Code of CUI Program



```
            Random rand = new Random();
            int random = rand.nextInt((9999 - 100) + 1) + 10;
            rnd = random;
            sende(email, random);
            System.out.println("OTP send to the mail");
            System.out.println("Enter the OTP");
            int otp = input.nextInt();
            Connection conn1 = null;
            Statement stmt1 = null;
            try {

                Class.forName("com.mysql.jdbc.Driver");
                conn1 = DriverManager.getConnection(DB_URL, USER, PASS);

                stmt1 = conn1.createStatement();
                System.out.println("Connection is created successfully:");
                String sql;
                String sql1;
                if (otp == rnd) {
                    sql1 = "Select * from login where usr='" + email + "'";
                    ResultSet rs = stmt1.executeQuery(sql1);
                    if (rs.next()) {
                        System.out.println("Username  exist");
                        check check = new check();
                        Login.check.check();

                        // textField_1.setText(x);
                    } else {
                        sql = "insert into login(Usr, pswd) values('" + email + "','" + password + "')";
                        stmt1.executeUpdate(sql);
                        System.out.println("Record is inserted in the table successfully.................");
                        String z = "User name :-" + email + "\n Password :-" + password;
                        System.out.println(z);
                        sende1(email, password);
                        check check = new check();
                        Login.check.check();
                    }
                    rs.close();
                    stmt1.close();
                    conn1.close();
                } else {
                    JOptionPane.showMessageDialog(null, "OTP Incorrect");
                }
```

Fig. 10. Main Menu Code of the CUI Program



```
        input = new Scanner(System.in);
        System.out.println("!!--------New User--------!!");
        System.out.println("Enter your email id");
        String email = input.next();
        System.out.println("Enter your passowrd");
        String password = input.next();
        System.out.println("Renter your passowrd");
        String rpassword = input.next();

        if (email.trim().isEmpty()) {
            System.out.println("Username  cannot be empty");
        } else if (password.trim().isEmpty()) {
            System.out.println("Password cannot be empty");
        } else if (rpassword.trim().isEmpty()) {
            System.out.println("Re-enter password field cannot be empty");
        } else {
            if (!password.equals(rpassword)) {
                System.out.println("Password and Re-entered password are not same");
                // actionPerformed(rand);

            } else if (password.equals(rpassword)) {

                Random rand = new Random();
                int random = rand.nextInt((9999 - 100) + 1) + 10;
                rnd = random;
                sende(email, random);
                System.out.println("OTP send to the mail");
                System.out.println("Enter the OTP");
                int otp = input.nextInt();
                Connection conn1 = null;
                Statement stmt1 = null;
                try {

                    Class.forName("com.mysql.jdbc.Driver");
                    conn1 = DriverManager.getConnection(DB_URL, USER, PASS);

                    stmt1 = conn1.createStatement();
                    System.out.println("Connection is created successfully:");
                    String sql;
                    String sql1;
                    if (otp == rnd) {
                        sql1 = "Select * from login where usr='" + email + "'";
                        ResultSet rs = stmt1.executeQuery(sql1);
                        if (rs.next()) {
```

Fig.11. Main Menu Code of the CUI Program

V. GRAPHICAL USER INTERFACE

Graphical user interface is a method which allows the users to interact with electronic devices through graphical icons and primary notation. It is easy to use has got high low precision, computing speed is low, is easy to operate, requires high memory is more flexible and the appearance can be customized.

The GUI interface of the program is more user friendly as compared to the CUI interface as it has got labels, text field and buttons which helps in better understanding of the program.

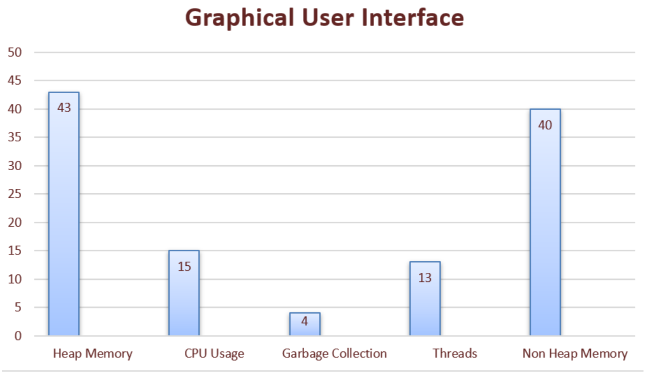
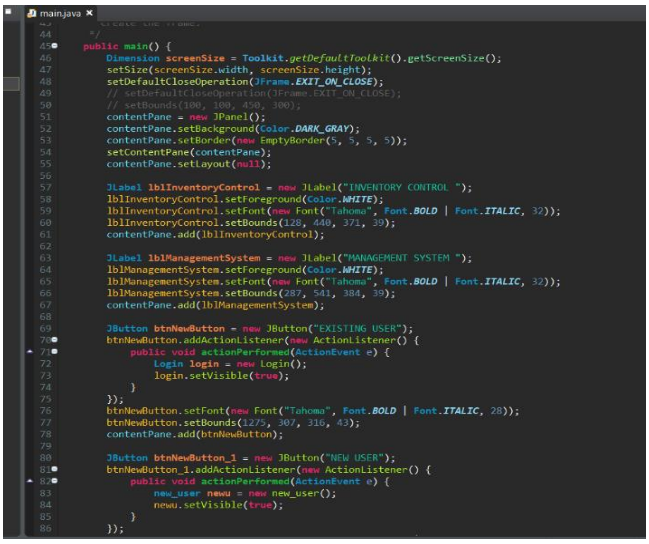
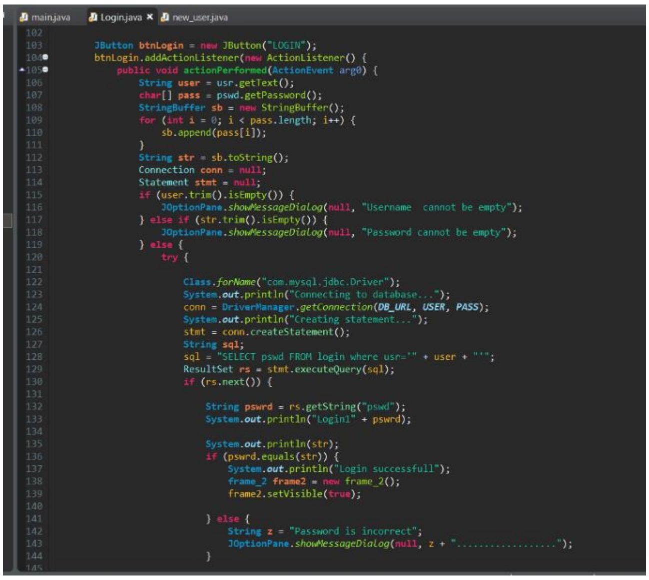


Fig. 12. The Memory, CPU, Threads Utilization and Displaying the Garbage Collection in GUI



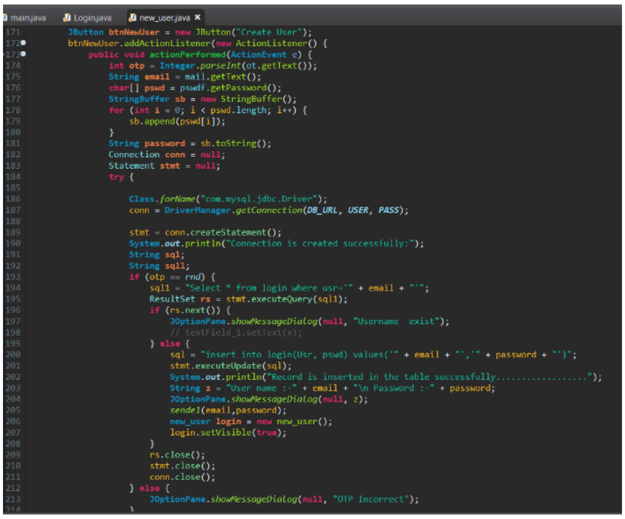
```
     * Create the frame.
     */
    public main() {
        Dimension screenSize = Toolkit.getDefaultToolkit().getScreenSize();
        setSize(screenSize.width, screenSize.height);
        setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
        // setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
        // setBounds(100, 100, 450, 300);
        contentPane = new JPanel();
        contentPane.setBackground(Color.DARK_GRAY);
        contentPane.setBorder(new EmptyBorder(5, 5, 5, 5));
        setContentPane(contentPane);
        contentPane.setLayout(null);

        JLabel lblInventoryControl = new JLabel("INVENTORY CONTROL ");
        lblInventoryControl.setForeground(Color.WHITE);
        lblInventoryControl.setFont(new Font("Tahoma", Font.BOLD | Font.ITALIC, 32));
        lblInventoryControl.setBounds(128, 440, 371, 39);
        contentPane.add(lblInventoryControl);

        JLabel lblManagementSystem = new JLabel("MANAGEMENT SYSTEM ");
        lblManagementSystem.setForeground(Color.WHITE);
        lblManagementSystem.setFont(new Font("Tahoma", Font.BOLD | Font.ITALIC, 32));
        lblManagementSystem.setBounds(287, 541, 384, 39);
        contentPane.add(lblManagementSystem);

        JButton btnNewButton = new JButton("EXISTING USER");
        btnNewButton.addActionListener(new ActionListener() {
            public void actionPerformed(ActionEvent e) {
                Login login = new Login();
                login.setVisible(true);
            }
        });
        btnNewButton.setFont(new Font("Tahoma", Font.BOLD | Font.ITALIC, 28));
        btnNewButton.setBounds(1275, 307, 316, 43);
        contentPane.add(btnNewButton);

        JButton btnNewButton_1 = new JButton("NEW USER");
        btnNewButton_1.addActionListener(new ActionListener() {
            public void actionPerformed(ActionEvent e) {
                new_user newu = new new_user();
                newu.setVisible(true);
            }
        });
```

Fig. 13. New User Code of CUI Program



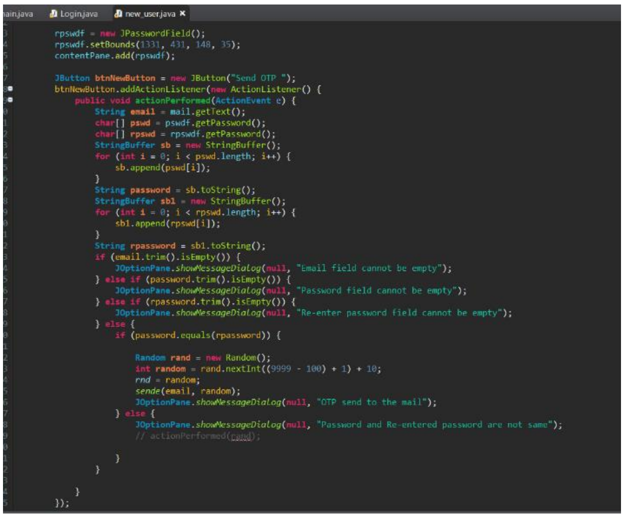
```

        JButton btnLogin = new JButton("LOGIN");
        btnLogin.addActionListener(new ActionListener() {
            public void actionPerformed(ActionEvent arg0) {
                String user = usr.getText();
                char[] pass = pswd.getPassword();
                StringBuffer sb = new StringBuffer();
                for (int i = 0; i < pass.length; i++) {
                    sb.append(pass[i]);
                }
                String str = sb.toString();
                Connection conn = null;
                Statement stmt = null;
                if (user.trim().isEmpty()) {
                    JOptionPane.showMessageDialog(null, "Username  cannot be empty");
                } else if (str.trim().isEmpty()) {
                    JOptionPane.showMessageDialog(null, "Password cannot be empty");
                } else {
                    try {

                        Class.forName("com.mysql.jdbc.Driver");
                        System.out.println("Connecting to database...");
                        conn = DriverManager.getConnection(DB_URL, USER, PASS);
                        System.out.println("Creating statement...");
                        stmt = conn.createStatement();
                        String sql;
                        sql = "SELECT pswd FROM login where usr='" + user + "'";
                        ResultSet rs = stmt.executeQuery(sql);
                        if (rs.next()) {

                            String pswrd = rs.getString("pswd");
                            System.out.println("Login1" + pswrd);

                            System.out.println(str);
                            if (pswrd.equals(str)) {
                                System.out.println("Login successfull");
                                frame_2 frame2 = new frame_2();
                                frame2.setVisible(true);

                            } else {
                                String z = "Password is incorrect";
                                JOptionPane.showMessageDialog(null, z + ".................");
                            }

```

Fig. 15. Main Menu Code of the CUI Program



```
        JButton btnNewUser = new JButton("Create User");
        btnNewUser.addActionListener(new ActionListener() {
            public void actionPerformed(ActionEvent e) {
                int otp = Integer.parseInt(ot.getText());
                String email = mail.getText();
                char[] pswd = pswdf.getPassword();
                StringBuffer sb = new StringBuffer();
                for (int i = 0; i < pswd.length; i++) {
                    sb.append(pswd[i]);
                }
                String password = sb.toString();
                Connection conn = null;
                Statement stmt = null;
                try {

                    Class.forName("com.mysql.jdbc.Driver");
                    conn = DriverManager.getConnection(DB_URL, USER, PASS);

                    stmt = conn.createStatement();
                    System.out.println("Connection is created successfully:");
                    String sql;
                    String sql1;
                    if (otp == rnd) {
                        sql1 = "Select * from login where usr='" + email + "'";
                        ResultSet rs = stmt.executeQuery(sql1);
                        if (rs.next()) {
                            JOptionPane.showMessageDialog(null, "Username  exist");
                            // textField_1.setText(x);
                        } else {
                            sql = "insert into login(Usr, pswd) values('" + email + "','" + password + "')";
                            stmt.executeUpdate(sql);
                            System.out.println("Record is inserted in the table successfully..................");
                            String z = "User name :-" + email + "\n Password :-" + password;
                            JOptionPane.showMessageDialog(null, z);
                            sende1(email,password);
                            new_user login = new new_user();
                            login.setVisible(true);
                        }
                        rs.close();
                        stmt.close();
                        conn.close();
                    } else {
                        JOptionPane.showMessageDialog(null, "OTP Incorrect");
                    }
```

Fig. 16. Main Menu Code of the CUI Program



```
        rpswdf = new JPasswordField();
        rpswdf.setBounds(1331, 431, 148, 35);
        contentPane.add(rpswdf);

        JButton btnNewButton = new JButton("Send OTP ");
        btnNewButton.addActionListener(new ActionListener() {
            public void actionPerformed(ActionEvent e) {
                String email = mail.getText();
                char[] pswd = pswdf.getPassword();
                char[] rpswd = rpswdf.getPassword();
                StringBuffer sb = new StringBuffer();
                for (int i = 0; i < pswd.length; i++) {
                    sb.append(pswd[i]);
                }
                String password = sb.toString();
                StringBuffer sb1 = new StringBuffer();
                for (int i = 0; i < rpswd.length; i++) {
                    sb1.append(rpswd[i]);
                }
                String rpassword = sb1.toString();
                if (email.trim().isEmpty()) {
                    JOptionPane.showMessageDialog(null, "Email field cannot be empty");
                } else if (password.trim().isEmpty()) {
                    JOptionPane.showMessageDialog(null, "Password field cannot be empty");
                } else if (rpassword.trim().isEmpty()) {
                    JOptionPane.showMessageDialog(null, "Re-enter password field cannot be empty");
                } else {
                    if (password.equals(rpassword)) {

                        Random rand = new Random();
                        int random = rand.nextInt((9999 - 100) + 1) + 10;
                        rnd = random;
                        sende(email, random);
                        JOptionPane.showMessageDialog(null, "OTP send to the mail");
                    } else {
                        JOptionPane.showMessageDialog(null, "Password and Re-entered password are not same");
                        // actionPerformed(rand);

                    }
                }

            }
        });
```

Fig. 17. Main Menu Code of the CUI Program

VI. RESEARCH STUDY WITH OUTPUTS

To find out the more appropriate result of the performance of both the CUI and GUI interfaces we conducted the t-test based upon the data which has been collected during the performance analysis of the program with the help of different software.

t-test: -is a statistical hypothesis test which follows a distribution in null hypothesis.

Formula

$$\mathit{Two - sampled\ test}\ t = \frac{\bar{x}_1 + \bar{x}_2}{sx_1x_2\sqrt{{}^{1}/_{n_1} + 1}\Big/ n_2}$$

$$df = n_1 + n_2 - 2$$

t-Test: Two-Sample Assuming Equal Variances		
	20	*43*
Mean	13.75	18
Variance	122.9167	238
Observations	4	4
Pooled Variance	180.4583	
Hypothesized Mean Difference	0	
df	6	
t Stat	-0.44742	
P(T<=t) one-tail	0.335136	
t Critical one-tail	1.94318	
P(T<=t) two-tail	0.670271	
t Critical two-tail	2.446912	

Table 5. Statistical Result of t-test

Based upon the test we got the p value > 0.5 which shows that the CUI interface is 67% better performing and faster and more reliable than the GUI based interface.

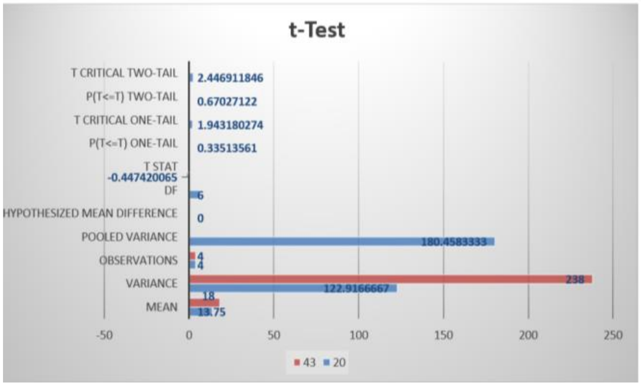


Fig. 18. New User Code of CUI Program(extended)

Graphical User Interface (GUI)

Fig. 19. Performance Utilization of GUI

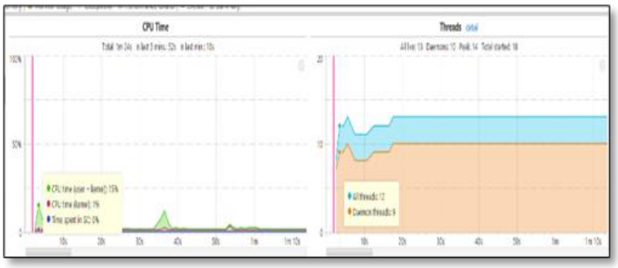
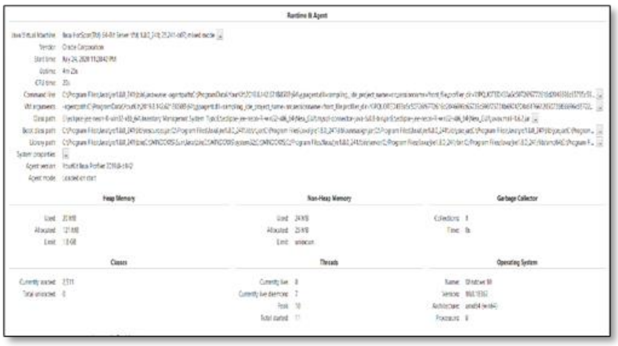


Fig. 20. CPU Utilization of GUI

Character User Interface CUI


Runtime & Agent

Vendor: Oracle Corporation

Command line: [illegible]

VM arguments: [illegible]

Class path: [illegible]

Boot class path: [illegible]

Library path: [illegible]

System properties

Agent version: [illegible]

Agent mode: [illegible]

Heap Memory: Used, Allocated, Limit

Non-Heap Memory: Used, Allocated, Limit

Garbage Collector: Collections, Time

Classes: Currently loaded, Total unloaded

Threads: Currently live, Currently live daemons, Peak, Total started

Operating System: Name, Version, Architecture, Processors

Fig. 21. CPU Utilization of GUI

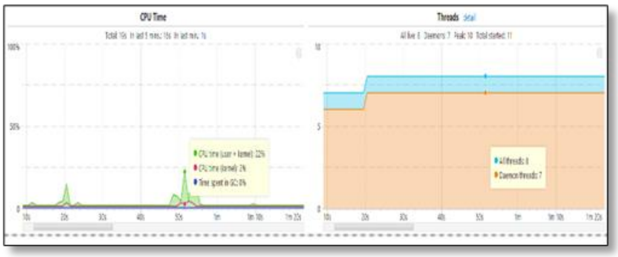


Fig. 23. CPU Utilization of GUI

CONCLUSION

Based upon the entire research work and checking the performance of the program using the Your Kit Java profiler in which we compared the CPU usage of CUI and GUI in which we found out that the program was better performing in the CUI interface , using the same software we also checked the heap memory of the program in which we found out that CUI was using much less heap memory than the GUI interface of the program on further checking the different parameters of the program such as the garbage collection we found out that CUI had the lowest garbage collection over the GUI interface , the CUI interface of the program used much less no of threads than the GUI interface of the program and also the run time of both the CUI and GUI interface when compared we found out that CUI just took 4minutes.25seccond as compared to GUI which took 7minutes.25seconds for the entire program to run .Looking at the results we got from comparing both the CUI and GUI interface we can say that although the GUI interface of the also be changed if needed but still the CUI interface of the program is faster and better performing and will be much more reliable to use .

ACKNOWLEDGMENT

We have taken the support of various research work done by researchers and published papers. We would like to thank all of them as their research work has provided the insight and expertise to us and their work has helped us to complete my research. I would like to thank to my children and family members who cooperated with me during this pandemic and given us well sufficient time to perform research. We would like to thank various REST videos, as the guidance given by them helped me during the course of writing this research paper. I am immensely grateful to the reviewers for their comments on an earlier version of the manuscript, although any errors are my own and should not tarnish the reputations of these esteemed

Reference

[1] Performance Monitoring Of JAVA Application

[2] Analyzing the Complexity of Java Programs using Object Oriented Software Metrics.

[3] Dynamic analysis of Java program concepts for visualization and profiling

[4] Apache Software Foundation, Log4J

[5] S. Browne, J. Dongarra, N. Garner, G. Ho, P. Mucci, A Portable Programming Interface for Performance Evaluation on Modern Processors, The International Journal of High-Performance Computing Applications 14, 3:189-204 (Fall), 2000.

[6] M. Dahm, The Byte Code Engineering Library, 2001.

[7] E. Gamma, R. Helm, R. Johnson, J. Vlissides, Design Patterns: Elements of Reusable Object-Oriented Software, Addison-Wesley, 1995.

[8] J. Gosling, B. Joy, G. Steele, The Java Language Specification, Addison-Wesley, 1996.

[9] C.A.R. Hoare, Monitors: An Operating System Structuring Concept, Comm. ACM 17, 10:549-557 (October), 1974.

[10] M. Henning, S. Vinoski, Advanced CORBA Programming with C++, ISBN 0201379279, Addison-Wesley, 1999.

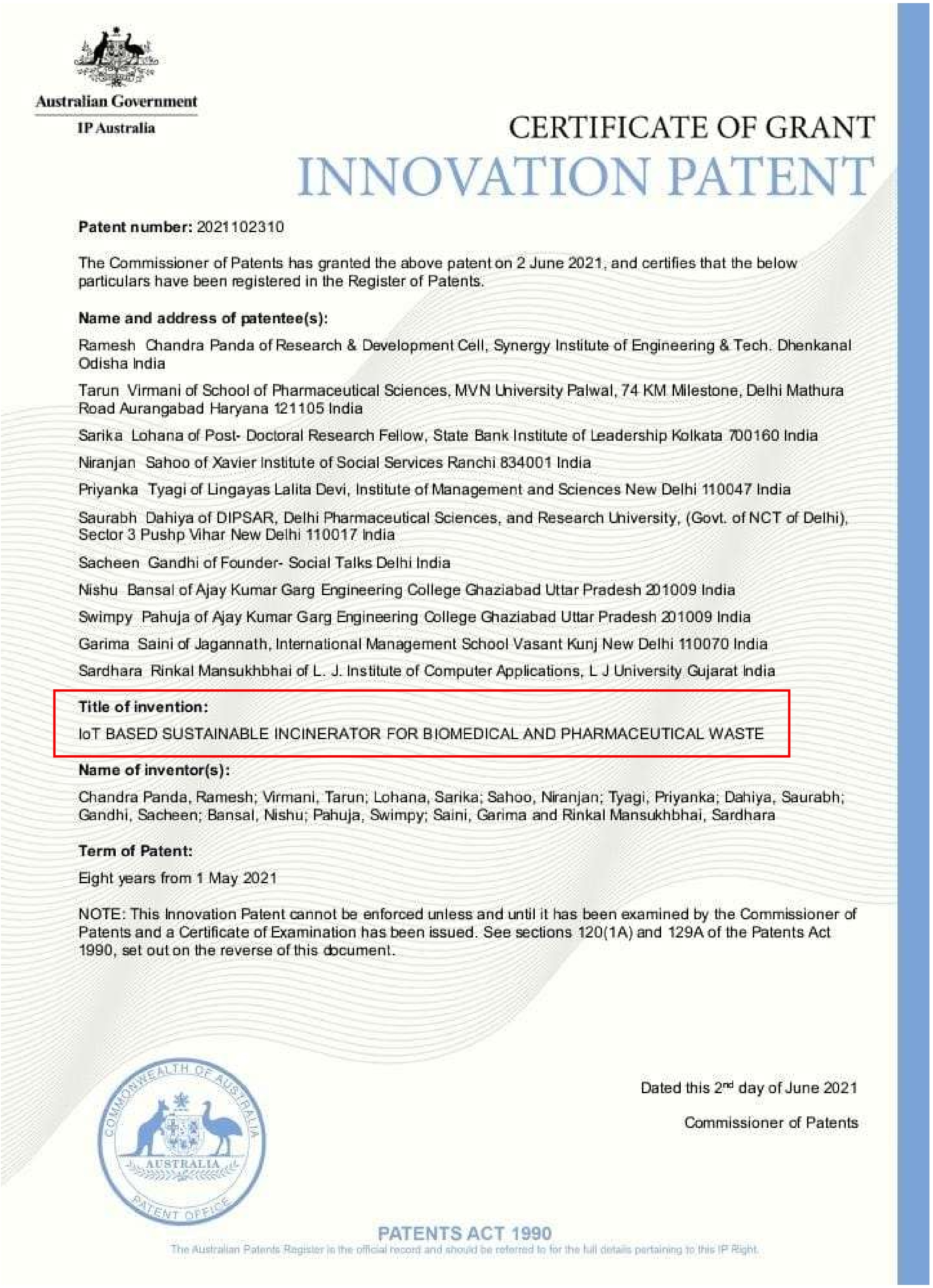
[11] IBM Research, Jinsight project,2001.

[12] Intel, VTune Performance Analyzer,2001.

[13] Intel Corporation, Intel Architecture Software Developer's Manual Volume 3: System Programming Guide, 1997.

[14] IONA Technologies, Object Oriented Concepts Inc., ORBacus 4 for Java, 2000.

[15] R, Jain, The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling, John Wiley & Sons, 1991.



Australian Government

IP Australia

CERTIFICATE OF GRANT
INNOVATION PATENT

Patent number: 2021102310

The Commissioner of Patents has granted the above patent on 2 June 2021, and certifies that the below particulars have been registered in the Register of Patents.

Name and address of patentee(s):

Ramesh Chandra Panda of Research & Development Cell, Synergy Institute of Engineering & Tech. Dhenkanal Odisha India

Tarun Virmani of School of Pharmaceutical Sciences, MVN University Palwal, 74 KM Milestone, Delhi Mathura Road Aurangabad Haryana 121105 India

Sarika Lohana of Post- Doctoral Research Fellow, State Bank Institute of Leadership Kolkata 700160 India

Niranjan Sahoo of Xavier Institute of Social Services Ranchi 834001 India

Priyanka Tyagi of Lingayas Lalita Devi, Institute of Management and Sciences New Delhi 110047 India

Saurabh Dahiya of DIPSAR, Delhi Pharmaceutical Sciences, and Research University, (Govt. of NCT of Delhi), Sector 3 Pushp Vihar New Delhi 110017 India

Sacheen Gandhi of Founder- Social Talks Delhi India

Nishu Bansal of Ajay Kumar Garg Engineering College Ghaziabad Uttar Pradesh 201009 India

Swimpy Pahuja of Ajay Kumar Garg Engineering College Ghaziabad Uttar Pradesh 201009 India

Garima Saini of Jagannath, International Management School Vasant Kunj New Delhi 110070 India

Sardhara Rinkal Mansukhbhai of L. J. Institute of Computer Applications, L J University Gujarat India

Title of invention:

IoT BASED SUSTAINABLE INCINERATOR FOR BIOMEDICAL AND PHARMACEUTICAL WASTE

Name of inventor(s):

Chandra Panda, Ramesh; Virmani, Tarun; Lohana, Sarika; Sahoo, Niranjan; Tyagi, Priyanka; Dahiya, Saurabh; Gandhi, Sacheen; Bansal, Nishu; Pahuja, Swimpy; Saini, Garima and Rinkal Mansukhbhai, Sardhara

Term of Patent:

Eight years from 1 May 2021

NOTE: This Innovation Patent cannot be enforced unless and until it has been examined by the Commissioner of Patents and a Certificate of Examination has been issued. See sections 120(1A) and 129A of the Patents Act 1990, set out on the reverse of this document.

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

Dated this 2nd day of June 2021

Commissioner of Patents

PATENTS ACT 1990

The Australian Patents Register is the official record and should be referred to for the full details pertaining to this IP Right.

Australian Government

IP Australia

CERTIFICATE OF GRANT
INNOVATION PATENT

Patent number: 2021102487

The Commissioner of Patents has granted the above patent on 16 June 2021, and certifies that the below particulars have been registered in the Register of Patents.

Name and address of patentee(s):

Priyanka Tyagi of Lingayas Lalita Devi, Institute of Management and Sciences New Delhi Delhi 110047 India

Anisha C. D. of PSG College of Technology, Peelamedu Coimbatore Tamilnadu 641001 India

Arun Kumar of Prerna Society of Technical Education, and Research New Delhi Delhi 110092 India

Nishu Bansal of Ajay Kumar Garg Engineering College Ghaziabad Uttar Pradesh 201009 India

Garima Saini of Jagannath, International Management School, Vasant Kunj New Delhi Delhi 110070 India

Divya Sharma of Lingayas's Vidyapeeth, Nachauli, Jasana Road, Old Faridabad Faridabad Haryana 121002 India

Kajol Rana of Jagannath, International Management School, Vasant Kunj New Delhi Delhi 110070 India

Surabhi Singh of Institute of Management Studies, GT Road, Lal Kuan Ghaziabad India

Bijendra Kumar of Department of Civil Engineering, Bakhtiyarpur College of Engineering, Dedaur, Bakhtiyarpur Patna 803212 India

Chintan Ajaybhai Shah of Bhagwan Mahavir, College of Business Administration (BBA), BMEF Campus, VIP Road Vesu, Surat Gujarat 395007 India

Sanjay Ramkrishna Bhoyar of Department of Mathematics, Phulsing Naik Mahavidyalaya Pusad Maharashtra 445216 India

Shanti Verma of L. J. Institute of Computer Applications, L.J. University Ahmedabad Gujarat India

Ramesh Chandra Panda of Research & Development Cell, Synergy Institute of Engineering & Tech. Dhenkanal Odisha 759001 India

Title of invention:

ARTIFICIAL INTELLIGENCE BASED SURVEILLANCE SYSTEM FOR OXYGEN CONCENTRATOR AT INVENTORY LEVEL

Name of inventor(s):

Tyagi, Priyanka; C. D., Anisha; Kumar, Arun; Bansal, Nishu; Saini, Garima; Sharma, Divya; Rana, Kajol; Singh, Surabhi; Kumar, Bijendra; Ajaybhai Shah, Chintan; Ramkrishna Bhoyar, Sanjay; Verma, Shanti and Chandra Panda, Ramesh

Term of Patent:

Eight years from 12 May 2021

Dated this 16th day of June 2021

Commissioner of Patents

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

PATENTS ACT 1990

The Australian Patents Register is the official record and should be referred to for the full details pertaining to this IP Right.

Australian Government
IP Australia

CERTIFICATE OF GRANT
INNOVATION PATENT

Patent number: 2021102487

NOTE: This Innovation Patent cannot be enforced unless and until it has been examined by the Commissioner of Patents and a Certificate of Examination has been issued. See sections 120(1A) and 129A of the Patents Act 1990, set out on the reverse of this document.

Dated this 16th day of June 2021

Commissioner of Patents

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

PATENTS ACT 1990

The Australian Patents Register is the official record and should be referred to for the full details pertaining to this IP Right.

Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, June 2021:342- 362

Research Article

Approach of Malicious Nodes and Environmental in Vehicular Ad-Hoc Networks

GarimaSaini[1], Dr.Javalkar Dinesh Kumar[2]

Abstract

Vehicular Adhoc Network (VANET), a specialized form of MANET in which safety is the major concern as critical information related to driver's safety and assistance need to be disseminated between the vehicle nodes. The security of the nodes can be increased, if the network availability is increased. The characteristics of VANETs, such as high mobility, network partitioning, intermittent connectivity and obstacles in city environments, make routing a challenging task. Due to these characteristics of VANETs, the performance of a routing protocol is degraded. The position-based routing is considered to be the most significant approach in VANETs.

The availability of the network is decreased, if there is Denial of Service Attacks (DoS) in the network.. This technology establishes connection among cars about 100 to 300 meters of each other and, thus, generates a wide-ranging network. In the current scenario, remarkable growth in the vehicles' quantity deployed with computational tools and wireless devices has contributed in the evolution of new application strategies that were impossible in the past. in this paper , DoS affects network performance greatly with regard to throughput and other metrics. threshold- based technique is devised for eradicating adversaries from the vehicular network. The proposed algorithm was NS2 simulator for applying the new approach and outcomes are compared in terms of routing overhead, throughput and packetloss. It is analyzed that in terms of every parameter new approach works more effciently in contrast to the approaches presented in the past.

Keywords* – *VANETs; DoSattacks; Packet detection; malicious nodes; irrelevant data

[1]Research Scholar,LingayasVidhyapeeth,Faridabad, Haryana, India.
[2]Assistant Professor of Computer Science,LingayasVidyapeeth,Faridabad, Haryana, India

Received Accepted

Introduction

A Vehicular Adhoc Network (VANET) is remarkable achievement towards road safety with various state-of-artsafety applications. A VANET is self organized network which enable Vehicle-to-Vehicle and Vehicle-to-Infrastructure communication for the exchange safety messages. This network probably will play a major role for enabling comfortable traffic system on roads and will also help in avoiding unnatural traffic mishaps. The short range radios are being installed in all the communicated nodes. The transmission range between the vehicle nodes is very short that is less than 300mThilak (2016) . Road Side Units(RSU) are installed randomly depending on the categorization of the network in that specific area. The authorities and vehicle nodes can communicate through RSU.

The automobile industry is growing day by day. Vehicular ad-hoc network (VANET) is a part of ITS which provides security, traffic efficiency and ease to the user. Vehicular network is a subclass of mobile ad-hoc network (MANET) in which vehicle acts as a mobile node in the network (Arya and Tripathi2013). Vehicles can communicate and transfer messages with other vehicles as well as roadside units using the VANET. In VANET multiple vehicles are connected in ad-hoc fashion for exchanging the useful information. VANET is the main part of Intelligence transportation system (ITS). It uses the WAVE (wireless access for the vehicular environment) technology based on the IEEE 802.11p standard (Ltifi et al. 2015). Two main parts of the vehicular network are Smart vehicles installed with the onboard unit (OBU) and roadside units. Mainly two types of communication possible in VANET first is communication between vehicle to vehicle (V2V) and second is communication between vehicle and roadside infrastructure (V2I). In VANET vehicles has a limited range for the transmission of messages, so it uses multi-hop communication to transfer the messages using different routing algorithms. In multi-hop data transfer one has to rely on other nodes also. So security and routing are the two major issues in the vehicular ad-hoc network. Every-one needs to secure the vehicular network from the insider and outsider attackers. Our proposed model detects the rouge nodes inside the network with the use of lightweight trust based algorithm. Selection of the observer node minimizes the load on all the nodes. Proposed work detects the faulty nodes with less overhead and complexity. Var-ious other proposed pre-existing models provide security with lots of complexity and overheads (Yao et al. 2017). To minimize the overhead we use the entity-centric trust-based model with the selection of the observer node. Various abbreviations used in this article are defined in Table 1.

Table 1. Abbreviation used

Abbreviation	**Full name**

VANET	Vehicular ad-hoc network
BH	Black hole
NS	Network simulator
DOS	Denial of service
AODV	Ad-hoc on-demand distance vector
PDF	Packet delivery fraction
ITS	Intelligence transportation system
DSR	Dynamic source routing
RSU	Road side unit
NRL	Normalized routing load
DSDV	Destination sequenced distance vector

Various authors (Kerrache et al. 2016a, b; Khan et al. 2015; Li and Song 2016; Ltifi et al. 2015) use the trust-based solutions to find the trustable and rouge node in the network. As trust based algorithms require fewer calculations and can per-form better if the attacker is from inside the network. In trust-based model authors mainly use the concept of direct trust, recommendation trust and historical trust (Kerrache et al. 2016a, b) as well. The other alternative security mechanism that used most widely is cryptography based model to secure the communication network. Cryptography based solution provides security from internal and outsider intruder. These types of solutions increase the complexity of the model in terms of calculation overhead. Some authors use cryptography-based solutions (Kumar and Maheshwari2014; Lim and Manivannan2016; Pooja et al. 2014) to ensure the security of the vehicular network. As we know cryptography-based solutions require more cal-culations to implement the algorithm so it creates some delay in the transfer of messages due to large calculations. But it covers all types of attacks in the vehicular network. Some authors (Khan et al. 2017; Kumar and Chilamkurti2014; Mokdad et al. 2015; Sedjelmaci et al. 2014; Tyagi and Dembla2016; Zaidi et al. 2016) proposed intrusion detection and prevention schemes to detect the faulty or attacker node present in the vehicular network.

VANET will be responsible for improved traffic safety and driver assistanceMallaet al. (2013). In VANETs, vehicles send alert in the network regarding road conditions, collision ahead, traffic jam, weather conditions and location based services such as parking area nearby etcZeadallyet al. (2010).The data which is received from the nodes is forwarded toother nodes after checking its reliability. The reliability ischecked by the devices acting as communicators. These needs tobe checked as the data or messages which are received are notuseful for all the nodes. The decisions related to usefulness ofthe received data need to be made by the communicatordevicesZeadallyet al. (2010).

High mobility, dynamic mobility, regular disconnection, restricted bandwidth, attenuations, limited transmitting capacity, energy storage, and computing are just a few of the VANET characteristics that set them apart.

In the VANET model, various types of entities are involved. Vehicle nodes are the most important of the different organizations included since they perform the most basic and important roles of communication. They are capable of communicating in a variety of situations. However, in order to understand how VANET works, all of the various entities and how they communicate with one another must be thoroughly discussed and studied.

Malicious Nodes

Vehicular ad-hoc network (VANET) is the application of traditional mobile ad hoc network (MANET) in traffic road. As a new type of multi-hop wireless communication network, VANET has become a research hotspot in recent years. With-out centralized management, each vehicle in VANET acts as both a wireless router and a network node to maintain the communication of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Through the frequent interaction of real-time data on road conditions by wireless sensors, vehicles can obtain road conditions [3] like congestion, icing, accidents or other transport incidents in advance, so the safety of vehicles is well guaranteed. However, the great openness of VANET makes it more vulnerable to various attacks than traditional networks. For attackers outside VANET, security schemes based one ncryption and authentication can be a good solution.

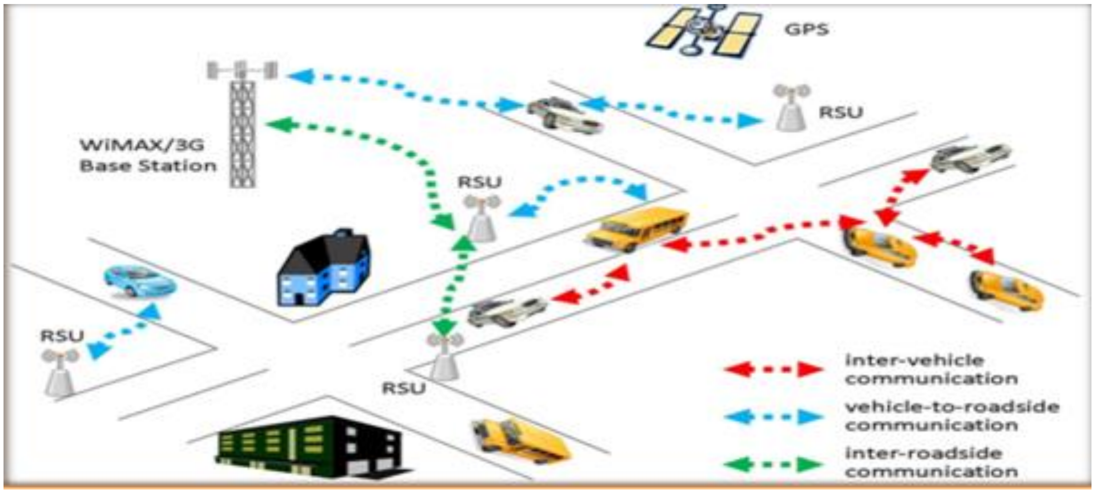
Nevertheless, these defensive schemes have no effect on the attacks inside VANET. Attacks inside VANET can greatly impede data interaction between vehicles. Because messages between vehicles contain the key information of life safety, itis of great significance to identify malicious nodes in VANET so as to ensure the success of communication. To cope with the threat brought by malicious nodes inside VANET efficiently, reputation-based malicious node identification schemes have been proposed and gains ever-growing attention. The source nodes identify a node whether it is malicious based on its reputation and then choose a satisfying route for communication. Based on that, a series of work have been conducted: Wenjia Li et al. focus on the data trust and node trust simultaneously to identify malicious nodes; Chakeret al. propose a solution based on the adaptive detection threshold to identify malicious behaviors. employ theTrusty Dynamic Software Agent (TDSA) to eliminate black hole attacks from VANET; Watchdog model is proposedto detect black hole attacks. ID-Based signature, Hash MessageAuthentication Code (HMAC) and RSA based algorithm[11] are used in the trust model to detect malice and integratemassages. study the influence on SAODV and ARAN caused by black hole attacks. Reputation-based schemes in and pay attention to the problem of slander and harboring.However, these methods still have many shortcomings and limitations, such as only effective for specific attack, high computational complexity and poor scalability. In conclusion, the existing schemes have the following major drawbacks:•Many methods like only take one specific at-tack behavior into account. Consequently, these methods are only effective for specific attack mode and lacking in good scalability.• Some researches such as attempt to secure the exchange of information based on cryptography, which contributes to the high cost in terms of computational complexity and mobility adaptation

.•Schemes like MOO and FGT-OLSR calculate the reputation of nodes by combining direct and indirect reputation, but these methods ignore the feedback of communication results. This leads to the low efficiency and effectiveness.

VANETs in the Urban Environment

The vehicular ad-hoc network (VANET) is also called network on wheels, which is used to provide communication between vehicular nodes. It is an offshoot of mobile ad-hoc networks. In VANETs, vehicular nodes are self-organized and communicate with each other in aninfrastructureless environment . Knowing the importance of vehicular ad-hoc network for providing safety-related applications in Intelligent Transportation System (ITS), the IEEE committee has developed the IEEE 802.11p standard for VANETs [1]. The US Federal Communication Commission (FFC) department has assigned 75 MHz of bandwidth at 5.9 GHz for dedicated short-range communication (DSRC), which is used to provide communications between vehicle to vehicle and vehicle to infrastructure . The main aim of VANETs is to build an intelligent transportation system. DSRC can play an important role in building communications between vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). The range of DSRC is about one thousand meters . From the last few years, inter-networking over VANETs has been achieving massive momentum. Realizing its intensifying significance, academia, major car manufacturers, and governmental institutes are making efforts to develop VANETs. Various significant projects are initiated by different countries and famous industrial firms such as Daimler-Chrysler, Toyota, and BMW for inter-vehicular communications. Some of these prominent projects include CarTALK2000 , Car-to-Car Communication Consortium (C2CCC) [10], Advanced Driver Assistance Systems (ADASE2), California Partners for Advanced Transit and Highways (California PATH) , FleetNet , DEMO 2000 by Japan Automobile Research Institute (JSK) , Chauffeur in EU , and Crash Avoidance Metrics Partnership (CAMP) . These developments are a key step toward the recognition of intelligent transportation services.

The position-based routing protocols use the geographical position of source and destination to accomplish communication between them destination to accomplish communication between them. Every node is aware of its position due to global positioning system (GPS). The position of the neighboring node is found through beacons exchange. The position of the destination node is found using location services. When source node or intermediate node wants to send data to the destination node, if the destination node is in its transmission range than it directly forwards packet to the destination node. If the destination node is not in the transmission range it will forward the packet to a neighbor node that is the nearest to the destination node. In this way, the packet is relayed to destination [8,15–18]. In position-based routing, every node maintains one-hope neighbor information. Existing position-based routing protocols are developed for highway environment and urban environment. The highway environment consists of straight roads architecture without obstacles. On the other hand, urban environment consists of obstacles in the form of buildings. It is composed of streets and junctions. The points where two or more streets meet each other are called junctions. The data packets are routed towards destination through a set of junctions .The routing of data in an urban environment is challenging because of obstacles. In the existing literature, there are many position-based routing protocols proposed for V2V and V2I communications considering the urban environment.


GPS
WiMAX/3G
Base Station
RSU
RSU
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

The architecture of VANET in two separate environments is shown in Figure 1.

a) Infrastructure environment:

Many of the organizations in the network are permanently interconnected in the infrastructure environment. The agencies present manage all types of traffic and external services. Manufacturers, legal authorities, (trusted third party) TTP, service providers, and manufacturing processes all play a role in the infrastructure environment. VANET models sometimes provide legal authority Sari et al. (2015).

Despite the fact that each country's laws and regulations vary, there are two main tasks: vehicle registration and offence reporting. Any vehicle in the administrative region receives a license plate after it is manufactured. TTP is also a part of this ecosystem, providing services such as credential management and time stamping. In VANET, service providers are also taken into account. Location Based Services (LBS) Fuentes et al. (2010)are among the services available.

b) Adhoc environment:-

In this type of network, vehicles and RSUs communicate on a regular basis. All of the vehicle nodes in this setting have three separate devices: an On Board Unit (OBU), a series of sensors, and a Trusted Platform Module (TPM). V2V and V2I communication is done by OBUs. With the assistance of sensors, knowledge about the status that can be exchanged with other vehicle nodes is communicated and judged Fuentes et al. (2010) .This method of contact contributed to improved road safety. TPM, which is installed on cars, can be used to store user credentials and crash information Papadimitratoset al. (2006) .

Attacks on Denial of Service (DOS)

The attacker attacks the communication medium to trigger a channel jam in this attack. The channel will no longer be open to nodes, and they will be unable to reach itLa and Cavalli(2014) .The basic concept is to overburden the network with traffic, rendering the network and services inaccessible to legitimate nodes. The vehicle nodes and network infrastructure would be destroyed and overworked as a result of this.

The network would be unable to execute accurately, denying services to authentic nodes and performing other tasks that are irrelevant Hasbullahet al. (2010)Insiders and outsiders are also capable of attacking VANETs.

The main goal is to make the network inaccessible to legitimate users. This can be accomplished by flooding the control channel with a large number of irrelevant messages. A DoS attack has a significant impact on main resources such as bandwidth, CPU, and memory. Attackers can disrupt the network and launch a DoS attack by jamming channels, overloading servers, or falling packets.

The different stages of DoS attacks are listed below:-

A. Basic Level: Overwhelm the Node Resources:-

The attacker's main goal is to use the network's resources so that legitimate users can no longer use them. As a result, the vehicle nodes in the network are unable to perform all of the essential and appropriate activities, and information cannot be shared between them.

Case 1:

DoS attack in V2V Communication: In this scenario, the attacker sends out a warning message about an accident at a specific venue. The victim node, which is behind the attacker node, receives the post. However, the sender node will continue to send messages because its aim is to keep the attacked node occupied with the verification process rather than doing useful work.

Case 2:

DoS attack on V2R communication: In this case, the attacker targets the RSU (Road Side Unit), The RSU will be preoccupied with verification proofs and will not be able to assist the nodes in their contact efforts. The RSU will no longer be accessible to the network's vehicle nodes. Knowledge about human protection and lives will not be transmitted to network nodes, which can be dangerous in some cases Hasbullahet al. (2010).

A. Extended Level: - Jamming the Channel: - In this situation, the intruder jammed the communication channel, making it unavailable for all other nodes in the network to communicate.

- Case 1:

In this scenario, the intruder sends a high-frequency channel to jam communication between any vehicles at random. Due to this attack, vehicles in this domain will be unable to send or receive messages. If they leave the attack domain, they can send and receive messages Hasbullahet al. (2010).

Case 2: Due to a jammed communication path, communication between the vehicles and the RSU is not possible in this case.

In this scenario, an attacker attacks the infrastructure to jam the channel, making it impossible to send or receive messages to/from the nodes and the RSU due to the inaccessible network Hasbullahet al. (2010).

I. Background

VANET is an infrastructure less architecture with various heterogeneous technologies used for wired and wireless communication to provide the intra-vehicle and inter-vehicle communication. Detailed overview of Architecture of VANET, Routing in VANET, Security Challenges and Applications of VANET discussed in the following subsections:

Table 2 Comparison of various proposed security schemes on VANET

Algorithm	Type of solution	Attack covered	Parameter	Tools	Remark
DOS attack-‘‘signature based authentication’’ in VANETs (Pooja et al. 2014)	Cryptography base (authentication using HMAC)	Inside and outside DOS	Authentication delay	NS-2.34	Not effective if the attacker floods the system with valid signature
Prevention of Sybil attack using ‘‘priority batch verification’’ (Kumar and Maheshwari 2014)	Encryption based	Sybil attack	Encryption time	No simulation	Provide security in a restricted manner
‘‘Trust-based scheme for alert spreading in VANET’’ (Ltifi et al. 2015)	Trust based (Cluster based trust management	False warning	Average delay	NS-3	This solution is totally based on vehicle cooperation

	system)				
ART:’’attack-resistant trust management scheme’’ (Li and Song 2016)	Trust based (trust calculation)	Simple attack, bad mouth attack	Precision, recall, communication overhead	GloMoSim 2.03	Calculate data and node trust, increases overhead
‘‘Hierarchical and adaptive trust based solution for vehicular networks’’ (Kerrache et al. 2016a,b)	Trust based solution based on three level architecture	Dishonest node detection	Detection ratio, end to end delay	NS-2	Complex and more overhead
Detection and prevention system against collaborative attacks (Khan et al. 2017)	Detection and prevention	Worm hole attack	Packet drop rate, false positive rate, detection time	NS-2	Increases the overhead on nodes, Limited to wormhole attack
‘‘Adaptive trust and privacy management framework’’ (Pham and Yeo 2018)	Trust and encryption based method	Internal and external attacks	Detection rate, trust linkability	ONE simulator	Framework address the trade-off between trust and privacy protection
Coupling of privacy and safety in VANETs (Wahid et al. 2019)	Pseudonym and encryption based	Syntactic/ semantic linking attack, Sybil attack etc.	Congestion confirmation delay, entropy of anonymity set	NS-2 and SUMO	Maximizes anonymity level of a moving vehicle as well as maintains the QoS of safety Applications

Algorithms for Detecting Existing Packets

A. Attacked Packet Detection Algorithm(APDA)

Every RSU is equipped with the APDA algorithm, which allows all vehicles to communicate with each other and with RSUs using only this algorithm. This algorithm aided in the identification of vehicle locations in the network.

After the location is detected, it is saved in an RSU for later usage. Devices such as OBU and TAMPERPROOF are installed on each vehicle and store detailed information such as speed and location. The OBU, frequency, and velocity of the vehicles actually aid in the identification of vehicle positions in the network.The algorithm can aid in the identification of malicious nodes by detecting malicious packets. The location saved in RSURoselinMaryet al.(2013) can be used to track down the malicious car.

B. Enhanced Attacked Packet Detection Algorithm(EAPDA)

RSU is used to communicate in this model, and control packets are used to communicate.The EAPDA algorithm was used by RSU to request and verify vehicles.Only vehicles that have been checked by RSU will be given services and network resources, while all nodes that are responsible for DoS attacks by flooding communication channels will be denied access to any network resources.This would improve the network's performance by increasing the availability of network resources to legitimate nodes.During the verification process, DoS attackers are identified.RSU calculates the time at which requests are sent and received, as well as the number of vehicles that send the request, in order to allot time slots to all nodes.

Vehicle id is used by the RSU to monitor a vehicle's future requests.In the time allocated.The number of packets being transmitted from each node will be analyzed by RSU.If a node's rate of sending packets exceeds a threshold value, it is considered malicious and must be removed from the network for successful communicationSingh and Sharma(2015).

C. Malicious and Irrelevant Packet Detection Algorithm(MIPDA)

This algorithm is an improved version of the APDA algorithm.It detects malicious nodes and packets based on frequency, velocity, speed, and road characteristics, just like APDA.Unlike APDA, it detects real packets by taking frequency and velocity values into account.This algorithm improves device security while reducing latency and overhead Quyoomet al. (2015)

Algorithm Proposed

This algorithm will aid networks in resisting DoS attacks, and if the network is attacked by malicious nodes, this algorithm will detect the malicious nodes and remove them from the network.packets that they send through the network.

As a result, this algorithm would aid in the continuous availability of the network for the dissemination of essential life-related knowledge.With the assistance of Road Side Units, this mechanism can aid in the identification of malicious nodes by detecting irrelevant packets (RSU).Each node will communicate with the RSU, allowing the RSU to save each vehicle's details.

Then, when a node sends harmful messages, the vehicle can be detected and tested using the information in RSU about its location.This algorithm is capable of detecting several malicious nodes as well as the meaningless packets they send through the network.This algorithm belongs to the packet detection algorithm category.

A. Algorithm 1: Identification of Multiple Malicious Nodes

Input: Frequency (freq), Velocity (vel), multiple number of nodes (N), threshold value range of freq and vel (low, high)

```
Identify (Malicious Packets and nodes)
Begin
    RSU will track all nodes in the network
    iffreq and vel both high for multiple nodes
        packet is from malicious node.
        track that malicious vehicle.
        drop all the packets sent from them.
    Else if freq and vel both are low,
        packet is irrelevant
    Else freq and vel is between high and low
        packets are genuine and disseminated into network.
    End if
    End if
End
```

There are several nodes in the network. When multiple nodes in a network try to disseminate knowledge, they always communicate via RSU. RSU will examine the frequency and velocity of each node in the network and equate them to the upper and lower bounds of the threshold. If a node's freq and vel are greater than the prescribed range, the node is classified as malicious. Since those nodes are capable of launching DoS attacks, they must be isolated as soon as possible. The RSU keeps track of these nodes, both in terms of their location and the messages they send out into the network. Following their detection, these nodes are disconnected from the network and forbidden from sending any packets to legitimate users. The packets are useless and will not be forwarded in the network to legitimate users if the freq and vel are both big. Malicious nodes send these packets to jam the networks, which can result in a DoS attack at any time. If both the freq and the vel are tiny, these packets aren't from malicious nodes, but instead contain valuable information about the network node or the traffic ahead climate conditions As a result, all packets with this configuration are forwarded to all nodes in the network. So, using the proposed algorithm, we can detect several malicious nodes and distinguish between nodes that send malicious and meaningless packets and nodes that send genuine packets in the network.

The following output parameters were used to evaluate this work:
a) Packet Loss: This is the ratio of packet loss to total packets sent to the destination by any node.Its value is determined by network congestion, which causes packets to fail to reach their destinationMokhtar and Azab (2015) Nethravathy and Maragatham (2016).

b) Network lifetime: A network's lifetime is described as the amount of time that its vehicles are able to successfully route data.

The network's lifespan ends if any amount of nodes run out of energy or lose functionality for any cause.

c) Network Throughput: The value of network throughput is the percentage of data sent from the originator node to the final node in a given amount of time.
The higher the throughput value, the more data is sent between the source and destination.

d) Packet Delivery Ratio: The value of the packet delivery ratio is determined by the accuracy with which packets are delivered from the originator to the destination.It's the ratio of the total number of packets to the number of packets reachedNethravathy and Maragatham (2016)

e) Dead and alive nodes: The number of nodes that stop operating is referred to as dead nodes, while the number of nodes that disseminate information throughout the network is referred to as alive nodes.
The simulation was completed entirely in NS-2. Since the network must deal with several nodes, the first simulation is carried out with just five nodes.

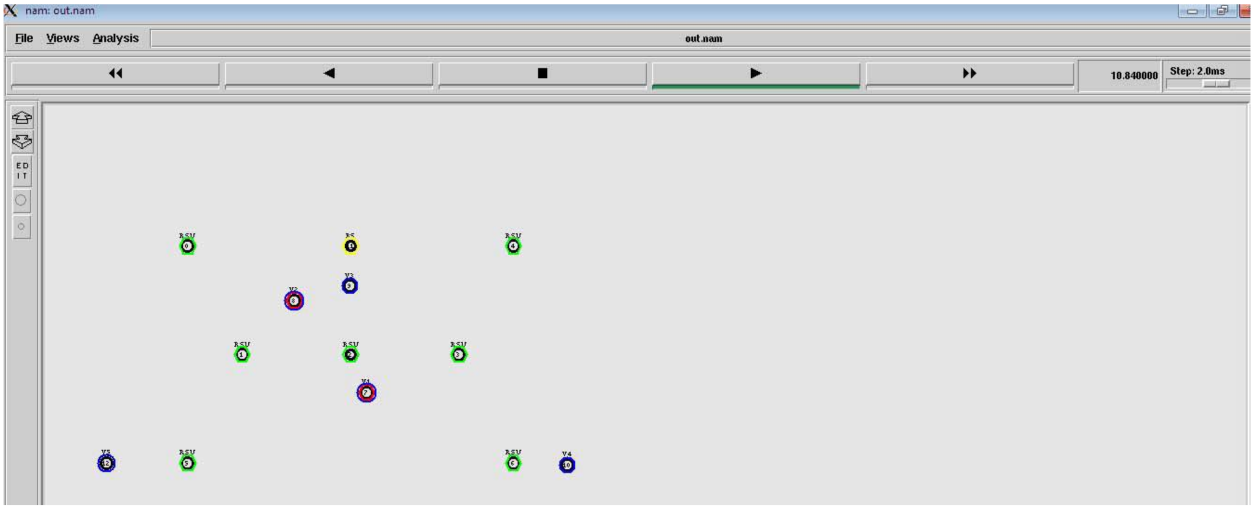


Fig. 2. Multiple nodes in simulation environment

Figure 2 shows the simulation screen in NS-2 which contains number of nodes in the network. All the nodes willcommunicate with each other by disseminating useful information through RSU. The network throughput is shown in Figure 3 which is measured n Gbps (Gigabits per second). and Figure 4 showsthe network lifetime of the network which is increased as the multiple malicious nodes are detected well in time that is during verification time. The network lifetime of the network depends on the time when the network is fully operative.

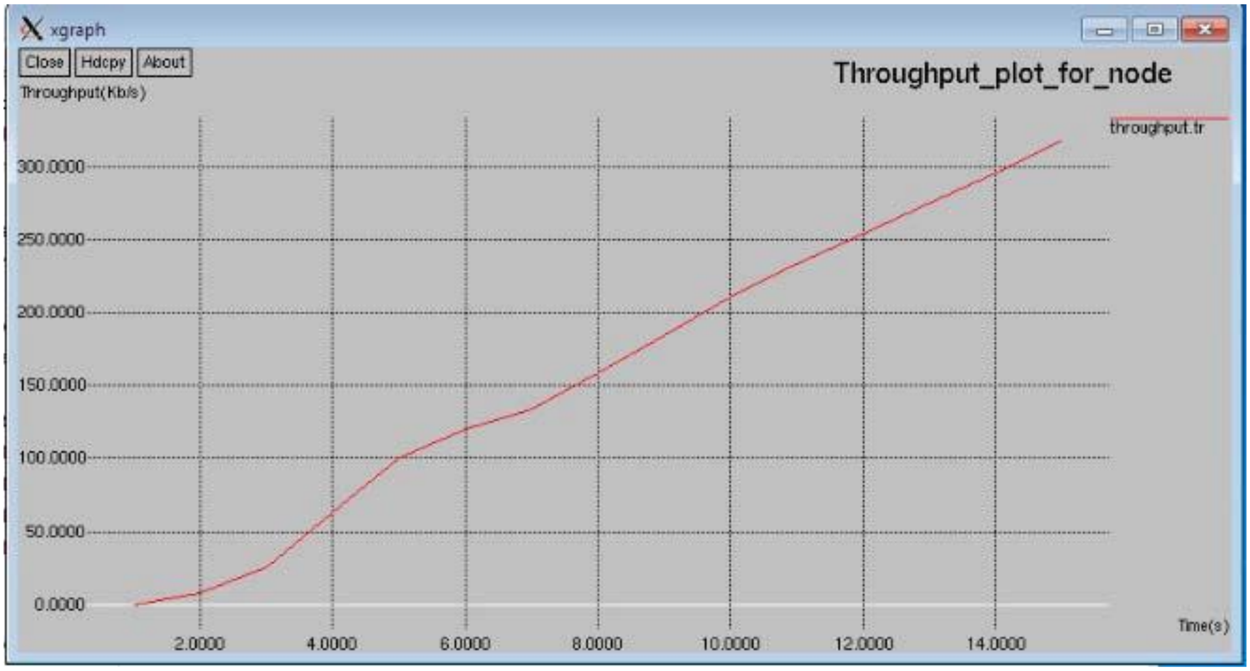


Fig. 3. Network Throughput with 5 nodes in network

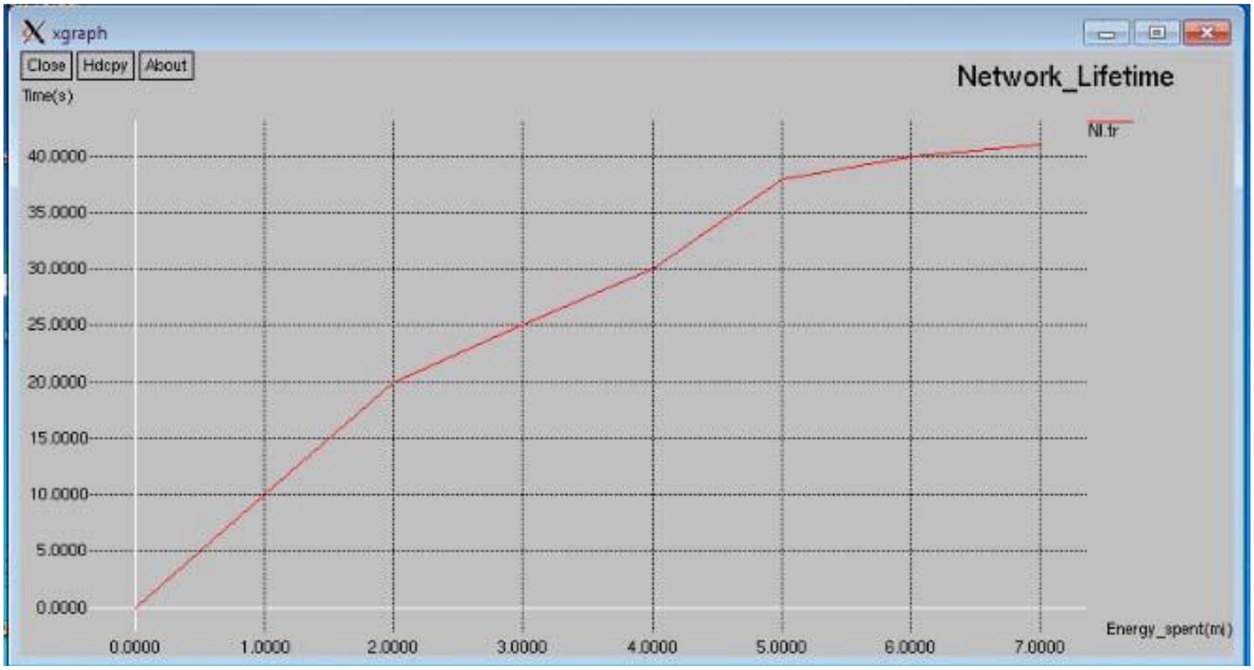


Fig. 4. Network Lifetime

The packet delivery ratio is shown in Figure 5. The graph shows that the packets sent by the sender for destination does not received fully by the destination. Another parameter for the evaluation was packet loss ratio. The packet loss ratio clearly defines the number of packets which does not reach for the destination but are sent by the sender which is shown in Figure 8. Packet Delivery ratio is increased in comparison with the existing techniques that is number of packets that are delivered to the destination from the source is increased. Packet Loss Ratio is decreased as the delivery ratio is increased, the loss ratio will be decreased. That is, the number of packets that are lost during the communication process is very less and all the useful information is disseminated in the network effectively.

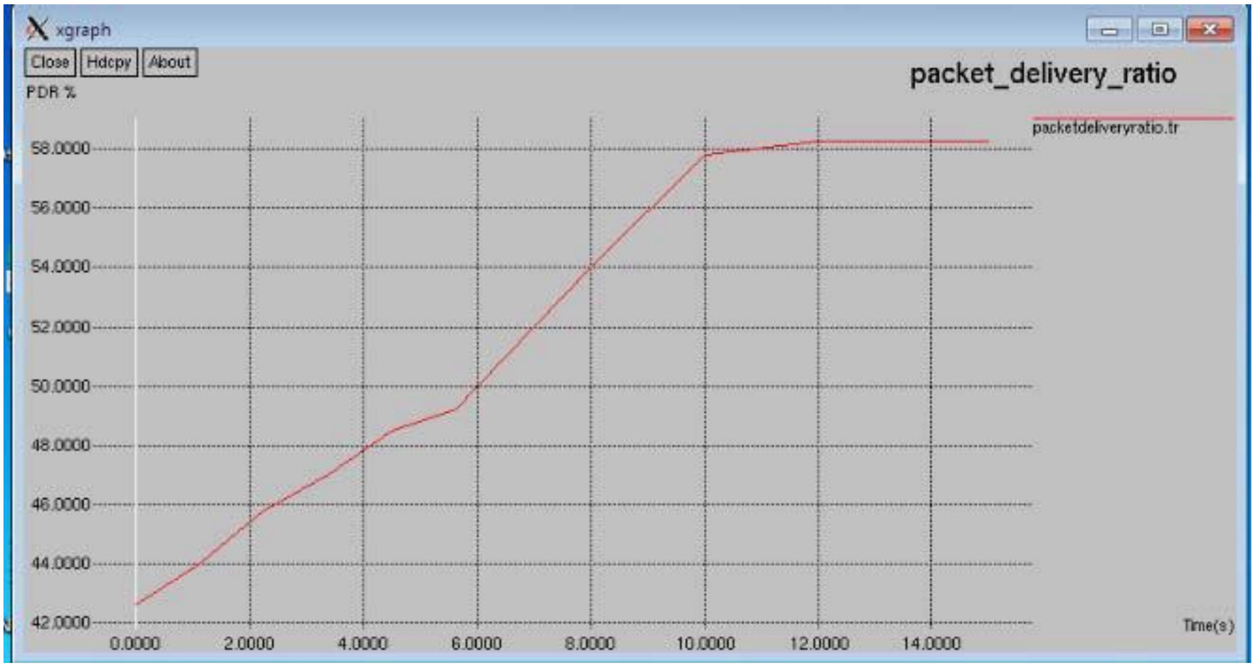


Fig. 5. Packet Delivery Ratio

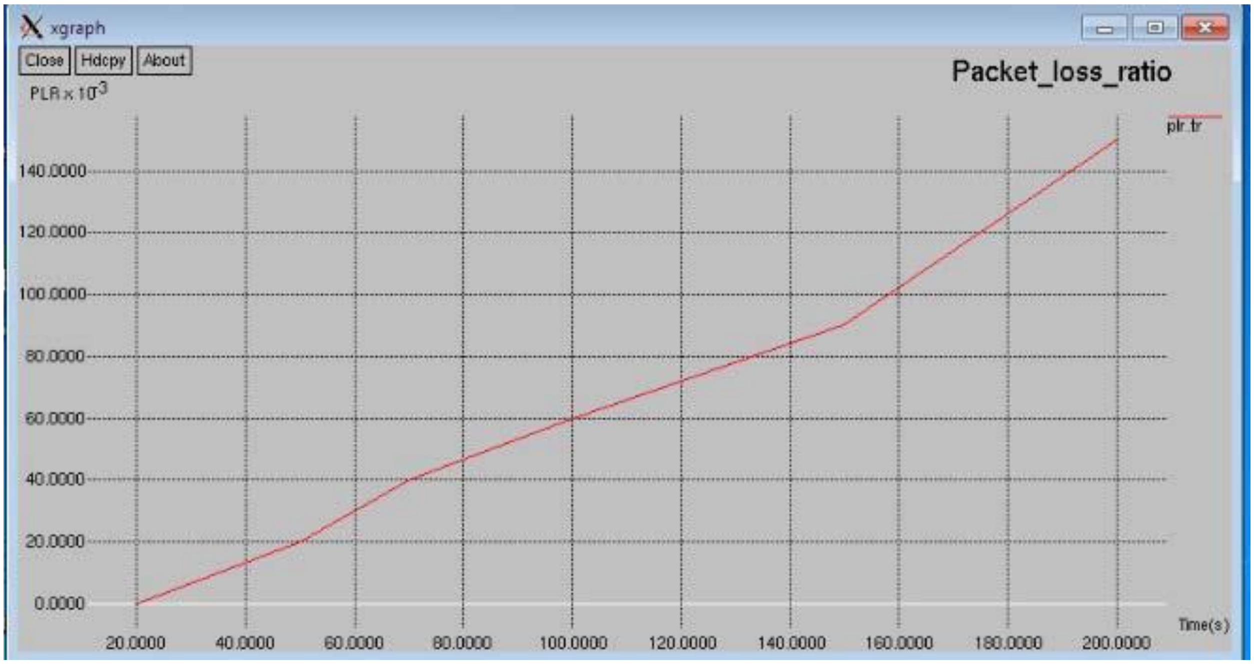


Fig. 6. Packet Loss Ratio

The proposed algorthm for detection of multiple malicious nodes is simulated using different number of nodesthat is taking 5, 8, 10 and 12 number of nodes. Figure7 shows the simulation of 12 nodes with multiple RSUs.

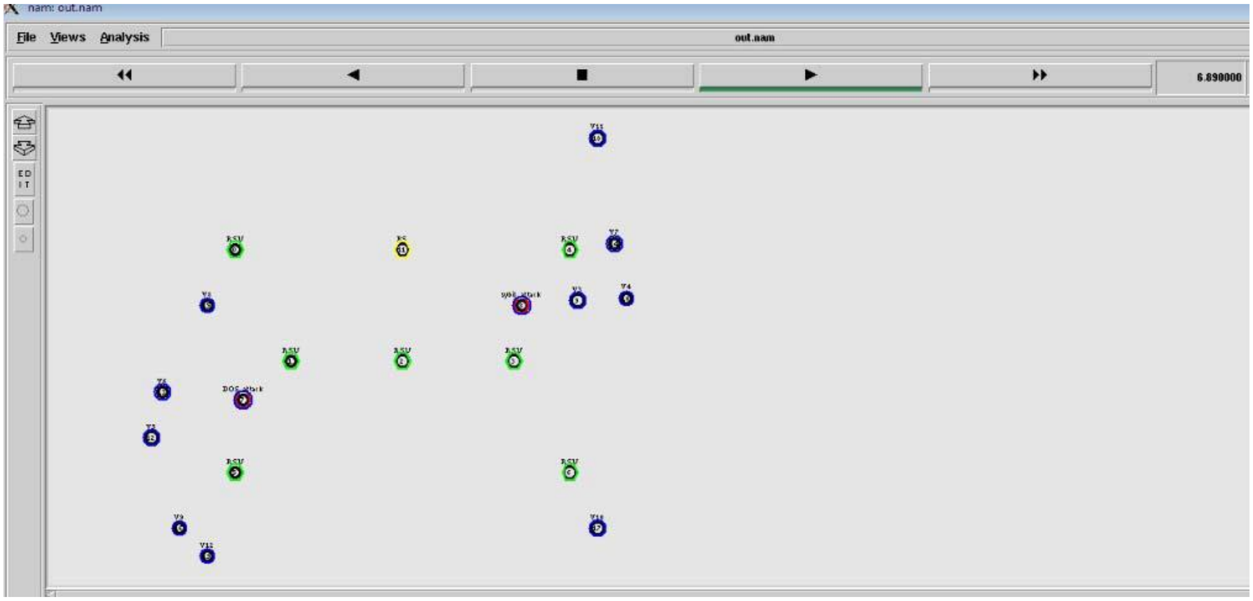


Figure7: Simulation with 12 nodes

The existing algorithm was able to detect single malicious node at one time. Also the RSU was not able to track number of vehicles at same time. But the proposed algorithm is capable of checking multiple malicious nodes at same time and also RSU can communicate with number of nodes at the same time.

TABLE I: PERFORMANCE PARAMETERS TABLE

Number of nodes	Throughput of network	Packet Delivery Ratio	Packet Loss Ratio	Network Life time
5	250	58	300	41
8	300	59	190	39
10	350	62	152	38
12	360	68	130	37.5

The proposed technique is capable for detecting Sybil as well as DoS attacks if implementing on 12 nodes but all other techniques can only detect DoS attack. All the calculated parameters show that the proposed algorithm is far better than the existing one. The throughput of the network is increased; packet delivery ratio is also increased. Although the network lifetime is decreased slightly but the packet loss ratio is decreased dramatically.

Conclusion

On the basis of frequency and velocity, the nodes responsible for attacking the network are described in this paper.This algorithm is capable of detecting both irrelevant and genuine packets.Unlike existing algorithms, which can only detect a single node attacking the network, the algorithm can detect multiple nodes attacking the network. The network's lifespan is extended by detecting intruder nodes in a timely manner. Other output parameters also indicate a significant difference in values, indicating that the proposed algorithm is a better version of current packet detection algorithms.

Reference

K.Thilak,” DoS attack in VANET Routing and possible defending solutions – a survey”, Proc in IntConf on Information Communication and Embedded Systems, IEEE, 2016 doi 10.1109/ICICES.2016.7518892.

A. Malla , R Sahu ., “Security Attacks with an effective solution for DoS attacks in VANETs”

IJCA(0975-8887), Vol 66, No 22, March 2013, pp 45-49.

S. Zeadally, R. Hunt, Y. Chen,A. Irwin, A. Hassan,” Vehicular Adhoc Networks (VANETs):status, results and challenges,” Springer Science and Business Media, LLC 2010, pp 217-241, doi 10.1007/s11235-010- 9400-5.

R. Fotohi , Y. Ebazadeh , M. Seyyar , “A New Approach for improvement security against DoS attacks in Vehicular Adhoc Network”
IJACSA, Vol 7, No.7, 2016, pp 10-16.

H. Hasbullah, I. Soomro, J. Manan, “ Denial of Service (DoS) attack and its possible solutions in VANET”, World Academy of Science, Engg, &Tech., IJECE, Vol 4, Issue 5, 2010, DOI scholar.waset.org/1307-6872/15804.

A. Singh, and P. Sharma, “A novel mechanism for detecting DOS Attack in VANET using Enhanced Attacked Packet Detection Algorithm” Proc. IEEE International Conference RACES,21-22 December, 2015, doi 10.1109/RACES.2015.7453358.

S. RoselinMary , M Maheshwari ., M. Thamaraiselvan , “Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)” Proc. IEEE, ICICES, February 2013, doi 10.1109/ICICES.2013.6508250.

A. Quyoom, Ali, N. Gouttam , H Sharma ,"A Novel Mechanism ofDetection of Denial of Service Attack in VANET using Malicious and Irrelevant Packet Detection Algorithm,'' Proc. IEEE in ICCCA ,pp.414-419, IEEE 2015, doi 10.1109/CCAA.2015.7148411.

K.Thilak,"DoS attack in VANET Routing and possible defendingsolutions – a survey", Proc in IntConf on Information Communicationand Embedded Systems, IEEE, 2016 doi10.1109/ICICES.2016.7518892.

J. Fuentes, A. Tablas, A. Ribagorda,"Overview of security issues inVehicular Adhoc Networks", Handbook of Research on Mobility andComputing, IGI Global, 2010.

P. Papadimitratos, L.Buttyan,J.Hubaux,"Architecture for Secure and Private Vehicular Communcations, 7th International Conference on ITS,pp 1-6.

S. Zeadally, R. Hunt, Y. Chen,A. Irwin, A. Hassan,"VehicularAdhocNetworks (VANETs):status, results and challenges,"Springer Scienceand Business Media, LLC 2010, pp 217-241, doi 10.1007/s11235-010-9400-5.

A. Sari, O. Onursal, M.Akkaya, "Review of the Security Issues inVehicular Adhoc Networks (VANETs)" Int J. Communications, Network and System Sciences, 2015, Vol 8, pp 552-566, doi10.4236/ijcns.2015.813050.

A. Malla , R Sahu ., "Security Attacks with an effective solution for DoSattacks in VANETs" IJCA(0975-8887), Vol 66, No 22, March 2013, pp45-49.

B. Mokhtar, M. Azab, "Survey on Securiy Issues in Vehicular AdhocNetworks" Alexandria Engineering Journal, Science Direct, Vol. 54, Issue 4, December 2015, pp 1115-1126.

V. La, A. Cavalli,"Security attacks and solutions in Vehicular AdhocNetworks – A Survey" Int Journal of Adhoc Networking System, Vol. 4,No. 2, April 2014, doi 10.5121/ijans.2014.4201.

J. Nethravathy, G. Maragatham,"Identifying Malicious Nodes andPerformance Analysis in VANET" Int Journal of Applied EngineeringResearch, Vol. 11, No. 9 (2016), pp 6716-6719.

Arya KV, Tripathi KN (2013) Power aware and secure routing in mobile and ad-hoc networks. In: 2013 IEEE 8th international conference on industrial and information systems, pp 477–482 Bedi P, Jindal V (2014) Use of big data technology in vehicular ad-hoc networks. In: International conference on advances in computing, communications and informatics (ICACCI), pp 1677–1683

Eiza MH, Ni Q, Owens T, Min G (2013) Investigation of routing reliability of vehicular ad hoc networks. EURASIP J WirelCommunNetw 1(1):179.

Issariyakul T, Hossain E (2009) Introduction to network simulator 2 (NS2). In: Introduction to network simulator NS2. Springer, Boston, pp 1–18

Kerrache CA, Calafate CT, Lagraa N, Cano JC, Manzoni P (2016a) Hierarchical adaptive trust establishment solution for vehicular networks. In: 2016 IEEE 27th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp 1–6

Kerrache CA, Lagraa N, Calafate CT, Lakas A (2016b) TFDD: a trust-based framework for reliable data delivery and DoS defense in VANETs. VehCommun 1(9):254–267.

Khan U, Agrawal S, Silakari S (2015) Detection of malicious nodes (DMN) in vehicular ad-hoc networks. ProcediaComputSci 1(46):965–972.

Khan FA, Imran M, Abbas H, Durad MH (2017) A detection and prevention system against collaborative attacks in mobile ad hoc networks. Future GenerComputSyst 1(68):416–427.

Krajzewicz D, Hertkorn G, Ro¨ssel C, Wagner P (2002) SUMO (simulation of urban mobility)—an open-source traffic simula-tion. In: Proceedings of the 4th middle east symposium on simulation and modelling (MESM20002), pp 183–187

Kumar N, Chilamkurti N (2014) Collaborative trust aware intelligent intrusion detection in VANETs. ComputElectrEng 40(6):1981–1996.

Kumar PV, Maheshwari M (2014) Prevention of Sybil attack and priority batch verification in VANETs. In: International confer-ence on information communication and embedded systems (ICICES 2014), pp 1–5.

Kumar V, Mishra S, Chand N (2013) Applications of VANETs: present & future. CommunNetw 5(01):12.

Li W, Song H (2016) ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans IntellTranspSyst 17(4):960–969.

Lim K, Manivannan D (2016) An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. VehCommun 1(4):30–37.

Ltifi A, Zouinkhi A, Bouhlel MS (2015) Trust-based scheme for alert spreading in VANET. ProcediaComputSci 1(73):282–289.

Lu Z, Qu G, Liu Z (2018) A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans IntellTranspSyst 23(99):1–7.

Mokdad L, Ben-Othman J, Nguyen AT (2015) DJAVAN: detecting jamming attacks in vehicle ad hoc networks. Perform Eval 1(87):47–59.

Pham TN, Yeo CK (2018) Adaptive trust and privacy management framework for vehicular networks. VehCommun 13:1–2.

Pooja B, Pai MM, Pai RM, Ajam N, Mouzna J. (2014) Mitigation of insider and outsider DoS attack against signature based authen-tication in VANETs. In: 2014 Asia-Pacific conference on computer aided system engineering (APCASE), pp 152–157.

Saleh AI, Gamel SA, Abo-Al-Ez KM (2017) A reliable routing protocol for vehicular ad hoc networks. ComputElectrEng 1(64):473–495.

Sedjelmaci H, Senouci SM, Abu-Rgheff MA (2014) An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. IEEE Internet Things J 1(6):570–577.

Sharma S, Chang V, Tim US, Wong J, Gadia S (2019) Cloud and IoT-based emerging services systems. Cluster Computing 22(1):71–91.

Singh A, Sharma P (2015) A novel mechanism for detecting DOS attack in VANET using enhanced attacked packet detection algorithm (EAPDA). In: 2015 2nd international conference on recent advances in engineering & computational sciences (RAECS), pp 1–5

Tyagi P, Dembla D (2016) Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET). Egypt Inform J 18(2):133–139.

Wahid A, Yasmeen H, Shah MA, Alam M, Shah SC (2019) Holistic approach for coupling privacy with safety in VANETs. ComputNetw 148:214–230.

Yao X, Zhang X, Ning H, Li P (2017) Using trust model to ensure reliable data acquisition in VANETs. Ad Hoc Netw 1(55):107–118.

Zaidi K, Milojevic MB, Rakocevic V, Nallanathan A, Rajarajan M (2016) Host-based intrusion detection for vanets: a statistical approach to rogue node detection. IEEE Trans VehTechnol 65(8):6703–6714

Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, June 2021: 5034 – 5049

Research Article

Recent Trust Based Models and Security Frameworks for Secure IoT Ecosystem

Kajol Rana[1], Dr. Ajay Vikram Singh[2], Dr. P. Vijaya[3]

Abstract

Internet of Things is an arrangement that provides machine to machine communication with the help of internet where devices can be a physical device's, vehicle's, home appliances or any type of electronic appliances. With the growth of IOT the number of devices connected on the internet is also increasing so, to efficiently implement IOT into the network we need to closely deploy the constraints of IOT. Major challenge in deploying IOT are the security issue since IOT requires an end to end security and any breach can lead to the failure of the entire concept. To overcome this challenge many techniques have been built. In this research paper we are performing a comparative study on different security frameworks along with special focus on different Trust Based Security frameworks developed for IOT.

***Index Terms*—**Cryptography, Internet of Things, Near Field Communication, Security and Trust.

I. INTRODUCTION

IoT is a network that contains physical devices, vehicles,electronic appliances, etc. all enclosed with sensors and medium to communicate. It allows the sensors to study the object and enables the object to connect and exchange data without any form of human intervention.

According to a recent survey, it has been predicted that by the year 2020, number of devices connected to Internet will be 2.5 times. With the inclusion of more devices and more data, comes adverse security risks.In 2016, an attack named Mirai Botnet, lead to paralysis of global access to high profile Internet services for a few hours, leaving all forms of data vulnerable and even exposing highly secret documents of the countries.[1]

IoT although very useful, but at times can be disastrous if not dealt with carefully. For instance, if all the devices in a hospital are connected using IoT and some notorious person attacks the system and can access the system, then the life of the patients is at high grade of risk or a burglar is able to crack the security of your house then it can lead to huge financial loss. We have a wide web interface which is highly insecure, leading to major attacks onto the system; we still do not have the right mechanism for authentication of the correct user, we can find so many fake accounts even after so many security aspects; already existing networks, encryption algorithms for transmitting of information are also not strong enough that they can be relied on; cloud services and mobile interfaces are easy to crack; the software's and hardware's are also not able to defend attacks on themselves after an extent and we can also say that the physical security of the device also plays an important role for developing a good IoT; we are still not able to find beforehand if our system is compromised or not, so identifying the various security breaches is also a task, there is no way of predicting the attacks.[2] In this

paper, we are going to review various security frameworks as well as security framework based on trust and try to understand and identify the difference among them.

II. RELATED RESEARCH WORK

The Discrete technologies introduce new forms of designing and working issues. Internet of things has bought an evolution in the field of Artificial Intelligence and is seen to be useful in many areas of interest. However, when working with this kind of huge data, requirement of very high standards of security becomes mandatory. For overcoming this issue various security frameworks have been developed over the years.

LLCPS utilized for Near Field Communication (NFC) provides peer to peer secured transaction by making use of Transport Layer Security. It consists of four layersNear Field Communication Interface and Protocol-1 layer (Works on initialization, target detection and hence forms a data path that avoids this route)[3]; Logical Link Control Protocol layer (Works as a means to encapsulate and secure the packets to be transmitted)[4]; Transport Layer Security layer (Works as an authentication system); Service layer (key is encrypted as per NFC Data Exchange Format to lockdown the target)[5].[6]

Digital Forensics Investigation Framework is used by digital forensics. It forms its base from ISO. Major work is to initialize and investigate material to form modules of digital forensics via reactive and proactive processing.[7]

Software Defined Networking- based security framework forms cluster for IoT devices [8]. It does intrusion detection as well as prevention from malicious attacks.[9] SecIoT provides all forms of basic security features, such as, authentication, authorization, etc. Working with trust as a parameter is still a future scope for this framework.[10] Radio Frequency Identification security framework focuses on novel identification technique to provide security benefits by making use of hash operations and probability evaluations.[11] SAFIR (Secure Access Framework for IoT) provides security for small IoT network by performing access control, authentication, authorization, etc. It also provides secured parameters for the establishment of flexible sharing models.[12]

III. SECURITY FRAMEWORKS

Security is a major hurdle in the growth of IoT. Decisions made prior to a breach in security can result into better functioning of IoT applications. In this section we will be studying in detail about various recently developed security frameworks for IoT.

A. Cisco Framework

This framework (figure1) helps in prevention from physical attacks like Data at Rest and Intrusion detection. To maintain the standards for security it constitutes of four layers of security as given in figure 1. The framework consists of four entities. Firstly, Authentication is Done using Radio Frequency Identification, shared secret key and

X.509 certificates [13] and does not work on IEEE 802.1Xand hence, provides with, lesser credential types, intensive cryptographic constructs and authentication protocols. Secondly, Authorization's job is to only allow access to recognized personnel. It stores the identity information of an entity and hence establishing a trust relationship between the IoT devices. Thirdly, Network Enforced Policyare always some of the protocols applied according to the nature of the work of the devices and to keep the channel secured. Lastly, Secure Analytics: Visibility and Control does threat detections and preventive measures to avoid any foreseen threats are fixed.[14]

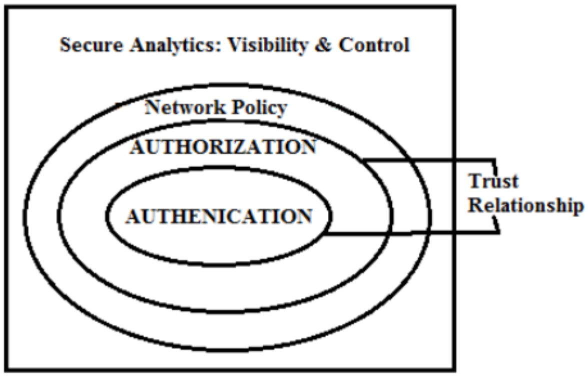


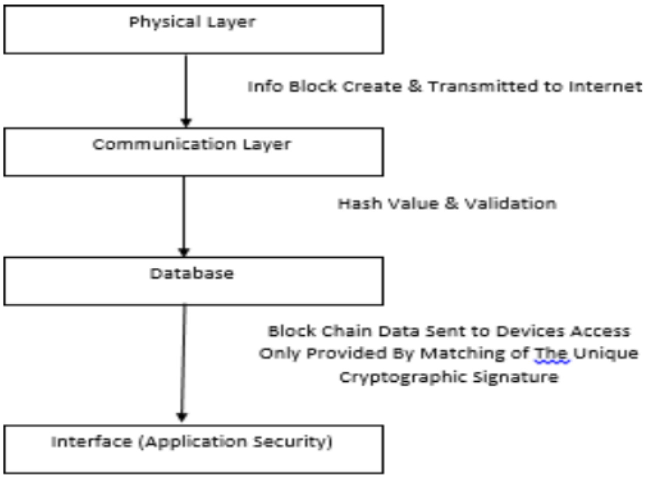
Fig.1. Cisco Framework for IoT

B. Floodgate Framework

This framework works completely according to the ISA/IEC 62443 compliance (cyber security). It allows the entities to prevent from present or upcoming cyber threats and is not favorable for low power devices, as it requires high battery power and storage space and hence it is called as a best fit for Infrastructure security framework. It maintains Internet security, Security for specific applications and security measures are taken at the Run- time for checking the integrity.[15]

C. Intelligent Security Framework

It instruments Asymmetric key Encryption to communicate the session key between nodes and then use this session key for sending the message. Authentication between devices and services is established mutually by using the unique ID of the sensors to generate the key. For the purpose of communication, it makes use of lightweight asymmetric key cryptography (Used for securing the communication between sensors and gateways, by making use of sensor unique ID and gateway unique ID. Using the two above unique ID's and applying Advanced Encryption Standard Algorithm a secret key is created.) and public key encryption – digital signature (Used for securing the communication between device gateway and cloud service). In this framework (figure 2), we can remove most of the fake and faulty packets, as a result, performance improvement is seen and in addition to it, it provides reduced bandwidth consumption and security is established against Quantum Attacks. [16]


Physical Layer
Info Block Create & Transmitted to Internet
Communication Layer
Hash Value & Validation
Database
Block Chain Data Sent to Devices Access Only Provided By Matching of The Unique Cryptographic Signature
Interface (Application Security)

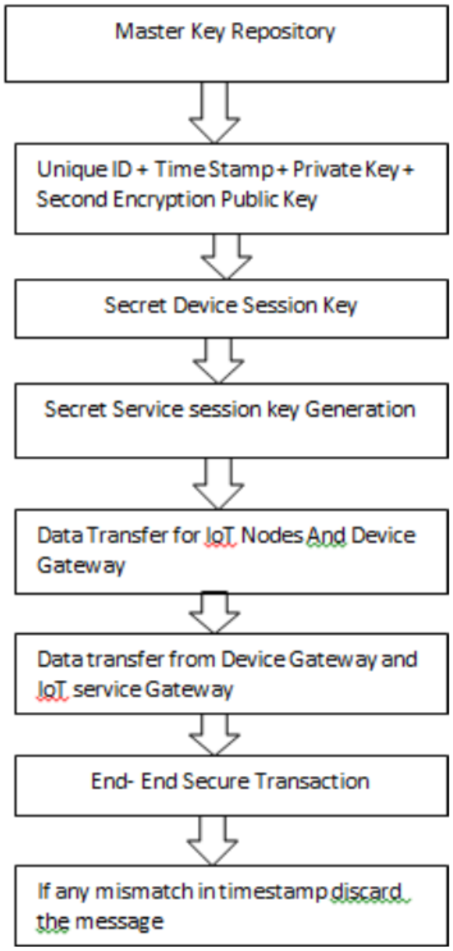

Master Key Repository
Unique ID + Time Stamp + Private Key + Second Encryption Public Key
Secret Device Session Key
Secret Service session key Generation
Data Transfer for IoT Nodes And Device Gateway
Data transfer from Device Gateway and IoT service Gateway
End- End Secure Transaction
If any mismatch in timestamp discard the message

Fig. 2. Intelligent security framework for IoT

D. Security Framework for IoT against Wireless Threat

For maintaining security against the wireless threats, this framework enables the block chain technique. Block chain technique sustains a database which constitutes of all the data set records, which are, distributed in nature. The benefit of using this technique is that only the nodes whose participation is required are given the copy of the chain and it is very cost effective.

It consists of four layers (figure 3), namely, Physical (Does the encryption work), Communication layer (Follows the Block Chain Protocol) [17], Database (Records are saved here for future use and each record consists of time constraints and unique cryptographic signatures) and Interface layer (It provides with the Application Security). [18] Fig.3. Security Framework for IoT against Wireless Threat

E. IoT Security Model

The IoTSM model is based on end to end security. The model (figure 4) presents a general view of security for any organization working in the area of IoT. It helps the organizations to model an end to end security for its day to day work. Its base is designed by using the Software Assurance maturity model.[19]It constitutes of five layers as shown in the figure 4. The task of the first layer Governance is to create security awareness by educating the employees and designing a soft model of security using the design process and standards. Second layer, Construction wherein, all the risks are identified,and assessment is done to check the level of the risks. Majorly ISO 27001 and OCTAVE are used. Threat modelling is also a part of this layer. Threat modelling is done using two methods: Attack- tree based (identify the possible attacks on the tree structure of the work) and Stochastic model (Analyzed using the state transition metrics). Third layer, Security Requirement and Architecture in which, security measures are implied, such as, Physical security is provided using Encryption, Network security is provided by using privacy and integrity, data security by using authentication and so on. Fourth layer, Verification is done to check the reliability of the system developed. It does artifact review for reviewing the codes and security testing is done for inspection of any vulnerability in the software. Lastly, Operation in which, IoT systems are updated by using a secured as well as verified channel to rule out any threat possibilities.

This model is seen to work better than Software Assurance maturity model, Building Security inMaturity Model [20], Comprehensive Lightweight Application Security Process [21] and Microsoft Security Development Lifecycle [22], as it involves cloud and data security at every point. [23]

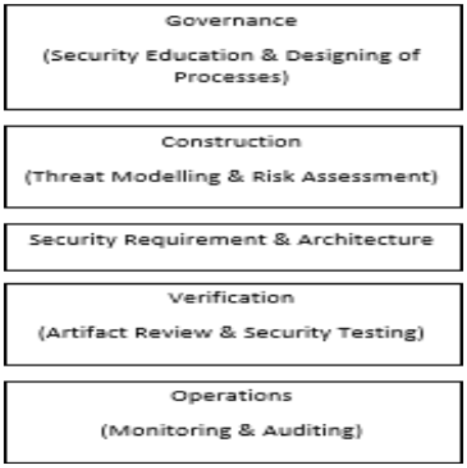

Governance
(Security Education & Designing of Processes)
Construction
(Threat Modelling & Risk Assessment)
Security Requirement & Architecture
Verification
(Artifact Review & Security Testing)
Operations
(Monitoring & Auditing)

Fig.4. IoTSM (IoT Security Model)

F. U-POT A Honeypot Framework

The honeypot framework [24][25][26][27][28][29] is applied on Universal Plug and Play Devices [30], which constitute of Controlled devices (Servers responsible for delivery of service) and control points (Smart phone Application).

Working of the framework is shown in figure 5

a. Target Device: - The use of Belkin WeMo smart switch is done.[31]

b. State scanner: - Its work is to reap the description layer of the target device.

i. Crawling: - If there are multiple descriptions, all the files are creeped through extracted URL's and HTTP Get Method and stored in a local file system. The data collected is searched thoroughly to identify the list of state variables.

ii. Scanning: - It enables the initial handshaking with the control point of the UPnP Device.

c. U-PoT Devices: - Its work is to create mimic devices which can listen to any approaching request on the channel and return/update its state accordingly.

i. Discovery Mode:- All the information of the device and its state are extracted by scanning through the information.

ii. Normal Operations Mode: - Its work is to accept the request and perform update/change according to the request made.

This framework is seen to work better than other algorithms and has low overhead on response time.[32]

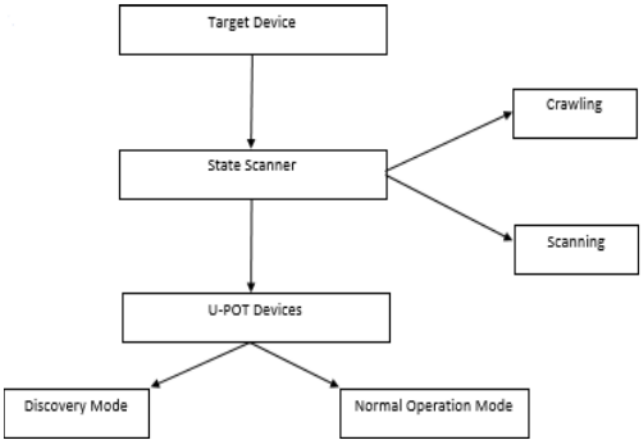


Fig.5. U-PoT: Honeypot Framework for IoT

G. *Cloud Computing Framework For Improving IoT Security*

This framework is designed specifically for cloud services. It has separated IoT functions from the physical devices and runs confined IoT functions on cloud environment. It applies Dripcast framework [33], [34], [35], [36], as it is a transparent programming framework for IoT Devices.
In which Clientlayer has a small Java library that works on the client's device. Used to send CREATE request to the Relay. All jobs in the library are assigned a unique ID for identification and verification purpose.Relay layer contains a set of servers, known as, Relays. Its job is to accept the request from client and send it to the engine servers. It is protected using strict access controls and authentication is required. Engine layer contains a set of Engine servers, with assigned key space for every server. Its job is to accept the request of the client and process the output for the client. Not connected to any public internet and the only possible way to reach it is relay.Store layer is a Database storing all the information. Information can be only accessed using GET, PUT and REMOVE. This is also not connected to any public internet.[37]

H. *PoLIoT (Polytechnic IoT)*

It is used for threat identification and management. It is developed by using three frameworks, namely, Power IoT framework (Important features depend upon the risk assessment and security rules, majorly works upon intelligent devices and has 4 layers, namely, application, platform, physical & network) [38], IoT Education Framework (it is used to protect all forms of assets from threats, makes use of SDRAM, FLASH, ROM, etc. and has three layers, namely, Security protocol, software platform and hardware platform.) [39] and Embedded Security Framework (Awareness and education is the main motivation and works majorly on LAN, consists of five layers, namely, Response layer, Control layer, Network layer, Perception layer and Site/base layer) [40]. It is adequate as network systems deployed in polytechnic are of

medium size and comprise of basic technology. It consists of three layers: Device layer, Access layer and Data & Application layer. All the layers are used for threat management.
Device layer consists of the information of the device and the description layer of the device. Access layer allows access to only authorized members. Data and Application layer which uses different measures like intrusion prevention, authorization and access control. [41]

IV. TRUST MODELS

Trust is a behavioral pattern of human beings. Usage of trust in the field of IoT has led to the development of security in IoT.
Some of the security framework based on trust for IoT have been studied in detail in this section.

A. *Security and Reputation based trust assessment for cloud services for IoT*

In this paper, trust evaluation is done on cloud services to safeguard the security of cloud based IoT context through combined services from security and reputation. It develops a security metrics to compute security levels for a cloud service. For the quantification of reputation, feedback is collected. This framework is seen to outperform other trust assessment methods.
It has three main parts: -

a. Security based trust assessment: - Security based trust assessment is done by following three main steps, namely, security metric definition, security metrics quantification and security level evaluation.

i. Security Metric Definition: - Its job is to form security control deliverables which constitutes
of cloud specific security metrics (metrics defines the security requirement of the client).

ii. Security metric quantification: - All the security metrics are quantified, so that, comparison can be done based on security capabilities. Quantification can either be done in Yes/No manner or 0/1 manner.

iii. Security level Evaluation: - Forms its basis from TOPSIS. [42] An ideal decision matrix is developed, and positive/negative solutions are identified. Then the difference is calculated in concordance to the ideal value. Relative closeness can then be identified for each of the CSP's (Cloud service Providers).

b. Reputation based trust assessment: - It is done by following the four main steps given below: -

i. Data Collection and processing: -Data is collected from the feedback ratings and then the required information is normalized to form multi-tuples, which are combined to form a data repository.

ii. Weight factor assignment: - Reputation based Trust Assessment is used to determine the weight factors to be considered.

iii. Local objective reputation: - Calculation of Local Objective Reputation is done by combining feedback rating of each CSC.

iv. Global objective reputation: - Global Objective Reputation can be calculated using the time-based weighted Local Objective Reputation within a specific time window.

c. Integrated Trust Assessment: - It follows the objective weight assignment method to identify the important weights of security and reputation levels and then based on the identified weights trust can be evaluated.[43]

B. *Blockchain based secure and trustworthy IoT*

This paper utilizes trust framework along with block- chain framework for SDN (Software Defined Networks) enabled 5G VANET's (Vehicular Ad-hoc Networks)[44] and provides privacy and avoids malicious attacks. The working of the security model can be majorly divided into two parts, as follows, firstly, blockchain Framework, in which the vehicle is identified by using SIM, which is a unique identification given to the DL number of a vehicle on the network. After the registration symmetric key SKE is used to encrypt the hash value of video. Data transmission is encrypted and message sharing between vehicles is block-chained, so that the records remain immutable as well as the vehicle sending messages can be easily traced. It helps us to avoid any form of malicious attacks. [45] Second comes Trust management which contains Traffic Information collection that does the judgment of road condition tags is done by either +1 or -1. Road Side Unit (RSU) receives messages and classifies it into a set {Ej,1, Ej,2,….Ej,n}. Ej,p is broadcasted to reach all the vehicles.Trust value computation in which, RSU classifies the scores made by forwarding vehicles it has received into {Sj,1, Sj,2, …, Sj,p}. Distance from vehicle is found and RSU finds and tags the vehicle ID's giving high frequency of false positives by using blockchain method.Miner Election in which, Proof-of- stake is used to elect and value of trust is determined and lastly Vehicle Credibility assessment is used in case of any accident, it can use the videos to know the reason of accident and re-route all other vehicles to a free road. [46]

C. *CTRUST (Centric Trust For IoT)*

The performance of the following framework was calculated based on the utility obtained and trust's accuracy, convergence and resiliency. Parameters involved are communication speed, reliability, rate of work, etc. Weights assignment depends upon the decision of the trustier. In this framework, the nodes required for context criteria are assessed and a partial trust score is obtained, then weights are assigned to the criteria and with the help of previous trust scores the trust database is updated and final decision is then made using the updated trust database. Working of the CTRUST framework is shown in the figure. [47]

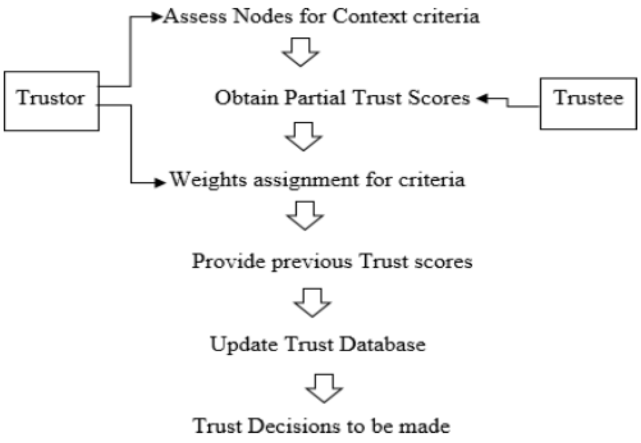

Assess Nodes for Context criteria
Trustor
Obtain Partial Trust Scores
Trustee
Weights assignment for criteria
Provide previous Trust scores
Update Trust Database
Trust Decisions to be made

Fig. 6. CTRUST (Centric Trust) for IoT

V. COMPARISON OF VARIOUS SECURITY FRAMEWORKS AND TRUST BASED SECURITY FRAMEWORKS

In Table 1 comparison of various security frameworks is done, so that a better understanding can be established of the frameworks and their applicability can be underlined. It can be seen that all the frameworks work for different problems certain attacks like intrusion detection and privacy is taken care of in almost all the described frameworks.

TABLE I
COMPARISON BETWEEN VARIOUS SECURITY FRAMEWORKS FOR IOT

S.No.	Security Framework	References	Attributes	Attacks/ Facilities
1	Cisco	[14]	RFID X.509 Certificates	Data at Rest Intrusion Detection
2	Floodgate	[15]	ISA/IEC 62443	Cyber Threats

3	OSCAR	[48]	Privacy Coupling content encryption key	Eavesdrop Relay attacks
4	Intelligent Security	[16]	Asymmetric key cryptography Lattice based cryptography	Fake and faulty packets Quantum attacks
5	Security Framework for IoT Against Wireless Threat	[18]	Block chain technique Unique cryptographic signatures	Wireless threats like Rogue access points, denial of service, passive capturing and Eavesdropping
6	IoTSM (IoT Security Model)	[23]	Software Assurance maturity model Threat modelling ISO 27001 OCTAVE	Intrusion detection Eavesdropping Brute Force
7	U-PoT: A Honeypot Framework	[32]	Honeypot Framework	IoT candy Jar [49] Malicious attacks
8	Cloud computing framework for improving IoT security	[37]	Dripcast Framework	Intrusion Detection Privacy
9	PoLIoT (Polytechnic IoT)	[41]	Power IoT Framework IoT Education Framework Embedded Security Framework	Intrusion Detection Authorization Access Control
10	Elliptic curve cryptography-based security framework for IoT	[50]	Elliptic curve cryptography	Unique Authentication Integrity Confidentiality Privacy

In Table 2 comparison of various trust based security framework is done to see how trust as a factor can be included to provide better security and it can be seen that various major attacks are taken care of by making use of different pillars of trust(Reputation, belief, authentication, etc.). Trust can be considered as a good example for security issues as it provides a better understanding for the human brain and with more consideration in this field we can develop a better and secure environment for IoT.

TABLE II
COMPARISON OF SECURITY FRAMEWORK BASED ON TRUST FOR IOT

S.No.	Security Framework based on Trust	References	Attributes	Attacks
1	Security & Reputation based trust assessment for cloud services.	[43]	Security based trust assessment Reputation based trust assessment	Self-promotional attack [51] Slandering attack [52]
2	Block chain based secure and trustworthy IoT	[46]	Trust framework Block chain framework	Privacy preventio n Malicious attack
3	CTRUST	[47]	Trust assessment (Objective and subjective) Decay recommendati o n Aggregation function	Malicious attack
4	Architectur e based trust in M- IoT	[53]	Centralized Framework [54] Distributed Framework [55] Hierarchical Framework [56]	Authenticati on Integrity Confidential ity Access Control Authorizatio n
5	SPTP (Secure, Private & Trustworthy Protocol)	[57]	Platform for Privacy preferences P3P [58] Access control list	Reputation Access control Web cookies

VI. CONCLUSION

After reviewing all the above security frameworks, it can be predicted that working of IoT is more focused on providing services, rather than, securing the existing. The security frameworks designed till date, provide only basic form of security, leading to a highly risky platform. It is observed from the above frameworks that trust based approaches are providing more efficient and secured environment for IoT than the others. The framework IoTSM with certain advances can prove to be a nice approach for industrial operations in the field of IoT . It has also been noticed that majorly cryptographic techniques are used to provide a standard level of security. When talking about Internet of Things and Billions of devices then security standards must go beyond authentication, privacy, integrity and certain predictable attacks. By the above paper, we can conclude that there is a requirement for better security approaches, which are able to provide peer to peer security or device to device security, so that the entire concept of IoT can be established to avoid attacks like CandyJar, Mirai Botnet, Slandering attacks, etc completely.

REFERENCES

[1] Sebastian Bellagamba, “Trust by design: The Internet of things”, ITU, 2018.

[2] Colin Tankard, “The security issues of the IoT”, Elsevier, 2015, p.p:- 11-14.

[3] “Near Field Communication Interface and Protocol”, Standard ECMA- 340, December 2004.

[4] “Logical Link Control Protocol”, Technical Specification, NFC Forum™, LLCP 1.1, June 2011.

[5] “NFC Data Exchange Format” Technical Specification, NFC Forum™, NDEF 1.0, July 2006.

[6] Pascal Urien, “LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things”, IEEE, 2013, p.p:-845- 846.

[7] V.R. Kebande, I.Ray, “A generic digital forensics investigation framework for internet of things”. IEEE, 2016, p.p:-356-362.

[8] O.Flauzac, C.Gonzalez, F.Nolot, “SDN based architecture for clustered WSN. Innovative mobile and internet services in ubiquitous computing” 9th International Conference, p.p:-342-347,2015.

[9] C.Gonzalez, S.M. Charfadine, O.Flauzac, F.Nolot, “Sdn-based security framework for the iot in distributed grid”, IEEE, 2014, p.p:- 1-5.

[10] X.Huang, P.Craig, H.Lin, Z.Yan, “Seciot: a security framework for the internet of things”, Security and communication networks, vol.9, no 16, 2016, p.p:-3083-3094.

[11] B.R.Ray, J.Abawajy, M.Chowdhury, “Scalable rfid security framework and protocol supporting internet of things”, Computer networks, vol.67, 2014, p.p:-89-103.

[12] J.L.Hernandez-Ramos, M.V.Moreno, J.B.Barnabe, D.G.Carrillo, A.F. Skarmeta, “Safir: Secure access framework for iot-enabled services on smart buildings”, Journal of Computer and system sciences, vol.81, no.8, 2105, p.p:- 1452-1463.

[13] Zakia El Uahhabi, Hanan El Bakkali, “An approach for evaluating trust in X.509 certificates”, ICITST, IEEE, 2106, p.p:- 196-203.

[14] Z. Bakshi, A. Balador and J.Mustafa, “Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models”, IEEE, 2018, p.p:- 173-178.

[15] Mohammad Irshad, “A systematic review of information security frameworks in Internet of things”, IEEE,2016, p.p:- 1270-1275.

[16] S.Sridhar, S.Syms, "Intelligent security framework for IoT devices", ICISC, IEEE, 2017, p.p:-1-5.

[17] Konstantinos Christids, and Michael Devetsikiotis," Blockchains and Smart Contracts for the Internet of Things", Special Section on the Plethora of Research in Internet of Things (IoT), 2016.

[18] Himanshu Gupta, Garima Varshney, "A security framework for IoT devices against wireless threat", TEL-NET, IEEE, 2017.

[19] OWASP, "Software Assurance Maturity Model," OWASP, 2018. [Online]. Available:https://goo.gl/9cCA4h.

[20] Gary McGraw, S. Migues, and J. West, "Building Security In Maturity Model (BSIMM)," 2018. [Online]. Available: https://goo.gl/JUAtbF.

[21] D. Graham, "Introduction to the CLASP Process," 2006. [Online]. Available: https://goo.gl/wducjb.

[22] M. Howard and S. Lipner, "The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software," *MicrosoftPress*, vol. 8, 2006.

[23] Joseph Bugeja, Bahtijar Vogel, Andreas Jacobsson, "IoTSM: An End- to-end Security Model for IoT Ecosystems", IEEE, 2019, p.p:- 267-272.

[24] Mitsuaki Akiyama, Makoto Iwamura, Yuhei Kawakoya, Kazufumi Aoki, and Mitsutaka Itoh. Design and implementation of high interaction client honeypot for drive-by-download attacks. IEICE transactions on communications, , 2010 p.p:- :1131–1139.

[25] Yaser Alosefer and Omer Rana "Honeyware: a web-based low interaction client honeypot" (ICSTW), IEEE, 2010, p.p :- 410–417.

[26] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, and Christian Rossow, "Iotpot: analysing the rise of iot compromises", 2015.

[27] Adrian Pauna and Victor Valeriu Patriciu "Casshh–case adaptive ssh honeypot. In International Conference on Security in Computer Networks and Distributed Systems", Springer, 2014, p.p:- 322–333.

[28] Haris ˇSemi´c and Sasa Mrdovic."Iot honeypot: A multi-component solution for handling manual and mirai-based attacks."(TELFOR), IEEE, 2017, p.p:- 1–4.

[29] G´erard Wagener, Radu State, Thomas Engel, and Alexandre Dulaunoy.,"Adaptive and self-configurable honeypots" (IM), 2011 IFIP/IEEE International Symposium, IEEE,2011, p.p:- 345–352.

[30] UPnP Forum. UPnP upnp device architecture. http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecturev1.1.pdf.

[31] Belkin International. belkin wemo. https://www.belkin.com/us/.

[32] Muhammad A. Hakim, Hidayet Aksu, A. Selcuk Uluagac, Kemal Akkaya, "U-PoT: A Honeypot Framework for UPnP-Based IoT Devices", IEEE, 2018.

[33] Ikuo Nakagawa, Masahiro Hiji, Hiroshi Esaki: “Dripcast - Server-less Java Programming Framework for Billions of IoT Devices”, Proc of IEEE COMPSAC, Jul., 2014. pp:- 186-191,

[34] Ikuo Nakagawa, Masahiro Hiji, Hiroshi Esaki: “Dripcast – architecture and implementation of server-less Java programming framework for
billions of IoT devices”, JIP Journal, 23 (4), 2015.

[35] Ikuo Nakagawa, Masahiro Hiji, Hiroshi Esaki: “Design and Implementation of Global Reference and Indirect Method Invocation Mechanisms
in the Dripcast”, Proc. of IEEE COMPSAC, , Jun, 2016, pp:- 338-343.

[36] Ikuo Nakagawa, Masahiro Hiji, Hiroshi Esaki: “Global reference model and global garbage collection in the Dripcast”, PRAGMA 32, Apr, 2017.

[37] Ikuo Nakagawa, Shinji Shimojo, “IoT Agent Platform mechanismwith Transparent Cloud Computing Framework for improving IoT Security”, IEEE, 2017, p.p:- 684-689.

[38] Zhang Y., Zoun W., Chen X., Yang C., Cao J, “*The Security for Power Internet of Things: Framework, Policies and Countermeasures,* in International Conference on Cyber-EnabledDistributed Computing and Knowledge Discovery”, 2014.

[39] Zhang Tianbo, “*The Internet of Things Promoting Higher Education Revolution”*, Fourth International Conference on
Multimedia Information Networking and Security, 2012, pp:- 790-793.

[40] Babar S., Stango A., Prasad N., Sen J., Prasad R., “Proposed Embedded Security Framework for Internet of Things (IoT)”, IEEE Journal, 2011.

[41] Zulkarnain Md. Ali, Mohamad Azuan Bin Mohamed Arshad, Marini Abu Bakar, “POLIoT : Internet Of Things Framework In Managing Network Threats At Metro Polytechnic Tasek Gelugor” , IEEE, 2018.

[42] M. Behzadian, S. K. Otaghsara, M. Yazdani, and J. Ignatius, ``A state-of the-art survey of TOPSIS applications,'' *Expert Syst. Appl.*, vol. 39, no. 17, , 2012, pp:- 13051_13069.

[43] Xiang li, Gixu wang , Xiao lan, Xingshu chen, Ning zhang , Dajiang chen, “Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration ofSecurity and Reputation Approach”, IEEE, 2019, p.p:- 9368-9383.

[44] I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, and N. Guizani,
``Overcoming the key challenges to establishing vehicular communication: Is SDN the answer?'' *IEEE Commun. Mag.*, vol. 55, no. 7, Jul. 2017, pp. 128_134,

[45] M. H. Eiza, Q. Ni, and Q. Shi, ``Secure and privacy-aware cloud- assisted video reporting service in 5G-enabled vehicular networks,'' *IEEE Trans.Veh. Technol.*, vol. 65, no. 10, Oct. 2016, pp. 7868_7881.

[46] Lixia xie, Ying ding, Hongyu yang , Xinmu wang, “Blockchain- Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G- VANETs”, IEEE, 2019, p.p:- 56656-56666.

[47] Anuoluwapo A. Adewuyi, Hui Cheng, Qi Shi, Jiannong Cao, Áine MacDermott, Xingwei Wang, “CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things”, IEEE, 2019, p.p:- 5432-5445.

[48] H. Zhou, et al.,, “*A Cognitive Adopted Framework for IoT Big-Data Management and Knowledge discovery Prospective*,”IEEE.

[49] Tongbo Luo, Zhaoyan Xu, Xing Jin, Yanhui Jia, and Xin Ouyang, “Iotcandyjar: Towards an intelligent-interaction honeypot for iot devices.”, Black Hat, 2017.

[50] T Daisy Premila Bai, K Michael Raj, S Albert Rabara, “Elliptic Curve Cryptography based security framework for Internet of Things Enabled Samrt card ”, WCCCT, 2017, p.p:- 43-46.

[51] K. Hoffman, D. Zage, and C. Nita-Rotaru, ``A survey of attack and defense techniques for

reputation systems,'' *ACM Comput. Surv.*, vol. 42, no. 1, 2009, Art. no. 1.

[52] P. Chandrasekaran and B. Esfandiari, ``A model for a testbed for evaluating reputation systems,'' in *Proc. IEEE 10th Int. Conf. Trust, Secur. PrivacyComput. Commun. (TrustCom)*, Nov. 2011, pp. 296_303. [53]Vishal Sharma, Ilsun You, Karl Andersson, Francesco Palmieri, Mubashir Husain Rehmani, "Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey", IEEE, 2019, p.p:-1-45.

[54] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the internet of things (ctm-iot)," in International Conference on Broadband and Wireless Computing, Communication and Applications, Springer, 2017 pp. 533–543.

[55] R. Chen, J. Guo, and F. Bao, "Trust management for soa-based iot and its application to service composition," IEEE Transactions on ServicesComputing, vol. 9, no. 3, 2016, pp. 482–495.

[56] X. Wu and F. Li, "A multi-domain trust management model for supporting rfid applications of iot," PloS one, vol. 12, no. 7, 2017.
[57] Ivor D. Addo, Ji-Jiang Yang, Sheikh I. Ahamed, "SPTP: A Trust Management Protocol for Online and
Ubiquitous Systems" IEEE, 2018, p.p:- 590-595.
[58] R. Wenning, W3C, "Platform for Privacy Preferences Project," *P3P Public Overview*, October 2007, Retrieved from http://www.w3.org/P3P/.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
doi: https://doicatalog.org/19.4103/jjue.v40i6.1990

MONITORING OF VEHICULAR AD-HOC NETWORKS TO DETECT MALICIOUS VEHICLES (DMV)

Garima Saini[1] and Dinesh Javalkar[2]

1 Research Scholar, Lingayas Vidyapeeth, Faridabad
2 Asst. Professor Lingayas Vidyapeeth, Faridabad

1. INTRODUCTION

Traditional wired networks are protected by various defence mechanisms such as gateways and firewalls. Wireless networks, on the other hand, are vulnerable to security threats that can threaten the entire network from either direction. Because of the lack of centralised administration, VANETs, As an ad hoc network, different misconducts such as messages manipulation, eavesdropping are vulnerable, spamming, masquerading, and so on (Al-kahtani. MS. 2012)(Mishra B, et al.,2011) (Liu Y et al.,2009)..[1] ,[5] [21] One of the major challenges has been described as the security of VANETs. VANET applications permit ongoing correspondence and handle life-basic data. To secure against aggressors and noxious vehicular hubs, it should stick to security principles like genuineness, secrecy, namelessness, non-disavowal, and verification.

Researchers have suggested various misbehaviour identification systems to arrange the assailants liable for offense in VANETs. The identification of such malignant hubs and dubious organization movement is basic to define precaution measures. DMN (Detection of Malicious Nodes) is a hub driven identification plot proposed in this paper that viably identifies malevolent hubs that drop and copy parcels in the organization utilizing an observing strategy. The verifiers who qualify the choice edge watch out for the nodes. As an outcome, as opposed to picking the entirety of the dependable hubs, just the most suitable hubs play out the undertaking of checking the activities of different hubs. This guides in the appropriate utilization of

Article to Cite:
Garima Saini & Dinesh Javalkar. (2021). Monitoring of vehicular ad-hoc networks to detect malicious vehicles (DMV), Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition), 40(6). doi: https://doicatalog.org/19.4103/jjue.v40i6.1990

organization assets, which is frequently disregarded by scientists in their location schemes. As an outcome, network proficiency expands, which is a vital necessity of protection schemes for complex networks like VANETs.(Daeinabi A et al.,2013)(Isaac JT, et al.,2010) (Hussain et al.,2012)[3],[7]

2. SIGNIFICANCE OF THE STUDY

Nowadays VANET occupies a major role in the intelligent Transportation System (ITS) which is connected with Cyber Physical System (CPS). Because of this a huge research gap is created in designing a secured VANET networks. An effective communication system for VANETs is very essential to protect the network from the vulnerabilities. And on the other side the increased vehicular traffic leads to roadside accidents. So there is a need of intelligent vehicle system which can act smartly during the emergency situation compared with the normal condition.

3.REVIEW OF RELATED STUDIES

In Vehicular Impromptu Organizations, various plans have been proposed to identify trouble making and malignant hubs. The accompanying two types of mischief ID frameworks might be barely ordered: There are two kinds of bad conduct recognizable proof plans: hub driven and information driven. Recognition Plans for Hub Driven Mischief Verification is utilized in hub driven strategies to separate between different hubs. To verify the hub moving the parcel, security qualifications, computerized marks, and different strategies are utilized. The hubs communicating the messages, as opposed to the information moved, are the focal point of such plans. Gosh et al. recommended a complete plan to distinguish malevolent vehicles for the Post Accident Warning application in their examination paper (Ghosh M et al.,2010),(Ghosh M et al.,2009). [9] ,[10]. They considered the likelihood of a vehicle's phony area subtleties in the PCN, just as a bogus accident cautioning in (Ghosh M et al.,2009). (Kim. CH et al.,2012)[10] [6] presented another Mischief Based Standing Administration Plan (MBRMS) that comprises of three areas. For the

ID and filtration of bogus data in vehicular specially appointed organizations, there are three algorithms:

a) Rowdiness discovery,

b) Occasion rebroadcast

c) Worldwide expulsion calculations.

Daeinabi et al. [3] proposed the DMV discovery calculation to recognize vindictive hubs by seeing how they rehash or drop got bundles and disengage them from legit hubs.

Vehicles are set apart with a question esteem and followed by the verifier hubs doled out to them. (Wahab. OA et al.,2014) [16] utilized a DempsterShafer based helpful guard dog model to identify noxious vehicles in a VANET utilizing the Nature of Administration Advanced Association State Directing (QoS-OLSR) grouping calculation. With an improvement in recognition likelihood, this methodology jam administration unwavering quality and productivity while decreasing the quantity of egotistical hubs and bogus negatives. (KadamM et al.,2014)[14] have proposed another methodology for recognizing malignant vehicles assaults as well as keeping them from entering the Vehicular Ad hoc Network. It is an improvement to the Acknowledgment of DMV algorithm (Daeinabi A et al.,2013)[3] . This technique limited the effect of a dark opening assault inside the VANET and is more powerful and stable than DMV.

3.1 Data-Centric Misconduct Detection Methodologies

To distinguish mischievous activities, an information driven methodology investigates the information sent between nodes.It is more worried about interfacing a larger number of communications compared to the people who operate the individual hubs. The information that is disseminated by the organization's hubs is assessed and contrasted with the data acquired by different hubs to decide the best course of action.Verify the exactness of the got notice messages.

Coming up next are a couple of exploration commitments to the information driven misconduct recognition plot.

In the research work, (Vulimiri A, et al.,2010)[2] (have discovered trouble making in VANETs dependent on the auxiliary data or admonitions that are made in light of the essential alarms for PCN application..(Ruj. S,et al.,2011) [20] proposed a new misbehaviour detection system based on a data-centric misbehaviour detection algorithmic programme.After warning messages have been received, the vehicle's activities are monitored to detect fake alert messages and misbehaving nodes..(Rezgui.J et al.,2011)[18] created VARM, a mechanism that gathers information about any neighbour transmission at a single vehicle in order to locate the malicious vehicle..(Rawat. DB et al.,2011)[17] recommended a novel calculation to get correspondence in the Vehicular Specially appointed Organization by utilizing a probabilistic technique to distinguish noxious drivers.It calculates the message's trustworthiness and determines if the message came from a trustworthy vehicle.(Grover.J et al.,2011)[13] have proposed a security system that uses machine learning to categorise a variety of VANET misbehaviors. In light of the highlights processed by the eyewitness hubs, it recognizes malevolent and legit hubs..(Grover.J et al.,2011) [13] utilized a group fundamentally based AI way to deal with present a security structure for identifying mischievous activities in VANETs.

A focal appraisal system15 dependent on bad conduct recognition frameworks working on vehicles and side of the road foundation units is introduced, fully intent on distinguishing and barring assailants from the network.Barnwal et al. presented a momentary rowdiness location plot in their examination paper4 that can recognize a pernicious hub.(Harit.SK et al.,2012)[11] have proposed a plan zeroed in on an information driven methodology for distinguishing the accuracy of got data, basically deciding the security worth of any vehicular hub dependent on its present position and speed.Huang et al. proposed a con artist distinguishing proof convention in paper (Huang.D.et al.,2012)[7] that recognizes vindictive vehicles that transmission counterfeit clog data in the organization for their own narrow minded reasons and imitate other non-existing vehicles.

In this case, radar estimates of surrounding speed and distance are used to confirm the occurence of a blockage that was generated by a vehicle hub.

In an IDS designed to detect malevolent attacks, the team (Coussement, et al., 2013)[19] proposed that the system be able to self-diagnose. Convention developed to aid secure transportation networks in VANETs provides an option for each arriving and active parcel to be identified and verified.

3. 2 Definitions and Models of Networks

Vehicles and Street Side Units (RSUs) speak with one another through short-range radio correspondence in the VANET.Certificate Specialists are outsider elements that give verification and assurance in VANETs (CAs).

CAs are responsible for dealing with the characters of the vehicles in the organization, just as checking bad conduct .Each vehicle has a white summary given by its gathering head, similarly as a blacklist containing an overview of malignant center points given by CA.

4. DESCRIPTION OF THE ALGORITHM

The three fundamental rules that the Location of Noxious Hub calculation depends on are:

1. A vehicle is considered to be acting unusually on the off chance that it drops or copies parcels shipped off it to cause network clog, mislead other vehicular hubs, or erase basic directives for individual addition.

2. A legitimate vehicle sends the messages it gets to different hubs in the organization in the right request or produces the right directives for transmission.

3. A vehicle will be marked vindictive on the off chance that it displays dubious movement regularly enough that its question esteem, DV, surpasses the edge esteem TMD.

Vindictive Hub Location in Vehicular Impromptu Organizations - DMN Calculation

In VANET correspondence, a hub fills in as a source, or the information generator. Another hub fills in as the message's objective, and there are moreover middle hubs between the source and the objective. as hubs that hand-off data When a vehicular hub VN goes about as a handing-off hub, it is observed by other confided in vehicles that go about as verifiers. VehicleVU tests the quantity of parcels got by VN (addressed by boundary a) and the quantity of bundles that VN drops or copies as seen by VU when going about as a VN verifier (addressed by boundary b).

In the event that, after a specific measure of time has passed PL, vehicle VN neglects to advance a got parcel or sends a few duplicates of it, verifier VU believes this to be sporadic conduct and raises the worth of boundary b by one unit. Every vehicle has a boundary called DV (doubt esteem), which changes when unusual conduct is distinguished. The two neighbors are recounted the new question esteem, and their rundowns are refreshed as needs be.

When on the white rundown, vehicles consent to each other in light of the fact that their Dv is not exactly the limit. On the off chance that it arrives at the edge, the vehicle's ID is hailed as a malevolent hub by the CA. The vindictive hub's ID is then transmission to any remaining hubs by CA. The verifier in the proposed Recognition of Vindictive Hubs (DMN) calculation is picked dependent on three boundaries: question significance, burden, and degree.

Those hubs in the area r are picked as verifiers whose Choice boundary, DP, is not exactly the Choice Edge, TVS, among other close by hubs (CH, VN). This technique streamlines the choice of verifier hubs, bringing about network transfer speed reserve funds and improved organization effectiveness.

Nodes in the r region are thought to be verifiers.

The crossing point space of vehicular hub VN and its CH is indicated by the locale r. The transmission scope of a vehicle is characterized by its space, and the space of a vehicle VN is resolved utilizing the recipe in Eq (1). Thus, the two verifiers will report mischief to the CH.

Region (VN) = TR(VN) – PL (Smx - Smn) (1)

where,

TR(VN) - Transmission scope of vehicle VN.

PL- vehicle’s Parcel inactivity.

Smx – vehicle’s Greatest speed .

Smn–Least Speed of vehicle

The boundaries for choice of verifiers in the space r are clarified beneath:

(L_D) – Also known as load. It refers to the number of hubs that are observed by a vehicle. The check position between the hubs is adapted. This is considered. Afterwards, a hub with less burden than others have a more significant opportunity to be selected as a verifier.

(D_V) - Also known as Distrust value. The fraction of the vehicle's trustworthiness is referred to. It means less esteem for doubt, more trustworthy is a hub. Should a vehicle exhibit an odd behavior, that value is also increased, as opposed to the limit for fitting options, i.e., a car should stay a white summary or a vehicle called dangerous and be placed to the blacklist.

(D_S) - Also known as Distance. If the distance between a hub and the vehicle is smaller, the hub will remain in the vehicle transmission range at this point for a time frame that is more precise. This therefore leads to improved perceptions and dynamics.

DP is defined by the heap, distance, and doubt of the hub by the following conditions for each of the hubs examined for verifier choice. (2).

$DP = W1 * LD + W2 * DV + W3 * DS$(2)

where, W1, W2, and W3 are the weight factors for boundaries Burden (LD), Doubt Worth (Dv) and Distance (DS) individually to such an extent that,

$W1+W2+W3 =1$(3)

Rather than choosing every one of the hubs with more modest doubt esteem than the vehicular hub VN, distributing not many checking measure helps in better revelation of toxic centers similarly as improves network execution. As couple of hubs play out the work of observing the hub VN, this saves network assets utilized for announcing the conduct furthermore, moderate their time for handling the noticed conduct for every one of the hubs. As the organization usage is improved, it brings about better transmissions in the organization.

This technique increases the selection of verifier emphasis. Cars understand the value of the vulnerability of various vehicles around. In particular, CH insists on the VU DV when a VU vehicle reports an odd direct from another VN vehicle that it is lower or indistinguishable from the VN DV. CH is seen as the strongest and most reliable focus of a social opportunity. Thereafter, checkers for an authentic focus point are not allocated to vehicles that are odd immediately as such cars have higher observable DVs when shown to match a conventional focus point. Chances that, CH is displaced by a truster vehicle are determined to be pernicious. As needed, the participants see the vehicles in all directions to perceive the focus on poison. In addition, the proposed technique enhances the determination of verifiers, which improves the usage of membership and re-designs implementation.

Stage 2: Get the gathering keys.

Stage 3: Register the boundaries Burden, Doubt Worth and Distance for the hubs in space of VN for verifier choice.

Step4: Compute the Choice boundary for verifier determination, DP.

$DP = W1 * LD + W2 * DV + W3 * DS$

Where,

$W1 + W2 + W3 = 1$.

W1, W2, and W3 are the weight factors for boundaries Burden (LD), Doubt Worth (DV) and Distance (DS) separately.

Stage 5: Discover hubs with Choice boundary esteem less then Choice Edge, i.e

$(DP < TVS)$

Stage 6: Apportion hubs got from Stage 5 as verifiers to the as of late joined vehicle VN.

Stage 7: Verifiers screen conduct of vehicle VN.

Stage 8: If (verifier recognizes vehicle VN showing unusual conduct)

Report to the group head (CH)

goto stage 9;

else

goto stage 7;

Stage 9: CH ascertains new doubt esteem (DV) of VN.

Stage 10: If doubt esteem is not exactly or equivalent to discovery edge i.e

assuming (DV < = TMD)

update the white rundown and goto 7

else

goto 11

Stage 11: Cautioning message is ship off any remaining hubs.

Stage 12: Update the passage of Vehicle VN in boycott.

Stage 13: Detach the recognized noxious vehicle from the organization.

5. PERFORMANCE EVALUATION

We used Network Simulator -2 to reproduce the proposed calculation Identification of Malevolent Hubs in Vehicular Specially appointed Organization (DMN) and assess its exhibition. For the calculation of the choice boundary, the weight factors for burden, distance, and doubt esteem are set to 40%, 30%, and 30%, individually. The proposed DMN calculation's proficiency is estimated as far as Bundle Conveyance Proportion, Normal Finish to End Deferral, and Throughput. Table 1 shows the reproduction boundaries used to assess the productivity of the DMN and DMV calculations.

Sr. No	**Parameter**	**Value**
1	No. of Nodes	50 , 100 , 200
2	Traffic Pattern	TCP/FTP, UDP/CBR
3	Network Size	2500×50 , 2000×100
4	Simulation Time	100 sec
5	Speed of Vechicles	70-120 km/hr
6	Packet transmission rate	5 packets/sec
7	Number of Malicious Nodes	5,8,10,25

Table 1.Simulation Parameters.

Metrics of Performance

The accompanying yield boundaries are contrasted with dmv to evaluate the exhibition of our proposed dmn calculation. normal throughput - throughput is characterized as the measure of information sent per unit of time or the normal pace of compelling message transmissions each second over a correspondence channel. bits each second (bits/s or bps) is the most widely recognized unit of measurement.(total got bundles)/((stop time - start time)) = throughput (four) parcel conveyance proportion - this measurement estimates the proportion of information bundles gotten by objective hubs to those produced by source hubs. parcel conveyance proportion = (information bundles got by objections)/(information bundles got by objections)/(information bundles got by objections)/(information parcel created by the sources) (no. 5) . start to finish delay - the period between bundle beginning at the source and parcel appearance time at the objective is known as start to finish delay. in the event that an information parcel. bundle conveyance time at objective - parcel beginning time at source = start to finish delay (6).imilar investigation of the above measurements of dmn and dmv is appeared in figure 1, figure 2, and figure 3**.**

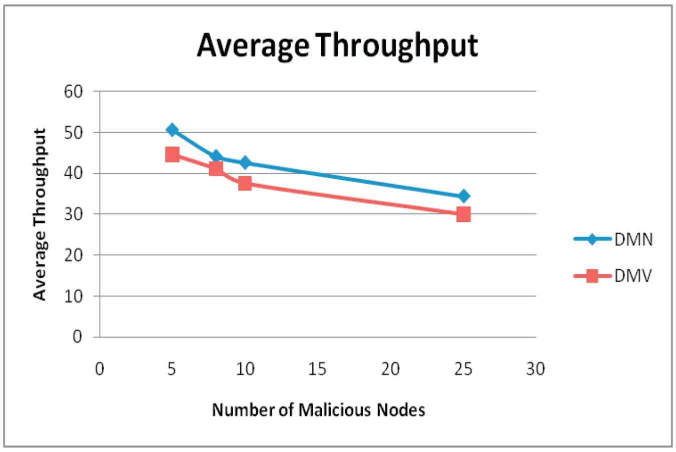


Figure1. Close to normal DMN and DMV performance research

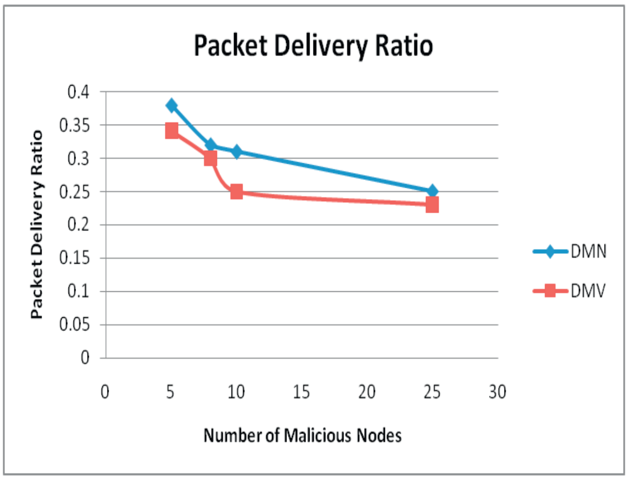


Figure 2. Near review of the DMN and DMV bundle transport ratio

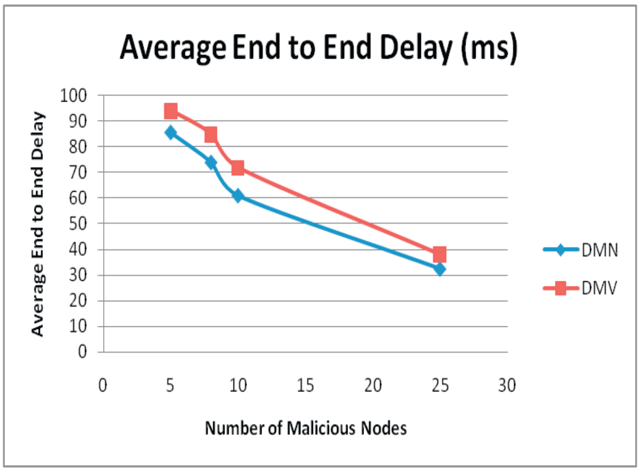


Figure 3. Relative review of normal beginning to complete DMN and DMV postponement

From the outcomes obtained, it is analyzed that DMN increases the likelihood of network execution of DMV by increasing the frequency with which verifier hubs are identified. It clearly and unequivocally demonstrates the higher levels of Normal Throughput, Parcel Conveyance Proportion, and Postponement Time vs the DMV, as far as what the preferred outcomes were.

6.Conclusion

We created DMN, a novel calculation for distinguishing mischievous activities and malignant vehicular hubs in VANETs (Discovery of Pernicious Hubs in VANETs). The DMN calculation is intended to seclude strangely acting hubs while as yet expanding network execution. DMN enhances the arrangement of verifier hubs, which play out the reason for checking hub conduct . DMN improves the DMV calculation, which chooses all hubs with a doubt esteem not exactly the vehicle to be checked as verifiers. Our proposed DMN calculation improved it by considering three boundaries when choosing fitting verifiers: burden, distance, and doubt esteem. These boundaries are utilized to decide a choice worth, which is then contrasted with the verifier determination limit. Picking the best verifiers improves the organization thus. By expanding network usage, this improves network unwavering quality. The reproduction results show that DMN has a higher throughput, a superior parcel transmission proportion, and a lower start to finish inertness than the DMV calculation tried in various situations in our reenactment setting. A vindictive hub security system could be applied to the proposed work. In the event that the proposed approach is applied continuously, it is simpler to gauge and test its exhibition under certifiable things.

REFERENCES

[1] Al-kahtani, MS. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In: 6th International Conference on Signal Processing and Communication Systems (ICSPCS); 2012. p. 1-9.

[2] Vulimiri A, Gupta A, Roy P, Muthaiah SN, Kherani AA. Application of Secondary Information for Misbehavior Detection in VANETs. Springer, IFIP, LNCS 2010. 6091: 385-396.

[3] Daeinabi A, Rahbar AG. Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks. Springer, Multimedia Tools and Applications 2013. 66: 325-338.

[4] Barnwal RP, Ghosh SK. Heartbeat Message Based Misbehavior Detection Scheme for Vehicular Ad-hoc Networks. In: International Conference on Connected Vehicles and Expo (ICCVE) 2012; p. 29-34.

[5] Mishra B, Nayak P, Behera S, Jena D. Security in vehicular adhoc networks: a survey. ACM, ICCCS; 2011. p. 590-595.

[6] Kim CH, Bae IH. A Misbehavior based reputation management system for vanets. Springer, LNEE 2012. 181: 441-450.

[7] Huang D, Williams SA, Shere S. Cheater Detection in Vehicular Networks. In: 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2012. p.193-200.

[8] Fonseca E, Festag A. A survey of existing approaches for secure ad hoc routing and their applicability to VANETs. NEC Network Laboratories; 2006.

[9] Ghosh M, Varghese A, Gupta A, Kherani AA, Muthaiah SN. Detecting misbehaviors in VANET with integrated root-cause analysis. Elsevier Ad Hoc Network, 2010; 8:778±790.

[10] Ghosh M, Varghese A, Kherani AA, Gupta A. Distributed Misbehavior Detection in VANETs. Wireless Communications and Networking Conference 2009; p.1-6.

[11] Harit SK, Singh G, Tyagi N. Fox-Hole Model for Data-centric Misbehaviour Detection in VANETs. In: Third International Conference on Computer and Communication Technology (ICCCT), 2012; p. 271-277.

[12] Grover J, Prajapati NK, Laxmi V, and Gaur MS. Machine Learning Approach for Multiple Misbehavior Detection in VANET. Springer, CCIS, 2011; 192: 644-653.

[13] Grover J, Laxmi V, Gaur MS. Misbehavior Detection Based on Ensemble Learning in VANET. Springer, LNCS, ADCONS, 2011; 7135: 602-611.

[14] Kadam M, Limkar S. Performance Investigation of DMV (Detecting Malicious Vehicle) and D&PMV (Detection and Prevention of Misbehave/Malicious Vehicles): Future Road Map. AISC Springer 2014; 247: 379±387.

[15] Bißmeyer N, Njeukam J, Petit J, Bayarou KM. Central Misbehavior Evaluation for VANETs based on Mobility Data Plausibility. ACM 9$1(7¶12, 2012.

[16] Wahab OA, Otrok H, Mourad A. A cooperative watchdog model based on Dempster±Shafer for detecting misbehaving vehicles. Elsevier, Computer communications 2014; 41: 43-54.

[17] Rawat DB, Bista BB, Gongjun Y, Weigle MC. Securing Vehicular Ad-hoc Networks Against Malicious Drivers: A Probabilistic Approach. In: International Conference on Complex, Intelligent and Software Intensive Systems (CISIS); 2011. p. 146-151.

[18] Rezgui, J.; Cherkaoui, S. Detecting faulty and malicious vehicles using rule based communications data mining. In: 36th Conference on Local Computer Networks (LCN), IEEE; 2011. p. 827-834.

[19] Coussement R, Saber BAB, Biskri I. Decision support protocol for intrusion detection in VANETs. ACM, DIVANet '13; 2013. p. 31-38.

[20] Ruj S, Cavenaghi MA, Huang Z, Nayak A, Stojmenovic I. On Data-Centric Misbehavior Detection in VANETs. In: Vehicular Technology Conference (VTC Fall), IEEE; 2011. p.1-5.

[21] Liu Y; Bi J, Yang J. Research on Vehicular Ad Hoc Networks. In: Control and Decision Conference; 2009. p. 4430-4435.

[22] Isaac JT, Zeadally S, Camara JS. Security attacks and solution for Vehicular ad hoc Networks, IET communication 2010; 4: 894-903.

[23] Hussain R, Son J, Oh H. Anti Sybil: Standing against Sybil attacks in privacy preserved VANETs. In: International Conference on Connected Vehicles and Expo, IEEE; 2012. p. 108-113.

Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 6, July2021: 9262 - 9266

SPAM: Electronic Advertisement Tool in Information Sector

Dr. Ruchi Singhal
Associate Professor
Department of Information Technology
Jagannath International Management School, New Delhi

Dr. Shalu Tandon
Assistant Professor
Department of Information Technology
Jagannath International Management School, New Delhi

Abstract

Usually, e-mails spammers search for economic income by promoting services and products. Performing mail bombing is neither difficult nor expensive. If appropriately used, internet advertising can be appealing to consumers and cost-effective to advertisers. The purpose of most spam e-mail messages distributed over the Internet today is to entice the recipients into visiting World-Wide sites advertised through spam. E-mail spamming is a campaign that broadcasts in the Information sector at a massive scale and a minimum cost for the advertisers and those advertised.

The characteristics of spam-advertised websites, however, have not been widely examined. This paper will explore the properties of URL dissemination through spam e-mail and how the spammer in the information sector received the e-mail addresses and sends this advertisement to the user. Ultimately, dealing with Internet advertising is like dealing with any other type of advertising is discussed.

Keywords: Internet, e-mail, Spam, Type of Spam, URL, Facts & Figure**.**

1. INTRODUCTION

An increasing number of people see an ad on the Internet and click on it for more information. For these people, the Internet is a way to slow down business. Depending on the professionalism of the ad, the viewer may be able to obtain product details, comparative details of other products, a list of current retailers selling the product (and the price per item), and an electronic order form. People may buy everything on the Internet, from plane tickets to online businesses, and they are enticed to online products by advertisements. The Internet is an attractive tool for advertisers and advertisers. An ad posted on the Internet has the potential to reach millions of people anywhere in the world. An Internet user who sees an ad can choose to click on it and be added to their e-mail list if they choose, while the uninterested person may ignore the ad. Many people would like to be on such a list. These lists can allow the consumer to receive information about new products and special offers via e-mail. Users can do advertising via e-mail. It is a low-cost method for businesses to reach out to potential clients or buyers. Usually, the company will pick up the customers' e-mail addresses and ask them if they wish to receive special offers or company news via e-mail. Those who say yes will receive periodic product updates as well as specialized online shopping officials. Customers can log in or out of the system. An E-mail has the advantage of fast delivery and low cost; even a company without a website can send an e-mail.

Unsolicited electronic advertising, or spam, has become a prevalent problem for anyone with an e-mail account. Spam is an unsolicited e-mail and is very popular with advertisers because it is easy and because it costs a small part of what it costs many people to send. By posting the truth, the advertiser must pay for paper, print, and postage. With e-mail ads, none of these costs is available. Spam is considered an electronic advertisement in this study. The following section discusses the types of spam. How is the spam in the media getting e-mail addresses, and how to send this ad to the user for-profit and receives the products with a single click? Facts and costs define the number of spam marketing growth statistics. The final section concludes with the words.

2. Spam as Electronic Advertisement

If you are using e-mail, you may have recently received spam meaning an unsolicited, unwanted message sent to you without your permission. The Internet version of junk e-mail is phone sales during lunch, unanswered calls, and brochures attached to the city, all wrapped up in one annoying bullet. Spam is divide into three sorts, each of which is further subdivided into categories.

2.1 Advertising Spam

Most spam is a commercial ad, usually a direct product offering. Spam costs less to send, compared to other advertising methods. The lowest categories of ad spam are: -

- Online Pharmacy spam: Spam that promotes various forms of Viagra, Cialis, anti-depressant pills can be purchased online.
- Pornography or dating: Spam was frequently used to promote pornography and dating services.
- Pirate Software Spam: Spam that offers pirate software, usually cheaper than official prices.
- Penny Stock Spam: Spam that promotes stocks encourages people to buy cheaper stocks.
- Online Casino Spam: Spam that promotes gambling at online casinos
- Mule job spam: Promoting jobs 'working at home.
- Spamming of Fake degree: Spammers regularly try to sell fake ranges and diplomas.

2.2 Spam Advertising Spam

While the ad spam has at least a slight chance that the respondent can get something with the money sent, the financial spam is trying to trick people and get their money in some way, without the opportunity to buy anything. There are different types of financial spam:

- Lottery Spam: Similar to the 419 scams, these spammers say, 'You have already won X Million' to try to withdraw money etc.
- 419 scams: Many people seek assistance to withdraw millions of dollars from a foreign bank account.

2.3 Criminal Advertising Spam for phishing scams

Spam phishing scam alerts fake PayPal banks, eBay etc. You are also requesting verification, verification or lease of information to defraud people with their data. Fake credentials are frequently used in spam phishing schemes to collect user information (e.g., passwords) and exploit that information to steal money or products. The term "identity theft" was coined as a result of fraud. Fraudulent e-mails hurt their victims with financial loss and identity theft. They are also back in online business because people are losing trust in online transactions. Phishing e-mails use the most listed methods:

- Company logo: fraudulent e-mails often have the company logo and use the same fonts and colour schemes.
- Real Company Site Links: The central link in a fake e-mail sends the recipient to this fraudulent website, but most fraudulent e-mails include other links that send the recipient to the honest company's website sections.
- E-mail appears to be from a corrupt company: To continue to make the recipient available as an e-mail from the company, spam using an e-mail address that appears to be from the company, for example @ eBay.co @paypal .com.

The next section of the paper discusses how spammers get a user's e-mail addresses.

3. Download E-mail ID by Spammer

Using advertising as a way to track customers and their interests is not new. The 20th century saw an increase in targeted advertising based on information provided voluntarily by consumers. There are various ways to achieve this, with the twofold goal of determining which advertising is most effective and which customers accept the most. In the current context, the Internet is a powerful tool. Most users use e-mail to receive and send information. IT is a highly efficient technique to communicate via the Internet. Apart from this, it is a vast question how these spammers get their e-mail addresses. There are many spam ways to get id to send an ad. newsgroups and chat rooms of significant sites. People, especially first-time users, often use their names on the screen or leave their e-mail addresses in newsgroups. Spam uses software fragments to remove screen names and e-mail addresses automatically. Another way to e-mail addresses is the Web itself. There are tens of millions of sites, and spammers can build web spiders search engines that look for the "@" sign that indicates an e-mail address. Spidering programs are often called spambots.

Additionally, there are many sites explicitly created to attract e-mail addresses. For example, spam started the site, "Win $ 1 million !!! type an e-mail address here! ". In the past, many large sites also sold their members' e-mail addresses. Or sites that have created an 'opt-in' e-mail list by asking, 'Would you like to receive e-mail newsletters from partners? If yes, the e-mail address will then be sold to spam. The most typical supply of e-mail addresses is dictionary seek of e-mail servers for massive electronic mail hosting companies consisting of MSN, AOL or Hotmail.

4. Spam marketing statistics

Spammers can send more messages every day due to the ever-growing power of bandwidth and computer power.

4.1 Facts and Diagram

According to the latest figures published by Brightmail, the largest commercial company fighting spam before being introduced by Symantec. As of January 2004, 60% of all e-mails they viewed were spam. Their most recent survey in July 2004 showed a spam rate of 63%. According to Message Labs, 72 per cent of all e-mails were sent to spam as of July 2004. In September 2004, they received approximately 1.2 billion spam e-mails making up about 64% of tested e-mails. Statistics from April 2005 showed that 67% of Internet users do not like spam, and 33% dislike spam and cause them anxiety, while only 33% of users have no problem with it. Although the image shows an average of 33 per cent, it is essential to note that two-thirds of users have a problem with spam. Most Internet users still rely on e-mail. In February 2003 and 2007, 91% of internet users reported using e-mail. A few other e-mail users now say spam has completed their e-mail creation. In the survey, 19% of users said spam had lowered the number of e-mail users, down from 22% in 2005, 29% in 2004, and 25% in 2003. This number is increasing day by day. Not surprisingly, people who are likely to report reduced e-mail usage are those who say spam is a big problem for them. 18% of electronic mail customers who say unsolicited mail is a prime hassle, about one-third (37%) say that junk mail has brought about them to use e-mail much less. Best 15% of different e-mail customers, who are barely laid low with spam, claim that junk mail has reduced their e-mail usage. These surprisingly large numbers make it clear that the increase in spam is still growing. For most types of advertising, the cost of sending each message is high, especially when it comes to product costs and market size.

A full-page ad in a major newspaper can cost anywhere from $ 24 for a regular standalone ad to $ 25,000 for a full-page ad. Sending a catalogue to 100,000 people can cost anywhere from $ 50,000 to $ 150,000, depending on the size of the ledger, print quality, and the type of shipping used. Compare these costs with the cost of sending an e-mail message or sending an article to Usenet. A typical Internet-connected computer with a 28.8 kbps dialling module can send over 100 letters per minute, translate 864,000 messages per day, or 26 million per month on average. With ISPs offering unlimited dial-up access to the Internet for $ 20 a month or less and a dedicated phone line costing another $ 15, spam can send up to 10,000 e-mail messages per pen. Even if you add up the cost of buying a computer (maybe $ 1,000), electronic advertising is the cheapest way to reach the audience. These low costs encourage spammers to send even bigger messages. Businesses that advertise the use of traditional media make an effort to get their notifications across. The common denominator is that there is no reason to send an ad to someone who can't afford the advertised product - there is no reason to spend money advertising dog food to cat owners. But spam has no intention of identifying its messages, as the cost of electronic messaging is meagre.

5. Revolution with Spam Marketing

Most of the spam messages on the Internet today are ads from individuals and small businesses from time to time looking for a way to make quick money. Spam mails are frequently transmitted using sophisticated techniques that conceal the genuine senders of messages and points. Spammers use various methods to find e-mail addresses, such as picking them up from web pages and downloading them from the e-mail address references used by Internet service providers (ISPs). But spam today may change. Last year, AT&T, Amazon.com, and OneSale.com all tried with multiple e-mails. Although companies explicitly disclose themselves in mail messages, this mass delivery can create many of the same problems as spam messages from people and less responsive companies. If these companies continue their testing, and if they join others, we will see a tremendous increase in the amount of spam on the Net. People who send messages say that e-mail is a form of electronic marketing and Internet equivalent to radio ads and newspaper ads. However, there is a significant difference between electronic spam and traditional marketing methods, and if spam can be removed, the Internet may be abandoned.

6. Conclusions

These days' human beings use the word "spam" to consult nearly any form of an unwanted e-mail message or news article they receive. E-mail spam serves as a cheap and easy way to distribute URLs advertised with spam and their websites to millions of Internet users in the information sector. As a result, advertising on these websites may be considered the cause of the spam e-mail problem. As a result, spamming is a continuous campaign that promotes URL addresses to marketers and advertisers at a high and low cost. There are, however, significant differences between spam and general advertising campaigns. Available campaigns seek to make the names of products and services known and easily recognizable.

In contrast, spam campaigns promote URL addresses that are intentional, inaccessible, and therefore easily identifiable. However, this information shall come out attractively and credibly to attract recipients to take immediate action. They are addressing this concern by investigating the use of voting procedures, collaborative identification and classification of suspicious URL addresses that use spam as a means of advertising. Spam can advertise anything from magazines to electronics to travel packages. But one of the most widespread and most offensive spam uses for advertising on pornographic and e-books websites.

7. REFERENCES

[1]. J.Provost, NaiVe-Bayes vs rule-learning in classification of E-mail, Technical-report, University of Texas at Austin, 1999.

[2]. Kojima H.. Chung C., Westen C., Strategy on the landslide type analysis based on the expert knowledge and the quantitative prediction model, ISPRS 2000, Amsterdam.

[3]. L. Zhang and T-Yao. Filtering Junk Mail with a maximum

[4]. Entropy Model. In Proceeding of the 20th International Conferences on Computer Processing of Oriental Languages, (2003) Pages 446-453.

[5]. Jon Praed "Latest trends in the Legal Fighter Against Spammers" Spam Conference 2004.

Design Engineering

ISSN: 0011-9342
Issue: 7 | Pages: 5097-5101

Deny All – A Matter of Trust in Network Security

Dr. Shalu Tandon
Assistant Professor
Department of Information Technology
Jagannath International Management School, New Delhi

Ms. Priyanka Rattan
Assistant Professor
Department of Information Technology
Jagannath International Management School, New Delhi

Dr. Ruchi Singhal
Associate Professor
Department of Information Technology
Jagannath International Management School,
New Delhi

Abstract

In the Recent Developing years, there has been forever a dialogue on whether or not to digitalize everything doable or undue to that online security has become a heatedly debated topic. A good variety of people are unit exacting to own access to any or all of their digital resources anyplace anytime; however, thanks to the increasing variety of users, the number of cybercrimes will increase at the same time. This analysis paper focuses on elaborating on what is zero-trust approach and its info security framework.

Keywords— Zero Trust Network, info Security Network framework, cybercrime, Deny All

INTRODUCTION

The term 'zero trusts' was coined by an Associate in Nursing analyst at Forrester analysis Iraqi National Congress. in 2010 once the model for the thought was given first. some years later, Google proclaimed that it had enforced zero trust security in its network, that junction rectifier to a growing interest in adoption among the technical school community.[1]

Zero Trust, in contrast to the traditional model, has as its principle "never trust, forever verify," wherever each internal and external network cannot be sure. This principle is that the basis for reducing the chance of attacks is not solely external however can be jointly internal.

The framework dictates that solely echt and approved users and devices will access applications and knowledge. At constant times, it protects those applications and users from advanced threats on the net.

At the starting of zero-trust security, it needed careful implementation by security engineers that junction rectifier the most target the core principles and technologies as per the organization. However, as per the introduction of Cloudflare Access, any organization will currently quickly and implement a zero-trust security system on their network.

Access management technologies are an essential unit to use to a Zero Trust approach. To stay things as economical as doable, Command and management over WHO accesses the network and ultimately, the info is vital to Zero Trust. The zero trust model brings new ideas to style Associate in Nursing info security network, which permits increasing the micro-segmentation of a network to own additional visibility overall traffic by inspecting every kind of user and device that connect within the network.

BeyondCorp is an Associate in Nursing example of a zero-trust design designed by Google.[4]

HISTORY OF ZERO TRUST SECURITY NETWORK

John Kindervag first explored the Zero Trusty Model at Forrester analysis INC. in 2010. Connected frameworks embrace Google's BeyondCorp, Gartner's CARTA and MobileIron’s zero trust models. Once the model for the conception was first bestowed. Some years later, Google proclaimed that they had enforced zero trust security in their network, that semiconductor diode to a growing interest in adoption at intervals the technical school community.

In 2014, Google printed BeyondCorp as an employee of the Zero Trust framework. BeyondCorp suggests three key ideas: connecting from a specific network must not verify the services you will be able to access; access ought to be granted what is well-known regarding the user and the device; and at last, all access to services should be echt, approved and encrypted.

The idea of a sure internal perimeter leaves the organization in danger if that perimeter is compromised or an associate corporate executive turns malicious. Organizations have evolved their secure network framework and their parameters conjointly due to technologies, and the state of affairs has grown since 2009.

THEORETICAL ANALYSIS

With the modern workforce turning into on the go, accessing of the applications using various personal & unmanaged devices from different locations of the business perimeter, enterprises have adopted a "network security framework" model which suggests if somebody has the proper user credentials, they are admitted to whichever website, app, or the device they are requesting. Because of the increasing variety of electronic devices obtaining connected to the cloud and also the increasing variety of users day by day at the same time, the amount of cybercrime, invasion of privacy, unauthorized access, and security breaches are reaching new heights.

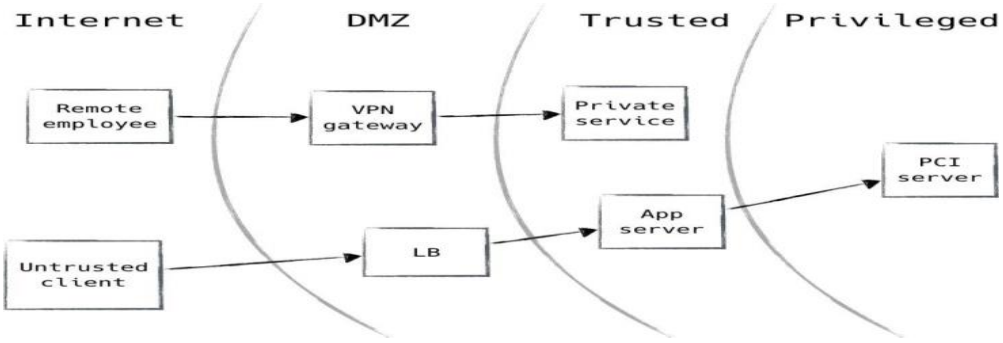
This leads to associate increasing risk of exposure, dissolving what was once the sure city district of Management and several organizations are exposed to information breaches, malware and ransomware attacks. Protection is currently required wherever applications and information, and users and devices, are placed. Zero trust security means nobody is sure by default from within or outside the network, and verification is needed from everybody attempting to access resources on the web. This intercalary layer of security has been shown to stop information breaches. A recent IBM-sponsored study incontestable that the standard price of one information breach is over $3 million. Considering that figure, it ought to return as no surprise that several organizations currently want to adopt a zero-trust security policy. Due to a rise in the mobile workforce and also the widespread adoption of cloud services, it is not safe to assume that your information is secure just because a certificate checks out. With most information breaches involving taken credentials, approved and unauthorized access will look identical. The standard perimeter has rapt on the far side of the network to where the user is attempting to access the information.

IMPLEMENTATION

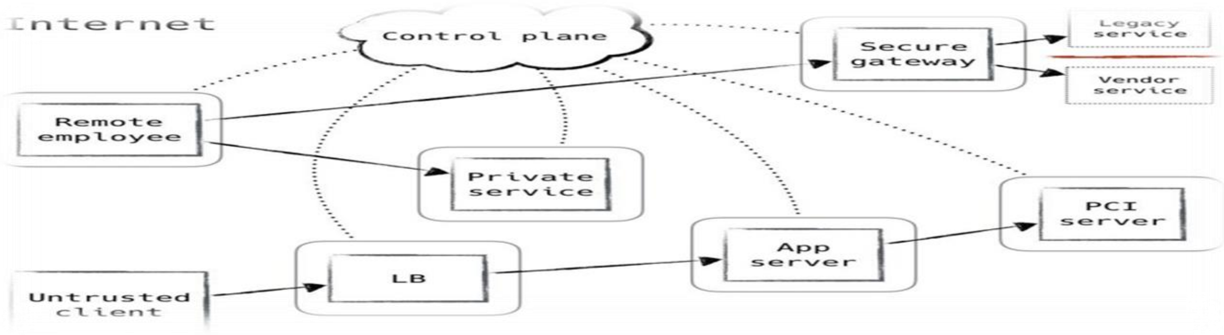
As the typical models are not helpful, we won't let the protection of our organization be relied upon strictly on a firewall or intrusion hindrance system. The Zero Trust could be a security model developed by JohnKindervag at Forrester analysis that has the principle of "never trust, continually verify,", This design is intended to mitigate threats at intervals of network-specific information or assets additional granular rules will be applied. In keeping with analysis, Zero Trust isn't creating networks, clouds, or endpoints additional reliable. However, it is functioning on eliminating the thought of invasion with authorization from digital systems. Therefore Zero Trust is all concerning. However, you think that there are no singular means for implementing this sort of design. Once building a network with zero trusts their area unit, some necessary aspects that you simply ought to detain mind that area unit is as follows:

- Ensure all information area units firmly accessed supported users and sites.
- The use of access management is powerfully advised/required.
- Inspect the logs of all traffic.

This is necessary in a world where quality is apace changing into dominant tablets, smartphones, laptops, and IoT devices accessing the web. These devices got to access these resources Associate in Nursing exceedingly|in a very} secure means and also the accessibility of any help ought to be encapsulated at intervals in an envelope of the zero-trust security framework. Traditional network security design breaks different networks into zones that are unit secured by one or additional firewalls. Every zone is granted some level of Trust that determines the network resources permissible to its reach. This model provides sturdy weaponry.[3] For example, resources classified additional risky, like internet servers that face the general public web, area units placed in Associate in a Nursing exclusion zone, wherever traffic will be tightly monitored and controlled severally and vividly. Such an Associate in Nursing approach offers rise to Associate in Nursing design that's just like some you would possibly have seen before. The Traditional Model of network security is more detailed through the following diagram:



If the standard security design is replaced with the new and evolved Zero Trust Security design, it'll flip the complete model and the thought of security up-side-down. The Zero Trust model of network security is more detailed through the following diagram:



A zero-trust network is constructed upon five bare assertions.

- The web is often assumed to be hostile.
- External and internal threats exist on the network in respect to times.
- A network neighbourhood isn't adequate for deciding Trust in the same network.
- Every device, user, and network flow is echt and approved.
- Policies should be dynamic and calculated as several sources of knowledge as doable.

The Zero Trust approach depends on varied technologies and governance processes to secure the enterprise atmosphere.

It entails enterprises to leverage micro-segmentation and granular perimeter social control supported users, their locations and alternative information to determine whether or not to trust a user, machine or application seeking access to a specific part of the enterprise.

Zero Trust attracts multi-issue authentication, IAM, orchestration, analytics, encryption, grading and classification system permissions. Zero Trust conjointly entails governance policies like giving users a quantity} amount of access they have to accomplish a particular task.

CYBERCRIME AND SECURITY

Security and technology consultants say the standard means isn’t operating. They aim to the fact that a number of the foremost conspicuous information breaches happened due to hackers, once they gained access within company firewalls, were ready to move through internal systems while not a lot of resistance. One of the inherent issues we've in it's we tend to let too several things run means too brazenly with too several default connections. That's the rationale why the web took off as a result of everybody might share everything all the time. however, it's conjointly a key fail point: If you trust everything, you don't have an opportunity to fix something security-wise.[2]

With the rise within the variety of devices connected to the web and consequently additional attack areas for cybercriminals, the financial values concerned in cybersecurity have been increasing. Cybersecurity is involving protective info and cyber threat systems. Threats are being exposed as malware

(malware, ransomware, phishing, worms) on unmanaged devices. These weapons are more and more subtle and automatic and are being purchased at low value. With this, firms have a "punctual products" approach to combat these threats.

Zero Trust could be a philosophy that brings innumerable blessings on many levels to the corporate hierarchy. Zero Trust delivers security and spectacular business results in keeping with the new and advanced design of the security framework. From a very back-end perspective, it provides reduced time to breach detection and acquire visibility into all of your company traffic by inspecting the user request, devices, and data. In a very front-end perspective, Zero trust avoids the terms and conditions of economic prices in security audits, maintaining a proper name towards alternative firms. Some attacks against the Zero Trust networks area unit are well mitigated, whereas others can solely sight the attack. No model is ideal and 100% effective; however, we can scale back the impacts caused by any attack.

CONCLUSION

The Zero Trust model of data security primarily kicks to the curb the previous mentality that had organizations targeted on defensive their perimeters whereas assumptive everything already within didn't cause a threat and so was cleared for access. Experts say that today's enterprise IT departments need a brand new method of thinking as a result of, for the foremost half, a personal itself now not exists in isolation because it once did. Firms that don't have company knowledge centres serving a contained network of systems. However, instead, these days generally have some applications on-premises and a few within the cloud with users like staff, partners, customers accessing applications from various devices from multiple locations and even doubtless from around the globe. All these small still as macro changes have junction rectifiers to the current new model that points out only 1 question: Can we secure ourselves during this new model? Senior vice chairman of merchandise and chief product officer at Centrify firm aforementioned that the new firewall is on the point of the quality you're attempting to shield during this new world.

REFERENCES

[1]. Pedro Assunção (2019), A Zero Trust Approach to Network Security (10.11228/dpsc.01.01)[1]
[2]. DaynaEidle, Si Ya Ni, CasimerDeCusatis, Anthony Sager Oct2017)Autonomicsecurityforzerotrustnetworks[2]
[3]. CasimerDeCusatis, PiradonLiengtiraphan, Anthony Sager, Mark Pinelli (Nov 2016) Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication.[3]
[4]. Mary K. Pratt (Jan 2018) What is Zero Trust? A Model for more effective security.[4]
[5]. Chase Chunninham (Mar 2018) Next-generation access and zero Trust.[5]
[6]. Doug Brath, Evan Gilman - Zero trust networks.[6]

पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 33/2021	शुक्रवार	दिनांक: 13/08/2021
ISSUE NO. 33/2021	FRIDAY	DATE: 13/08/2021

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

(12) PATENT APPLICATION PUBLICATION (21) Application No.202141034643 A

(19) INDIA

(22) Date of filing of Application :02/08/2021 (43) Publication Date : 13/08/2021

(54) Title of the invention : AUTOMATIC CONTROL OF WINDOW CURTAINS USING ALEXA AND ARUDINO

(51) International classification	:G05B0015020000, G06F0008300000, H04L0012280000, E06B0009240000, G10L0013000000
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(86) International Application No	:NA
Filing Date	:NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number	:NA
Filing Date	:NA
(62) Divisional to Application Number	:NA
Filing Date	:NA

(71)**Name of Applicant :**
1) Dr. R. MANIKANDAN
Address of Applicant :ASSISTANT PROFESSOR & HEAD, DEPARTMENT OF COMPUTER SCIENCE, THE QUAIDE MILLETH COLLEGE FOR MEN, MEDAVAKKAM, CHENNAI - 600100, TAMILNADU, INDIA. Tamil Nadu India
2)Dr. PALLAVI KAPOORIA
3)Dr. GUNJAN ANAND
4)Dr. MUKESH THAKUR
5)Mr. DEEPAK SHARMA
6)Dr. V. P. MUHAMMED BASHEER
7)Dr. SAURABH SINGH
8)Dr. S.S.K. DEEPAK
9)Mr. PAPARAO, KAMBALA
10)Dr. ALFRED YUSUF SHAIKH

(72)**Name of Inventor :**
1) Dr. R. MANIKANDAN
2)Dr. PALLAVI KAPOORIA
3)Dr. GUNJAN ANAND
4)Dr. MUKESH THAKUR
5)Mr. DEEPAK SHARMA
6)Dr. V. P. MUHAMMED BASHEER
7)Dr. SAURABH SINGH
8)Dr. S.S.K. DEEPAK
9)Mr. PAPARAO, KAMBALA
10)Dr. ALFRED YUSUF SHAIKH

(57) Abstract :

The present invention is related to the field computer science and engineering. Smart curtains allow-to save time and makes the home a smart one. It helps to create a smart home with its innovative way in opening and closing of curtains upon commands from humans. This proposal provides the implementation of automatic opening and closure of window curtains in home/offices using electronic and telecommunication systems. The allowable input is the voice command via Alexa that proceeds with the operation of smart curtains upon the comfort of the user. The window curtains are built with Arduino microcontroller module that helps in opening and closure operations. The Arduino connected with amazon Alexa device gets the input signal via humans regarding the opening and closure of window curtains. The embedding of Alexa unit helps in controlling the smart curtains even the user is in remote locations.

No. of Pages : 14 No. of Claims : 6

पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 40/2021	शुक्रवार	दिनांक: 01/10/2021
ISSUE NO. 40/2021	FRIDAY	DATE: 01/10/2021

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

INTRODUCTION

In view of the recent amendment made in the Patents Act, 1970 by the Patents (Amendment) Act, 2005 effective from 01st January 2005, the Official Journal of The Patent Office is required to be published under the Statute. This Journal is being published on weekly basis on every Friday covering the various proceedings on Patents as required according to the provision of Section 145 of the Patents Act 1970. All the enquiries on this Official Journal and other information as required by the public should be addressed to the Controller General of Patents, Designs & Trade Marks. Suggestions and comments are requested from all quarters so that the content can be enriched.

(Shri Rajendra Ratnoo)
CONTROLLER GENERAL OF PATENTS, DESIGNS & TRADE MARKS

1ST OCTOBER, 2021

CONTENTS

(12) PATENT APPLICATION PUBLICATION
(21) Application No.202111042101 A

(19) INDIA

(22) Date of filing of Application :17/09/2021
(43) Publication Date : 01/10/2021

(54) Title of the invention : STUDENT ATTENDANCE MANAGEMENT SYSTEM AND METHOD THEREOF

(51) International classification	:G06Q 50/20
(86) International Application No	:NA
Filing Date	:NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number	:NA
Filing Date	:NA
(62) Divisional to Application Number	:NA
Filing Date	:NA

(71)**Name of Applicant :**
1)Dr. Shalu Tandon
Address of Applicant :Assistant Professor, Jagannath International Management School, Vasant Kunj, New Delhi, India ----------- -----------
2)Dr. Neha Arora
3)Dr. Manpreet Arora
4)Ms. Priyanka Rattan
5)Dr. AR.Saranakumar
6)Dr. R.RADHA
7)Dr. Shreevamshi
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr. Shalu Tandon
Address of Applicant :Assistant Professor, Jagannath International Management School, Vasant Kunj, New Delhi, India ----------- -----------
2)Dr. Neha Arora
Address of Applicant :Post Graduate Teacher (Informatics Practices), Army Public School, Mumbai, Maharashtra, India ----------- -----------
3)Dr. Manpreet Arora
Address of Applicant :Post Graduate Teacher (Computer Science), Kendriya Vidyalaya No. 3, Colaba, Mumbai, Maharashtra, India ----------- -----------
4)Ms. Priyanka Rattan
Address of Applicant :Assistant Professor, Jagannath International Management School, Vasant Kunj, New Delhi, India ----------- -----------
5)Dr. AR.Saranakumar
Address of Applicant :Assistant Professor (Stage-3), Department of Education, DDE & Head Incharge, Department of History, Alagappa University, Karaikudi, Tamil Nadu, India ----------- -----------
6)Dr. R.RADHA
Address of Applicant :Teaching Assistant, Department of History, Alagappa University, Karaikudi, Tamil Nadu, India ----------- -----------
7)Dr. Shreevamshi
Address of Applicant :HOD, BMS Department, School of Commerce, Jain (Deemed to be University), Bangalore, India ----------- -----------

(57) Abstract :

A student attendance management system and method comprising managing attendance in online mode (100) as well as offline mode (201). The online mode system comprises a student ID with QR code (101); a website with QR code verification system (103); a database (104); a user platform (105); internet (106). The offline mode (201) system comprises a student ID card with RFID (207); a RFID reader at school/ college door (208); a face camera unit (209); database (210); intranet (211). The system and method provides a quick and precise attendance system with camera analysis and class review, which help in verifying the attandancy person

No. of Pages : 18 No. of Claims : 10

पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 53/2021	शुक्रवार	दिनांक: 31/12/2021
ISSUE NO. 53/2021	**FRIDAY**	**DATE: 31/12/2021**

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

INTRODUCTION

In view of the recent amendment made in the Patents Act, 1970 by the Patents (Amendment) Act, 2005 effective from 01st January 2005, the Official Journal of The Patent Office is required to be published under the Statute. This Journal is being published on weekly basis on every Friday covering the various proceedings on Patents as required according to the provision of Section 145 of the Patents Act 1970. All the enquiries on this Official Journal and other information as required by the public should be addressed to the Controller General of Patents, Designs & Trade Marks. Suggestions and comments are requested from all quarters so that the content can be enriched.

(Shri Rajendra Ratnoo)
CONTROLLER GENERAL OF PATENTS, DESIGNS & TRADE MARKS

31st DECEMBER, 2021

CONTENTS

(12) PATENT APPLICATION PUBLICATION (21) Application No.202111059550 A

(19) INDIA

(22) Date of filing of Application :20/12/2021 (43) Publication Date : 31/12/2021

(54) Title of the invention : AN IOT BASED COMPUTER SYSTEM FOR EFFICIENT HEALTHCARE DA0TA MANAGEMENT

(51) International classification	:H04L0029080000, G16H0010600000, G06Q0050220000, H04L0029060000, G16H0050700000
(86) International Application No	:NA
Filing Date	:NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number	:NA
Filing Date	:NA
(62) Divisional to Application Number	:NA
Filing Date	:NA

(71)**Name of Applicant :**

1)Mr. Deepak Sharma

Address of Applicant :Assistant Professor, Dept. of Information Technology, Jagannath International Management School, New Delhi, India ----------- -----------

2)Dr. Meenakshi Narula

3)Dr. Archana Chaudhary

4)Dr. Seema Bargale

5)Dr. Ruchi Singhal

6)Veeresh Rampur

7)Omdev Dahiya

8)Deepjyoti Santra

9)Arindam Pal

10)Mr. Sam Paul B

11)Ankur Gupta

Name of Applicant : NA

Address of Applicant : NA

(72)**Name of Inventor :**

1)Mr. Deepak Sharma

Address of Applicant :Assistant Professor, Dept. of Information Technology, Jagannath International Management School, New Delhi, India ----------- -----------

2)Dr. Meenakshi Narula

Address of Applicant :Professor, Dept. of Information Technology, Jagannath International Management School, New Delhi ----------- -----------

3)Dr. Archana Chaudhary

Address of Applicant :Associate Professor, Faculty of Science (FOSC), SGT University, Gurugram, Haryana, India ----------- -----------

4)Dr. Seema Bargale

Address of Applicant :Professor, Dept. of Pediatric and Preventive Dentistry, K M Shah Dental College and Hospital, Sumandeep Vidhyapeeth Deemed to be University, Vadodara-391760, Gujarat, India ----------- -----------

5)Dr. Ruchi Singhal

Address of Applicant :Associate Professor, Dept. of Information Technology, Jagannath International Management School, New Delhi, India ----------- -----------

6)Veeresh Rampur

Address of Applicant :Assistant Professor, Dept. of Electronics, Government First Grade College, Bidar, Karnataka, India ----------- -----------

7)Omdev Dahiya

Address of Applicant :Assistant Professor, School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India ----------- -----------

8)Deepjyoti Santra

Address of Applicant :Assistant Professor, Dept. of Electrical Engineering, Global Institute of Management and Technology, Krishnanagar, Nadia, West Bengal, India ----------- -----------

9)Arindam Pal

Address of Applicant :Assistant Professor, Dept. of Electrical Engineering, Global Institute of Management and Technology, Krishnanagar, Nadia, West Bengal, India ----------- -----------

10)Mr. Sam Paul B

Address of Applicant :Assistant Professor (OG), Dept. of Management Studies, SRM Valliammai Engineering College, Kattankulathur, Chengalpattu, Tamil Nadu, India ----------- -----------

11)Ankur Gupta

Address of Applicant :Assistant Professor, Dept. of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India ----------- -----------

(57) Abstract :

In this invention, the issue of outsourcing of data in cloud is addressed by the method of key generation for cloud user. Cloud computing, besides providing a maximized effectiveness of shared resources, also provides an easy way of storing and retrieving data. Personal Health Records (PHRs) are designed to maintain lifelong details of patients. Automated Patient Identifier and Patient Care System is designed to count hospitalized patients based on the concept of Current Procedure Terminology (CPT) manager. Cloud storage service is accessed through the cloud computer service, web service application programming interface or by a cloud storage gateway. The cloud based workspace is centralized providing easy functionality to share. The cloud environment can provide improvements in system efficiency & density.

No. of Pages : 14 No. of Claims : 4

Advances and Applications in Mathematical Sciences
Volume 20, Issue 10, August 2021, Pages 2127-2135
© 2021 Mili Publications

IMPLEMENTING AUTOMATED ALGORITHMIC COMMODITY TRADING USING PYTHON

MEENAKSHI NARULA and DIVISHA ROHATGI

Department of Information Technology
Jagannath International Management School
Kalkaji, New Delhi-110019, India

Abstract

All the main stock and commodity exchanges throughout the world are using electronic trade execution systems which have opened up doors for use of automated trading program within the business insight frameworks for any money related or investment company. This kind of automated trading systems can rule out the negative impact of human emotions such as fear and greed on trading activities. Various online trading platforms are also motivating traders to use such automated system by providing them interface, technical support and allowing them to integrate third party software and tools with their trading platforms. To design such reliable automated trading systems which can use predefined strategies and can place high frequency trades, is becoming a challenge. In this paper an automated algorithmic trading application has been implemented using a price action strategy and tested in real time commodity exchange (MCX).

I. Introduction

Before the evolution of electronic trading, the trading of stocks used to be a paper-based activity. There used to be physical stock certificates and the buyer and seller were required to be physically present there for trading the stocks. After that the era of dematerialization (DEMAT) was evolved. Physical certificates were replaced with the electronic form and buying selling of the stocks was done by registering or transferring electronically. The result of this was more fluctuations in the stock-prices due to faster execution of trade. Now due to technological developments the era of ALGORITHM TRADING has begun. Now, an algorithm can be written in advance to instruct a computer through a program to buy or sell stocks based

2020 Mathematics Subject Classification: 68W27, 93C85, 68T20, 68T27.
Keywords: Automated algo trading, robo trading, commodity trading.
Received October 7, 2020; Accepted January 15, 2021

on pre-defined conditions. With these program-based trading, the speed and frequency of trades can be so rapid which is inconceivable for human broker. The algorithmic trading process can either be fully automated for semi-automated. Thus, the process is termed as automated algorithm trading. It is becoming one of the popular areas in the world on stock market. It establishes explicit standards for trade entry and exit that can be consequently executed by the computer once programmed. The U.S. stock exchange traded roughly about 75% of shares via automatic trading systems [1]. A detailed review studies was carried out on trading systems constructed utilizing different techniques and observationally assessed the strategies by gathering them into three kinds: technical analysis, textual or fundamental analysis and high recurrence trading. The preferences and drawbacks of each methods was also evaluated and their future prospects were assessed and was discovered the most ambiguous and important research areas in regions of these two sorts, in which the factual method PST, AI applications and textual analysis were featured. [2], which became the inspiration for this study.

II. Commodity Trading

A commodity market could be a physical or virtual commercial center for purchasing, offering and trading unrefined or essential items, and starting at now there are around 50 significant commodity markets far and wide that empower speculation exchange of approximately 100 essential commodities like grain, precious metals base metals, oil and natural gas etc. “The commodity market has a special tool which is used for managing the risks related to the price fluctuation in the market” [3].

For virtual trading of commodities in India, Multi Commodity Exchange of India Ltd. (MCX) s an autonomous commodity exchange n Mumbai and was set up in the year 2003. The MCX is India’s biggest commodity exchange and the turnover of the exchange for quarter finished in 30 June 2019 was 110.84 crore rupees. The MCX has secured third position as the world’s biggest commodity exchange is unrefined petroleum fates. With such a growing market more and more people are interested in Trading in commodities like crude oil.

While trading in the commodity market most of the trader's trade manually by themselves or by seeking advice from other sources which may lead to a very risky investment as they lack the basic understanding of how the commodity market works. "In manual trading the user is required to place an order telephonically or physically to the broker or online using some web trading platform provided by their broker" [6].

Online manual trading may pose following problems:

Manual Traders can be affected by behavioral biases, making them settle on nonsensical choices and trade on feelings, such as greed and fear. The trader may choose to give the stock run access in the expectation of understanding a significantly bigger benefit or the trader could lose the extra benefits along with a bit of their original investment. In manual trading identifying the opportunities not just requires observing the market for whatever number of hours in the day as could be expected under the circumstances, yet in addition the accessibility to execute the trade in the short window of time for which it introduces itself, due to this the investor may or may not be able to place trades when the market is most advantageous for him due to lack of time or busy work schedule.

III. Automated Algorithmic Trading

Automated Trading is a general phrasing used to describe computerized trading. The computer innovation has reformed budgetary markets, and these days these business sectors are exceptionally subject to computerized reasoning, big data analysis and modelling. "It involves a challenging task of predicting the price movements in the market and is also affected by various factors. There are two models that are used to solve the problem of future price predictions and these are fundamental analysis and technical analysis" [2].

Automated Trading is additionally known as algorithmic or robot trading, where diverse securities are exchanged automatically by computers and it generates an output flag based on information set and strategies. This flag could be produced by an calculation which is essentially a set of rule that a computer program executes in arrangement until a wanted conclusion point, frequently referred to as a technical trading rule [4]. By executing exchanges quicker and speedier, these speedier developing systems permit exchanging calculations to get data more rapidly than human traders.

An algorithm can be termed as following specific set of steps to transform the input values into an output value based on pre-defined computations. Similarly, trading algorithms can be understood as simply the set of predefined rules to convert input into output. It is therefore, trading algorithms are executed within Automated Trading Systems which facilitate data collection to get input values and to transform output values into an actual action. Black box or algorithmic trading became hugely profitable by the invention of Pair Trading way back in 1980. The main reason for adoption of algorithmic automated trading by traders was improved control mechanisms, reduction in costs, automatic recording of trade details and faster execution. In present scenario, algorithms have become a mainstream aid to the daily trader.

Algorithmic trading deals with complex formulas, mathematical models and human management, for settling on choices identified with purchase and sell of monetary protections on a trade. Algorithmic traders frequently utilize high-recurrence exchanging innovation, which can empower them to make a large number per second. “World’s to begin with electronic stock advertise was National Affiliation of Securities Dealers Automated Quotations (NASDAQ) which was set up within the year 1971 and electronic quotation system for competing market makers to trade securities was introduced”[4].

Automated Trading Systems (ATS) play an important role in the Business Intelligent Systems (BIS) of any financial or investment company. ATS has become a need in present condition, for fast versatility to the ever-changing economic situations. The computational and data processing speed is the primary plan necessities of any ATS [4].

The latency of a trade is very crucial in a market here speed is of the essence. Dormancy is the time it takes to complete an arrangement, drop a request or realize what’s going on in the market. [5]

IV. Proposed Algorithmic Automated Trading Application

Algorithmic Automated trading application deals with real time and historical price data of a share or commodity and performs the buy/sell operations of these shares by analyzing the market price using various algorithms” [7].

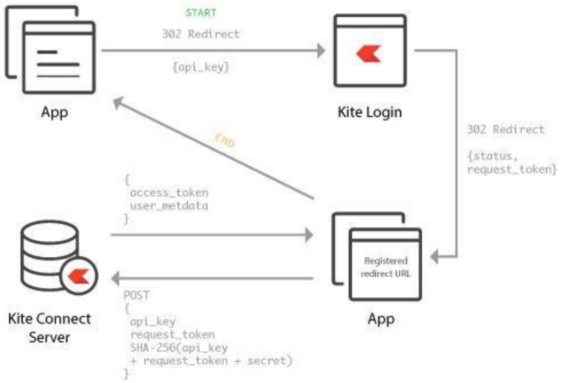


Figure 1. Zerodha Kite Connect Login flow.

Source: https://kite.trade/docs/connect/v3/user/

After placing the order, the system also monitors the live prices and on achieving the pre-defined target profit, it automatically exits from the trade. For handling minimal loss, the Margin Intraday Square-off (MIS) cover order has been used which has inherent property of putting a stop loss order alongside the first purchase/sell order.

The main advantages of using cover order are

• Discipline: It is very important to place a Stop Loss (SL) while Intraday trading but most of the time, traders have a stop loss price in their mind but do not put it on the System. Sometimes it also happens that a trader places a SL order but removes it in a hope of correction if the market starts moving drastically in opposite direction. This kind of human behavior which becomes the reason of huge losses in most of the trades is eliminated if a cover order is placed as a trader is required to compulsorily place a stop loss order within a 1.5% range from the entering price of the stock/contract and cannot remove or cancel SL till trade is exited. This limits the losses of a trader. The SL can be modified, but within the 1.5% range itself.

• Higher Leverage: Since losses are within a fixed range of the trade, it not only limits the losses and risk but also much higher intraday leverage is provided by the broker compared to regular Margin intraday Squared off (MIS) orders. The leverage provided also depends on the price of stop loss. [9]

The system has been developed using Python language version 3.7 and uses the API of Zerodha discount broker which are being provided to Zerodha Connect monthly subscribers.

V. System Architecture

The architecture for designing an Automated Algorithmic trading system was comprising of following four components to oversee various tasks of the algorithmic trading system [8]:

(i) The data handler:

Structured or unstructured or both data can be used in an Algorithmic Trading system. If the data is sorted out as per some pre-decided structure, for example, spreadsheets, CSV records, JSON documents, XML, Database, and Data-Structures, at that point it is treated as organized information. Generally, advertise related information, for example inter-day costs, end of day costs, and trade volumes is accessible in an organized format.

If data is not sorted out as indicated by any pre-decided structures, such as news, online networking, recordings, and audio then it is treated as unstructured data. It is intrinsically more complicated to process such type of data and requires data mining and data analytics techniques for analysis.

For our application we have used structured historic and live data received from the broker's API.

(ii) Model (Strategy) handler:

A model is the representation of the manual task with Algorithm. To assign the behavior of a human to a program is quite challenging. A number of different methodologies and techniques can be used to construct the model. The main objective of designing the model is to reduce a complex system into a sensible and quantifiable arrangement of rules which depict the conduct of the system in fluctuated situations. Most prevalently utilized methodologies incorporate, however are not restricted to symbolic and fuzzy logic systems, mathematical model, induction rule sets, decision trees and neural networks.

For our application we have used mathematical model which is based on analysis of the behavior of market and is also called quantitative finance model. It is based on the intrinsic expectations that market follows a specific behavior of price movement at a specific time of the day. This has been an extremely helpful suspicion which is at the core of nearly all derivatives cost activity models.

(iii) Trade execution handler:

This component is responsible for execution of identified buy or sell order (trade). For our application the intraday cover order was used which not only allows to place a buy or sell order but also automatically places the stop loss order of pre-defined value. We have used the pre-defined stop loss of 15 points making the risk and reward ratio of 3:5.

(iv) Monitoring handler:

Timely and profitable exit from a trade based on the pre-defined risk reward ratio, is equally important for an automated system. Our application has been programmed to keep monitoring the live data after placing the order and automatically places an exit order when the target profit is achieved.

VI. Result

After implementing the stated strategy on live data for two week, we have made profit on 6 out of 10 Working days. The total profit of (Day2, Day5, Day6, Day8, Day 9, 10) was 150 points and the total loss of (Day1, Day3, Day4, Day 7) was 80 points. At the end of the two week the system generated a profit of 70 points (Rs. 700).

The result is as follows:

Table 1. Two Weeks Result.

Test Period	Point	Result
Day 1	20	Loss
Day 2	25	Profit
Day 3	20	Loss

Day 4	20	Loss
Day 5	25	Profit
Day 6	25	Profit
Day 7	20	Loss
Day 8	25	Profit
Day 9	25	Profit
Day 10	25	Profit

After all the testing the 5:4 ratio has been found as the best ratio for profit and loss.

VII. Conclusion

We have developed an Application with a graphical user interface in Python Programming Language which is capable of 3 main tasks:

- Automatic Trading: This application can trade in Crude Oil Commodity in MCX Exchange automatically with the best tested strategy.
- Historical Data: This can provide you with Historical data of Crude Oil Commodity in MCX Exchange.
- Live Stream: This can show you the stream of the current data of Crude Oil Commodity in MCX Exchange.

The software Automated Algorithmic Trading for Crude Oil Commodity trade on specific strategy has been developed as per the requirement and has been tested in live market for any logical or syntax error and has been found working properly.

VIII. Future Scope

The capabilities of the software can be extended for trading other commodities in MCX. It can also be extended for trading of shares in other stock exchanges. The features can also be added for trading in other commodity exchanges. Different strategies can be tested and implemented in future and the user will have the option to change the strategy according to their needs.

References

[1] Investopedia-Automated Trading systems-Internet: https://www.investopedia.com/articles/trading/11/automated-trading-systems.asp

[2] Boming Huang, Yuxiang Huan, Li Da Xu, Lirong Zheng and Zhuo Zou, Automated trading systems statistical and machine learning methods and hardware implementation: a survey, Enterprise Information Systems (2019).

[3] R. Hariharan and B. A. Karunakara Reddy, A study onindian commodity market with special reference to commodity exchange, International Journal of Research Science and Management.

[4] Cristian Păuna, Automated Trading Software, Design and Integration in Business Intelligence Systems, Bucharest Academy of Economic Studies.

[5] A. Rajan Lakshmi and Vedala Naga Sailaja, Survey of Algorithmic Trading Strategies in Equities and Derivatives, International Journal of Mechanical Engineering and Technology.

[6] White Paper Online source: https://www.etfexpress.com/sites/default/files/import_attachments/FXaLL%20White%20Paper%20-20Algorithmic%20Trading%20in%20the%20Global%20FX%20Market%20.pdf

[7] Quantlnsti - Automated Trading Systems-Internet: https://blog.quantinsti.com/tag/automated-trading

[8] Quant Algorithms white paper, overview of Active Trader (ES) Package, design specifications, correlation analysis versus the *S* and *P* 500, post trading support methodology.

[9] https://towardsdatascience.com/algo-trading-101-for-dummies-like-me-b3938725d184

[10] https://zerodha.com/z-connect/tradezerodha/zerodha-trader-software-version/cover-orders-for-higher-leverage.

Advances and Applications in Mathematical Sciences
Volume 20, Issue 10, August 2021, Pages 2077-2083
© 2021 Mili Publications

ISSUES AND THREATSIN CLOUD NETWORK SECURITY

ANISHA TANDON[1], MAMTA MADAN[2] and MEENU DAVE[3]

[1]Research Scholar, [3]Professor
JaganNath University
Jaipur, India
E-mail: 184.anisha@gmail.com
meenu.s.dave@gmail.com

[2]Professor
VIPS, GGSIPU
Pitampura, India
E-mail: mamta.vips@gmail.com

Abstract

Being connected to people has become an indispensable part of our day-to-day lives. We stay constantly connected with the people around us. In simple words, Network security can be defined as a connection of multiple devices. With increasing connectivity of devices, it is essential that data shared among a group of devices stays private as intended by the participants of the group. Today's networking structure is intricate and is faced by constant threat from hackers. Loopholes in network security may lead to serious threats such as Data Modification, DOS attack, Eavesdropping, Botnet, Identity Spoofing, MITM attack, Password – Based attacks etc. This paper briefly introduces the concepts related to Network Security and the threats to which a network may be exposed. It also focuses on resolving various threats faced by networks such as Cryptography, Hashing, Firewalls, VPN, Proxy Servers, Anti-virus soft wares and SSL/TLS. This paper gives in depth consideration to wireless network security and a prospective solution to increase wireless network security.

1. Introduction

A network is a set of multiple devices (or nodes) that are connected to each other. These devices can deliver and/or accept information or resources to/from other devices [1]. Network security is the art of preventing misuse, unauthorized access, modification of data, or denial of a computer network

2010 Mathematics Subject Classification: 97P70, 68M12.
Keywords: Network, Security, Wireless Networks, Cryptography.
Received October 7, 2020; Accepted January 15, 2021

and its resources. Network can be secured by software methods or hardware methods [2]. Attacks on the network can be classified broadly in three ways [3].

Passive Attack. In a passive attack, the perpetrator only tries to read data or capture the information.

The aim of the attacker is not to influence the information across the network.

Active Attack. In an active attack, the perpetrator may attempt to influence the data and resources travelling across the network.

Insider Attack. An insider attack is usually related to a certain organisation. A person such as a discontented member [4] usually carries this out.

This research focuses on the security issues and threats of data over a cloud.

2. Related Work

Shailja Pandey [1] gives an in depth explanation of the concepts of network and the various threats to security of networks. Major importance has been given to the security of networks of an organisation rather than networks of individuals.

Figure 1. Networking.

Sankardas Roy et al. [5] have discussed about:

- Network Security
- Game Theory

- Taxonomy (General)
- Computer Security

Sumit Ahlawat and Anshul Anand have given the history of computers and networking along with characteristics of networks, networking protocols and threats to network security. The authors have also mentioned about the application of wireless technology [14].

Figure 2. Wireless Networking.

Monali S. Gaigole and M. A. Kalyankar highlighted the threats to network security and methods to increase network security [3].

Figure 3. Wireless Network Security.

Comparatively, networking in cloud provides more security than conventional networking [8] [9].

3. Network Security Issues in Cloud Computing

Network security [4] issues are the problems that are faced related to the security of a network. Loopholes in the security of a network may lead to compromising of important data. The data or resources may be subjected to snooping or in some cases manipulation or even permanent deletion/loss. Network security is the security provided to the network to prevent un authorised access to data and resources [5].

Based on the study, we found that there are several issues in cloud but security is the important concern, which is associated with cloud computing [10]. The issues in cloud computing environment are:

- Insecure API
- Insiders and Outsider Attacks
- Data Loss
- Data Crash
- loss of encryption keys

4. Network Security Threats

- Eavesdropping: Eavesdropping in general means listening to conversation, which is not intended for a particular person. Similarly, in case of network, eavesdropping can be defined as the unauthorised interception of data on a network. This data may include phone calls, messages, photos, videos or any other piece of information travelling through a network [6].

- Data Modification: The data being sent is intercepted by an unauthorised person and is changed or manipulated and then sent to the receiver. This leads to loss of confidentiality, authenticity and integrity of the data [7].

- Identity Spoofing: Identity spoofing is taking over the identity of a computer and then using that identity to achieve a certain objective. An attacker may use IP spoofing to assume the identity of another computer thereby hiding the real identity of the attacker.

- Password-Based-attacks: One of the most basic password-based-attacks is Brute Force attack. In a bruteforce attack, an attacker runs a script for a set of passwords against a username. This is a kind of hit and trial method. For Example, if the attacker has the list of usernames of an organisation, he/she can run a script for some common passwords and one of it might be a match. Another type of password-based-attack is Key Logger attack. Key logger software can be installed on the target computer, which would record every keystroke and send it to the attacker. The most common tool used in password-based-attacks is BurpSuite. A popular Key logger tool is BeeLogger.

- Denial-Of-Service Attack: Denial of Service attack is carried out to deny real users to access a network. It is carried out by sending fake traffic to the host until it becomes unresponsive to real users. The tools used for DOS attacks are Hping, Nmap, Metasploit and Aircrack-ng (Used for wireless access points) [11].

- Man-In-The-Middle Attack: As the name suggests, this attack means that an attacker between the sender and the receiver intercepts the data sent over a network.

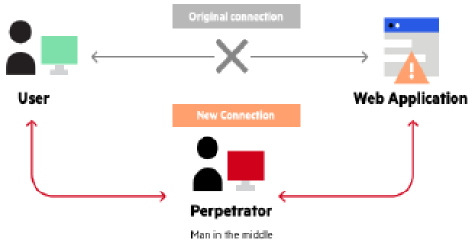


Figure 4. Man inthe Middle Attack.

- Botnets: Botnets can be defined as a network of compromised machines that can be remotely controlled to launch a large-scale attack. Botnets act like slaves that perform any type of attack intended by the attacker [12] [13].

5. Threats Challenges in Cloud Network Security

Security: Security is a major challenge of cloud. Cloud is actually based on the internet. Therefore, there can be a situation when the internet is suspended, personal information leakage and sometimes service provider can report the delay of service due to the maintenance issue, attack of viruses and low internet speed [15].

Usage: Due to Inappropriate, usage of cloud-computing test environments can increase the price [16].

Planning: The testing teams must plan testing environments. Expenses must be estimated such as encrypted data costing, costing for the testing cloud environment, CPU costing for extra memory etc [17].

Test Data: Test data management is a challenging task. To effectively perform testing, few of the testing tasks must be dependent upon the actual user or production data. Supplying production data to the third party is forbidden to the users in some cases [18] [19].

On-demand testing: Because of the on-demand requests, the services of testing must be controlled, managed and supervised. Many challenges and issues might increase due to this kind of testing services [20].

References

[1] Shailja Pandey, Modern network security: Issues and Challenges 3(5) (2011).

[2] Behrouz A. Forouzan, Data Communication and Networking.

[3] Monali S. Gaigole and M. A. Kalyankar, The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms; IJCSMC 4(5) (2015), 728-735.

[4] D. Acharjee and B. S. Panada, Enhancing Social Security through Network of Intelligent Human Nodes Trained by Comuter Algorithms.

[5] Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya and Qishi Wu, A Survey of Game Theory as Applied to Network Security.

[6] M. Benaiah Deva Kumar and B. Deepa, Computer Networking: A Survey.

[7] Mrs. Amandeep Kaur, An overview of quality of service computer network.

[8] Mamta Madan and Anisha Tandon, Cloud Computing Security and its Challenges, International Journal of Electrical electronics and Computer Science Engineering (2015), 68-71.

[9] Mamta Madan, Meenu Dave and Anisha Tandon, Challenges in Testing of Cloud Based Application, International Journal of Electrical electronics and Computer Science Engineering, 2016.

[10] Vinton G. Cerf, Computer Networking: Global Infrastructure for the 21st Century.

[11] Olivier Bonaventure; Computer Networking: Principles, Protocols and Practice.

[12] Raj Jain, Computer Networking: Recent Advances, Trends, and Issues.

[13] Raj Jain, Introduction to Computer Introduction to Computer Networking: Trends and Issues.

[14] Sumit Ahlawat and Anshul Anand, An Introduction To Computer Networking.

[15] Varsha and Amit Wadhwa, Study of Security Issues in Cloud Computing, International Journal of Computer Science and Mobile Computing 4(6) (2015), 230-234.

[16] Anisha Tandon, Implementing and Developing Cloud Computing on Web Application, International Journal of Computer Science and Mobile Computing, 2014.

[17] Anisha Tandon and Mamta Madan, Challenges in Testing of Web Applications, International Journal of Engineering and Computer Science 3(5) (2014) 5980-5984.

[18] Mamta Madan and Anisha Tandon, Testing Application on the web, International Journal of Advanced Research in Computer Science and Software Engineering (2013), 855-858.

[19] Mamta Madan, Meenu Dave and Anisha Tandon, Need and Usage of Traceability Matrix for Managing Requirements, International Journal of Engineering Research 5(8) (2016).

[20] Mamta Madan, Meenu Dave and Anisha Tandon, RTM and Testing Challenges in Cloud Based Application, in International Conference on Computers and Management (ICCM), Delhi, 2018.

Advances and Applications in Mathematical Sciences
Volume 20, Issue 10, August 2021, Pages 2095-2112
© 2021 Mili Publications

TWITTER BASED TRAFFIC ANALYSIS AND PREDICTION MODEL FOR PLANNED EVENTS

HARSHA S. RATNANI and SIDDHARTH KUMAR

Department of Information Technology
JIMS, VK, New Delhi, India
E-mail: harshapratnani@gmail.com
Indiasiddharth.kumar2506@gmail.com

Abstract

This paper has been written with the fact the study of extracting relative information from social media for long term and short term events and finding its link with traffic related management and control or finding better ways to manage huge traffic jams. As a newly emerged communication revolution, Day to day lives of people is now often connected to their social media accounts and is observed to be a platform for users to communicate, share, and follow the interesting things happening in their daily lives in an instantaneous channel. The number of posts posted online on any platform such as Twitter, WhatsApp or Facebook, related to any social event can somewhat represent its corresponding attention levels. We focused on tweets posted on Twitter for events, in which we used tweets of social events involving some kinds of trip requirements to and fro from the venue, as it usually leads to an obvious traffic increase in the surrounding area. To prove the correlation between twitter semantics and traffic conditions, our study focuses on using the tweets related to sporting games to predict the passenger flow, which is strategically important in metro transit system management.

I. Introduction

Often nowadays whenever we go for any major social event, the first hurdle we all have to face is the big traffic jam specially surrounding the venue, and especially during the start and end of the event on the way to that leads up to the venue. The general traffic operations may deteriorate around major social events including ceremony opening, celebrity death, festival parades, international conference, etc. Such major events across the world are vastly covered on social media platforms such as twitter.

2010 Mathematics Subject Classification: 62H11, 62H30, 62H35, 62M10, 62M30, 26E70, 83C75.

Keywords: Social Media, Traffic, Events, Twitter, Hashtag, Tweets, Prediction, Regression, Analysis.

Received October 7, 2020; Accepted January 15, 2021

It is observed that with expanding number of engine vehicles across the world, street traffic prediction is becoming necessary day by day and is has become critical component in modern smart transportation systems. Accurate and exact prediction of both the short-term and longer-term street traffic conditions can greatly help metro cities traffic management agencies in planning proactive strategies to handle the congestions on the street during peak hours. Not only that It can also help travelers to plan their trips accordingly either by leaving early or by avoiding those routes completely which are expected to be congested soon with huge traffic jam.

The social media platform Twitter has provided us with recently progressive technique for information diffusion, and this colossal volume of messages, data and information by Twitter has excited the interests in many researchers from various fields such as opinion polls, geographic data study, urban smart systems planning, audience movie reviews, etc. The majority of these research works have demonstrated promising outcomes which both upgrade the conventional systems and widen the new research spectrums. Motivated by the magnitude of the information present in online social media, in this paper, we try to analyse if we can use tweet-based semantics to provide clues about the traffic condition during the occurrence of a major event? To attain this, we take into consideration two types of analysis-Long Term and Short Term. Long term analysis focuses on taking twitter and traffic data for a long period (5 to 10 years), during the yearly occurrence of any major event, and find the correlation among them. Whereas the short term analysis takes into consideration the same data during the short span of time i.e., during the occurrence of the event. The duration may vary from single day to a week with respect to a given year.

In this study we took up the case of one of the most popular events in the world - The Wimbledon Tennis Championship, along with the case of football matches played by Manchester United at Old Trafford over a span of 10 years, for long term analysis. On the other hand, we have considered the case of a single day match of the Indian Premier League 2017 for the short term analysis during the day of the match between two teams. We found that tweet semantics can be a positive indicator for traffic judgment.

The rest of the paper has been organised as follows. In Section two, we intended to briefly review the prevailing research work on traffic prediction and data analysis based on social media aided gathered data. Then we have shown the study of our proposed methodology for both types of analysis long term and short term planning in Section three. The experimental results of the data which have gathered from specific case studies are presented in Section four. Finally, we tend to conclude the paper in Section five and have listed out all the references for this paper in Section six.

II. Referenced Work

Social Media Based Analysis

It's been observed by many researchers that the rich information available on social media platforms such as twitter, facebook, whatsapp etc. can be utilized for various application and data analytics purposes. As we all have seen recently, there is a lot of interest in using social media to detect emerging news or events: in Petrovic et al., [1], the researchers have addressed the problem of detecting new events or first story detection from a stream of Twitter posts using an algorithmic locality-sensitive hashing approach. They used method of adapting to the first story detection task by introducing a back off towards exact search. As claimed in the paper this adaptation greatly improved performance of the system and virtually eliminated variance in the results. They used this FSD system on a large-scale task of detecting new events from millions of Twitter posts;

Then in Sakaki et al., [3], the authors had investigated the interaction during natural calamities events such as earthquakes on Twitter, and proposed a probabilistic spatiotemporal model for the target event that can find the center and the trajectory of the event location, it was an application for earthquake reporting etc. They applied the semantic analyses to tweets to classify them into a positive and a negative class. They considered each Twitter user as a sensor, which can help in detecting an event based on sensory observations. They used in their research Location estimation methods such as Kalman filtering and particle filtering to estimate the locations of events. In Sankaranarayanan et al., [2], the authors proposed a news tweets processing system called to capture tweets that correspond to late breaking news, they named it as Twitter Stand. They used naïve Bayesian classier to improve the quality of the noisy feeds and employed a dynamic corpus to sensitize the classier to current news. They observed that the sheer enormity of the data means that algorithms will have to be online in nature, which can be challenging. The online clustering algorithm that they presented in their paper was useful along with being fast and robust for mitigating noise. In addition, they also described methods for geotagging news, as well as a user-interface for displaying news.

The other line of research is tweet classification focused on information filtering. It was found that in Go et al., [4], the authors test various algorithms for classifying the sentiment of tweets, such as SVM, Naive Bayes, etc based on author information and some other features within the tweets, it is known Bag-of-Words approach within the tweets. With such a system, users could subscribe to or view only certain types of tweets based on their interest. Though the approach didn't work with lot of noise into the data, hence any noise removal techniques needs to be applied first on are necessary in such cases; in Sriram et al.,[5], the researching team used a small set of domain related features along with the bag-of-words features to describe and then classify the tweets into a predefined set of classes; etc. show that changes in the public mood state can indeed be tracked from the content of large-scale Twitter feeds by means of rather simple text processing techniques and that such changes respond to a variety of socio-cultural drivers in a highly differentiated manner.

During our literature study and moving more in time, we discovered some group of analysts and researchers were extracting information from tweets which might be useful in another domain. Like in Bollen et al., [6], the authors tried to perform the research based correlation between public mood and other economic indicators. So in their research they started deriving collective mood states from the large scale Twitter Feeds and then performed the correlation analysis with the Dow Jones Industrial Average (DJIA) over time. Finally, they had concluded that the accuracy of DJIA by the inclusion of specific public mood dimensions, such as Calm the predictions could be significantly improved. Also, we found that in Eisenstein et al., [7] the authors proposed a multi-level generative model which was based on the geo-tagged social media, which brought the reasons jointly about latent topics and geographical regions into the light.

Road Traffic Prediction

In metros and otherwise big urban cities Traffic Prediction is an important as well as a critical component in any smart transportation systems. It's possible that if we can do the accurate prediction of traffic conditions, then this would help traffic management agencies to plan and handle the city traffic congestion problem with a proactive traffic operation strategy for avoiding it at first place and also help them to efficiently handle these congestions on roads knowing well in advance along with the common road travelers can also plan their trips accordingly ahead of time in case such warnings are issued publicly.

It came to our notice that studies based on long-term events based traffic prediction are rather very limited, essentially in light of the fact that extra factors other than the past and current traffic conditions start to play a very important role once the forecasting time period is beyond 60 minutes. We found out that only group of few researchers and private sector companies have attempted to analyse and utilise the correlation between the route traffic data and the other external factors such as weather and event schedules Maze et al., [8]; Mahmassani et al., [9].

Our proposed work focuses on analysing the correlation between Twitter and Traffic in context to a particular well known major event, and further predicting the traffic in future based on this analysis. This is inspired and motivated by observing the large occurrence of chats, posts and tweets shared on social media platform which are directly related to traffic conditions, as mentioned in Ni et al., [11], which describes forecasting subway passenger flow during event occurrences, and Ozdikis et al., [12], which further discusses about event detection based on the use of hashtags in twitter.

III. Proposed Methodology

In this proposed research study related to various public events data, we mainly used two kinds of data items for the study: the tweets and the traffic data. The first of them both we collected through Twitter Streaming with geo-location filter. To keep the study focused on fixed public events all tweets are paired with time and location information. The Traffic data is then extracted using the Google Maps to analyse the correlation between tweets and traffic conditions.

Long Term Analysis

During our study we first focused on long term data analysis just so that the certain event occurrences have a possibility of getting being affected by any unforeseen circumstances like any occurrence of an accident on the route or may be due to change of weather like heavy rainfall etc. So in prediction of the effects of tweets and its correlation with traffic in any place, we thought we must consider a long term data first (over a span of at least 10 years) for the study.

In this study we took up the case studies of two of the most popular events in the world - The Wimbledon Tennis Championship, and the football matches played by Manchester United at Old Trafford over a span of 10 years. The reason for these events being chosen is because of their invariability. The matches in Wimbledon take place at the same time each year, and continue for the exact same period of time. The tweets of this event have limited hashtags and are contained within or around the word “Wimbledon”, and for Manchester United, the hashtags are contained mostly around “GGMU”. Hence, search of tweets with these words arguably will contain all tweets related to the event.

While our study has considered the case of the football matches played by Manchester United to study the direct relation between tweet semantics and traffic data, the case of Wimbledon has been considered further to predict the amount of tweets in the future consisting of #Wimbledon, and then predict the amount of traffic on the roads being taken into consideration.

To accommodate the actual correlation analysis as per our suggestive model, we used two data record sets: the one was containing the traffic measurements, and the other one had the gathered tweets posted, during the period of the event. We generated the traffic data set by collecting measurements for two specific roads around the Wimbledon Stadium - B235 and Riverside Road. The cumulative traffic data for these two roads was obtained from 2006-2016, during the period when the Wimbledon Championship takes place. Using the geo-location filters based on latd/long bounding box on the gathered data, we obtained all the relative tweets.

After the data obtained from maximum number of attempts using twitter was gathered, we were able to figure out the number of tweets during that duration that contained #Wimbledon in it. To avoid any kind of spam, we also took care of applying a filter on the tweets that contain the regular expressions of “http:” or “www.”. For each tweet, we collected the information of respective user account, the tweet time stamp, the tweet content and the geo-location of the twitter user.

In order to figure out the trend of twitter popularity on events such as Wimbledon, the long term pattern needs to be plotted. The different values of the tweet concentration for various years are then analysed to predict a pattern. If a pattern is found, the mathematical analysis of the pattern can help in predicting future values. In the case of Wimbledon, the tweet concentration followed a linear pattern. This gave rise to a simple linear equation of $Ax + Bx + C = 0$ type. If not linear, the tweet concentration would’ve followed a non-linear pattern of the type $y = 3x^3 + x^2 - 7.$ Using this equation the concentration of tweets in the future years was predicted, which could be used as an input in the traffic prediction of the future. The data set collected showed a linear pattern in tweet concentration making it easy to predict the value of the future.

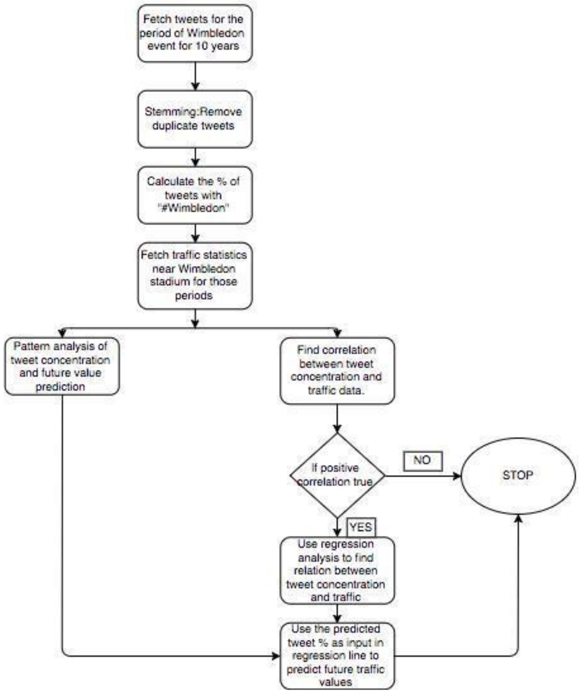
The correlation between tweets and actual traffic data needs to be mapped. Taking the data of past years, the relation between the tweet concentration of any particular event (Wimbledon) can be figured out by mathematical linear regression tool. This allows to take the data of the two distinct variables, find a correlation coefficient between them, and thus predict a mathematical equation that can be used to plot the values of each year, and extend this line into the next few years to predict one variable using the other. In this case the expected tweet concentration value was plugged in to predict what the traffic in the nearest roads to the event may look like sometime in the future.

Short Term Analysis

In contrast to the above analysis, the short term analysis considers the twitter and traffic data over the period of the occurrence of the event, on an hourly basis. In our study, we have considered the a cricket match of the Indian Premier League, that lasted for a single day, and had multiple variations of the amount of tweets and traffic during that particular duration.

For studying the short term analysis of the effects of tweets posted on any kind of traffic situation at any particular place, we developed a hashtag based event search algorithm. In order to collect the tweets which are being posted by Indian users, we first defined geographic bounding boxes that actually covers almost all of India, and added the same as our filtering criteria for the streaming service. The lat/long bounding box of "23.546471, 78.981548, 3000 km" is used to get tweets from this location, i.e., Madhya Pradesh, with a radius of 3000 km around it.

By extracting tweets based on their location, we further determine the traffic at that particular location using the traffic and transit layers of Google Maps. Google Maps allows you to add real-time traffic information to your maps using the Traffic Layer object. We store this traffic information for there quisite location with a timestamp in a SQL Database, and plot it on different graphs to analyse the correlation between the event in concern and the traffic at various hours of the day, which can be further used to accordingly prepare traffic management plans in case of other events in the same area in the future.


Fetch tweets for the period of Wimbledon event for 10 years
Stemming:Remove duplicate tweets
Calculate the % of tweets with "#Wimbledon"
Fetch traffic statistics near Wimbledon stadium for those periods
Pattern analysis of tweet concentration and future value prediction
Find correlation between tweet concentration and traffic data.
If positive correlation true
NO
STOP
YES
Use regression analysis to find relation between tweet concentration and traffic
Use the predicted tweet % as input in regression line to predict future traffic values

IV. Experimental Results

Long Term Analysis

United Kingdom is equipped with sensors across all major roads collecting data on traffic each day. This traffic data is stored in the UK Department of Traffic database and is accessible to anyone across the globe. The sensors store data on various parameters such as, average traffic per day, traffic for the year, traffic of different vehicle types etc. Such data is extremely valuable in data analysis and is a very helpful tool. By crawling through official site (https://www.dft.gov.uk/traffic-counts) and filtering data with respect to geo-location and time, exact traffic data was obtained and used directly in further analysis.

The graphs below (Figure 2 and Figure 3) show the number of motor vehicles across UK for 10 years. Similarly, information for every individual road can be extracted from the Department of Traffic database, and be plotted for better understanding of the correlation between tweets and traffic.

After extracting the traffic for the roads - B235 and Riverside Road, for the years 2006-2016, the tweets containing #Wimbledon were extracted for all of these years, and there spective graphs (Figure 2 and Figure 3) showed clear correlation between the number of tweets and corresponding change in traffic. The year of concern was tagged during extraction of twitter data, and all tweets were extracted until twitter blocking. This process was repeated multiple times and a compilation of all collected tweets from that year was made. Repetitive tweets were removed. The percentage of tweets that had them gave us the final tweet concentration which could then be used in further regression analysis.

Until 2010, the data was not sufficient to obtain a clear pattern or trend, i.e., the data was below the requisite confidence level. However, after 2010, the data showed a clear relation between the traffic in the two roads and the percentage of tweets consisting of #Wimbledon.

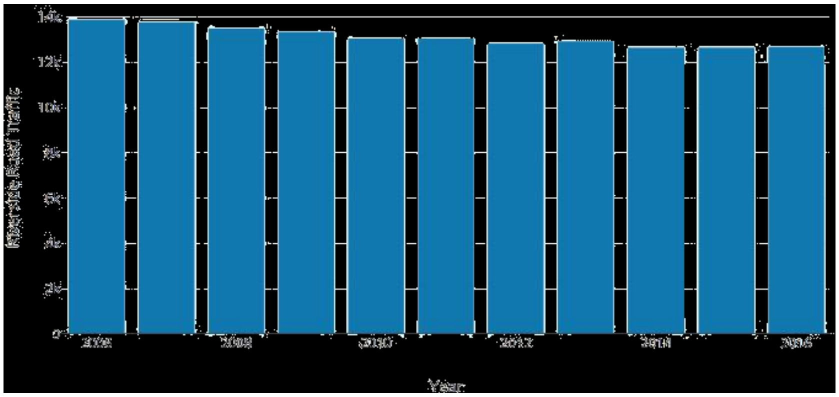


Figure 2. Amount of traffic on B235 from 2006-2016 during the Wimbledon Championship.

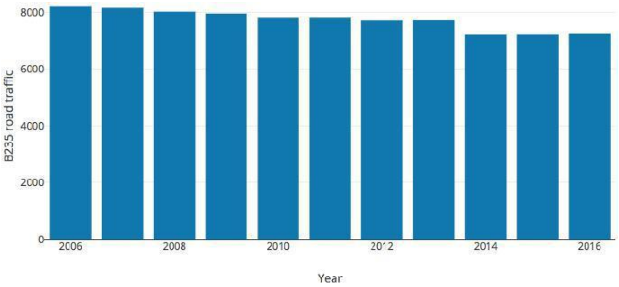
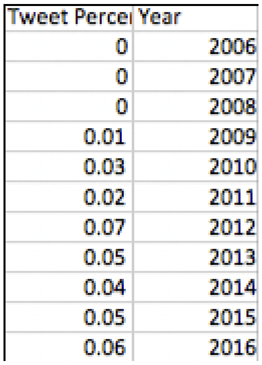


Figure 3. Amount of traffic on Riverside Road from 2006-2016 during the Wimbledon Championship.

Based on the above information, we plot the percentage of tweets consisting of #Wimbledon, during the period of the event, across 10 years, i.e., 2006-2016, with the amount of traffic, as shown. We observe that there is a positive correlation between the percentage of tweets and amount of traffic. Whenever the percentage of tweets consisting of #Wimbledon falls down, or rises in a particular year, there is a corresponding reduction or increase in the amount of traffic on the streets being considered, as can be seen in the graph shown below.

Due to lack of twitter usage during the years 2006, 2007, and 2008, the amount of data requisite for analysis was inadequate, and hence the percentage of tweets consisting of #Wimbledon has been taken 0 for this period.

Table 1. Tweets per year.



Tweet Percei	Year
0	2006
0	2007
0	2008
0.01	2009
0.03	2010
0.02	2011
0.07	2012
0.05	2013
0.04	2014
0.05	2015
0.06	2016

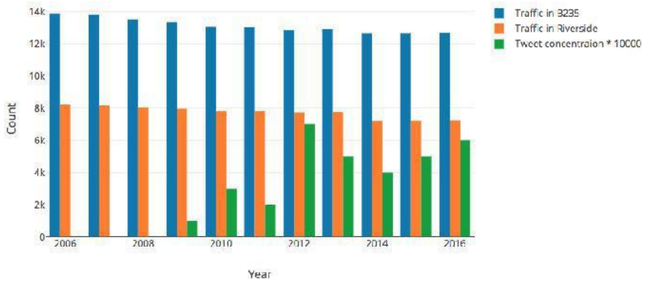


Figure 4. Tweet percentage per year (2006-2016) containing #Wimbledon (for the duration of the event) mapped to the traffic across the roads B235 and Riverside for the same duration.

To further analyse the correlation, we picked up the case of another event - a football match at Old Trafford Stadium in Manchester, London. Our analysis showed that with rise or fall in the number of tweets, the corresponding traffic for any particular year increased or decreased accordingly. #GGMU was used to extract tweets, which is the most used hashtag for the team - Manchester United, which plays its matches at Old Trafford.

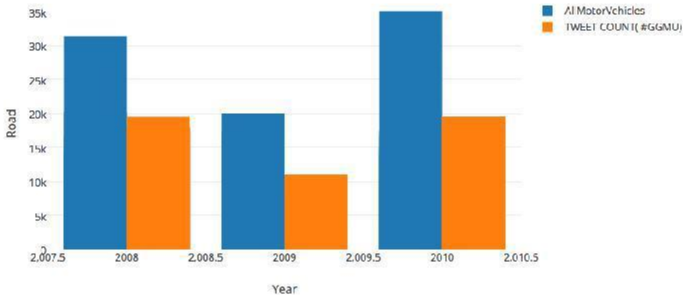


Figure 5. Number of tweets containing #GGMU and corresponding traffic in Manchester.

The main purpose of understanding the relation between tweets and corresponding traffic is to improve traffic management by prediction of traffic on particular roads for the future. Following steps are performed for the regression analysis of the case considered for #Wimbledon and roadsB235 and Riverside Road :

Step 1. Prediction of the percentage of tweets consisting of #Wimbledon in 2017, based on previously extracted data for10 years (2006-2016) for the duration of Wimbledon:

We calculate the percentage of tweets (y) consisting of #Wimbledon, where x is the index of the year of the tweet, when 10000 tweets are extracted for the period of 10 years, i.e., 2006-2016, during the duration of the event (Wimbledon) each year, in the equations given below:

$$2014 : y = 0.04\% (x = 1) \tag{1}$$

$$2015 : y = 0.05\% (x = 2) \tag{2}$$

$$2016 : y = 0.06\% (x = 3) \tag{3}$$

Using the obtained values mentioned above, we computed the type of correlation (linear, exponential or haphazard), and used the following mathematical equation:

$$y - Mean(y) = r^{*}(\text{Variance}(y)/\text{Variance}(x)) \tag{4}$$

where

$$\Gamma = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum y)^2][n\sum y^2 - (\sum y)^2]}}.$$

Mean $(y) = 0.05$ (From (1), (2) and (3))

Variance $(y) = 0.01$ (From (1), (2) and (3))

Variance $x = 1$ (From (1), (2) and (3))

to give

$$y = 0.024x.$$

From the obtained equation, we inferred that tweets follow a linear regression model and the percentage ratio of tweets consisting of #Wimbledon should be 7% in 2017.

Step 2. Prediction of the amount of traffic on the roads B235 and Riverside Road in 2017, based on the analysis in step 1, and previously available traffic data provided by the UK Department of Traffic :

Further, to predict the amount of traffic in 2017, in accordance with the percentage of tweets, we used another regression model. The traffic on the two roads for the three different years, for the duration of the event Wimbledon, is as given below in table 2:

Table 2. Number of vehicles on Riverside Road and B235 for three years.

Year	Riverside Road	B235
2014	12659	7212
2015	12660	7214
2016	12687	7239

$$\text{Mean of Traffic for Riverside Road} = 12668.67 \tag{5}$$

$$\text{Mean for Traffic for } B235 = 7221.67. \tag{6}$$

$$\text{Mean of Tweets concentration} = 0.05$$

(From (1), (2), and (3)).

We then substitute the values calculated above into equation (4), to get the following linear equations for prediction:

B235 :

$$y = 1400x + 12599. \tag{7}$$

Riverside Road:

$$B235 : y1350 + 7154. \tag{8}$$

In accordance with the equations above, we insert the values calculated in equations (5) and (6) into (8) and (7) respectively. Based on this calculation, we can easily predict that the number of motor vehicles on Riverside Road for the duration of Wimbledon 2017 would've been 12697; whereas for B235 Road, the number of vehicles would've been 7248.

Short Term Analysis

In the preprocessing step, we are supposed to toke nise the tweeted sentences into words by using space and punctuations as separators or stop words to be specific. After stop words are eliminated as much as possible we then remove the non-alpha numeric characters within these tweets. The tweets are required to be extracted using a particular twitter account but we have to take into consideration four major parameters for the tweet data gathering – What is the Consumer Key along with Consumer Secret Key also we need the Access Token and Access Token Secret to complete the process.

So to achieve that we collect the tweets through Twitter Streaming API with geo-location filter. The advantage of that is all tweets in this are paired with time and location information. To ensure that the locations are not repeated, we tokenise the location and separate them out using regex string functionality in Python.

The following actions were taken with respect to specific content in the tweets for better understanding of the correlation:

Table 3. Type of content in tweets with specific action.

Type of Content	Action
Emoticon	Remove
Location: New Delhi, India	Change to New Delhi
Location: Jaipur-The Pink City	Change to Jaipur

In our study for the short term analysis of the correlation between twitter and traffic, we took up the case of one of the most popular cricket league in the world - Indian Premier League. Our analysis began with selecting a particular match of the league, which in this case was between the teams Mumbai Indians and Delhi Daredevils in Feroz Shah Kotla Stadium, New Delhi. The analysis began with generating a hashtag based identification algorithm, that extracted tweets based on hashtags entered, which in this case were the official hashtags of the league - #IPL and #DDvMI. The tweets with no location, or with any of the exceptions mentioned above, are ignored. These tweets are stored in a SQL database with a timestamp and the location for further analysis.

The same step is performed for different time slots within the same day of the event. Along with the tweet information, the traffic information based on estimation of number of vehicles based on the colour code represented by the Traffic Layer of Google Maps, is also stored in the database. The traffic layer represents the amount of traffic on roads in the form of different colours. According to the Google Maps site, the colored stripes represents traffic conditions on major highways refer to the speed at which one can travel on that road. The deep red lines mean highway traffic is moving more or less at the speed less than 25 miles per hour and it clearly is an indication of a traffic jam or an accident related blockage or an unavoidable congestion on that route. Whereas if it shows yellow colored stripes over the map then it signifies traffic is moving faster atleast, from 25 to 50 miles per hour, and if the green stripes are visible in the google map then that indicates the route is good to go and the traffic is moving faster on that route at 50 miles or more per hour. In between we also often see grey lines, that just simply means that on that particular route there's no traffic information available at the time and we may also find the red-black line too visible in mapping app which happens to refers to extremely slow or stopped traffic.

If otherwise we have to analyze the traffic on metro city streets, with limitations of speed on motor vehicles such that the speed has to kept much lower than on the highways, in that case the colors on google map take on different color code relative meaning. In the reddish blacklines denote a slow going traffic along with general congestion most of the time. The yellow lined depict a better traffic prospect but still not the best and fast route for city travel, and the green denotes the traffic conditions are suitable to travel. Based on these facts, the traffic can be estimated, and given certain values for analysis for the event that begins at around evening 8pm. and ends around late at night 11pm.

By storing values of the number of tweets and the amount of traffic throughout the day of the event, we noticed a trend being followed. The map indicates the traffic condition around the stadium 4 hours before the match begins, i.e., 4:00 P.M. to be quite low. The condition changes drastically after this period, around 7:00 P.M., wherein the number of vehicles increases manifold. Similarly, the number of tweets with #IPL and #DDvMI from New Delhi go up considerably than other places from 6:00 P.M. until 8:00 P.M.; go down till 11:00 P.M., in accordance with the amount of traffic in the region, and as soon as the event ends, both the amount of traffic and tweets shoot up again.

The graph below shows the correlation between traffic with respect to time, with the traffic being estimated as per the colour codes indicated by the Traffic Layer of Google Maps.

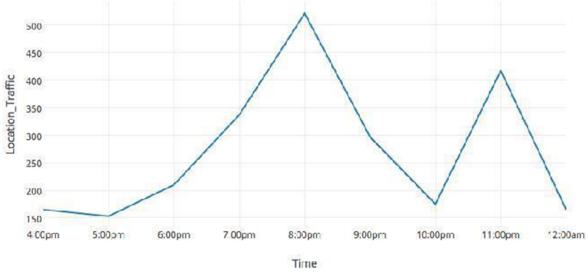


Figure 6. Traffic at Feroz Shah Kotla Stadium, New Delhi, at different time intervals on the day of the event.

V. Conclusion

In the above written research paper, we had been motivated and intrigued by the fact that nowadays more n more persons are in habit to post any public mass gathering event-related contents on popular social media platforms and also always are on the run to and from the place of the event. We answered the following question via this paper: can we utilize such information or tweets to improve traffic prediction for similar events in the future. To prove this aspect, we first performed correlation analysis between posted tweets counts and traffic measurements for a long term basis, by considering the case of Wimbledon - one of the biggest sporting events, and then work on a short term analysis by considering the example of the Indian Premier League. We analysed the tweets on a hashtag based event identification algorithm, and further used the Google Maps and its layers to predict traffic over a certain period, and then use it for future prediction. Based on the derived analysis, we have come to the conclusion that twitter semantics can surely be used for general traffic prediction for planned events, and hence improve traffic management. Experimental results on traffic data and Twitter data collected for United Kingdom clearly depicted the improved performance of our proposed model based on auto-regression over the existing traffic prediction model.

References

[1] S. Petrović, M. Osborne and V. Lavrenko, Streaming first story detection with application to twitter, In Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics (2010), (pp. 181-189). Association for Computational Linguistics.

[2] J. Sankaranarayanan, H. Samet, B. E. Teitler, M. D. Lieberman and J. Sperling, Twitterstand: news in tweets, In Proceedings of the 17th acm sigspatial international conference on advances in geographic information systems (2009), 42-51. ACM.

[3] T. Sakaki, M. Okazaki and Y. Matsuo, Earthquake shakes Twitter users: real-time event detection by social sensors, In Proceedings of the 19th International Conference on World Wide Web (2010), 851-860. ACM.

[4] A. Go, R. Bhayani and L. Huang, Twitter sentiment classification using distantsupervision, CS224N Project Report, Stanford 1 (2009), 12.

[5] B. Sriram, D. Fuhry, E. Demir, H. Ferhatosmanoglu and M. Demirbas, Short text classification in twitter to improve information filtering, In Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval (2010), 841-842. ACM.

[6] J. Bollen, H. Mao and X. Zeng, Twitter mood predicts the stock market, Journal of Computational Science 2(1) (2011), 1-8.

[7] J. Eisenstein, B. O'Connor, N. A. Smith and E. P. Xing, A latent variable model for geographic lexical variation, In Proceedings of the 2010 Conference on Empirical Methods in Natural Language Processing (2010), 1277-1287. Association for Computational Linguistics.

[8] T. Maze, M. Agarwai and G. Burchett, Whether weather matters to traffic demand, traffic safety, and traffic operations and flow, Transportation research record: Journal of the transportation research board (1948), 170-176.

[9] H. S. Mahmassani and J. Dong, Journal of the Transportation Research Board, No. 2391,

Transportation Research Board of the National Academies, Washington, D.C., 2013, pp. 56-68. DOI: 10.3141/2391-06

[10] J. Kim, R. B. Chen and B. Park, Incorporating weather impacts in traffic estimation and predication systems, US Department of Transport, Washington (2009), 108.

[11] M. Ni, Q. He and J. Gao, Forecasting the subway passenger flow under event occurrences with social media, IEEE Transactions on Intelligent Transportation Systems 18(6) (2017), 1623-1632.

[12] O. Ozdikis, P. Senkul and H. Oguztuzun, Semantic expansion of hashtags for enhanced event detection in Twitter, In Proceedings of the 1st international workshop on online social systems (2012).

[13] J. He, W. Shen, P. Divakaruni, L. Wynter and R. Lawrence, Improving traffic prediction with tweet semantics, In Twenty-Third International Joint Conference on Artificial Intelligence (2013, June).

Advances and Applications in Mathematical Sciences
Volume 20, Issue 10, August 2021, Pages 2061-2070
© 2021 Mili Publications

CYBER SECURITY: A NECESSITY, NOT AN OPTION

PRIYANKA RATTAN, SHALU TANDON and NIKHIL GARG

Jagannath International Management School
New Delhi, India
E-mail: priyanka.rattan@jagannath.org
shalu.tandon@jagannath.org

Abstract

Information Security is needed to safeguard an organisation's essential resources, such as sensitive data, hardware and software. By applying suitable safeguards an organisation's important work, research, data, resources and other tangible and intangible assets etc, can be made secure against theft and misuse. Many People see security as a waste of time and money. They perceive security measures as hindrances and find it bothersome for users, managers, and systems. Well-chosen security protocols and procedures are adopted just to safeguard valuable assets not clearly understanding their need and importance.

Building an information security program that adheres to the principle of security as a business enabler is an initiative in an enterprise's effort to create an efficient security program. Organizations must continuously (1) discover and evaluate information security risks to business operations; (2) regulate what policies, standards, and controls are worth applying to cut back these risks; (3) endorse awareness among the staff; and (4) evaluate compliance and control effectiveness. As with other varieties of internal controls, this is often a cycle of activity, not an exercise with an outlined beginning and end.

What is Cyber Security?

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. [1]

Researchers in cybercrimes have established that cyber attacks hit businesses in every day. The number of cybercrimes is rapidly increasing

2010 Mathematics Subject Classification: 97P70, 03B70, 92C42, 68U01.

Keywords: Social Media, Traffic, Events, Twitter, Hashtag, Tweets, Prediction, Regression, Analysis.

Received October 7, 2020; Accepted January 15, 2021

every year as people try to benefit from vulnerable business systems. Often attackers are looking for ransom. It has been found that the number has been increasing manifold every year. Some of the companies don't get to know that they have been hacked for quite some time.

Some cyber criminals have specific objectives in their mind while planning an attack. They know who they want to harm, and its potential benefits. They will go to any extent to achieve their goals. In this section we will describe significant threats faced by organisations and individuals during 2019-2020.

It is a type of attack in which user is unknowingly redirected to malicious sites. Instead of the user going to the intended site, he or she is led to a malicious site. Once you arrive at the malicious site, the attacker is now in a position to install malware, collect your credentials/confidential data, and even impersonate and act on your behalf.

2. Remote Access Trojans (RATs)

RATs include the ability to steal and temper saved usernames and passwords. Once they have usernames and passwords in their hands the attacker can log in to the shared server. Imagine you are working on a sensitive project and someone makes in roads in your system and he has access to all your confidential and sensitive information which he can use in a manner he desires.

3. Phishing

Phishing is a type of cyber crime in which target is contacted by e-mail, sms by a fraudster posing as a legitimate entity to lure an individual to provide sensitive details, usernames and passwords.

4. Social Engineering

It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information through a broad range of malicious activities.

There was a time when the locks on doors were counted as safety and security, but in today's world security breach in the cyber world can result in grave consequences to an individual, an organisation or a country. We are connected through the web to every person. Any unauthorized access to someone's personal, professional or organisations information is a security breach and hence strong measures are needed to prevent it and therefore comes the need for a secure and robust system to protect sensitive and vital information so that an organisation or company is not vulnerable against any cyber-attack or theft. [2] The overall security objectives comprise the following:

- Confidentiality
- Integrity, which may include authenticity and nonrepudiation
- Availability

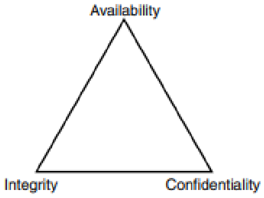


Figure 1. CIA Triad.

This is true for the majority of cyber security-related threats a user and/or organisation could be exposed to. However, this paper contends that cybersecurity threats don't form a part of the formally defined scope of data security. This section will briefly present a couple of scenarios as examples:

1. Ransomware Attack on a financial institution: For instance, some 35000 computers at the energy company Saudi Aramco were infected by the Samoon Virus which made business operations non operational for 10 days and destroyed 85% of the company’s hardware.

2. Cloud Security Breaches: No organization is completely safe from data breaches. With retail corporations like Target and insurance companies like Anthem previously experiencing breaches to customer data, the distress and probability of being the target of a cybersecurity breach is at an all-time high. Many businesses tend to believe securing sensitive data within the cloud would prevent hackers from gaining access to the data.

3. Cyber Terrorism: Cyber terrorists or competitor or enemy nation's spies might target a nation's critical and confidential information through cyberspace. This could either be indirect, for example, by influencing and manipulating the available information services using denial-of-service attacks or, more directly, defacement of government websites like the Supreme Court of India website. In the case of attacks against such critical infrastructure, the loss entails not only to the integrity or availability of information resources but also that of access to such vital services. Because In such cases, it is not an individual, but the welfare of society as a whole is at risk. An excellent example of such attacks is the attacks on Estonia in April/May of 2007.

These discussed scenarios deal with various aspects of cybersecurity where the interests of an individual, society, or nation, including their non-information-based assets, need to be shielded from risks stemming from interaction with cyberspace.

5. Risk Management

Risk analysis is a tool used to identify, determine, and evaluate risks and susceptibilities through a cyber-attack or threat. To define risk analysis more elaborately, it is a systematic process to examine the threats facing the information technology assets and the vulnerabilities of these assets and show the likelihood that these threats will be realised.

Thus, risk analysis is an aid by which risks to IT assets can be identified and quantified, also it can determine the probability of the risk occurring and the consequence if the adverse event actually happens. Risk analysis is, therefore required and is essential for securing IT assets. Once risk analysis is done, and vulnerabilities are identified, the identified risks have to be suitably managed, reduced and eliminated as far as possible through risk management by applying proper security measures.

Today is the information era, where information has become a vital resource and is extremely valuable to an organisation just like any other valuable asset information that needs to be adequately protected to ensure business viability and progress. Today we need to protect not only the technical information but also both business and personal information wherever it resides. The emphasis has thus shifted more towards the protection of information rather than just the infrastructure [3].

Although asset valuation is a vital portion of risk analysis, quantifying information could prove to be a rather frightening task. The quantification of risks to physical or tangible assets already showed to be an extremely tough task.

What is the need for Risk Management?

Recent focus and concern on information security breaches have led to a better understanding of information security issues. Increased instances of security breaches have led to the formulation of legislation addressing these risks.

Awareness and legislation to regulate and manage security risks have forced corporations in many sectors to employ various means to measure and find solutions to corporate assets' information security risks.

These affected agencies and firms have now got the motivation to at least implement the minimum-security practices. After years of unders pending in other industries in information technology improvements, the healthcare industry more recently began outspending these industries to make up for time-lapsed and to comply with the Health Insurance Portability and Accountability Act (HIPAA). Although the recent spurt of attention in this area appears to be new, regulations that require information security practices have been introduced and revised since the 1980s.

Management of Risk

Risk management "refers to planning, monitoring and controlling activities which are based on information produced by risk analysis activity". In contrast, the management of risk is described as the "overall process by which risks are analysed and managed" as illustrated in Figure 2.

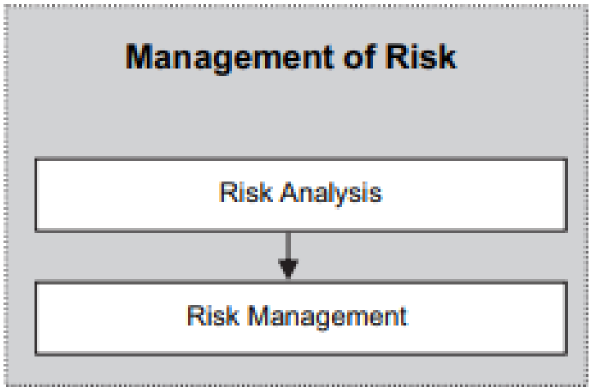


Figure 2. The Process within the overall management of risk.

According to the previous explanation, it may be concluded that risk analysis comes before risk management. Together, the method of risk analysis, followed by the method of risk management can be considered a part of the management of risk. Both these processes, risk analysis and risk management will independently be discussed in more detail.

Risk analysis

Risk analysis is the sum of risk identification, estimation, and evaluation. The basic phase of risk analysis, as illustrated in Figure 3, is risk identification.

The primary purpose of risk identification is to identify risks involved, weigh its probability and magnitude in different scenarios. Cybersecurity specialists follow a set method when evaluating risks. The first step is to determine what can go wrong, second is to assess its probability and lastly, to determine how severe impact would be if it actually did go wrong.

According to Kirkwood [4], the evaluation of risk as:

Risk=probability *x* severity of harm

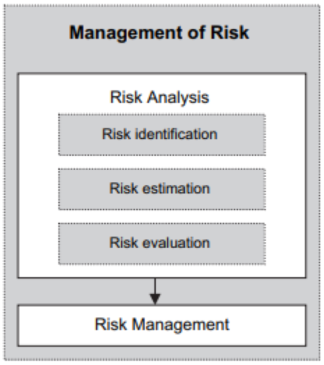


Figure 3. The sub-processes of risk analysis.

The evaluation of risk in this way places an undesirable connotation on risk and depicts that risk is wicked. Although bizarre at first, the risk is, however, still a neutral concept, as it used to be regarded during the late seventeenth and eighteenth century. It is equally accurate to see risk as something going right, like something going wrong.

6. Risk Assessment

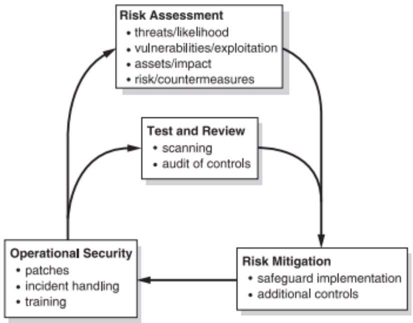
A significant side benefit of risk assessment is – an in-depth knowledge about a system and organisation. In order to make a system more secure, risk analysts try to figure out the interrelation between the systems and functions. The risk assessment process consists of four steps:

- Preparing for the assessment. This stage establishes a context for the risk assessment by applying the outcomes from the risk framing step of the risk management process. Risk framing classifies organizational information regarding policies and requirements for conducting risk assessments, specific assessment methodologies to be employed, procedures for selecting risk factors to be considered, the scope of the assessments, thoroughness of analyses, degree of formality, and requirements that facilitate steady and repeatable risk determinations across the organization. Organizations should use the risk management strategy to the extent feasible to obtain the desired information for the risk assessment and to prepare for the assessment.

- Conducting the assessment. This step produces a list of information security risks that can be arranged by risk level and used to inform risk response conclusions. Organizations analyse threats and vulnerabilities, impacts and likelihood of harm, and the doubt connected with the risk assessment process. They also gather essential information as a part of each task to assure that this step is conducted in accordance with the assessment context established in the previous step. The objective is to adequately cover the entire threat environment in accordance with the specific definitions, guidance, and direction established during the first step. To accomplish adequate coverage within available resources, organizations may have to simplify threat sources, threat events, and vulnerabilities and assess specific, thorough sources, events, and vulnerabilities necessary to achieve risk assessment objectives.

- Communicating assessment results. This step communicates the assessment results and helps the sharing of risk-related information. Once the decision maker come across the results, the organisation are made aware of the results and they now have the appropriate risk related information. It guides them in their risk decisions.

- Maintaining the assessment. In carrying out this phase, organizations should maintain the currency of their specific knowledge of the risk situation. The outcomes of risk assessments inform risk management decisions and guide risk responses. To support the ongoing review of risk management decisions, organizations should maintain their risk assessments by incorporating any changes noticed through risk monitoring. Risk monitoring delivers organizations with a continuing ability to determine the effectiveness of risk responses, to identify risk-impacting changes to organizational information systems and their operating environments, and to verify compliance. [6]



7. Risk Mitigation

Risk Mitigation is basically managing risks involved. It entails strategies devised to eliminate, reduce or control the impact of identified risks inherent with a specified undertaking before a severe injury or damage is done. The purpose of risk mitigation is to for see and deal with the risks involved.

8. Conclusion

With the rapid development of information technology, personal computers, telecommunications, and the internet, people can access the information at any place, at any time. Though most people acquire the information legally, hackers to bypass the security loophole and attack the computer systems for personal benefits or intention to cause losses and harm to different organisations, government and individuals. The attacker may be an insider or may be hired by a competitor ot it may even a guy with destructive intention. The attack can either be Denial of Service (DoS) or be significant damage to the whole framework. The concept of information security has become a burning issue for the entire world. To safeguard the computer systems and data, Risk analysis is done.

Risk analysis was conventionally used to analyse risks posing a threat to mostly IT assets. However, with the onset of the information age, a rising need for protecting information from risks currently faced by many organizations globally came about. As the protection of information is deemed crucial for the continued existence of most organisations an alternative, more comprehensive approach to risk analysis is suggested in this document. This is complex and difficult, if not impossible.

References

[1] School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth 6031, South Africa, 2013, From information security to cyber security.

[2] Thomas R. Petlier, Justin Petlier and John Blackley, Information Security Fundamentals.

[3] Douglas J. Landoll, The Security Risk Assessment Handbook, A Complete Guide for Performing Security Risk Assessments.

[4] Mariana Gerber and Rossouw Von Solms, Management of risk in the information age, 2005.

[5] M. Eric Johnson, Managing Information Risk and the Economics of Security

[6] NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments

[7] Kwo-Jean Farn, Shu-Kuo Lin and Andrew Ren-Wei Fung, A study on information security management system evaluation—assets, threat and vulnerability 2003,

[8] Yikai Xu, Yi Yang, Tianran Li, Jiaqi Ju and Qi Wang, Review on Cyber Vulnerabilities of Communication Protocols in industrial Control Systems.

[9] Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment, https://strategicstudyindia.blogspot.com/2019/10/cyber-risk-scenarios-financial-system.html.

[10] NIST SP 800-12, October 1995, An Introduction to Computer Security: the NIST Handbook.

Design Engineering

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5967-5983

Artificial Neural Network inspired Intelligent Trust based Routing Algorithm for IoT

Kajol Rana[1], Dr. Ajay Vikram Singh[2], Dr. P. Vijaya[3]

[1]Amity University, Noida
[2]Amity University, Noida
[3]Waljat college of Applied Sciences

Abstract

In the growing world of technology a new concept called Internet of Things(IoT) is opened to the world and has become very popular in a very small span of time due to the large applicability of this technology in making the human life more comfortable and automated For Example:- Development of smart homes, smart cities, etc. . But unfortunately, it also comes with substantial amount of risks and shortcomings. IoT makes use of low- powered devices and so secured, less time and energy consuming transmission (routing) of messages due to the limited availability of energy is one of the many and major concerns for the developers of IoT. The following paper presents a trust based routing scenario for IoT, which exploits the past transmission record from the log files in the cupcarbon simulator. Artificial Neural Network is used to grasp the knowledge of trust in quantified form and calculate the value of trust and share it among the other devices in the network. Trust being a human behavioral pattern provides a better approach for making routing decisions. If there is a tie in the values of trust and no alternative path is left then, remaining battery power is taken as a phenomenon to break the tie and make forwarding decision and it is also seen to provide a better utilization of the resources available. The proposed algorithm is seen to wield better energy consumption and routing decisions in comparison to traditional routing algorithms and enhances the pattern of communication.

Keywords: - Trust; ANN; Near field communication; low power devices; Sensors.

1 Introduction

Emerging in the early 1950's Internet has been a means to connect systems over the world that makes use of TCP/IP to transmit data.[1] With the growing times, internet has grown to a concept where all kinds of physical objects will be able to identify themselves as well as other devices over the Internet. IoT makes network communication possible using Internet protocol by discarding human interference. IoT makes use of scale-free networking, that is, the data ranges from tiny data blocks to high quality video.[2]It does not tolerate any form of delay. IoT makes use of Radio- Frequency identification [3] and Near-field communication [4], low energy Bluetooth [5] , wireless, LTE-A &Wifi-direct for networking in IoT [6]. To cumulate large number of devices, it makes use of IPv6 addressing. [7]

1.1 Routing in IoT

IoT is defined to be a combination of adhoc devices, sensors and heterogeneous natured devices which communicate with each other harmoniously, so building a system like this and making the devices communicate with each other is a tedious job. IoT makes use of 6LoWPAN protocol [8], to make the task of sending and receiving IPv6 packets over IEEE 802.15.4 [9] less complex.

Devices used in IoT are generally having low-power applications which result in lossy network since the devices do not have the sufficient power to support traditional data routing, as a result the data flow is limited and highly ordered. Data flow can either be point to point, point to multi-points or Multi-point to point. [10]

For the purpose of energy saving cluster based routing is used, to enhance the performance of nodes in an energy deficient environment. [11] Certain Cluster based routing protocols are LEACH (Low Energy Adaptive Clustering Hierarchy) it is used by nodes to outgrow from the power shortage issues faced by the network. Wireless sensor nodes are assigned into clusters. A broadcast message is then sent over to short distances. A cluster head is selected randomly, whose job is to collect data from the nodes and submit it to base station;[12][13] SEP (Stable Election Protocol) chooses its Cluster head by using weighted probability of nodes. Then on this basis the nodes are divided into two levels:- Advanced and Normal Nodes. Generally advanced nodes get the right to become cluster head.[14] This is the reason that this protocol is called stable;[15] HEED (Hybrid Energy Efficient Distributed Protocol) it firstly makes groups of nodes and out of the nodes selects a cluster head and makes use of the residual energy for CH selection; [16][17] TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol) makes use of threshold for data transmission and focusses on data centric method. Sensing of data is reported to absorb less energy than transmission of data. [18][19][20]

Trust

It is marked as the starting point of building any form of relationship. Trust is a feeling or we can say a flow of hormones that makes a person rely, have a feeling of safety and feel confident towards the other person. Trust is a complex phenomenon as its evaluation is completely dependent upon the response from the other end. Response can be in form of creation of confidence, beliefs of the person (which is bound to vary from one person to another), and expectations one casts onto the other, reputation of the person (which can be easily derived from prior knowledge and past experience), cooperativeness and honesty. Trust can be developed in many ways, whether it is direct trust (one is personally involved), indirect trust (when we have trust on a person and that person trusts some third person, we automatically develop a level of trust on the third person). [21] Strength of relationship based on trust is determined by the reason for trust, environment of trust and the imminence of trust. Privacy is an additional feature to trust. [22]

In real world, it can be illustrated by the relation of a buyer and seller or trust between members of a family. In a buyer-seller relation trust can be of two kinds: Calculated and Relational. Value of calculated trust is said to be predictive in nature. Buyer always perpetrates calculated trust towards the seller, whereas, a seller can have both calculated as well as relational trust on the buyer. Trust between both will depend upon the level of risk involved, quality of the item sold and will involve continuous values. On the contrary in a family, calculation of trust may involve the behavior and participation of the family members. In a family (Fig.1.), it is observed that the level of trust increases with the age and amount of experience gained by a person. A general pattern depicts that the level of trust is higher, of children towards their parents/grandparents but parents/grandparents may not trust their children to the same extent, so it can be concluded that trust is dependent upon the frame of reference and is lopsided (asymmetric) in nature.

For example, Hari and Ram members of the IJK family may or may not trust each other. In a framework where decision is to be made about the careers Hari may not trust Ram, whereas when it comes to the selection of a dress Hari may trust Ram. Thus we can say that trust constitutes of continuous values.

If we Consider T(v) as the function for trust and obtaining values between -1 to 1, we can say that,

T(v) = -1 - Untrustworthy

0 – Evenhanded

1 – Trustworthy

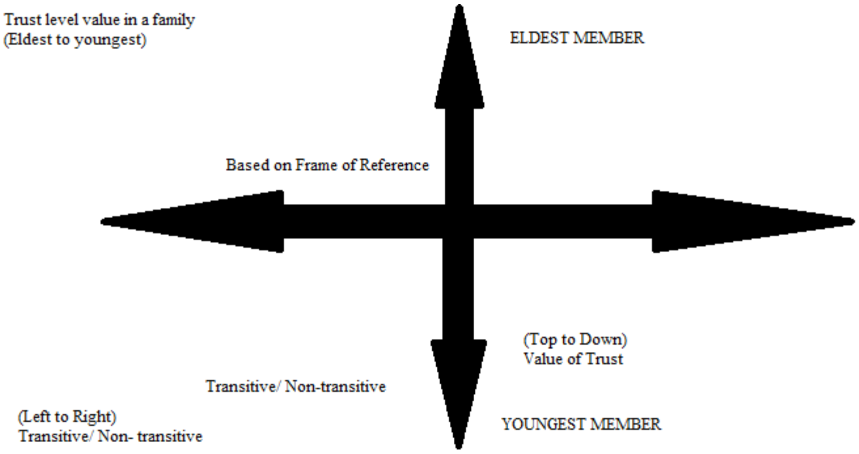

Trust level value in a family
(Eldest to youngest)
ELDEST MEMBER
Based on Frame of Reference
(Top to Down)
Value of Trust
Transitive/ Non-transitive
(Left to Right)
Transitive/ Non- transitive
YOUNGEST MEMBER

Fig.1. Illustrating level of trust in a family

2 Related Research Work

This section compares various related works in the field of IoT and trust management. A recent study states that for election of a leader in IoT, dominating tree routing algorithm [23] gives an efficient and fault tolerant environment, with low energy consumption of about 85%. [24] We know that IoT faces the challenge of memory management, so telescopic view is used to generate less network traffic volume with excellent latency. [25]When talking about routing in IoT, a cluster based hierarchy protocol called DEEC-VD is used for heterogeneous network which makes use of clusters and forms active cluster head [26] and to find the shortest path between the active cluster heads, it makes use of the Dijkastra algorithm [27] that gives better results as compared to other routing algorithms like DEEC, LEACH & SEP.[28][29] Another technique is known as Redundancy based WEP routing technology, which does query-driven data reporting and provides a coverage area of Machine to Machine mode and also ensures maximum stability period. [30] Another routing protocol which is focused on energy consumption is divided into two phases: The first phase, known as initialization phase, in which, each sensor node needs to find its neighbor nodes and form a cluster, whereas, the second phase is known as, maintenance phase, wherein, all the nodes maintain their information matrix and share these details with all the other nodes, on receiving a cluster head rotation control message. [31] AOMDV makes a connection between the internet and ordinary nodes within a network. Each node has to maintain two tables: 1) Internet Connecting table 2) Routing table. It can also be called as a reactive protocol [32] as it only works on demand. Does not provide any security, not context aware, finds the best route with regards to minimal hop count and do not consider energy efficiency and it only shortlists one path, so there are high chances of failure and delays; [33]Optimized link state routing protocol works as a table operated protocol and shares the details of the topology with the other participating nodes on a regular basis. Each node has to select a set of multipoint relays to make the communication possible. These MPR's should be only one hop neighbors to the node and must contain bi-directional linkages;[34] For NDN IoT in smart cities creation, we have a Light weight authentication and secured routing protocol, which provides deployment densities of 40,000 nodes/km^2 and also involves three stages, Network discovery and authentication, Sensor Node authentication & key delivery and Path advertisement; [35] Secured Multi-hop routing enables the IoT devices to combine the procedures of authentication and routing without creating any notable overheads with added features that enable it to segregate IoT devices based on their unique identifications and re-conceptualize logical networks previously formed inside the network by the IoT devices. It performs better than OLSR protocol [36] by inculcating four layers, known as, Application layer, transport layer, User controllable multi-layer(UML) and Data link layer, wherein, the routing task is provided to the UML layer along with ANDL module to secure the communication;[37]RPL is another routing algorithm introduced by IETF whose work is to develop a topological structure by consuming the energies provided by the intelligent devices and compute the required resources. A modification of RPL also called Multiparent-RPL works on the same phenomenon but considers two way routing and makes a hierarchical clustering topology, in which, many clusters cross path and ensures data arrival rates against common routing attacks. It has been proven to prevent black and wormhole attacks; [38][39] EARA is a bio-inspired algorithm. It considers the hop count as well as the energy efficiency. It also maintains data about the average energy of nodes and the lowest residual energy value; [40] PAIR includes information about: 1) Residual energy and the amount of power consumption. 2) Buffer space and the active load. 3) Distance between the node and neighbor. It is a context aware as well as multi-hop protocol. Security parameters are not considered and memory requirements are high. It makes the heterogeneous networks cooperate; [21] REL only makes decisions based on the Link Quality indicators and stores all the possible routes. Best route is found out by considering the following factors: 1) quality of the wireless links. 2) Residual energy. 3) Hop Count. [41]

2.1 Issues associated with IoT

IoT is a developing area and so it still has a lot of issues which need to be considered before enjoying the actual benefits of IoT. As per the study of HP, it is found that 80% of IoT devices are failing to provide personal privacy to its users and 60% are still having security issues, that makes the system highly vulnerable to attacks. IoT still lacks interoperability of applications making the system not fulfilling its main goal and requiring a mechanism to develop standards and inculcating the made standards into every device to be a part of IoT system. Although the growth of sensors and chipsets are on an increase but still we lack good objects to sense the environment and generate good quality of data. Security and privacy is a big concern of IoT, as we still do not have a good authentication and reliable algorithm through which we can send our data with 100% guarantee of safe delivery to the destination node. Maintenance of connectivity in an ad-hoc network is a highly challenging task. As IoT has a feature of connecting a large number of objects, the scalability of objects in here becomes a problem. There is a limited supply of energy to run the IoT devices, so we need a system wherein consumption of energy is minimum with maximum output. Management of memory space in small objects, where data collected is very high makes it hard for the user to accept the system. No device can give 100% CPU power to run the IoT application, no system can provide such high power to any applications due to their own dedicated tasks.

2.2 Routing Issues

Routing is a great issue as when talking about IoT, we require devices working on low power, links should be lossy in nature, IoT follows mesh topology with multiple-hop principle and the network conditions are vastly changing from device to device. On top of it IoT works on moving as well as stationary objects, requiring different protocols, for making an IoT we have to combine these protocols into a single protocol which works more efficiently, which is again a tedious task. So considering these situations, routing has large number of issues to be handled, such as, devices communicating, suppliers of devices may be same or different; existence of the source node and destination node may be on different networks; connection between the devices may be consistent or may not be; resource availability may be a challenge and devices of different kinds may not cooperate well along with each other due to the unavailability of resources; devices not utilizing the universally accepted addressing mechanism; varying communication range between devices creates a lot of chaos; environmental conditions highly affect the routing, due to breakage of various links, signal quality degradation, reaching server becomes an issue.; estimated delay in communicating the huge amount of data should always be less than the expiry time of the data; duplicate data must be removed before transmitting onto the network; energy requirement should be less, so that even very small devices are able to function properly and require less network lifetime; context creation, validation, accuracy of the data should be well maintained and with constrained memory we also need to maintain the context in such a way that storage is maintained.[42]

2.3 Factors affecting Trust

Trust keeps on growing at a rapid pace, till the devices are interacting continuously. Denial of service, whether from the intermediate node or destination node, can change the value of trust disastrously. If such an event occurs, we need to negate all the values, so we keep the value of the bias to be a very high negative value. Just like the real world, in the IoT world value of trust obtained in the past may not matter much, if the contact time is high. Record of the success rate and time difference between the last contact and current contact must be kept, for the proper working of Trust as a routing algorithm for making forwarding decision in an IoT environment.

3 Proposed Work

IoT nodes contain the combination of sensors and actuators which hold the responsibility of catching data and taking required actions. IoT is constructed on three building blocks, namely, hardware, platform and software. Sensors, gateways and actuators are a part of hardware. In IoT we talk about Device to Device Direct calculation, wherein, we need to be aware about the kind and sort of past experiences, without having the need of a trusted third party. We need to build a trust metric, on basis of which the credibility of a node can be recognized. So for making the forwarding decision, trust value are computed for each and every node along with the distance between each node, to find the nodes in the range of the source node.

3.1 Assumptions Made

IoT works with the coordination of all the sensors and gateways and thus it is assumed that all the sensors and gateways work in a coordinated manner. IoT works on real time and does not accept any sort of delays. In case of delays the error code is generated and the bias is activated. The value of trust is calculated at each and every node and flows continuously. All the nodes used are indistinguishable. Routing decisions are only taken on the basis of the value of trust computed and the propinquity of all the nodes.

4 ANN Based Trust Model

Made with the inspiration of a human nervous system, Artificial Neural Network learns how to function through examples similar to humans who learn from past experiences. It can handle variability in a good way. Researchers more often come across mobility patterns. In here, we will be quantifying the log_files values like time, repetition of messages and total time taken to deliver a message to evaluate the value of trust to increase the working of IoT.

4.1 Mapping

Trust value can be calculated by using Trust Metric only after we successfully map the log_file with the IoT Routing variables.

Let us consider the nodes to be as s_1, s_2, s_3, …, s_n . So we would define the initial value of trust to be zero, that is, $t(s_1) = t(s_2) = t(s_3) = \ldots = 0$. It is done to get a better understanding of trust. Destination node is found by routing the first message from the source node. For each sensor the value of remaining power is stored using $p_1,p_2,p_3\ldots..p_n$. Initial value of all the power for every sensor is set to 100%. So, $p_1 = p_2 = p_3 = \ldots.. = p_n = 100$.

4.2 Computation and learning

For computing the value of each node we need a function to quantify the variables:-

$f(s_1)$ = <Difference between time of the current and last messages trasnmitted f_1 , repetition of messages f_2, total time taken to deliver a message f_3>

To build a neural network we assign weights w_1, w_2 , w_3 to f_1, f_2, f_3 to erect the Binary Activation Function (Fig.2). Assigning the value of b (bias) = -999 (High negative value). Setting the null weight $w_0 = 1$, f_i = trust parameter and w_n = weight allocated to each variable.

f_1 = Difference between time of the current and last messages trasnmitted (i.e Time of current message - Time of Last message transmitted).

f_2 = Repetition of messages (i.e Frequency)

f_3 = Total time taken to deliver a message.

$w_1 \infty \frac{1}{f1}$ and $w_2 = w_3 = 1$.

For each node s_n function will be calculated for the other node, that is, $s_1, s_2, \ldots. s_{n-1}, s_n, s_{n=1}, s_{n+2}$, …and so on. For each node s_n a power value is generated and stored in the variable p_n, which will be responsible for storing the battery power dynamically. Initial value for power for all the sensors, will be set to 100.

$$f(v) = \sum_{i=0}^{3} f_i w_i$$

$$y = v + b$$

$$z = ø(y)$$

$$z = \begin{cases} 0 \; if \; y < 0 \\ 1 \; if \; y \; \geq 0 \end{cases}$$

The proposal of w_2 and w_3 to be equal to one is kept to find the correct values of f_2 and f_3. Under any unwanted condition the value of bias is owned. Trust is computed for each device by each device for the trust metric construction. Since, $w_1 \infty \frac{1}{f1}$ the value of trust becomes inversely proportional to the value of f_1. So if the time difference is low the value of trust will be high and contrariwise All the computed values of trust are kept in the cache. No negative or fraction value is considered. All the results must be absolute.

Notation :- Real Time variables are mentioned in Table I.

Sensors : s_1 to s_n

Battery Power: p_1 to p_n

t(old) = Trust value of the sensor on the last connection

t(new) = Current value of trust

log_file = Data of Past Transmissions

f_1 = Difference between time of the current and last messages trasnmitted (i.e Time of current message - Time of Last message transmitted).

f_2 = Repetition of messages (i.e Frequency)

f_3 = Total time taken to deliver a message.

TABLE I : Real Time Variables

S. No	Real Time Variables	Variables recognized
1	Transmitting Sensor	Source
2	Battery power	Battery power value
3	Receiving Sensor	Destination
4	Start Time of message transmission	Start_Time
5	Time taken for message to reach from source to destination	Total_time
6	Event of calling	COM_SEND, COM_RECIEVE,COM_UNKNOWN,COM_BREAK or COM_DELAY
7	Route from which transmission of message started	Check trust metric
8	Route from which message left the exchange	Check trust metric
9	Fault event	Bias is activated, so b = -999

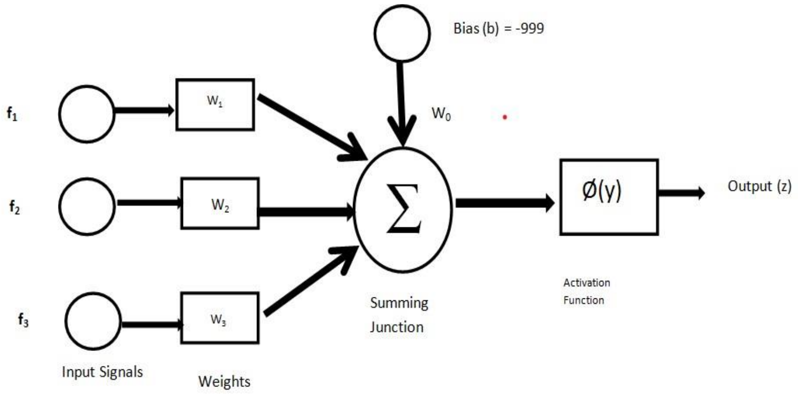


Fig.2. : Illustration of the Binary Activation function using variables of trust in an ANN

Algorithm :-

Algorithm1 :- Initial Algorithm for Computation of the value of Trust

```
Use Log File, Summon $f_1, f_2, f_3$
Evaluate the value of Z
Use cache, to summon $t_{old}(s_i, s_j)$
If $Z = 0$ do
                    $t_{old}(s_i, s_j) \rightarrow t_{new}(s_i, s_j)$
else if ($Z = 1$ &$t_{old}(s_i, s_j)$) is not in cache do
```

```
                    $t_{new}(s_i, s_j) = 1$
                      else if $Z=1$ & $t_{old}(s_i, s_j)$ is in cache and has some value do
                                      $t_{old}(s_i, s_j) +1 \longrightarrow t_{new}(s_i, s_j)$
                      end if
                    end if
end if
Repeat for all the nodes till the destination is found
```

Algorithm 2 :- Algorithm for the Intermediate Node to decide the routing path

```
Use Cache, check to find whether the sensor $s_1$ is the next node.
Evaluate the trust values $t_{new}(s_i, s_j)$ for all the sensors , $s_1, s_2, .... s_{n-1}, s_n$.
Sensor having the highest value of trust is to be selected
    else if check cache of $s_i$ , if multiple sensors have same trust value
        then using log file of $s_i$ fetch the value of $f_1$.
                Select the node having lesser value of $f_1$.
        else if values of $f_1$ of multiple sensors is same
            then check battery_power for multiple sensor
                Select the node with high value of p.
        end if
        end if
end if
Repeat for all sensors on the way until destination is found.
```

5 Metaphysical Illustrations

Illustration 1:

The initial values of all the sensors in the transference radius is set to be 0. The algorithm will work without the evaluation of trust values for the first time. The value of trust for all the sensors s_1, s_2, s_3,s_4 persists to be 0. Trust values for sensors s_5, $s_6$will be assigned as $-\infty$.(Table II and Fig 3) As both the sensors are way apart from the other sensors and do not fall in the communication range of any other sensor.

So, $t(s_1, s_2) = t(s_1,s_3) = t(s_1, s_4) = 0$ and $t(s_1,s_5) = t(s_1,s_6) = -\infty$.

Similarly $t(s_2,s_5) = t(s_3, s_5) = t(s_4,s_5)=t(s_2,s_6) = t(s_3, s_6) = t(s_4,s_6) = -\infty$.

So the initial trust metric will be similar to the following table :-

TABLE II : Trust values of sensors at initial state

Sender Node	Receiver Node	Trust value
s_1	s_1	--
s_1	s_2	0
s_1	s_3	0

s_1	s_4	0
s_1	s_5	-∞
s_1	s_6	-∞

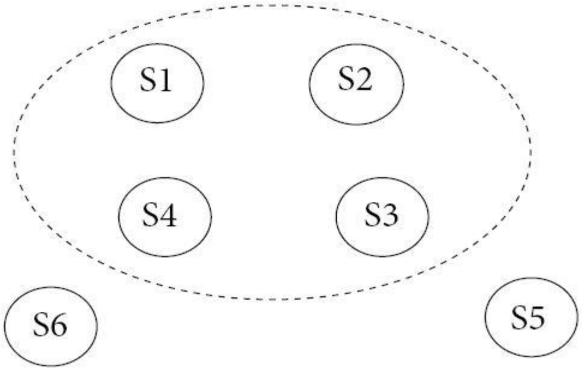


Fig.3. Initial state

Illustration 2:

Suppose that sensor s_1 communicates with sensor s_3 then the value of trust is calculated using the Artificial neural network and so,$t(s_1,s_3) = t(s_1,s_3)+1$. The table entries will change accordingly in the following way. (Table III and Fig.4)

TABLE III : Trust values of sensors for making forwarding decision

Sender Node	Receiver Node	Trust value
s_1	s_1	--
s_1	s_2	0
s_1	s_3	$t(s_1,s_3)+1$
s_1	s_4	0
s_1	s_5	-∞
s_1	s_6	-∞

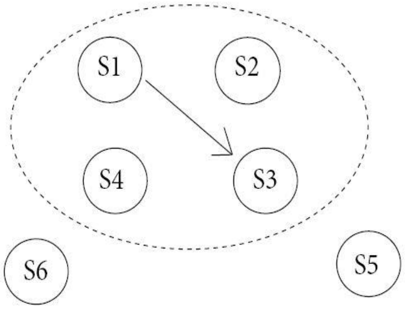


Fig.4. Forwarding decision

Illustration 3:

Supposing that sensors $s_5$and $s_6$come in the communication range of sensor s_1 at a given point of time, then,

$t(s_1, s_2) = t(s_1, s_4) = t(s_1,s_5) = t(s_1,s_6) = 0$ and $t(s_1,s_3) = t(s_1,s_3)+1$. (Table IV and Fig.5)

TABLE IV : Trust values when all sensors in communication range

Sender Node	Receiver Node	Trust value
s_1	s_1	--
s_1	s_2	0
s_1	s_3	$t(s_1,s_3)+1$
s_1	s_4	0
s_1	s_5	0
s_1	s_6	0

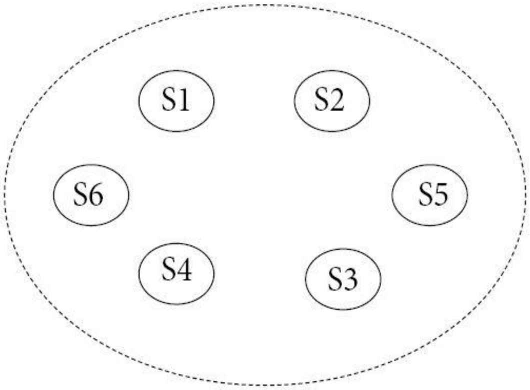


Fig.5. All the sensors in the communication range

Illustration 4:

Assuming that sensor s_1 is obtaining the same highest value of trust for two sensors, for example s_3, $s_4$then in that case, the path is identified using the most recent connection time, in case the value of f_1 is also equal for both the sensors. (Table V and Fig.6)

TABLE V : Equal trust values for two or more sensors

Sender Node	Receiver Node	Trust value
s_1	s_1	--
s_1	s_2	0
s_1	s_3	4
s_1	s_4	4
s_1	s_5	0
s_1	s_6	0

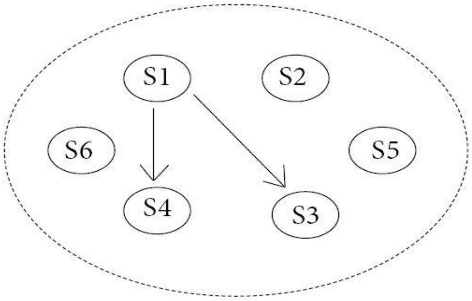


Fig. 6. Two paths for communication from a particular sensor.

Illustration 5

Assuming that the most recent connection time and the value of f_1 is also equal for both the sensors, which can be a case in big networks working with thousand's and lakh's of sensors, then we utilize the remaining battery power as a variable. The router will find the sensor with the highest amount of battery power remaining using the value of p and will direct the message towards that particular sensor. (Table VI and Fig.7)

TABLE VI : Equal trust value and most recent connection time for two or more sensors.

Sender Node	Receiver Node	Trust value	Most recent connection time
S1	S1	--	--
S1	S2	0	0
S1	S3	4	12.03
S1	S4	4	12.03
S1	S5	0	0
S1	S6	0	0

In this case the remaining battery power for both nodes s3 and s4 will be checked and the forward decision will be based upon the sensor which has the highest amount of battery power remaining.

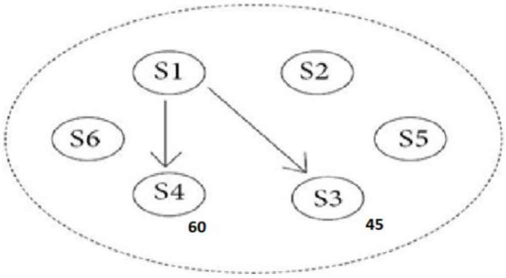


Fig.7. Two paths for communication from a particular sensor along with their remaining battery power (For s3 = 45% and for s4= 60%).

6 Performance Computation

The proposed algorithm has been simulated using the cup-carbon simulator of IoT using five sensors with the maximum energy of 19160 J and having sensor radius of 20m. The algorithm also proceeds with the shortest path model.

Cup-carbon is used for the development of a smart city, which includes the validation and debugging of the algorithms and collection of data for all kind of IoT applications like smart homes, smart city, etc. It works on geographical locations by making use of Open Street Maps. One can easily program the working of the sensors by making use of Senscript (algorithm for sensors, routers, mobiles, etc.). On each and every simulation two types of files are generated namely, log file (contains all the events executed by a sensor in the particular simulation) and rst file (contains the energy level of a sensor during the simulation). It contains three scenarios: Wireless sensor network simulation, Multi agent simulation environment and mobile simulation. Cupcarbon is a growing tool and is advantageous for researchers, academicians and enthusiastic students.

The proposed algorithm makes use of sensors to demonstrate the communication channel of real time devices. It also makes use of the battery consumption feature of cup carbon simulator for breaking the tie in case the value of trust and value of last connection time for the sensors are equal. The performance is evaluated by using two routing protocols, LASER(Lightweight Authentication and Secured Routing Algorithm) and REL(Routing Protocol Based on Energy & Link Quality) with comparison to the proposed algorithm. LASER is used as it provides high deployment density of 40,000 nodes/km^2 and is a reliable algorithm in terms of security and message delivery. RPL allows the use of energy accumulated from the smart devices and makes use of distance vector algorithm, while the proposed algorithm makes use of the remaining battery level of the nodes.

Performance is evaluated based on the variables simulation time (Fig.8), sent messages (Fig.9), received messages (Fig.10), lost/aborted messages (Fig.11) and the delivery probability (Fig.12). It is seen that the proposed algorithm has larger number of sent messages and also surpasses the other algorithms in the number of received messages and also takes very less time to simulate.

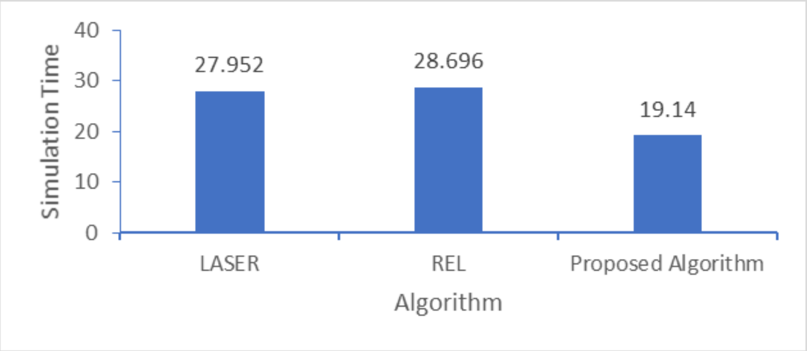


Fig.8. Total time taken for simulation

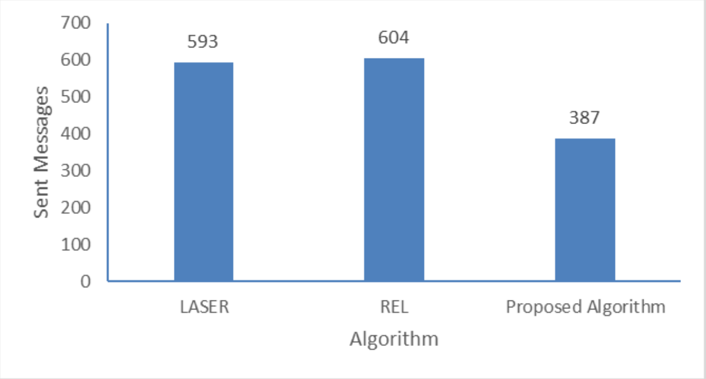


Fig.9. Total number of messages sent

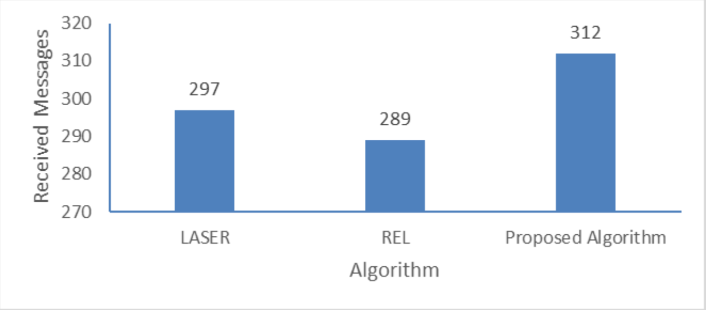


Fig.10. Total number of Received messages

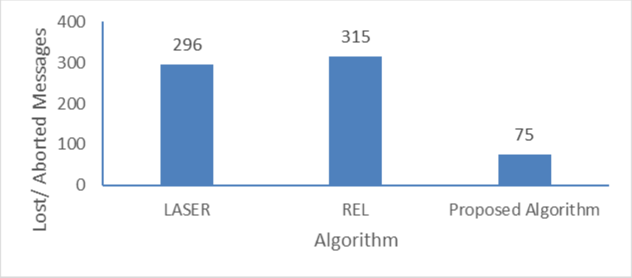


Fig.11. Total number of Lost/Aborted messages

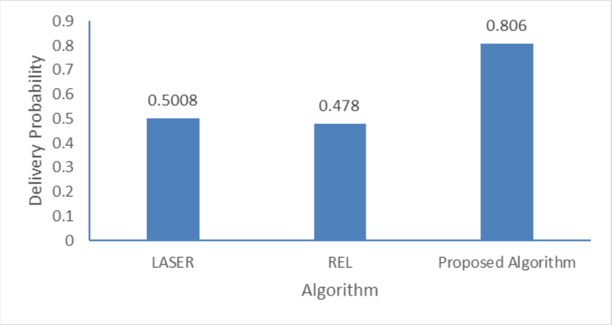


Fig.12. Delivery probability

7 Conclusion

In this paper, the researcher has made use of a trust based ANN. Trust is taken as a tool to guide for the forwarding decision. Trust is found to be a very practical approach for making routing decision, low routing overheads and is seen to be saving the evaluation time and also it does not require any form of authentication as compared to the other algorithms and thus it is said to have low security aloft. The implementation of trust in the practical world will lead IoT to greater heights, as it has low routing overheads, making the concept or emotion of trust to be quantified and also training the neural network to work according to this human behavior. The proposed algorithm works well, with more number of messages sent and received in comparison to the other algorithms namely, LASER and REL used in the paper. A certain amount of energy reduction and a skillfull use of energy as a variable is also achieved as the proposed algorithm makes use of the remaining battery power as a variable to sort out the tie in case the value of trust and the last communication time both result into equivalent value, which can occur in the real time network which involves large number of sensors, which is not a part of the traditional routing algorithms.

References

[1] D. Meyer and G. Zobrist, "TCP/IP versus OSI," in IEEE Potentials, vol. 9, 1990, pp. 16-19.

[2] Tetsuya Yokotani, “Requirements on the IoT communication platform and its standardization”, IEEE, 2017, p.p:- 1-4.

[3] X. Jia, Q. Feng, T. Fan and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, 2012, pp. 1282-1285.

[4] I. Turk, P. Angin and A. Cosar, "RONFC: A Novel Enabler-Independent NFC Protocol for Mobile Transactions," in IEEE Access, vol. 7, 2019, pp. 95327-95340.

[5] A. R. Chandan and V. D. Khairnar, "Bluetooth Low Energy (BLE) Crackdown Using IoT," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, 2018, pp. 1436-1441.

[6] M. Condoluci, L. Militano, A. Orsino, J. Alonso-Zarate and G. Araniti, "LTE-direct vs. WiFi-direct for machine-type communications over LTE-A systems," 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Hong Kong, 2015, pp. 2298-2302.

[7] N. S. Zarif, H. Najafi, M. Imani and A. Q. Moghadam, "A New Hybrid Method of IPv6 Addressing in the Internet of Things," 2019 Smart Grid Conference (SGC), Tehran, Iran, 2019, pp. 1-5.

[8] RFC 8138 [Online]. Available: https://tools.ietf.org/html/rfc8138.

[9] 802.15.4 [Online]. Available: standards.ieee.org/content/dam/ieeestandards/standard/web/documents/erratas/802.15.4-2015-errata.pdf.

[10] M. Lukić, Ž. Mihajlović and I. Mezei, "Data Flow in Low-Power Wide-Area IoT Applications," 2018 26th Telecommunications Forum (TELFOR), Belgrade, 2018, pp. 1-4.

[11] N. Nasser, L. Karim, A. Ali, M. Anan and N. Khelifi, "Routing in the Internet of Things," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6.

[12] Behera TM, Samal UC, Mohapatra SK, “Energy efficient modified LEACH protocol for IoT applications”, IET wireless sensor systems, 2018, p.p:- 223-228.

[13] M. N. Jambli, M. I. Bandan, K. S. Pillay and S. M. Suhaili, "An Analytical Study of LEACH Routing Protocol for Wireless Sensor Network," 2018 IEEE Conference on Wireless Sensors (ICWiSe), Langkawi, Malaysia, 2018, pp. 44-49.

[14] Liu, X. A Survey on Clustering Routing Protocols in Wireless Sensor Networks. *Sensors* **2012**, pp. 11113-11153.

[15] S. Iqbal, S. B. Shagrithaya, Sandeep Gowda G.P and M. B.S, "Performance analysis of Stable Election Protocol and its extensions in WSN," 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, Ramanathapuram, 2014, pp. 744-748.

[16] K THOMAS, Aby; R, Vallikannu; ADVAIT NARAYANAN, Sai. Minimizing the energy consumption of WSN by using modified hybrid energy efficient distributed clustering protocol. **International Journal of Engineering & Technology**, [S.l.], 2018, pp. 758-763.

[17] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," in IEEE Transactions on Mobile Computing, 2004, pp. 366-379.

[18] Manjeshwar, Arati & Agrawal, Dharma. (2001). TEEN: ARouting Protocol for Enhanced Efficiency in Wireless Sensor Networks.. Intl. Proc. of 15th Parallel and Distributed Processing Symp.

[19] Galshetwar V.M., Jeyakumar A., “Energy efficient and reliable clustering algorithms HEED and ADCP of wireless sensor network : A comparative study”, IEEE, 2014, p.p:- 1979-1983.

[20] Neha Rani, Pardeep Kumar, “Energy efficient hierarchical routing protocols for IoT”, IJEAT, 2019, p.p:- 2122-2125.

[21] Xue X., Leneutre J., Ben-Othman J. (2005) A Trust-Based Routing Protocol for Ad Hoc Networks. In: Belding-Royer E.M., Al Agha K., Pujolle G. (eds) Mobile and Wireless Communication Networks. MWCN 2004. IFIP International Federation for Information Processing, vol 162. Springer, Boston, MA, p.p : 251-262.

[22] Ajay Vikram Singh, Vandana Juyal, Ravish Saggar, “Trust based Intelligent routing algorithm for delay tolerant network using Artificial Neural Network”, Springer, 2016.

[23] Bounceur, Ahcene, et al. "A new dominating tree routing algorithm for efficient leader election in IoT networks." Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual. IEEE, 2018.

[24] Ahcene Bounceur, Madani Bezoui, Massinissa Lounis, Reinhardt Euler, Ciprian Terodorov, “A new dominating tree routing algorithm for efficient leader election in IoT network”, IEEE, 2018, p.p:- 1-2.

[25] Hessam Mocini, I-Ling Yen, Farok Bastani, “Routing in IoT network for dynamic service discovery”, 2017, IEEE, p.p:- 360-367.

[26] L. Qing, Q. Zhu and M. Wang, "Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks", *Comput. Commun.*,2006, pp. 2230-2237.

[27] S. Skiena, "Dijkstra's algorithm" in Implement. Discret. Math. Comb. Graph Theory with Math. Reading, MA:Addison-Wesley, 1990, pp. 225-227.

[28] T. Sharma, B. Kumar and G. S. Tomar, "Performance Comparision of LEACH SEP and DEEC Protocol in Wireless Sensor Network", *Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering*, 2012.

[29] T M Behera, SK Mohapatra, Proshikshya Mukherjee, HK Sahoo, “Work in Progress: DEEC-VD: A Hybrid energy utilization cluster based routing protocol for WSN for application in IoT”, International Conference on Information Technology, 2017, p.p:-97-100.

[30] K Anusha, “Redundancy based WEP routing technology (IoT-WSN)”, IEEE, 2015, p.p:-407-410.

[31] Bilal R. Al-Kaseem ; Hamed S. Al-Raweshidy, “Scalable M2M routing protocol for energy efficient IoT wireless applications”, IEEE, 2016, p.p:- 30-35.

[32] R. Ahuja, "Simulation based Performance Evaluation and Comparison of Reactive Proactive and Hybrid Routing Protocols based on Random Waypoint Mobility Model", *International Journal of Computer Applications*, 2010, pp. 20-24.

[33] Yicong Tian, Rui HOU, “An improved AOMDV Routing protocol for Internet of Things”, CiSE, 2010, p.p:-1-4.

[34] RFC 3626 [Online]. Available: https://tools.ietf.org/html/rfc3626.

[35] Travis Mick, Reza Tourani, Satyajayant Misra, “LASeR: Lightweight authentication and secured routing for NDN IoT in Smart cities”, IEEE.

[36] RFC3626 [Online]. Available: https://tools.ietf.org/html/rfc3626.

[37] Paul Lon Ruen Chze, Kan Siew Leong, “A secure multi hop routing for IoT communication”, IEEE, 2014, p.p:-428-432.

[38] Wallgren, Linus, Shahid Raza and Thiemo Voigt. “Routing Attacks and Countermeasures in the RPL-Based Internet of Things.” *International Journal of Distributed Sensor Networks* 9 ,2013.

[39] Guojun Ma, Xing Li, Quingqu Pei, Zi li, “A security routing protocol for Internet of Things based on RPL”, International conference on networking and network applications, p.p:- 209-213.

[40] Michael Frey, Friedrich Grose, Mesut Gunes, “Energy aware ant routing in wireless multi hop network”, IEEE, 2014, p.p:-190-196.

[41] Sharief M.A. Otcafy, Fadi M al-Turjman and Hossam S. Hassancin, “Pruned adaptive roputing in the Heterogeneous Internet of Things”, IEEE, 2012, p.p:- 214-219.

[42] Amol Dhumane, Rajesh Prasad, Jayshree Prasad, “Routing issues in Internet of Things: A survey”, IMECS, 2016.

[43] Prasad P. Lokulwar, Dr. Hemant R. Deshmukh, “Threat analysis and attacks modeling in routing towards IoT”, IEEE, 2017, p.p:-721-726.

Fake news: A Threat to the Credibility of Media-Ecosystem

Priyanka Tyagi (Assistant Professor, JIMS, Vasant Kunj, Delhi)

Charu Chandra Pathak (Research Scholar, GJU, S&T)

Abstract: Fake news is not a recent phenomenon. Hoax news, fabricated, misleading, manipulated content was always in circulation. However, it’s a new medium, i.e. new media, social networking sites, smartphones, which drastically magnified their reach and initiated a crisis of credibility. Claire Wardle disagrees with the use of ‘fake news’ and said it’s mis- and dis-information in the information ecosystem and categorizes it in seven types. PolitiFact named fake news its 2016 “Lie of the Year.” For the year 2016, Oxford dictionaries declared the term “post-truth” as it's international word of the year and explains that ‘objective facts are less influential in shaping public opinion than emotional appeals and personal belief.’ This paper attempts to explore various aspects of fake news and how much it is affecting the Indian media-ecosystem. Survey and interview methods are employed to delve deep into this topic. Surveys and interviews were conducted among media professionals and media students.

Keywords: Fake news, New media, SNS, Facebook, Post-truth

Introduction

The concept of fake news or misinformation is not new, several researchers and scholars have studied its impact, mechanism, and root cause. The role of media in the democratic system is widely discussed and researched among media practitioners and researchers. The major factor behind this is that the media can influence the thinking pattern of the masses. (Bennett, 2006). In his study on ‘News as Reality TV: Election Coverage and the Democratization of Truth,’ he has also explained the concept of news reality frame; which is that scenario where news reality frame blurs the connection between the new reality and its original surrounding context. So somewhere in his study, he was discussing how media can change the whole narrative associated with news. Media is supposed to bridge the gap between masses and authorities and they do this by acting as a watchdog to the authorities and their policies. Media have the right to criticize any governmental policy action or reaction in the public interest and this criticism is considered as the face of real and true journalism. However, there are several theories which discuss the concept of media content and power of media in creating public opinions, most of them are interpreting media with different perspectives like they are interpreting the impact of media content on the audience from their perspective as discussed by Gerbner in his cultivation theory or from the perspective of media professionals as discussed by Chomsky and Herman in Manufacturing Consent, but we are still looking for a theory which is talking about the ethical aspect of media and how one should define this. Now, we have accepted the fact that media is an industry, like any other industry and this acceptance gave several new ways to present a story to the audience and even also put some extra pressure on media to provide information as early as they can. Media, Democracy and Politics is a well-discussed issue (Gecer 2018), in his research Media, Politics and Democracy: A Critical Perspective he said that in a democratic system media and politics are coexisting they are mutually benefitted with the ally, as media professional needs politicians for their stories and politicians require them to send their messages to the masses. Specifically, in underdeveloped countries, it is more a monetary kind of relation between the media and the politicians and this is creating this whole nexus more complex. (Romano, 2013). Traditional media did work under these circumstances for so long and with the advent of social media or new media, researchers were thinking that this might bring some change, as we know that new media is a medium of mass communication which uses digital technologies to communicate and with the digitalization of news content, online journalism, and social media also participating equally in the information dissemination process. This whole scenario gave rise to social media campaigns and citizen journalism. As an audience, most of us never witnessed news first hand nor do we know how the whole process of collecting information to processing it and then sending it to the audience works. What we actually know about any issue is the stored data or information provided by someone to us. That, our decision-making stems not from individual rationality but from shared group-level narratives (Sloman & Fernbach, 2017). Humans are biased information-seekers: we prefer to receive information that confirms our existing views. These properties combine to make people asymmetric updaters about political issues (Sunstein et al., 2016).

Fake news is not completely false information rather it’s a combination of biased and misleading information gradually. In other words, fake news is fabricated information that looks like news but created to change or create public opinion. With the advent of technology and specifically with the emergence of social media this fake news dissemination culture is creating a huge impact on public opinion and their perception.

Post-truth was declared as word of the year of 2016 by oxford dictionary. While defining this word the officials explained that post-truth is relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief. Oxford Dictionaries’ president Casper Grathwohl explained it that the rise of social media as a new source of news and information-based media is primarily responsible for the growing distrust of facts offered by the establishment (NBC NEWS.COM). Even according to research conducted by Pew Research Centre on the 2016 presidential election it was found that 23% of the respondents shared a fabricated news story either by knowingly or unknowingly. So how can we define what is fake news? Prior to 2014, this word was not familiar to the news ecosystem rather it was only part of those satire based TV shows where they Mimic and create parody to any existing event. (Stroud, 2019). So Fake News or Fake content are those which are untrue but presented as true. ((Lyons, 2017). Hunt Allcott and Matthew Gentzkow (2016) in their paper explained that the concept of fake news is not new, this phenomenon is having its historical roots and they gave an example of great moon hoax of 1835 in which the New York Sun published a series of articles about the discovery of life on the moon. A more recent example is the 2006 “Flemish Secession Hoax,” in which a Belgian public television station reported that the Flemish parliament had declared independence from Belgium, a report that a large number of viewers misunderstood as true. In 2017, Collins dictionary declared 'fake news' as word of the year. They defined fake news as “false, often sensational, information disseminated under the guise of news reporting.” Helen Newstead, Collins’ head of language content, in her statement, said that “Fake news, either as a statement of fact or as an accusation, has been inescapable this year, contributing to the undermining of society's trust in news reporting." (The Hindu, 2017). Danah Boyd explained that this present scenario is like we are at war more precisely at an information war and we should be worried about this increasing culture of spreading misleading information, but we are more concerned about the impact of these systematic disinformation campaigns on masses. (The Hindu, 2017)

Salena Zito (2016) in an article in The Atlantic, writes that Trump supporters were 'taking him seriously, not literally' (while the press was taking him literally, not seriously). Recently, frustrated Trump spokeswoman Kellyanne Conway said to an interviewer: "Why is everything taken at face value? You always want to go by what's come out of his mouth rather than look at what's in his heart" (Blake, 2017). José Antonio Zarzalejos (2017) explained that Post-truth is not synonymous with lying; moreover, it is that scenario that can manipulate or create public opinion, and the facts this type of news contains are less factual and more emotional and based on personal belief.

Maren B. Hunsberger 2017 in his research on Fake News and Trust: How Do Audiences Respond to Science News in a 'Post-Fact' World? Explained that we cannot easily explain the relationship of the audience with media as it is based on trust and credibility. Later in his research, he concluded that lack of scientific temperament and excessive flow of these misinformation and fake news is creating mistrust among the masses and they are losing their credibility within the media. In this present research, researchers are explaining the concept of fake news within the Media, is there any ecosystem and how they are fighting against this new enemy of media credibility. This research is also attempting to understand the available methods of fake news and the cognitive approach of media professionals and upcoming media professionals regarding this culture of fake news.

Theoretical Framework

The framework of this present research is based on Agenda-setting theory proposed by Macomb and Shaw, though they have given this theory based on their study on 1968 presidential election but one can find the traces of it back in 1922 also when Walter Lipmann expressed his concerned about the power of media and said that media can influence the image of certain messages which can lead to public opinion (Lippmann 1922). In this present research, researchers are trying to understand the relationship between attitude and behavior of policymakers and agenda-setting and how these two are connected to this phenomenon of fake news.

Objectives: These are the major objectives of this research paper:

For Survey:

- To examine the understanding of media professionals about fake news.
- To investigate the understanding of media students about fake news.
- To compare the understanding of media professionals and media students about fake news.

For Interviews:

- To examine the methods to identify fake news.

Research Methodology

This research paper used a survey method to explore and compare the understanding of media professionals and media students about fake news. Two separate questionnaires were prepared to fulfill the objectives, where some questions were common for both the groups. Questionnaire for Media professionals contains some additional questions to understand that how media ecosystem treats fake news. 45 Media professionals and 60 Media students from Delhi-NCR were included in the survey. Google forms were used to collect responses. Moreover, the same group of media professionals and media students were asked some open-ended question to analyze how they identify a message is fake. Therefore, the interview method attempts to explore the issue in-depth.

The common questions asked from the students and the media-persons were taken as two different data sets and the mean values of their responses were compared to each other to find out if any significant difference existed in their perceptions towards the various aspects related to fake news. The data was predominantly on a 5-point scale, i.e. ordinal but for the purpose of calculation, it was assumed to be scaled. The data needs to fulfill certain conditions and the conditions clubbed with the objectives of the study allow the ordinal data to be considered as scale and mean value calculated for them (Sauro, 2016). Then a two-sample T-test was conducted to compare means using SPSS. The T-test came after conducting F-test to find out if variance assumed to be in the two data sets is equal or not. It was then followed by the T-test and the results are placed above. Spearman test was applied to find a correlation between Preference of sources of fake news (such as TV, Radio, Newspaper, Magazine, New Media, Social Media) and Agenda for Fake News (such as political, religious, smokescreen, ideological, election).

Answers collected from the Interviews were analyzed qualitatively and the points emerged from there discussed as a part of fake news and media ecosystem and various ways to identify fake news.

Sample size for survey and interview:

45 Media Professionals and 60 Media Students

Data Analysis and Interpretation

Discussion for the responses collected through Survey (Comparative)

The common questions asked from the students (60) and the media-professionals (45) were taken as two different data sets and the mean values of their responses were compared to each other to find out if any significant difference existed in their perceptions towards the various aspects related to fake news. The data was predominantly on a 5-point scale i.e. ordinal but for the purpose of calculation, it was assumed to be scale. The data needs to fulfill certain conditions and the conditions clubbed with the objectives of the study allow the ordinal data to be considered as scale and mean value calculated for them (Sauro, 2016).

Table 1: Independent Samples Test

Sl. No.	Independent Samples Test	t-test for Equality of Means		
		t	df	Sig. (2-tailed)
1.	Do you think media is important for a democratic system?	1.907	60.423	0.061
2.	Do you think media has an impact on masses?	0.834	103	0.406
3.	Do you think fake news is completely lie information?	-0.939	103	0.350
4.	Do you think fake news is a recent phenomenon?	0.950	103	0.344
5.	Do you think fake news is created to change or create public opinion?	0.480	103	0.632
6.	Do you think media organizations disseminate fake news	-1.574	83.336	0.119
7.	Do you think media organizations actively attempt to expose fake news	-0.296	103	0.768
8.	Do you think fake news is a sign of weak media	-1.508	103	0.135
9.	Do you think fake news has an impact on the masses	-2.623	102	0.010
10.	Do you think media professionals are aware about fake news	-2.254	103	0.026
11.	Do you think that people know how to cross-check to find a fake news	-4.038	103	0.000
12.	Do you think that social activists actively attempt to expose fake news	7.897	103	0.000

The two sample T-test was conducted to compare means using SPSS. The results recorded are shown above. Prior to T-test, we conducted F-test to find out if variance assumed to be in the two data sets is equal or not. It was then followed by the T-test and the results are placed above.

In all the questions, Null and Alternate hypothesis assumed were:

Null Hypothesis

H0: **µs-µm = 0 ; µs = the mean score of the perception of the students and µm= the mean score of the perception of the media-persons**

Alternate Hypothesis

H1: **µs-µm≠0 ; µs = the mean score of the perception of the students and µm= the mean score of the perception of the media-persons**

Let's discuss the results of the test in context to the responses obtained from the questionnaire:

1. For the first question, "is media is important for a democratic system," 95.23% respondents (59 students and 41 media professional) either agree or strongly agree that media is important for a democratic system. As per table 1, since P value (0.061) here is >0.05, the null hypothesis is accepted.

2. For the second question, "does media has an impact on masses," 97.1% respondents (59 students and 43 media professional) either agree or strongly agree that media do have an impact on masses. As per table 1, since P value (0.406) here is >0.05, the null hypothesis is accepted.

3. For the third question, "can we say that fake news completely lies information," 62.9% of respondents (34 students and 32 media professionals) either agree or strongly agree that fake news is completely lie information. As per table 1, since P value (0.350) here is >0.05, the null hypothesis is accepted.

4. For the fourth question, "is fake news a recent phenomenon," 38.1% of respondents (25 students and 15 media professional) either agree or strongly agree; while 40.1% respondents (23 students and 20 media professional) either disagree or strongly disagree that fake news a recent phenomenon. As per table 1, since P value (0.344) here is >0.05, the null hypothesis is accepted.

5. For the fifth question, "is fake news created to change or create public opinion," 82.86% of respondents (49 students and 38 media professional) either agree or strongly agree that fake news created to change or create public opinion. As per table 1, since P value (0.632) here is >0.05, the null hypothesis is accepted.

6. For the sixth question, "do media organizations disseminate fake news," 42.85% respondents (35 students and 10 media professional) said they cannot say surely about it, while 36.19% respondents (14 students and 24 media professional) either agree or strongly agree that media organizations disseminate fake news. As per table 1, since P value (0.119) here is >0.05, the null hypothesis is accepted. An interesting thing came out of the responses from media professionals, where 53.33% of respondents either agree or strongly agree that media organizations disseminate fake news; while only 23.33% of students responded in favor of this option.

7. For the seventh question, "do media organizations actively attempt to expose fake news," 43.81% respondents (28 students and 18 media professional) said they cannot say surely about it, while 32.38% respondents (18 students and 16 media professional) either agree or strongly agree that media organizations actively attempt to expose fake news. As per table 1, since P value (0.768) here is >0.05, the null hypothesis is accepted.

8. For the eighth question, "do you think fake news is a sign of weak media," 75.23% of respondents (42 students and 37 media professionals) either agree or strongly agree that fake news is a sign of weak media. As per table 1, since P value (0.135) here is >0.05, the null hypothesis is accepted.

9. For the ninth question, "do you think fake news has an impact on the masses," 91.43% respondents (52 students and 44 media professional) either agree or strongly agree that fake news has an impact on the masses. As per table 1, since P value (0.010) here is <0.05, the null hypothesis is rejected and the alternate hypothesis is accepted.

10. For the tenth question, "do you think media professionals are aware of fake news," 82.86% of respondents (45 students and 42 media professionals) either agree or strongly agree that media professionals are aware of fake news. As per table 1, since P value (0.026) here is <0.05, the null hypothesis is rejected and the alternate hypothesis is accepted.

11. For the eleventh question, "do you think that people know how to cross-check to find fake news," 56.19% respondents (27 students and 32 media professional) either disagree or strongly disagree people know how to cross-check to find a fake news; however, 29.52% respondents (22 students and 9 media professional) answered that they are not sure whether people know how to cross-check to find a fake news. As per table 1, since P value (0.000) here is <0.05, the null hypothesis is rejected and the alternate hypothesis is accepted.

This indicates that though, in totality, they agree that people do not know how to crosscheck the fact or fake news, however, there is a significant difference in opinion between both the groups. Among students, the dominant opinion emerged as they are not sure about it, while among media professionals it emerged that people do not know how to cross-check the fact or fake news.

12. For the twelfth question, "do you think that social activists actively attempt to expose fake news," 46.67% respondents (28 students and 21 media professional) either agree or strongly agree, while 47.62% respondents (28 students and 22 media professional) said they cannot say surely about it. As per table 1, since P value (0.000) here is <0.05, the null hypothesis is rejected and the alternate hypothesis is accepted.

This indicates that though, in totality, a significant number of respondents agree that social activists actively attempt to expose fake news, however, the number of respondents who were not sure about it was also slightly more than those who agree. This also shows that there is a significant difference in opinion among both groups.

The p-value of the response for most of the questions was greater than the critical value thus allowing the acceptance of the null hypothesis which means that the media students and the media professionals think alike. However, in 5 questions, the difference is significant.

Also the question regarding the impact of fake news on masses, the question of media professionals being aware of the fake news, and people’s ability to cross-check the fake news saw a significant difference in the perceptions. Means both, the students and the media-person have relative contradicting views over the question mentioned.

There is also a significant difference in the perception of the two groups regarding the role of social activists in actively attempting to expose the fake news.

Discussion for the responses collected through Survey

13. Apart from table 1, for the sixth question of the questionnaire, when respondents were asked which medium according to them is the main source of fake news, 41.6% (25 students) and 45% (27 media professionals) answered it as Social Media. Second preference is the first source of fake news, 25% (15 students) and 28.88% (13 media professionals) answered it as New Media. We can clearly see that both groups have similar responses in first and second preferences.

14. Apart from table 1, for the seventh question of the questionnaire, when respondents (media professionals) were asked that which formats of fake news is highly used, the priority order was: (i) Manipulated, (ii) False content and Misleading content, (iii) fabricated, (iv) false connection, (v) Imposter, (vi) satire/parody

15. Apart from table 1, for the eighth question of the questionnaire, when respondents were asked which agenda is fulfilled by fake news, the priority order was: (i) Political, (ii) Religious, (iii) Ideological and Elections, (iv) Smoke-screen. Top two priority orders were very clear from the responses.

Table 2: Correlations Table (between Preferences of sources of fake news and Agenda of Fake News preference)

Correlations Table						
	Agenda of Fake News Preference: Political	Agenda of Fake News Preference: Smokescreen	Agenda of Fake News Preference: ideological	Agenda of Fake News Preference: religious	Agenda of Fake News Preference: elections	Agenda of Fake News Preference: others
Preference of sources of fake news: TV	.382**	.337**	.316**	.288**	.242*	.216*
Preference of sources of fake news: Newspaper	-.299**	0.169	-0.032	-0.095	-0.125	0.082
Preference of sources of fake news: Radio	-.357**	0.183	-0.062	-.210*	-0.174	0.054
Preference of sources of fake news: Magazine	-.234*	.227*	0.059	-0.081	-0.079	0.046
Preference of sources of fake news: New Media	.551**	.549**	.489**	.636**	.568**	.330**
Preference of sources of fake news: Social Media	.635**	.307**	.396**	.570**	.584**	.309**
Preference of sources of fake news: Other	.234*	.388**	.285**	.330**	.301**	.434**

The table above shows the correlation results of media preferences for fake news tested against the perceived agenda sought. Since the preferences were taken in rank order form making it ordinal in nature, Spearman rank-order correlation was used to compute the statistical results.

The objective of applying this test was to find out how the preference attributed to a medium related to the different agenda set by the media. The list of the agenda was prepared using the information acquired during the stage of the review of literature.

The interpretations of the correlation results are as mentioned below:

1. The TV as the source of fake news is believed to be for primarily political agenda setting followed by smokescreen and ideological agenda setting. This indicates that the students and the media professionals most likely think that TV serves the fake news for setting the political agenda for the masses to get consumed into. The smokescreen function is next in the line wherein TV not only sets the agenda but also diverts the attention from issues that TV doesn’t want you to pay attention to.
2. The newspaper as the source of fake news is believed to be for smokescreen purpose. The correlation is however very weak. There is general perception regarding newspaper medium that it helps in diverting the attention. The weak correlation coefficient however indicates weak perception but also somewhat indicates that people believe newspapers to be indulging less in spreading fake news.
3. The radio as the source of fake news is believed to be primarily for the smokescreen creation with the correlation again being weak. The perception towards radio is similar to that of the newspaper which indicates a similar weak perception towards radio. Related literature suggests that radio and newspapers have witnessed declining interest. The declining interests in the medium and the correlation coefficient justify the observations. Also, it indicates, as mentioned in the case of newspaper, people believe radio to be indulging very less in the spreading of the fake news.
4. The magazine as the source of fake news is believed to be primarily for the smokescreen creation. The perception of the students and media professionals regarding magazine is also the same as newspaper and radio. It is used more to divert attention by attributing more significance and relevance to issues of lesser interest.
5. The new media as the source of fake news is believed to be primarily for the religious agenda followed by election-related agenda, political and then smokescreen. The students and the professionals believe that the new media spreads fake news primarily for fulfilling the religious agenda of the state powers. With the spread of the new media and with the advent of the convergence in media technology, bigotry and communalizing the issues have been more rampant than before. The correlational statistics indicate the same.
6. The social media as the source of fake news is believed to be primarily for the political agenda followed by election-related agenda and then religious agenda. This finding along with the recent increase of social media by the political parties adds to the reliability of the results.

7. The other media as the source of fake news is believed to be mainly for the agenda other than the ones mentioned followed by smokescreen agenda-setting by the other media.

Discussion for the responses collected through Interview (Media Students)

Both the groups, i.e., media students and media professionals, among which the survey was conducted, were asked a set of five open-ended questions. The summary of the answers is given below:

In response to the question asked to the respondents (29 media students) that "if they remember any incident when they saw/read fake news and believed in it," most of them believed in fake news at one or another point of time. These incidents were related to issues, like CAA, Protest in JNU, Bus service from Mumbai for migrant workers, Muslim protests, and even the ending of the world too. Some of them were not sure about the fact that whether they had ever believed in such stories. By analyzing responses to this question, researchers can say that events associated with the political issues or political angles are most likely to get viewers/readers' attention and they tend to believe in fake news.

In response to the question, "If they think that media professionals disseminate fake news? If yes, then they have been asked to provide examples of such incident(s)," however, the answer of the respondents (23 media students) was quite scattered. Approx. 56% of them straight away declined that media professionals do have or can have their role in disseminating fake news. However, almost 44% of the respondents did agree that media professional do have their role in this and they had supported their answer with examples like news channels were showing Lockdown is going to be imposed on Delhi after Delhi riots, a TV channel was telecasting number of Corona Patients in Arunachal Pradesh and was establishing its association to Tabligi Jamat which was not true and channel authorities apologized for the same. They had also shared the news stories related to Ram Mandir's judgment and the outbreak of fake news related to Muslim protests after that.

When respondents (30 media students) were asked that "do they think fake news proves itself effective to change or create public opinion," respondents clearly answered that fake news is effective in changing public opinion or creating a new narrative because the masses have a tendency of not verifying the information coming from big media houses. They also shared that with the help of pictures and text, this process becomes faster. Some of them also mentioned that the use of social media is quite involving/extensive in it. Some of them answered that this sort of information generally plays with the emotions and thought process of common people and can instigate hate messages. The respondents even think that illiteracy is also one of the key factors.

When the respondents (30 media students) were asked to tell "the root cause of fake news and how to cope up with this," they said that the root cause of this may be a lack of scientific temperament, illiteracy and lack of willpower to cross-check and verify the news. Some of them also said that smoke screening is also one of the reasons, but the root cause is to gain power and to have public opinion in their favor. Some respondents also talked about the nexus of political parties and media and they said that IT cells of the political parties are the new form of opinion leaders who are controlling minds of people as per their own wish and direction.

The last question was about "any other insights on Fake news, media, masses, and exposure of fake news." The respondents (17 media students) focused on two major things: fake news is dangerous and it is disturbing for the social harmony, which might lead to destroying democratic values; and, we as common people must imbibe this habit of cross-checking every information no matter from where we are receiving it and they also emphasized on imparting education and scientific temperament.

Key points that emerged from the answers are:

(i) People often encounter with fake news. Fake news grabs the attention of the people and they tend to believe in fake news

(ii) Majority of the media students do not agree that media professionals do have or can have their role in disseminating fake news.

(iii) Fake news is effective in changing public opinion or creating a new narrative because the masses have a tendency to not verifying information and illiteracy is also one of the key contributing factors.

(iv) Among the root causes of fake news includes lack of scientific temperament, illiteracy, and lack of willpower to cross-check and verify the news, nexus of political parties and media, IT cells of the political parties serving as a new form of opinion leaders.

(v) Habit of cross-checking every information and imparting education and scientific temperament are critical to counter with fake news.

Discussion for the responses collected through Interview (Media Professional)

Media professionals were also asked a set of five open-ended questions. The summary of the answers is given below:

In response to the question that "If they think that media organizations disseminate fake news and fake news serves interests of media organizations, and why do they think so," The answer (38 media professionals) to this question was surprising because most of the media professionals admitted to the fact that media is responsible for disseminating fake news, though some of them (approx. 27%) denied this as well. Those who suggested that media has their role in the dissemination of fake news said that there are several reasons for this, i.e., power game, TRP, lack of time to cross-check news due to pressure for breaking a news earlier than their competitors, and polarization for public opinion. Few of them also said that media houses have their own agendas and they know that viewers do not have a tendency to crosscheck the news information so they can present whatever they wish.

In response (37 media professionals) to the question that "If they think that media professionals are aware of fake news and know-how to cross-check to find fake news," in response to this question media professional said that majority of their fraternity is not well trained to crosscheck or verified fake news. However, only 16.21% agreed that all media professionals know how to cross-check an information. And methods of fact-checking, suggested by the media professionals include: Google and Facebook conduct workshops for journalists regarding fact-checking; reverse image search; investigative method; checking with official sources, Government sources, Police and the particular Authority concerned with a news; cross-checking with multiple sources; portals dedicated to exposing fake news and fact-checking; ground reports; check the sources and evidences, etc. They have also shared that journalists should be trained to cross-check any information and exposing fake news.

They were also asked to "comment that how do they think fake news proves itself effective to change or create public opinion," media professionals (33 media professionals) clearly answered that fake news is responsible for changing public opinion or can disseminate polarized information which can lead to propaganda and with this they achieve their set agendas. They also said that the main reason behind this is illiteracy and lack of verifying information. Some of them answered that this sort of information generally plays with the emotions and thought process of common people and can instigate hate messages.

Respondents were asked about "the root cause of fake news and how to cope up with this," they said (33 media professionals) that the root cause of fake news is social media primarily and use of IT cells for political gains. They have also shared that media and political parties' nexus is equally responsible for it. Some of them also emphasized on the fact that sensational information gets more TRP so to summarized it they said that these are the main factors responsible for fake news: 1. Political gain; 2. Election results; 3. Polarization; 4. Ideological shift; 5. To seek mass attention; 6. Publicity etc.

Respondents (25 media professionals) were also asked to "share any other insights on Fake news, media, masses, and exposure of fake news," they said that fake news is the reality of the present time and we need to develop a mechanism to deal with it. Various suggestions were given, such as Media Literacy Programs should be introduced right from middle school level to create awareness among students about fake news; people should also put their efforts in verifying the information; though media houses do not disseminate fake news, however, they should apologize if they mistakenly broadcast any fake news; media houses should focus on ground reporting for collecting news; so that chance of receiving misleading information can be avoided.

Key points that emerged from the answers are:

(i) Media has their role and/or agenda in the dissemination of fake news said that there are several reasons for this, i.e., power game, TRP, lack of time to cross-check news due to pressure for breaking a news earlier than their competitors, and polarization for public opinion.

(ii) Methods of fact-checking: Google and Facebook conduct workshops for journalists regarding fact-checking; reverse image search; investigative method; checking with official sources, Government sources, Police and the particular Authority concerned with a news;

cross-checking with multiple sources; portals dedicated to exposing fake news and fact-checking; ground reports; check the sources and evidences, etc. Journalists should be trained to crosscheck any information and exposing fake news.

(iii) Fake news is responsible for changing public opinion or can disseminate polarized information which can lead to propaganda.

(iv) Social media, nexus between media and political parties, and the use of IT cell for political gains primarily contribute to spreading fake news.

(v) Media Literacy Programs should be introduced right from the middle school level to create awareness among students about fake news; people should also put their efforts in verifying the information; media houses should apologize if they mistakenly broadcast any fake news and they should focus on ground reporting for collecting news.

Conclusion

Media is very crucial for a democratic system and has an impact on the masses. Fake news is fabricated information that looks like news but created to change or create public opinion, however concept of fake news is not new. Fake news can be in the form of satire or parody; misleading content, imposter and fabricated content, and can have false connection/context, false/manipulated content, etc. People often encounter with fake news. It grabs the attention of the people and they tend to believe in it, therefore it is very effective in changing public opinion or creating a new narrative. Masses have a tendency of not verifying information and illiteracy is also one of the key contributing factors. Social Media and New Media are considered as two main sources of fake news.

Fake news is a sign of weak and/or weakening media. People, mostly, do not know how to cross-check the fact or fake news and hence the role of media and media professionals is important in spreading awareness about it. Social activists and journalists often try to expose fake news; however, more efforts are required to have gain confidence for their efforts. The study shows that fake news serves for political agenda, smokescreen, and ideological agenda setting. It is also believed that fake news is used for the religious agenda, election-related agenda.

Media has their role and/or agenda in the dissemination of fake news and there are several reasons for this, i.e., power game, TRP, lack of time to cross-check news due to pressure for breaking a news earlier than their competitors, and polarization for public opinion. Among the root causes of fake news includes lack of scientific temperament, illiteracy, and lack of will power to crosscheck and verify the news. It is believed that nexus of political parties and media, IT cells of the political parties serving as a new form of opinion leaders.

Interviews suggested various methods/tools of fact-checking: Google and Facebook conduct workshops for journalists regarding fact-checking; reverse image search; investigative method; checking with official sources, Government sources, Police and the particular Authority concerned with a news; cross-checking with multiple sources; portals dedicated to exposing fake news and fact-checking; ground reports; check the sources and pieces of evidence, etc.

The study also shows that journalists should be trained to crosscheck any information and exposing fake news. Media Literacy Programs should be introduced right from the middle school level to create awareness among students about fake news; people should also put their efforts in verifying the information; media houses should apologize if they mistakenly broadcast any fake news and they should focus on ground reporting for collecting news.

References

- *An animated introduction to Noam Chomsky's manufacturing consent and how the media creates the illusion of democracy*. (2017, March 13). Open Culture. https://www.openculture.com/2017/03/an-animated-introduction-to-noam-chomskys-manufacturing-consent.html

- The age of post-truth politics. (2016, November 22). Retrieved from http://www.thehindu.com/opinion/lead/The-age-of-post-truth-politics/article16672033.ece
- Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. doi:10.3386/w23089
- Bhaskaran, H., Mishra, H., & Nair, P. (2017). Contextualizing Fake News in Post-truth Era: Journalism Education in India. *Asia Pacific Media Educator, 27*(1), 41-50. doi:10.1177/1326365x17702277
- *Confronting the real problems of fake news and media backlash in the digital age*. (2017, July 12). The Hub. https://hub.jhu.edu/2017/07/12/combat-fake-news-media-literacy/

- *Cultivation theory*. (2015, March 27). Communication Theory. https://www.communicationtheory.org/cultivation-theory/

- Explained: What is Fake news? | Social Media and Filter Bubbles. (2017, November 27). Retrieved from https://www.webwise.ie/teachers/what-is-fake-news/
- Fake News and Social Media: A Deadly Combination. (2017, September 9). Retrieved from https://sabrangindia.in/article/fake-news-and-social-media-deadly-combination
- Fake news and the spread of misinformation - Journalist's Resource. (2017, September 27). Retrieved from

https://journalistsresource.org/studies/society/internet/fake-news-conspiracy-theories-journalism-research

- The Future of Truth and Misinformation Online. (2017, October 19). Retrieved from http://www.pewinternet.org/2017/10/19/the-future-of-truth-and-misinformation-online/
- The Future of Truth and Misinformation Online. (2017, October 19). Retrieved from http://www.pewinternet.org/2017/10/19/the-future-of-truth-and-misinformation-online/
- The growing tide of fake news in India. (2017, December 10). Retrieved from http://www.aljazeera.com/news/2017/12/growing-tide-fake-news-india-171210122732217.html
- Gecer, E. (2018). Media, Politics and Democracy: A Critical Perspective. *Journal of Erciyes Communication*. https://dergipark.org.tr/en/download/article-file/516432
- Lance Bennett, W. (2005). News as reality TV: Election coverage and the democratization of truth. *Critical Studies in Media Communication*, *22*(2), 171-177. https://doi.org/10.1080/07393180500093802
- Lăzăroiu, G. (2018). Post-truth and the Journalist's Ethos. *Post-Truth, Fake News*, 113-120. doi:10.1007/978-981-10-8013-5_9
- Modreanu, S. (2017). The Post-Truth Era? *Human and Social Studies*, *6*(3). doi:10.1515/hssr-2017-0021
- Post-truth India. (2017, November 8). Retrieved from http://www.epw.in/journal/2017/1/editorials/post-truth-india.html
- Romano, A. (2013). Politics and the Press in Indonesia: Understanding an Evolving Political Culture. London: Routledge
- Satell, G. (2014, January 18). If You Doubt That Social Media Has Changed the World, Take A Look at Ukraine. Retrieved from https://www.forbes.com/sites/gregsatell/2014/01/18/if-you-doubt-that-social-media-has-changed-the-world-take-a-look-at-ukraine/#1def2a44a2c7
- Tackling fake news. (2017, November 2). Retrieved from http://www.thehindu.com/opinion/op-ed/tackling-fake-news/article19963184.ece
- This feels right: 'Post-truth' is Oxford's Word of the Year. (2016, November 17). Retrieved from https://www.nbcnews.com/news/us-news/post-truth-oxford-dictionaries-word-year-2016-n685081

Article

Role of Community Radio in Enhancing the Basic Mathematical Skills of Citizens in India

Asia Pacific Media Educator
30(2) 211–233, 2020
© 2020 University of
Wollongong, Australia
Reprints and permissions:
in.sagepub.com/journals-permissions-india
DOI: 10.1177/1326365X20970431
journals.sagepub.com/home/ame
SAGE

Ravi K. Dhar[1], **Rashmi Sharma**[2]
and Neeru Johri[1]

Abstract

This study was carried out with the specific objectives of mapping the present level of mathematical skills of community members, and their radio listening behaviour preferences, with a view to making recommendations for the nature of radio programmes to be produced and broadcast among community members to enhance their numerical ability. To this end, the study employed quantitative research design, which involved the survey of a sample of 12,000 respondents taken from among the community members constituting the audience of the community radio stations in the country. The study employed multi-stage sampling to first identify 12 community radio stations, in the first instance, followed by the identification of one thousand households in each of these community radio stations and one respondent from each of the selected households, giving due consideration to the parity of gender. The data collected from each of these 12,000 respondents was processed with the help of descriptive statistical tools to arrive at inferences necessary to achieve the purposes of the study. The study revealed that while community members were comfortable in solving simple mathematical sums and calculating their wages, they experienced difficulties in the use of mathematical skills in the computation of interest, discount, percentage and conversion of scales of measurement. The study further revealed that community members listened to radio extensively and were eager to not just listen to radio programmes based on the imparting of mathematical skills but also willing to adopt a participatory approach in their production, based on their competencies.

[1] Department of Media and Communication Studies, Jagannath International Management School, Vasant Kunj, New Delhi, Delhi, India.
[2] Department of Science and Technology, Ministry of Science and Technology, Government of India, New Delhi, Delhi, India.

Corresponding author:
Ravi K. Dhar, Department of Media and Communication Studies, Jagannath International Management School, Vasant Kunj, New Delhi, Delhi 110019, India.
E-mail: ravikdhar@gmail.com

Keywords

Community radio, community empowerment, mathematical literacy, poverty alleviation, community media

Introduction

India's Human Development Index (HDI) value stood at 0.640 in 2017,[1] registering an increase of 49.8 per cent from 1990 to 2017. Though this placed the country in the medium human development category, occupying the 130th place among 189 countries in the world, it fell short of the average of 0.645 for countries in this category. Furthermore, what is of note is the precipitous fall in the HDI value, when it is adjusted for inequality in the country. The inequality-adjusted Human Development Index (IHDI) fell from 0.640 to 0.468, a loss of 26.8 per cent compared to 25.1 per cent for the countries in the medium human development category. This steep decline in the HDI was attributable to the inequality in the HDI dimension indices. With a human inequality coefficient of 26.3 per cent, the country had inequality in life expectancy at birth (21.4%), inequality in education (38.7%) and inequality in income (18.8%). In terms of gender differences, the Gender Development Index (GDI) for India stood at 0.841, compared to 0.878 for countries in the medium human development category, with female HDI at 0.575 and male HDI at 0.683. In contrast, the Gender Inequality Index (GII) for India stood at 0.524, compared to 0.489 for the countries in this category, placing it at number 127 out of 160 countries in the 2017 index.

Insofar as the sustainable development indicators are concerned,[2] India's performance did not differ much from that of its HDI. As per the Tendulkar Committee Report, 21.92 per cent of the Indian population lived below the poverty line in 2011–2012. The figure is a conservative estimate in view of the manner in which poverty was defined by the committee. According to the National Family Health Survey (NFHS-4), almost half of pregnant Indian women aged 15 and 49 were reported anaemic and more than one-third of women had a low body mass index. Among children aged below 5, 38.4 per cent had low height-for-age and 21 per cent had low weight-for-age, on account of malnutrition. As per the SDG India Index Baseline Report, 'Food security and nutrition pose a challenge in India because of a number of factors such as inadequate access to food, structural inequalities (gender, caste and social groups), lack of water and sanitation, micronutrient deficiencies and illiteracy'. In the parameter of health, the maternal mortality rate was 130 per 100,000 live births and for every 1,000 live births, 50 children aged under 5 die. Besides, the country reported 138 cases of tuberculosis per 100,000 people. As against this, there were only 221 government health workers for every 100,000 people. Besides, though India reported a literacy rate of 74 per cent, with male literacy pegged at 82.1 per cent and female literacy at 65.5 per cent,[3] the literacy rate by completed years of levels of education was not encouraging. As per Census 2011,[4] only 6.9 per cent of people aged 5 and above had a graduate degree and above, with 49.1 per cent of literates being concentrated in the category of people having studied up to upper primary school only.

Obviously, the divide between the haves and the have-nots is skewed unfavourably against the latter.

The model of development that India adopted in the aftermath of its independence was the top-down one, famous as the Nehru–Mahalanobis model. Though post liberalization, it underwent a change, but that did not impinge on the model as such. Liberalization only dismantled the command economy structure to liberate the impulse for free enterprise with a view to unleash the people's power to develop. But with so many inequalities to contend with, it only helped to further accentuate the fault lines of community development as is borne out by the statistics of sustainable development reported here. With the change in the government at the federal level and in most states, a new way of looking upon development began to emerge. This veered closer to the Gandhian model of Gram Swaraj, wherein the focus is on grassroots community development. For the first time in the history of independent India, the federal government started engaging directly with the public institutions at the bottom of the administrative pyramid, the Panchayati Raj institutions. This was made possible with the extensive use of the information and communication technologies which helped to connect the nation directly with the head of the government. The other initiative adopted to make this direct liaison between the highest echelons of the government and the community at the grassroots level possible was the radio. *Mann ki Baat* (radio programme hosted by the Prime Minister of India, Mr. Narendra Modi) became a constant fixture as did Internet-enabled social networking and video conferencing.

The government also turned attention towards the revitalization of the community radio as a medium of mainstreaming the community in the national development discourse. The initial impulse for community radio came from the Supreme Court judgement in 1995 which reiterated that the radio waves belonged to the people and the government was only a caretaker.[5] In the initial stage, granting of community radio license was restricted to reputed educational institutions only (Dutta & Ray, 2017–2018; Ediga, 2015). Though in 2006, the government allowed non-profit organizations to run community radio stations as a strong tool for community mobilization for empowerment, community radio could not make much of an impact in the country except in certain pockets because of the lack of an enabling and facilitating environment (Dutta & Ray, 2017–2018; Ediga, 2015). This changed with the swearing in of the new government in 2014, which seized it as an opportunity not only to mobilize support for its development agenda but also to involve the community and its institutions in the developmental initiatives.

As education is the key to community empowerment, the Department of Science & Technology of the Government of India conceived the Radio Mathematics Project for enhancing the mathematical skills of the people through community radio. It is pertinent to note here that successive annual status of education reviews has been critical of the mathematical and language skills competencies of school going children. The 13th Annual Status of Education Report[6] released in New Delhi on 15 January 2019 reported that the proportion of Standard V students who could read Standard II level texts had declined steadily since the high of 2008 till 2012 and had since been rising only marginally and that the proportion in 2018 was still below the 2008 level. The National Achievement Survey

2017[7] did not have a different story to tell. As the data on literacy and levels of completed education show that the bulk of the Indian population of ages 5 and above lies at the bottom of the educational pyramid, one can understand their inability to participate in the mainstream economy of the nation. As per the result of a survey on employment and unemployment conducted in 2011–2012 by National Sample Survey Office (NSSO) and Ministry of Statistics and Programme Implementation, the number of estimated employed persons in 2011–2012 on usual status basis was 474.1 million, of which 82.7 per cent of workforce (391.4 million persons) was in the unorganized sector.[8] With 30 million persons unemployed, 26 million officially underemployed, 40 million seeking additional work and 35 million looking for alternative modes of livelihood, the situation takes on a grim face. Uplifting these large numbers out of the morass of poverty can only be possible if they are given the right skills that can help them to earn livelihood.

Review of Literature

Most research studies on community radio regard it as an engine of equitable community development. One study examines how community radio contributes to community development by providing information about community services made available by the government (Dutta & Ray, 2012). Another study examines the role played by community radio in educating the nomads of Nigeria through the open distance learning mode (Ngwu, Ekwe, & Chukwuma, 2012). Similarly, another study explores the role played by community radio stations in community development, particularly rural and remote, in Bangladesh (Khan et al., 2017). A case study on Sadhana Community Radio beneficiary farmers was carried out in India with a view to map their listening behaviour vis-à-vis the programmes broadcast (Ratanparkhi et al., 2016). There has also been a study of the role that All India Radio, public broadcaster, has played, much before the advent of community radio, to overcome the literacy barrier among highly diversified audiences in the Indian subcontinent (Srivastava & Sekhar, 2017).

Some studies explore the challenges faced by community radio stations to ensure their sustainability and to serve the local communities (Dutta & Ray, 2017–2018; Muswede, 2009; Seth, 2013; Singh & Kumari, 2018). Similarly, one study examines the capability of community radio to address the issues of social change and development in Cuba (Bautista, 2018). Also, another study on community radio investigates the reasons for the slower growth of community radio in India in comparison with the phenomenal progress in countries such as Nepal, Thailand, Columbia and the Democratic Republic of Congo (Pavarala, 2013). Yet another study looks at the challenges faced by community radio in Western developed economies where community radio operates on the fringes as much of the public audience is engaged with the mainstream mass media (Cammaerts, 2009). One study examines the innovative practices followed by community radio stations in India (Dutta, 2014). Research has also focussed on the creation of a theoretical framework of value for community radio in terms of the benefits of participation and those of community listening (Order, 2013).

While studies have been carried out on the role played by community radio in community development, in general, and education, in particular, we could not come across studies that focussed on the use of community radio for teaching mathematical skills. It is in this context that the Radio Mathematics Project was conceived as an action research-based project with support from the Department of Science and Technology (DST) of Government of India. The project envisaged a baseline study, in the first instance, to explore the need for such a mediated intervention in community, followed by the broadcast of some 180 radio programmes to be broadcast among community members. The present study is based on the baseline survey carried out for this action-based research project.

Objectives of the Study

This study was carried out with the following specific objectives:

1. Mapping of the level of numerical ability of community members;
2. mapping of their radio listening behaviour preferences; and
3. making recommendations for the nature of radio mathematics interventions.

Research Design and Methods

The baseline study employed a multistage quantitative research design for achieving its objectives. In the first instance, it was important to identify the community radio stations which would form a part of the Radio Mathematics project. To this end, proposals were invited for participation in the project from all community radio stations throughout the country. Based on the need to have a diversified sample of community members, representative of the diverse social and economic conditions of the country, and the willingness of the community radio stations to participate in such a study, a sample of 12 community radio stations was selected. These were: Jagannath International Management School (JIMS) Vasant Kunj (VK), New Delhi, Kamalvani, Kolsiya, Rajasthan, Jnan Taranga, Krishna Kanta Handiqui State Open University, Guwahati, Assam, Vanya, Khalwa, Khandwa District, Madhya Pradesh, Popcorn, Bhopal, Madhya Pradesh, Alwar Ki Awaz, Alwar, Rajasthan, Vasundhara Vahini, Baramati, Pune District, Maharashtra, The Film and Television Institute of India (FTII), Pune, Maharashtra, Pasumai, Dindigul, Tamil Nadu, Jana Dhwani, Saragur, H. D. Kote Taluk, Mysore district, Karnataka, Active, Bengaluru, Karnataka, Periyar, Periyar Maniammai University, Thanjavur, Tamil Nadu.

Once, the community radio stations had been selected, it was important to select a sample of respondents from within the communities of each of these radio stations. In the first stage, the areas falling within the range of the air waves of each of the 12 community radio stations were identified. In the second stage, a sample of 1,000 households from each Community Radio (CR) was selected randomly, resulting in a total sample size of 12,000 households for all the 12 identified CRs. In the third stage, one respondent was chosen from each household and due care was taken to ensure that the number of respondents comprised of equal number of men and women and were aged above 18 years. The standardized questionnaire developed by Media4 Community Foundation after translation in the regional language of the station was administered to each of the 12,000 respondents forming the sample. The entire process of field survey, right from the stage of the identification of individual respondents to data collection and data processing, was done by the respective CRs. Each CR station identified teams comprising of community volunteers, CR staff and students in case of educational institutions and field supervisors. Data processing, was done on the day of data collection and the survey was completed in 3 to 4 days in each of the CR. Data were analysed using a pre-designed analysis framework.

Results and Discussion

Profile of the Respondents

Occupational Distribution

As is clear from Table 1, the sample distribution across various occupational categories in each of the 12 community radio stations was divergent. Only two community radio stations had substantial agriculture-based listener–respondent concentration. While CRs Jana Dhwani had 28.92 per cent listeners drawn from the agricultural community, Periyar had as high as 97.47 per cent listeners from agriculture. Another notable variation was the almost exclusive concentration of listeners in the unemployed category at Pasumai, which was a phenomenal 95.60 per cent. Similarly, CRs Vasundhara Vahini had 95.56 per cent of its listener respondents drawn from the skilled workers' category. The remaining nine CRs had their listening audience distributed over the non-agricultural categories. Among these, only three CRs had a considerable category of listener–respondents as students: CRs JIMS VK (22.11%), FTII (18.57%) and Popcorn (11.30%). While the listener–respondents of CRs Popcorn, JIMS VK and Kamalvani were distributed across any four to five non-agricultural occupational categories of skilled workers, homemakers, unskilled workers, self-employed and students, those of CRs Alwar, Jana Dhwani, Vanya and Active were concentrated in any two of the categories of skilled workers, homemakers and unskilled workers, and those of FTII and Jnan Taranga in any three of the categories of skilled workers, homemakers, students and private/government employment.

Monthly Household Income

As is clear from Table 2, 6 of the 12 CRs had more than 50 per cent of their respondents falling in the category of households earning less than ₹60,000 per annum, with 4 of these having more than a third of their respondents having no household income. Vanya had the highest concentration of respondents (91.45%) having annual household income below ₹60,000, followed by Kamalvani

Table 1. Occupational Distribution

CRs	Student	Agriculture	Petty Trader	Skilled Worker	Home Maker	Unskilled Worker	Pvt/Govt Employee	Unemployed	Self-Employed
Popcorn	11.30%	0.14%	0.14%	21.89%	22.46%	16.84%	9.45%	0.21%	16.63%
JIMS, VK	23.11%	0.00%	4.82%	12.68%	14.26%	16.52%	9.44%	1.38%	16.32%
Kamalvani	2.94%	0.20%	0.00%	43.68%	28.50%	7.93%	1.08%	0.20%	12.63%
Alwar Ki Awaz	4.93%	4.18%	0.19%	27.70%	8.74%	40.24%	4.00%	0.37%	9.20%
Jnan Taranga	5.57%	0.00%	0.00%	26.17%	39.55%	2.54%	16.60%	0.29%	7.52%
Janadhwani	1.37%	28.92%	0.20%	2.84%	9.22%	51.67%	1.37%	0.20%	3.04%
Vanya	5.67%	2.88%	0.00%	5.30%	37.55%	44.89%	0.84%	0.00%	1.77%
Periyar	0.00%	97.47%	0.00%	0.00%	0.54%	0.00%	0.00%	0.09%	1.44%
Active	2.26%	0.29%	0.00%	1.57%	14.43%	78.21%	0.98%	0.00%	1.37%
FTII	18.57%	0.00%	0.00%	51.93%	17.41%	2.80%	5.51%	0.10%	0.97%
Vasundhara Vahini	0.73%	0.00%	0.00%	95.56%	0.91%	1.00%	0.18%	0.00%	0.36%
Pasumai	0.00%	0.00%	0.00%	0.00%	0.47%	1.31%	0.00%	95.60%	0.00%

Source: Author’s own.

Table 2. Monthly Household Income

CRs	Not Earning	Below ₹5,000	₹5,000–10,000	₹10,000–20,000	₹20,000 and above
Alwar Ki Awaz	11.99%	30.86%	36.06%	15.99%	4.83%
FTII	37.14%	15.09%	25.24%	14.70%	7.06%
Janadhwani	3.14%	29.90%	50.88%	13.43%	2.06%
JIMS, VK	37.66%	10.42%	24.78%	19.37%	7.47%
Jnan Taranga	35.06%	17.77%	22.75%	17.58%	6.74%
Kamalvani	24.78%	58.86%	11.85%	3.53%	0.78%
Vanya	33.36%	58.09%	6.32%	1.21%	0.28%
Pasumai	0.47%	22.21%	71.23%	5.06%	0.56%
Popcorn	21.39%	24.02%	39.16%	13.57%	1.63%
Active	5.00%	51.42%	35.23%	7.36%	0.49%
Periyar	12.73%	63.27%	18.23%	3.61%	1.62%
Vasundhara Vahini	1.27%	0.63%	74.89%	21.12%	1.90%

Source: Author's own.

(83.64%), Periyar (76.00%), Active (56.42%), Jnan Taranga (52.83%) and FTII (52.23%). Five of the 12 CRs participating in the Baseline Survey for Radio Mathematics had more than 20 per cent of their respondents with an annual household income of₹120,000 and above. JIMS VK had the highest concentration of 26.84 per cent, followed by Jnan Taranga (24.32%), Vasundhara Vahini (23.02%), FTII (21.76%) and Alwar (20.82%). Only three of these CRs had more than 5 per cent of their respondents earning an annual household income of ₹240,000 and above. The variation in the structure of household income across the CRs points to the character of their listeners/communities. While CRs in the rural hinterland have poorer people, those in or near towns or cities tend to have better household incomes.

Level of Formal Education

As Table 3 shows, the respondents of only four CRs have more than 10 per cent of listeners with educational qualification beyond 12th class. CR with the highest concentration of graduates/postgraduates is Jnan Taranga (25.98%), followed by Popcorn (14.64%), FTII (13.54%) and Vasundhara Vahini (11.70%). On the other end of the spectrum are the respondents with no formal schooling. The situation here is abysmally pathetic. Vanya has the highest number of respondents (70.26%) with no formal schooling, followed by Jana Dhwani (60.49%), Kamalvani (45.54%) and Active (40.73%). The situation continues to be bleak when we add to the aforementioned category the number of respondents who have studied up to 5th class. More than 50 per cent of the respondents in eight CRs fall in the two categories of no formal schooling and have not studied beyond 5th class. Vanya has the highest concentration of respondents (90.80%) in the lowest two categories, followed by Jana Dhwani (86.08%), Kamalvani (77.76%), Pasumai (77.31%), Alwar Ki Awaz (73.33%), Active (67.02%), Periyar (55.69%) and JIMS VK (53.60%). The high percentage of such scantily educated respondents calls for strong non-formal inputs of all kinds of literacy, be it verbal or mathematical.

Table 3. Level of Formal Education

CRs	No Formal Education	Up to 5th	Up to 8th	Up to 10th	Up to 12th	Graduate/ Postgraduate
Alwar Ki Awaz	29.28%	44.05%	1.30%	2.79%	14.87%	7.71%
FTII	12.77%	26.01%	7.74%	17.50%	22.44%	13.54%
Janadhwani	60.49%	25.59%	0.20%	10.10%	2.35%	1.27%
JIMS, VK	20.85%	32.75%	20.35%	0.88%	17.21%	7.96%
Jnan Taranga	6.54%	28.61%	2.05%	0.00%	36.82%	25.98%
Kamalvani	45.54%	32.22%	1.67%	0.59%	12.93%	7.05%
Vanya	70.26%	20.54%	2.04%	1.49%	3.90%	1.77%
Pasumai	17.62%	59.69%	0.09%	13.50%	6.19%	2.91%
Popcorn	22.03%	19.19%	4.48%	19.26%	20.40%	14.64%
Active	40.73%	26.29%	0.88%	13.94%	16.00%	2.16%
Periyar	24.64%	31.05%	0.45%	13.81%	22.56%	7.49%
Vasundhara Vahini	4.44%	25.47%	1.45%	13.78%	43.16%	11.70%

Source: Author's own.

The analysis of the sample profile across the 12 community radio stations reveals that there is a heavy preponderance of illiterate population who are caught up in the vortex of poverty on account of being involved in no or unskilled occupations. Reaching out to this segment of population to uplift them from the vicious cycle of poverty through educational broadcasts such as those on everyday Mathematics can ameliorate their lot.

Mapping of Mathematical Ability

This section presents the findings of the survey regarding the frequency of use of mathematics and the comfort and competence level of the respondents in meeting the challenge of using everyday mathematics in the course of transacting the business of life.

Table 4. Use of Simple Mathematical Calculations for Various Purposes

CRs	Rarely	Sometimes	Quite Often	Very Much
Alwar Ki Awaz	6%	33%	27%	34%
FTII	30%	28%	29%	13%
Jnan Taranga	18%	41%	16%	25%
Kamalvani	33%	33%	23%	11%
Pasumai	25%	22%	34%	19%
Periyar	47%	35%	13%	5%
JIMS, VK	14%	33%	28%	25%
Popcorn	34%	29%	29%	8%
Vanya	23%	73%	4%	0%
Vasundhara Vahini	1%	11%	27%	61%
Active	0%	2%	54%	44%
Janadhwani	31%	34%	23%	12%

Source: Author's own.

Use of Simple Mathematical Calculations for Various Purposes

When the respondents across the 12 CRs were asked about the frequency with which they used simple mathematics and calculations in their everyday life, they came up with interesting responses. Table 4 shows that more than a half of the respondents in 7 of the 12 CRs felt that they used simple mathematics either rarely or only sometimes in their daily life. Vanya had the highest concentration of such respondents (96%), followed by Periyar (82%), Kamalvani (66%), Jana Dhwani (65%), Popcorn (63%), Jnan Taranga (59%) and FTII (58%). In contrast, more than 50 per cent of the respondents in 5 of the 12 CRs felt that they used simple mathematics and calculations quite often and very much in their daily life. Obviously, those in the grip of poverty do not even realize how much mathematics finds application in their everyday life. Hence, these people need not only mathematical inputs but also a reorientation of their perception to the ways in which mathematics impinges their lives.

Level of Ease in Everyday Calculation

As shown in Table 5, more than 70 per cent of the respondents in only six CRs felt that they could manage to solve simple mathematical problems on their own. Vasundhara had the highest concentration of respondents (86%) with the confidence that they could solve mathematical problems easily without any help, followed by FTII (79%), Alwar Ki Awaz (77%), Jnan Taranga (72%) and Periyar and Active (70% each). The other CRs had a considerable section of respondents who either needed someone else's help fully or at times. More than 30 per cent of the respondents in eight CRs felt that they needed help with even simple calculations. Vanya had the highest concentration of such respondents (88%), followed by Kamalvani (56%), JIMS, VK (48%), Jana Dhwani (46%), Periyar (41%), Popcorn (39%, Pasumai and Active (30% each).

Level of Ease and Competence in Solving Simple Addition- and Subtraction-based Problems

A set of simple Maths questions in order of increasing degree of difficulty was asked to the respondents in order to understand their level of ease and competence in solving them. Table 6 shows that subtraction posed a bigger challenge than addition to the respondents. Most of the respondents returned correct answers to the addition problems, with very few reporting errors in their calculations. The percentage of incorrect additions ranged from 2 to 9 for most of the CRs, with the exception of Vanya which recorded 15 per cent incorrect answers. In stark contrast, the percentage of incorrect answers reported in the case of subtraction questions ranged from 5 to 45, with Alwar ki Awaz reporting the highest percentage of incorrect answers (45), followed by Popcorn and Jana Dhwani (36 each), JIMS VK (35), Pasumai (28), Periyar (26), Kamalvani (25), FTII (21), Vasundhara Vahini (13), Jnan Taranga (7), Active (6) and Vanya (5).

Level of Ease and Competence in Solving Application-Based Multiplication Problems

Table 7 shows that when the respondents were asked questions with regard to the calculation of wages, fare, time and work, most of the respondents in each of the CRs replied correctly, though in the case of certain CRs, the results were not very

Table 5. Level of Ease in Everyday Calculation

CRs	Depend on Others	Manage with Little Help from Others	Manage on My Own
Alwar Ki Awaz	6%	17%	77%
FTII	4%	17%	79%
Jnan Taranga	4%	24%	72%
Kamalvani	10%	46%	44%
Pasumai	11%	19%	70%
Periyar	7%	34%	59%
JIMS, VK	9%	39%	52%
Popcorn	9%	30%	61%
Vanya	19%	69%	12%
Vasundhara Vahini	4%	10%	86%
Active	8%	22%	70%
Janadhwani	18%	28%	54%

Source: Author's own.

Table 6. Level of Ease and Competence in Solving Simple Addition and Subtraction-based Problems

	Addition		Subtraction	
CRs	Right	Wrong	Right	Wrong
Alwar Ki Awaz	95%	5%	55%	45%
FTII	98%	2%	79%	21%
Jnan Taranga	98%	2%	93%	7%
Kamalvani	94%	6%	75%	25%
Pasumai	96%	4%	72%	28%
Periyar	91%	9%	74%	26%
JIMS, VK	94%	6%	65%	35%
Popcorn	96%	4%	64%	36%
Vanya	85%	15%	95%	5%
Vasundhara Vahini	99%	1%	87%	13%
Active	99%	1%	94%	6%
Janadhwani	94%	6%	64%	36%

Source: Author's own.

Table 7. Level of Ease and Competence in Solving Application-based Multiplication Problems

	Calculation of Wages		Calculation of Fare		Calculation of Time and Work	
CRs	Right	Wrong	Right	Wrong	Right	Wrong
Alwar Ki Awaz	71%	29%	76%	24%	77%	23%
FTII	86%	14%	93%	7%	93%	7%
Jnan Taranga	89%	11%	93%	7%	93%	7%
Kamalvani	80%	20%	85%	15%	85%	15%
Pasumai	80%	20%	82%	18%	80%	20%

(Table 7 continued)

(Table 7 continued)

	Calculation of Wages		Calculation of Fare		Calculation of Time and Work	
CRs	Right	Wrong	Right	Wrong	Right	Wrong
Periyar	83%	17%	84%	16%	84%	16%
JIMS, VK	64%	36%	82%	18%	85%	15%
Popcorn	60%	40%	76%	34%	73%	27%
Vanya	86%	14%	58%	42%	55%	45%
Vasundhara Vahini	83%	17%	91%	9%	90%	10%
Active	92%	8%	97%	3%	94%	6%
Janadhwani	55%	45%	73%	27%	77%	23%

Source: Author's own.

encouraging. In regard to the question on calculation of wages, which was 'If the daily wage of a person is 130 rupees, how much does he earn in eight days?', only 3 stations recorded more than one-third incorrect answers. These were: Jana Dhwani (45%), followed by Popcorn (40%) and JIMS VK (36%). With regard to calculation of fare, which was 'If a person spends 50 rupees a day on auto fare, how much does he spend in 6 days?' respondents in only 2 CRs recorded more than one-third incorrect answers. These were: CR Vanya (42%), followed by Popcorn (34%). In the case of questions on time and work, which was 'If a woman stitches three dresses in a day, how many can she stitch in four days?', the respondents of only one CR, Vanya, recorded more than one-third incorrect answers, which was 45 per cent.

Calculation of Percentage, Discount and Interest

In sharp contrast with the responses to the questions discussed in the previous section, Table 8 presents the responses of the respondents to the questions involving calculation of percentage, discount and interest, which were incorrect in an

Table 8. Calculation of Percentage, Calculation of Discount and Calculation of Interest

	Calculation of Percentage		Calculation of Discount		Calculation of Interest	
CRs	Right	Wrong	Right	Wrong	Right	Wrong
Alwar Ki Awaz	23%	77%	76%	24%	29%	71%
FTII	56%	44%	44%	56%	63%	37%
Jnan Taranga	51%	49%	61%	39%	60%	40%
Kamalvani	56%	44%	57%	43%	46%	54%
Pasumai	60%	40%	55%	45%	62%	38%
Periyar	61%	39%	39%	61%	50%	50%
JIMS, VK	20%	80%	23%	77%	22%	78%
Popcorn	25%	75%	21%	79%	22%	78%
Vanya	32%	68%	29%	71%	28%	72%
Vasundhara Vahini	57%	43%	56%	44%	56%	44%
Active	80%	20%	79%	21%	82%	18%
Janadhwani	91%	9%	90%	10%	79%	21%

Source: Author's own.

overwhelmingly large number of cases. With the exception of Jana Dhwani, where the incorrect responses recorded to the question on calculation of percentage was of the order of 9 per cent, the incorrect responses recorded in CRs JIMS VK were the highest (80%) followed by Alwar Ki Awaz (77%) Popcorn (75%), Vanya (68%), Jnan Taranga (49%), FTII and Kamalvani (44% each), Vasundhara Vahini (43%), Pasumai (40%), Periyar (39%) and Active (20%). Respondents in five CRs came up with more than 50 per cent incorrect responses to questions on calculation of discount. While the highest percentage was recorded by Radio Popcorn (79%), it was followed by Radio JIMS (77%), Vanya (71%), Periyar (61%) and FTII (56%). Similarly, when it came to calculating interest, either half or more than half of the respondents in six CRs could not give a correct answer. These were CRs: JIMS VK and Popcorn (78% each), Vanya (72%), Alwar Ki Awaz (71%), Kamalvani (54%) and Periyar (50%). The inability of a large section of respondents across all the CRs to solve mathematical problems with slight complexity drives home the need for improving the mathematical literacy of the people in these areas.

Conversion from Foot to Inches and Time Conversion

The other everyday mathematical problems on which the respondents' mathematical competence was tested were conversions of units of distance and time. The inaccurate responses to the conversion of the units of measuring distance ranged from 41 per cent recorded in CRs Popcorn to 13 per cent in Active, with four stations registering more than one-third inaccurate answers. These were: Alwar ki Awaz (38%), Periyar (34%) and JIMS VK (33%), other than Popcorn. For conversion of time from a 24-h format to a 12-h format, the highest percentage of respondents who were not able to give the right answer was seen in CRs Periyar (47%) and lowest in Active (10%), as shown in Table 9.

The observation of the method employed by the respondents to solve the questions showed that despite possessing a pen/pencil or a calculator (on their phones), they did not know how to apply a method or the logic behind the

Table 9. Conversion from Foot to Inches and Time Conversion

	Conversion from Feet to Inches		Time Conversion	
CRs	Right	Wrong	Right	Wrong
Alwar Ki Awaz	62%	38%	55%	45%
FTII	75%	25%	83%	17%
Jnan Taranga	78%	22%	72%	28%
Kamalvani	70%	30%	71%	29%
Pasumai	83%	17%	74%	26%
Periyar	66%	34%	53%	47%
JIMS, VK	67%	33%	77%	23%
Popcorn	59%	41%	71%	29%
Vanya	72%	28%	77%	23%
Vasundhara Vahini	84%	16%	85%	15%
Active	87%	13%	90%	10%
Janadhwani	73%	27%	80%	20%

Source: Author's own.

calculation. Clearly, the mathematical skills of the respondents were too inadequate to help them confront everyday situations involving the use of basic mathematical knowledge.

Feeling of Being Cheated Because of Low Mathematical Ability

Often, the awareness of their own lack of knowledge comes to the surface when one feels cheated or exploited as a result of not being able to calculate correctly. Hence, the question to the respondents was whether they had felt cheated at any time. This awareness also often fuels the need to learn.

The analysis as per Table 10 shows that an overwhelming percentage, more than 60 per cent, of respondents in 7 of the 12 community radio stations admitted that they had felt cheated at one time or the other because of their inability to calculate correctly. A majority of them cited 'during shopping or purchasing' as the time when they had 'felt cheated'. The problems faced at the time of shopping included inability to calculate big amounts, getting the wrong amount of change from shopkeepers or giving extra money to them by mistake. Some also mentioned being cheated by employers. Being cheated or exploited, as the respondents admitted, was not just about money and calculation. It carried with it an underlying emotion of 'feeling ashamed' and 'feeling bad' due to the inability to calculate correctly.

The mapping of mathematical skills among the listening audiences of the 12 community radio stations shows that their basic numerical ability is far from desirable from the point of its requirement for everyday personal and professional purposes. Besides, the survey reveals that many of them also feel embarrassed about their inability to cope up with situations that call for these skills. Hence, there is a strong need to bolster their skills and also their confidence so that their participation in the national economy may be mainstreamed. In view of the extensive reach of the mass media, it could be employed for the purpose.

Table 10. Feeling of Being Cheated Because of Low Mathematical Ability

CRs	YES	NO
Alwar Ki Awaz	10%	90%
FTII	87%	13%
Jnan Taranga	20%	80%
Kamalvani	16%	84%
Pasumai	14%	86%
Periyar	20%	80%
JIMS, VK	31%	69%
Radio Popcorn	33%	67%
Vanya	84%	16%
Vasundhara Vahini	89%	11%
Active	80%	20%
Janadhwani	91%	9%

Source: Author's own.

Mapping of Radio Listening Behaviour

As radio has the highest penetration and the maximum reach, it is one of the most suitable mass media for reaching out to such audiences. Besides, as it has easy access both by way of cheap radio sets and/or mobile phone app, it is appropriate for delivering messages to audiences from economically weaker sections. However, with a view to assessing the suitability of the medium for making mediated educational interventions for these audiences, the survey sought responses to map their radio listening behaviour.

Radio Listenership

Table 11 shows that from among the sample of respondents, those who listened to radio programmes in each of the 12 CRs ranged from 59.45 per cent in the case of Kamalvani to 99.91 per cent in the case of Vasundhara Vahini. With such high listenership percentage figure, CRs could squeeze in and gain the attention of the communities for the purposes of delivering their specific messages to them.

Location of Listening to Radio

The place(s) where the listeners access the radio programmes is important insofar as it indicates the level of engagement/attention the radio programme is able to command from its listeners. The survey revealed that across all community radio stations, as shown in Table 12, the respondents preferred to listen to radio at home instead of any other location. The only exception was Pasumai where 73.66 per cent of the respondents reported listening to radio while at work. The listenership of radio stations at home ranged from 51.95 per cent in the case of Popcorn to 87.64 per cent in the case of Vanya.

Time of Listening to Radio

Table 13 shows that the popularity of time slots varied from one CR to another. The three main time slots that listeners preferred in CRs, Alwar Ki Awaz were 0600 to

Table 11. Radio Listenership

	Radio Listenership	
CRs	Yes	No
Alwar Ki Awaz	77.97%	22.03%
FTII	78.34%	21.57%
Janadhwani	68.43%	31.57%
JIMS, VK	83.58%	16.22%
Jnan Taranga	91.60%	8.30%
Kamalvani	59.45%	40.45%
Vanya	99.26%	0.74%
Pasumai	99.81%	0.19%
Popcorn	65.81%	34.12%
Active	91.17%	8.73%
Periyar	94.40%	5.60%
Vasundhara Vahini	99.91%	0.09%

Source: Author’s own.

Table 12. Location of Listening to Radio

	Location of listening to radio						
CRs	At Home	At Work	Group Listening	While Driving	Neighbor's House	On the Farm	Other
Alwar Ki Awaz	63.38%	10.59%	0.65%	2.42%	0.56%	0.37%	21.84%
FTII	58.32%	15.18%	0.29%	3.58%	0.39%	0.00%	21.47%
Janadhwani	58.43%	7.65%	0.49%	0.49%	0.98%	0.39%	31.47%
JIMS, VK	62.05%	11.31%	1.38%	7.67%	0.69%	0.79%	15.63%
Jnan Taranga	83.11%	4.30%	0.20%	2.93%	0.29%	0.78%	8.20%
Kamalvani	54.36%	1.96%	0.88%	0.49%	0.59%	0.98%	40.16%
Vanya	87.64%	1.02%	1.67%	0.19%	4.74%	3.25%	0.74%
Pasumai	23.43%	73.66%	0.75%	0.47%	0.66%	0.47%	0.19%
Popcorn	51.95%	8.10%	0.36%	2.77%	0.43%	2.20%	33.97%
Active	84.49%	4.42%	0.10%	0.49%	1.57%	0.00%	8.73%
Periyar	68.68%	17.33%	0.81%	3.16%	0.81%	3.61%	5.51%
Vasundhara Vahini	64.91%	33.45%	0.27%	0.63%	0.00%	0.09%	0.09%

Source: Author's own.

Table 13. Time of Listening to Radio

CRs	6.00 to 8.00 AM	8.00 to 10.00 AM	10.00 AM to 12.00 NOON	12.00 to 2.00 PM	2.00 to 4.00 PM	6.00 to 8.00 PM	After 8.00 PM	4.00 to 6.00 PM	Not Interested
Alwar Ki Awaz	10.69%	8.36%	1.39%	5.30%	4.46%	5.20%	24.26%	17.66%	21.75%
FTII	12.96%	11.12%	3.97%	10.74%	20.21%	3.97%	6.67%	8.32%	21.47%
Janadhwani	10.49%	6.08%	1.37%	2.75%	7.16%	22.45%	13.04%	4.41%	31.37%
JIMS, VK	15.73%	8.06%	6.10%	9.93%	11.41%	15.83%	7.18%	9.05%	15.93%
Jnan Taranga	28.71%	4.69%	11.82%	8.59%	7.62%	14.06%	7.71%	7.91%	8.20%
Kamalvani	9.11%	6.95%	2.74%	17.43%	14.79%	4.90%	0.88%	2.25%	39.96%
Vanya	56.04%	17.84%	0.65%	1.67%	0.93%	18.59%	2.42%	1.02%	0.74%
Pasumai	23.15%	32.43%	13.31%	9.56%	12.56%	2.91%	0.19%	5.25%	0.19%
Popcorn	5.19%	5.05%	5.54%	10.45%	17.13%	9.24%	7.25%	5.61%	33.90%
Active	3.53%	3.83%	1.96%	3.34%	72.72%	1.47%	0.49%	3.04%	8.73%
Periyar	21.12%	8.03%	3.70%	6.41%	6.23%	38.00%	0.00%	10.56%	5.51%
Vasundhara Vahini	30.37%	22.94%	7.07%	5.89%	8.34%	18.31%	3.72%	2.81%	0.09%

Source: Author’s own.

0800 h (10.69%), 1600 to 1800 hours (17.66%) and after 2000 hours (24.26%), in FTII were 0600 to 0800 hours (12.96%), 1200 to 1400 hours (10.74%) and 1400 to 1600 hours (20.21%), in Jana Dhwani 1800 to 2000 hours (22.45%), after 2000 hours (13.04%) and 0600 to 0800 hours (10.49%), in JIMS VK 0600 to 0800 hours (15.73%), 1400 to 1600 hours (11.41%)and 1800 to 2000 hours (15.83%, in Jnan Taranga 0600 to 0800 hours (28.71%), 1000 to 1200 hours (11.82%) and 1800 to 2000 hours (14.06%), in Kamalvani 0600 to 0800 hours (9.11%), 1200 to 1400 hours (17.43%) and 1400 to 1600 hours (14.79%), in Vanya 0600 to 0800 hours (56.04%), 0800 to 1000 hours (17.84%) and 1800 to 2000 hours (18.59), in Pasumai 0600 to 0800 hours (23.15%), 0800 to 1000 hours (32.43%) and 1000 to 1200 hours (13.31%), in Popcorn 1200 to 1400 hours (10.45%), 1400 to 1600 hours (17.13%) and 1800 to 2000 hours (9.24%), in Periyar 0600 to 0800 hours (21.12%), 1600 to 1800 hours (38.00%) and 1800 to 2000 hours (10.56%) and in Vasundhara Vahini 0600 to 0800 hours (30.37%), 0800 to 1000 hours (22.94%) and 1800 to 2000 hours (18.31), with the exception of Active where an overwhelming percentage of respondents (72.72) preferred 1400 to 1600 hours' time slot.

Instruments Used for Listening to Radio Programmes

Table 14 shows the instruments used for listening to radio programmes. Listeners in five community radio stations preferred to listen to radio programmes on traditional radio sets. Listeners in Kamalvani (61%), Pasumai (96%), Periyar (78%), Vanya (88%) and Vasundhara Vahini (74%) used traditional radio sets to listen to radio programmes. Listeners in seven other community radio stations preferred to listen to radio programmes on mobile phones. On the whole, the listeners are almost evenly divided between the uses of the two kinds of instruments, pointing to the inroads being made gradually by the new communication technology of mobile phones into their lives.

Perception of the Usefulness of Radio Mathematics

When asked if they felt it would be helpful for them to listen to the broadcast of Radio Mathematics programme, the response was overwhelmingly positive, as shown in Table 15. Their affirmative responses ranged from the high of 100 per cent in CRs Vanya to the low of 77 per cent in Pasumai and Active. With such clear enunciation of the need for an intervention like Radio Mathematics, it stood to reason that the project be launched in all the 12 community radio stations.

Listeners' Willingness to Participate in Radio Maths Programmes

Table 16 shows the listeners' willingness to participate in Radio Maths Programmes. When asked if they would be interested in participating in the production of Radio Mathematics programmes, the respondents in the 12 community radio station areas were divided in their readiness to do so. More than one-third of the respondents in 6 of the 12 CRs were hesitant in participating in programme production, while an overwhelming number of respondents in the other six CRs were keen to participate in the production effort. Among those who were willing to participate in programme production, a majority of the listeners in eight CRs were comfortable with only phoning in their questions to CRs. Again, while respondents in FTII (45.26%) were keen to participate in discussion-based programmes, respondents in Vanya (52.29%)

Table 14. Instruments Used for Listening to Radio Programs

	Gadget on Which Radio is Listened to	
CRs	Radio Set	Mobile Phone
Alwar Ki Awaz	47%	51%
FTII	33%	62%
Jnan Taranga	37%	58%
Kamalvani	61%	35%
Pasumai	96%	3%
Periyar	78%	12%
JIMS, VK	14%	42%
Radio Popcorn	48%	49%
Vanya	88%	5%
Vasundhara Vahini	74%	26%
Active	34%	65%
Janadhwani	46%	52%

Source: Author's own.

Table 15. Perception of the Usefulness of Radio Mathematics

	Would Radio Mathematics be Helpful?	
CRs	Yes	No
Alwar Ki Awaz	88%	12%
FTII	96%	4%
Jnan Taranga	95%	5%
Kamalvani	78%	22%
Pasumai	77%	23%
Periyar	90%	10%
JIMS, VK	93%	7%
Radio Popcorn	79%	21%
Vanya	100%	0%
Vasundhara Vahini	99%	1%
Active	89%	11%
Janadhwani	77%	23%

Source: Author's own.

were willing to participate in drama-based programmes. Interestingly enough, there were no takers for scriptwriting in any of the 12 CRs.

The preceding discussion yields the following findings:

1. While assessing the level of awareness of community members in regard to the use of simple mathematical problems in their daily lives, it was surprisingly found that most of them had a very low level of awareness.
2. While analysing the level of ease experienced by the community members in solving everyday mathematical problems, it was found that respondents in other CRs did not face major issues while solving problems related to simple addition. However, they experienced significant level of difficulty

Table 16. Listeners' Willingness to Participate in Radio Mathematics Programs

	Yes					
CRs	Phone In	Script Writing	Discussions	Drama	No	No Response
Alwar Ki Awaz	60.97%	1.77%	15.61%	1.02%	19.70%	0.93%
FTII	26.79%	3.97%	45.26%	8.51%	13.93%	1.55%
Janadhwani	39.51%	1.57%	6.67%	4.90%	46.86%	0.49%
JIMS, VK	21.04%	3.74%	21.83%	6.49%	46.51%	0.39%
Jnan Taranga	20.41%	2.34%	10.25%	12.21%	53.91%	0.98%
Kamalvani	43.78%	1.27%	8.42%	3.43%	42.02%	1.08%
Vanya	30.22%	2.47%	6.59%	52.29%	7.88%	0.55%
Pasumai	50.80%	7.69%	4.40%	1.12%	34.11%	1.87%
Popcorn	45.44%	4.22%	15.01%	5.99%	28.56%	0.79%
Active	47.11%	0.79%	23.95%	15.80%	11.68%	0.69%
Periyar	45.31%	2.26%	14.08%	1.17%	36.46%	0.72%
Vasundhara Vahini	67.09%	4.26%	15.32%	4.90%	7.71%	0.73%

Source: Author's own.

in solving problems related to subtraction. Similarly, community members, with the exception of those in one CR, did not face much difficulty in solving mathematical problems involving multiplication in regard to the calculation of wages, fare and time and work. In sharp contrast, community members in overwhelming numbers faced problems in using mathematical skills to calculate percentage, discount, interest and conversions of scales such as from foot to inches. In such situations, they got stuck and looked for support.

3. Majority of the community members reported that they had felt cheated at one time or another because of their inability to calculate correctly. They also reported that they felt robbed not only of their money but also of their self-esteem in such situations.
4. The study also shows that more than 60 per cent of community members listened to radio programmes. In regard to the location where they preferred to listen to these programmes, they expressed a preference for their homes. However, in regard to the preferred listening time, with the exception of three community radios, the community members in other CRs preferred either afternoon or late evening. In respect of the instruments on which the community members preferred to listen to radio broadcasts, the study revealed that the community members were almost evenly divided, with community members in five stations preferring traditional radio sets and those in the others the mobile handsets.
5. Regarding the perceived usefulness of listening to mathematics-based radio programmes, an overwhelming percentage of community members showed their desire to do so. However, when asked if they would be interested in participating in the production of such programmes, the response received was a mixed one, with more than one-third of the community members hesitant in doing so in six of the CRs in contrast to an overwhelming percentage of community members in the other CRs keen to do so. Most of the community members who were inclined to participating in the production of the programmes were comfortable with phone-ins only, while a few were willing participate in discussion-based programmes.

Conclusions and Recommendations

The results of the baseline survey clearly show that there is an urgent need to make a mediated intervention in shoring up the competence and the confidence of marginalized communities with respect to their everyday numerical ability. Besides, the survey reveals that across all community radio stations spread across the various regions of India, community members continue to rely on radio as their mediated point of contact with the wide world not just for information but also for learning and entertainment. Delivering inputs of everyday numerical ability through radio could be much useful. Furthermore, as community radio stations operate in a niche space with greater interface between producers and consumers of information involving the participation of the community not simply as listeners but also as producers of information, production and broadcasting of radio programmes on everyday numerical ability could be much useful and desirable.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The authors received no financial support for the research, authorship and/or publication of this article.

ORCID iD

Ravi K. Dhar https://orcid.org/0000-0003-0127-3871

Notes

1. The figures related to India's Human Development have been taken from the UNDP report 'Human Development Indices and Indicators: 2018 Statistical Update'. http://hdr.undp.org/en/countries/profiles/IND
2. SDG India Index Baseline Report, 2018. https://in.one.un.org/wp-content/uploads/2018/12/SDX-Index-India-21-12-2018.pdf
3. Status of Literacy. http://censusindia.gov.in/2011-prov-results/data_files/mp/07 Literacy.pdf
4. Chapter 3: Literacy and Education. http://www.mospi.gov.in/sites/default/files/reports_and_publication/statistical_publication/social_statistics/Chapter_3.pdf
5. https://mib.gov.in/document/supreme-court-judgement-airwaves
6. http://www.asercentre.org/Keywords/p/346.html
7. http://www.ncert.nic.in/programmes/NAS/SRC.html
8. Dattatreya, *Workforce in organised/unorganised sector*. This information was provided by Shri Bandaru Dattatreya, the Minister of State (IC) for the Ministry of Labour and Employment in reply to a question in Lok Sabha on 25 July 2016.

References

Cammaerts, B. (2009). Community radio in the West—A legacy of struggle for survival in a state and capitalist controlled media environment. *International Communication Gazette, 71*(8), 635–654.

Bautista, L. A. de la N. (2018). Community radio depending on development. *Estudios del Desarrollo: Social: Cuba y America Latina, 6*(2), 31–37.

Dattatreya, S. B. *Workforce in organised/unorganised sector*. Press Information Bureau Government of India. http://pib.nic.in/newsite/PrintRelease.aspx?relid=147634

Dutta, A. (2014). *Innovations in community radio: With special reference to India*. Ministry of Information & Broadcasting, Govt of India. http://mib.nic.in

Dutta, A., & Ray, A. (2012). A laudable community radio initiative. *Vidura, 4*(2), 20–21.

———. (2017–2018). Journey ahead towards a robust community radio sector in India: Perspectives on challenges & elucidations. *Prajna: Annual Journal of Gauhati University Teachers' Association, XXVII*, 14–28.

Ediga, S. (2015). *Government procedure is the biggest hurdle in the growth of community radio in India*. https://factly.in/community-radio-in-india-government-procedure-is-the-biggest-hurdle-in-the-growth/

Khan, M. A. A., Khan, M. M. R., Hassan, M., Ahmed, F., & Haque, S. M. R. (2017). Role of community radio for community development in Bangladesh. *The International Technology Management Review, 6*(3), 94–102.

Muswede, T. (2009). *Sustainability challenges facing community radio: A comparative study of three community radio stations in Limpopo Province*. http://ulspace.ul.ac.za/bitstream/handle/10386/231/MATRIL%20T%20Moswede.pdf?sequence=1

Ngwu, C. C., Ekwe, O., & Chukwuma, O. (2012, July). Community radio and nomadic education in Northern Nigeria: The Jigawa state experience. *Cameroon Journal of Studies in the Commonwealth*, pp. 1–18. https://www.researchgate.net/publication/325763096

Order, S. (2013). The Altruism of community radio? *Asia Pacific Media Educator, 23*(2), 381–401.

Pavarala, V. (2013). *Ten years of community radio in India: Towards new solidarities*. https://www.researchgate.net/publication/259501203

Ratanparkhi, H. H., Chinchmalatpure, U., & Katole, R. T. (2016). Listening behaviour of sadhana community radio beneficiary farmers. *Journal of Global Communication*, *Special Issue*, 100–109.

Seth, A. Community radio movement in India. https://gramvaani.org/wp-content/uploads/2013/05/community-radio-indian-history.pdf

Singh, P., & Kumari, N. (2018, October–December). Challenge before community radio stations in India: A study of two community radio stations of Jharkhand. *Media Mimansa*, 2–12. https://www.researchgate.net/publication/334389333

Srivastava, M. K., & Sekhar, P. C. (2017). *Innovations in educational broadcasts by All India Radio*. Conference Paper. https://www.researchgate.net/publication/316700981

Authors’ bio-sketches

Ravi K. Dhar is the Director of Jagannath International Management School (JIMS), Vasant Kunj, New Delhi, India. He has published an edited book, *Media in the Swirl* (2012), apart from research papers in the area of communication rights and new media.

Rashmi Sharma is a Science Communicator, working in the Department of Science & Technology, Government of India. She has published a number of papers and articles for the popularization of science in India.

Neeru Johri is Professor and Head, Department of Media and Communication Studies, JIMS, Vasant Kunj, New Delhi, India. She has worked extensively in the tribal belt of Jharkhand, India, in the area of public health and gender empowerment.