



## Cloud Computing Challenges and Concerts in VM Migration Technology

<sup>1</sup>Dr.S.Prem Kumar, <sup>2</sup>CH. Lakshmi Veenadhari and <sup>3</sup>I.Kali Pradeep

<sup>1</sup>Professor, Dept. of CSE, G. Pullaiah College of Engineering and Technology Kurnool

<sup>2</sup>Assistant Professor, Dept of CSE, Shri Vishnu College of Engineering, Bhimavaram

<sup>3</sup>Assistant Professor, Dept of CSE, S.V. College of Engineering, Kadapa

premkumar@gpct.ac.in, lakshmiveenadhari@gmail.com, immidikalipradeep@gmail.com

**Abstract:** Cloud computing is the new movement in the technology world. It is an internet based service delivery model which provides internet based services, computing and storage for users in all market including financial, health care & government. This paper discuss the characteristics and benefits of cloud Computing and services in a cloud computing. It proceeds to discuss the deployment models in a cloud computing (public, private, and hybrid), various advantages and challenges of different models.

**Keywords**— Cloud, Cloud computing, IAAS, PAAS, SAAS& deployment.

### I. INTRODUCTION

A cloud is a place where IT resources such as computer hardware, operating systems, networks, storage, databases, and even entire software applications are available instantly, on-demand. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications.



Figure 1: cloud computing

#### A. Characteristics of Cloud Computing:

- a. **On-demand self-service:** A user can directly access the needed computing capabilities from the source, no matter what specific resource is required [1].
- b. **Broad network access:** A user is not tied to one location but can access resources from anywhere the network (typically the Internet) is available.
- c. **Resource pooling:** Many users share the same overall set of resources from a provider, using what they need, without having to concern them selves with where those resources originate.
- d. **Rapid elasticity:** Users can quickly increase or decrease their use of a computing resource in

response to their immediate needs.

- a. **Measured service:** The amount of usage by a customer is monitored by the provider and can be used for billing or other purposes.

#### B. Benefits of Cloud Computing:

- a. Cloud technology is paid incrementally, saving organizations money [3].
- b. Organizations can store more data than on private computer systems.
- c. No longer do IT personnel need to worry about keeping software up to date.
- d. Cloud computing offers much more flexibility than past computing methods.
- e. Employees can access information wherever they are, rather than having to remain at their desks.
- f. No longer having to worry about constant server updates and other computing issues, government organizations will be free to concentrate on innovation.
- g. Decoupling and separation of the business service from the infrastructure needed to run it (virtualization).
- h. Flexibility to choose multiple vendors that provide reliable and scalable business services, development environments, and infrastructure that can be leveraged out of the box and billed on a metered basis—with no long term contracts
- i. Elastic nature of the infrastructure to rapidly allocate and de-allocate massively scalable resources to business services on a demand basis.
- j. Cost allocation flexibility for customers wanting to move CapEx into OpEx
- k. Reduced costs due to operational efficiencies, and more rapid deployment of new business services [6].

#### THREE BASIC SERVICE MODELS:

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).



## **Cross Entropy Based Long Short Term Memory Recurrent Neural Network Model for Analyzing the Time Series on Stock Market Price**

**Dwaram Jayanarayana Reddy<sup>1\*</sup>    Akepogu David Donald<sup>1</sup>    Kothapalli Seshadri Ramana<sup>1</sup>  
 Karanam Srividya Lakshmi<sup>1</sup>    Pullala Cheruvu Sai Divya<sup>1</sup>**

<sup>1</sup>*G Pullaiah College of Engineering and Technology (Autonomous),  
 Department of Computer Science and Engineering, Kurnool, India*

\* Corresponding author's Email: [djnreddy@gmail.com](mailto:djnreddy@gmail.com)

---

**Abstract:** In the financial stock market, a sequence of prices obtained from the share market with respect to the time series is usually examined. Generally, time series in finance, particularly shows importance in predicting investment in today's share market. Since there are too many factors such as public opinions, general economic conditions, or political events, vulnerability in the economy are directly or indirectly reflects on the evolution of financial time series. The desire of the investor is to predict the future stock prices neglecting whether the investor is a long-term investor or a day-trader. A major challenge is to develop and design an efficient predictive model that guides investors to make appropriate decisions. In this research work, Long Short Term Memory-Recurrent Neural Network (LSTM-RNN) is developed to overcome such disputes and contributing an efficient technique for predicting the future stock prices financially. In addition to the model, cross entropy is calculated using a Mutual Information feature selection model to minimize the optimization problems that create the time complexity in the system. The proposed LSTM-RNN has achieved best accuracy of 61.33% of prediction accuracy compared to state-of-the-art techniques.

**Keywords:** Cross entropy, Global financial crisis, Long short term model, Recurrent neural network, Stock market.

---

### **1. Introduction**

The stock market is a place where the aggregation of both buyers and sellers happens in a single platform for offering shares to the general public. Meanwhile, the capital is raised on products needed for expansion of new operations [1]. During the past two decades, the stock market has been advanced as the main form of investment in numerous organizations as well as individuals for arranging huge investment funds [2]. As a result, many companies have been listed in stock markets around the world and investing a huge amount of their capital regularly. The time series analysis and topic modelling have been used in various applications such as the environment, the economy, health, and politics, even the social media. An overview of time series analysis of social media in different settings and focus areas were provided [3]. The traditional financial theory is a foundation for deciding the

effective market system that shows the investors are fully rational. The stock price in turn reflects all available information precisely at any time. The mood factors affect the judgment of investors and behaviour of investors that impact on the stock price in great demand. The investors sometimes overreact to good news when they are in a good mood or for bad news. Thus, investors tend to buy more or sell less stocks when they are in a good mood than they are in a bad mood, which causes the abnormal change in stock price [4]. In order to reduce the dimensionality of time series in univariate data, an Asynchronism Principal Component Analysis (APCA) was developed based on Dynamic Time Warping (DTW). ARIMA (Auto Regressive Integrated Moving Average) model was developed for the prediction of stock market movement. The Univariate time series models reduce the range of economical phenomena through the historical behaviour of a dependent variable. The accuracy

# An Energy Efficient Routing Protocol for Wireless Sensor Networks using A-star Algorithm

P. Suman Prakash

Assistant Professor  
Department of Computer Engineering  
College of Engineering, G.Pullaiah  
College of Engineering and  
Technology, Kurnool, India  
Email id:sumanprakash@gpcet.ac.in

## ABSTRACT

Sensors are regarded as significant components of electronic devices. In most applications of wireless sensor networks (WSNs), important and critical information must be delivered to the sink in a multi-hop and energy-efficient manner. Inasmuch as the energy of sensor nodes is limited, prolonging network lifetime in WSNs is considered to be a critical issue. In order to extend the network lifetime, researchers should consider energy consumption in routing protocols of WSNs. In this paper, a new energy-efficient routing protocol (EERP) has been proposed for WSNs using A-star algorithm. The proposed routing scheme improves the network lifetime by forwarding data packets via the optimal shortest path. The optimal path can be discovered with regard to the maximum residual energy of the next hop sensor node, high link quality, buffer occupancy and minimum hop counts. Simulation results indicate that the proposed scheme improves network lifetime in comparison with A-star and fuzzy logic(A&F) protocol.

Keywords: Wireless sensor networks (WSNs), network lifetime, energy efficiency, A-star.

## 1. Introduction

Recent advances in micro-electro-mechanical systems (MEMS) and wireless communications have highlighted the significance of WSNs as essential reporting devices. Indeed, sensor nodes in WSNs are deemed to be resource constrained in terms of energy, communication range, memory capacity and processing capability. WSNs include specifications and applications such as target tracking, environmental monitoring and battlefield applications. The main purpose of WSNs is to disseminate the information from the source to the sink in multi-hop scheme [1].

In general, since energy sources are scarce and constrained and batteries are low-powered, energy-efficient data forwarding is supposed to be a critical challenge in WSN applications. As Fig.1 illustrates, sensor nodes send fire detection information to the sink node efficiently in real-time. Hence, it can be argued that energy consumption should be managed so that network lifetime of WSNs is significantly prolonged. On the other hand, the majority of routing algorithms in WSNs require reliable and real-time data forwarding to the sink node in many-to-one scheme [2, 3]. Thus, energy-efficiency and QoS-based data routing are

considered as a crucial challenge in WSNs and there is a trade-off between energy-efficiency and QoS parameters [1, 3-5]. On the other hand, non-uniform energy consumption and load unbalancing are vital problems in many routing protocols of WSNs which result in network partitioning. Consequently, network partitioning has a negative impact on the successful packet delivery to the sink and hence it hinders the performance and the proper function of WSNs. With regard to the significance of WSNs' applications, reduction in the packet delivery ratio will have a negative impact on the energy consumption and hence network lifetime of WSNs.

In WSNs, transmission and reception of data packets are considered as the chief sources of energy consumption [6, 7]. As a result, to design energy-aware routing protocols for WSNs, we must efficiently control and manage energy consumption. Due to many-to-one traffic scheme, lack of energy consumption management will result in the quick loss and destruction of energy resource of the nodes near the sink; this is referred to as energy hole problem [8]. In the majority of routing algorithms, the periodical choice of the

# A Pattern Recognition Model of Python Programming using Artificial Neural Network via NeMo



M.Janardhan, M.Srilakshmi, S Prem Kumar

**Abstract:** *Background/Objectives:* In the field of software development, the diversity of programming languages increases dramatically with the increase in their complexity. This leads both programmers and researchers to develop and investigate automated tools to distinguish these programming languages. Different efforts were conducted to achieve this task using keywords of source codes of these programming languages. Therefore, instead of using keywords classification for recognition, this work is conducted to investigate the ability to detect the pattern of a programming language characteristic by using NeMo(High-performance spiking neural network simulator) of neural network and testing the ability of this toolkit to provide detailed analyzable results. *Methods/Statistical analysis:* the method of achieving these objectives is by using a back propagation neural network via NeMo based on pattern recognition methodology. *Findings:* The results show that the NeMo neural network of pattern recognition can identify and recognize the pattern of python programming language with high accuracy. It also shows the ability of the NeMo toolkit to represent the analyzable results through a percentage of certainty. *Improvements/Applications:* it can be noticed from the results the ability of NeMo simulator to provide beneficial platform for studying and analyzing the complexity of the backpropagation neural network model.

**Keywords:** NeMo, Pattern recognition, artificial neural network, Backpropagation neural network.

## I. INTRODUCTION

NeMo (Neural Modules) is a Python framework-agnostic toolkit for creating AI applications through re-usability, abstraction, and composition. NeMo is built around neural modules, conceptual blocks of neural networks that takes typed inputs and produce typed outputs. Such modules typically represent data layers, encoders, decoders, language models, loss functions, or methods of combining activations. NeMo makes it easy to combine and re-use these building blocks while providing a level of semantic correctness checking via its neural type system.

Manuscript published on January 30, 2020.

\* Correspondence Author

**M.Janardhan\***, Associate Professor, Department of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology (Autonomous).

**M.Srilakshmi**, Assistant Professor, Department of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology (Autonomous).

**Dr.S Prem Kumar**, Professor & Dean, Department of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology (Autonomous).

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](http://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

In the last decade, a wide range of programming languages for a variety of tasks have been created in the software development field (Philip Mayer, April 2015). This diversity makes it difficult for new students and developers to recognize the exact programming language that been used in complex systems.

Especially in the systems that require using a combination of programming languages such as python, Java or Ruby (Philip Mayer, April 2015). Therefore, it would be beneficial to develop a tool for identifying programming language codes based on its pattern. One of the attempts to achieve this task is conducted by M. Robson (Montenegro, 2016) and (Jyotiska Nath Khasnabish, 2014) through training a neural network model to classify programming codes based on its language. According to M. Robson (Montenegro, 2016), this classifier identifies programming languages based on syntax codes in the form of words. Robson suggests using the characters' patterns of the programming language instead of these keywords. Therefore, instead of using the classification of keywords in the codes for different programming languages, this work aims to investigate the ability of back propagation neural network (BNN) to identify and recognize the programming language (python) based on the pattern of each particular code characteristics. This paper also aims to investigate the ability of NeMo, a neural network simulation, to represent analyzable results.

## II. BACKGROUND

### 2.1 Pattern Recognition

Pattern recognition can be defined as a methodology of designing systems that can identify or classify patterns in complex environment (Sargur N. Srihari, 1993). It also "can be seen as a classification process" (SALIBA, 2014). It aims to study and monitor environment for a potential pattern and make a proper decision about it (Jayanta Kumar Basu, 2010). According to Sharma and Kaur (Priyanka Sharma, 2013), the basic algorithm of pattern recognition can be illustrated in Figure 1



# Secure Intelligence Model for Big Data Security

Dr.K. Seshadri Ramana\*, Professor, Department of Computer Science and Engineering, G. Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India. E-mail: ramana.kothapalli@gmail.com

K. Bala Chowdappa, Assistant Professor, CSE Department, G. Pulla Reddy Engineering College, Kurnool.

E-mail: balak06@gmail.com

V. Suresh, Assistant Professor, CSE Department, G. Pulla Reddy Engineering College, Kurnool. E-mail: sureshv@gmail.com

**Abstract**--- Now a day's big data plays a vital role in several organizations like medical, educational, banking and e-commerce, etc. Due to the velocity, variety, and volume of big data, security and privacy issues are magnified, while storing, sharing and analyzing which results in the data leakage or misuses the sensitive data. Sensitivities around big data security and privacy are a hurdle that organizations need to overcome. This paper analyses the current data security in big data and its feasibilities and difficulties. Furthermore, in this paper, we also introduced security intelligence model which enhance security. This research aims to summarize, organize and classify the information iavailable in the literature to identify any gaps in current research and suggest areas for scholars and security researchers for further exploration.

**Keywords**--- Big Data, Data Integrity, Privacy and Security, Secure Intelligence Model.

## I. Introduction

Big data is an evolving term that describes any voluminous amount of structured, semi-structured and unstructured data that has the potential to be mined for information. The appearance of big data concept and the related technologies that allowed collecting, storing and processing the considerable type volume of data. There is a massive amount of information available today that is in "UNSTRUCTURED FORM." We have social networking websites, online articles, forms, etc. where people talk and share.

Big Data needs an innovative platform for enhanced insights, understanding and decision making. But, 90% of the data getting generated today is unstructured and cannot be handled by our traditional technologies. Data management and It analysis play an essential role in, i.e., data collecting, storing, analyzing in time. Quite recently, considerable attention has been paid on search, sharing, Privacy and Data Security. Big data majorly connected with three essential components such as 3V called volume, variety, and velocity.

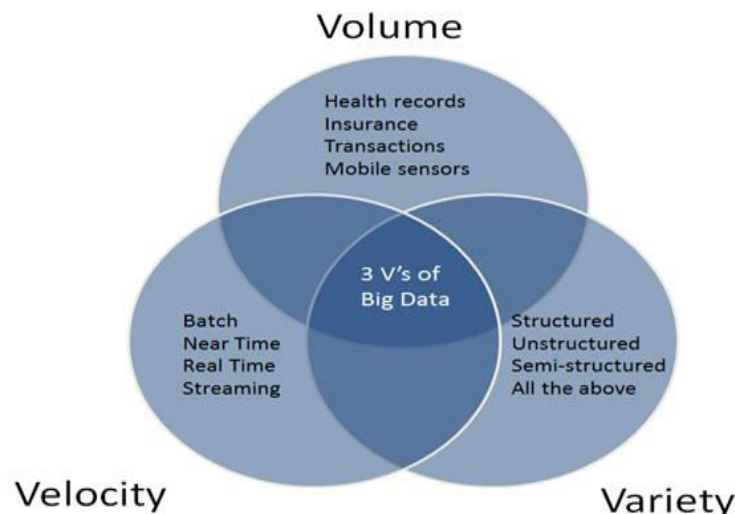


Figure 1: Illustration of Big Data 3V

# Machine Learning Centric Product Endorsement on Flipkart Database

M.Sri Lakshmi, S Prem Kumar, M.Janardhan



**Abstract:** The growing need for individual mining information from text leads to analyzing sentiment and viewpoints. Retailers, E-commerce companies, product companies, media houses, real estate firms, and whom all have recognized that sentiment analysis is the key to success. They perform sentiment analysis necessary to get customer information related to feelings; attitudes, reactions, and opinions of existing and potential buyers towards their product or services. In this context, evaluating an individual's viewpoint or humor from a piece of text is challenging. In recent years the need for this analysis has increased due to the benefits obtained from it. In this paper, we conduct sentiment analysis on Flipkart product reviews using machine learning techniques to address the above challenge.

**Keywords:** Sentiment analysis, Machine Learning, Flipkart, Product Analysis.

## I. INTRODUCTION

Nowadays, people are spending more time on e-commerce websites for purchasing items, and the online platform almost entirely covers the global business site. For this reason, it is also common to read and understand the reviews for the products before purchasing them. Apparently, customers are more likely to buy a product if it has been given with positive reviews; therefore, analyzing these customer review data is essential to make them more dynamic. The major attention of this paper is to classify the positive and negative sentiments of the consumers over different products and articulate a supervised learning model to polarize a large number of reviews [8]. A study on online e-commerce sales increases due to its product reviews shown as per the survey, in the figure 1.

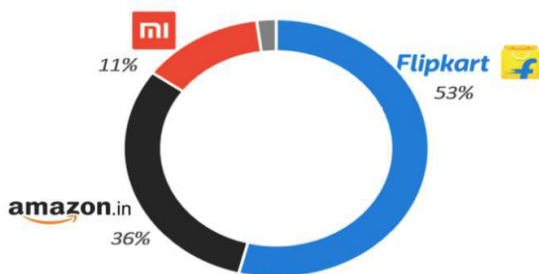


Figure 1. Online share in India over eCommerce business

Revised Manuscript Received on October 30, 2019.

\* Correspondence Author

M.Sri Lakshmi \*, Assistant Professor, Department of CSE, G.Pullaiah College of Engineering and Technology, Kurnool.

Dr.S Prem Kumar, Professor & Dean, Department of CSE, G.Pullaiah College of Engineering and Technology, Kurnool.

M.Janardhan, Associate Professor, Department of CSE, G.Pullaiah College of Engineering and Technology, Kurnool.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

In E-commerce market, customer reviews testimonials, or even social media posts which influence the growth of the company's business potential when company gains customer trust. Figure 2 demonstrates how effective is the customer content at increasing the conversion from product visits to purchases.

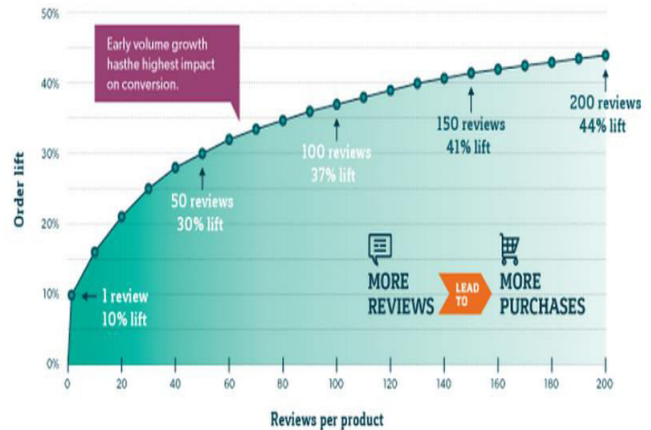


Figure 2. Increasing sales based on Reviews

Sentiment Analysis also known as Opinion Mining is a field within Natural Language Processing (NLP) that builds systems which try to identify and extract opinions within text. Usually, besides identifying the opinion, these systems extract attributes of the expression e.g.

**Polarity:** a positive or negative opinion that the speaker expresses,

**Subject:** the thing that is being talked about,

**Opinion holder:** the person, or entity that expresses

the opinion.

**The Impact of Reviews:** In this digital era, people are overwhelmingly using the internet to search and research online. Daily, purchase decisions are being made, while pre-purchase research is being done mostly online. Reports and studies show that 9 out of 10 consumers conducted online research via search engines before making a purchase [7]. More importantly, a large portion of that research comes from browsing reviews. Negative reviews have become quite influential in undermining a business' reputation, leading to consequences:

- **Reputational risk:** Negative reviews cause potential customers to trust a company, lesser.
  - **Hard to fix:** Having an abundance of negative reviews makes it difficult to regain trust and rebrand.
- On the other hand, positive reviews provide a business with a positive reinforcement loop:

## Exploration on Cloud Foundry Industry-Standard Cloud Platform

D.Jayanarayana Reddy<sup>1</sup>, Prof. Sharaf Alhomdy<sup>2</sup>

<sup>1</sup>Assistant Professor, Dept of CSE, G. Pullaiah College of Engineering and Technology, Kurnool, India

<sup>2</sup>Faculty of Computer and Information Technology (FCIT), Sana'a University, Yemen

<sup>1</sup>email id: dwaramjayanarayana@gpcet.ac.in

<sup>2</sup>email id: sharaf.sana@gpcet.ac.in

### Abstract

Nowadays Cloud Computing is rapidly increasing its growth in the IT industry in recent years which provides a new way to manage the different information systems. The rapid development of technology makes it important to use this technology and to benefit from its advantages. There are various characteristics to organizations advancing toward cloud-based information stockpiling. These contain improved IT infrastructure and the administration remote distant access from successfully anyplace on the planet with a settled Internet association and the cost efficiencies that cloud computing can be accomplished. While we are moving towards the idea of on-request administration, asset pooling, moving everything on the distributive environment. Security and privacy challenges are the main issues that are always considered which is of worry to Researchers from the scholarly community, industry, and standards organizations have given potential solutions for these Challenges in the recently published studies. Cloud data security risks, cloud attacks, and identified vulnerabilities for different variables impacting cloud computing were presented in this study analysis. This analysis is actually intended to examine the different components of cloud computing as well as existing key security and security issues. Additionally, this paper presented various sorts of security threats with some new security concepts and alleviation techniques and recommend future directions.

**Category:** Cloud Computing and security issues

**Keywords:** Security Requirement, Threats, Attack, Mitigation Techniques, Cloud Computing

### I. INTRODUCTION

Back to the 1960s dates, the Cloud computing technology was available on mainframe systems only and over time it was developed into the cloud. The term cloud has risen up out of network diagrams in which the internet was being represented as a cloud symbol [1]. Cloud computing connects several computing resources, software resources, and storage resources to shape a huge shared virtual resource pool, from which clients can purchase corresponding services, for example, hydropower. With the fast popularization of cloud computing applications, cloud computing has penetrated different fields, such as education, production, scientific research, consumption, entertainment, etc. The cloud technology itself is a combination of several technologies such as Virtualization, Grid computing, clustering, and which not just offers low cost to business users as well as also eliminates the

maintenance cost to keep up an interior data center. Cloud computing, a developed networking technology, empowers better utilization of services and resource usage, at a reduced operational cost [2]. The computing world has excelled in dealing with cloud computing services, but gaps occur through which threats to Threats and Risks arise in the Cloud Computing Environment. The context of threats to cloud computing is storing IT risks as a result of all the things that lead to the loss of company assets [3]. the major factor in determining the value of risk is a form of threat, that emerge are an integral part of all business activities, Threats to data and information of both applications and data (technology assets) will have an effect on the organization's operations and resources. added to that the technology risk is a procedure that incorporates the way toward distinguishing risks as per their inclination, conceivable outcomes, likely effects, then can be assessed and controlled The threat to IT case with

## Research Article

# Fuzzy Subnets and System Theory and Applications

<sup>1</sup>Dr.S.Prem Kumar, <sup>2</sup>S.Sandeep Kumar

<sup>1</sup>Professor, Dept of CSE, G. Pullaiah Engineering College, Kurnool, India

<sup>2</sup>Assistant professor, Dept of IT, Sree Vidyanikethan, Tirupati, India

<sup>1</sup>premkumar@gpcet.ac.in, <sup>2</sup>s.sandeep@vidyanikethan.ac.in

## 1. Introduction

In 2001, Maji et al. [1] combined fuzzy sets [2] with soft sets [3] and proposed the concept of fuzzy soft sets. After that, the fuzzy soft set was applied to group theory, decision-making, medical diagnosis, and other fields (see [4–13]). Meanwhile, the theory of fuzzy soft set has been developed rapidly. In particular, the research on fuzzy soft topology has made a lot of achievements (see [14–24]).

Noting the contribution of the pointed approach in fuzzy topology, Roy and Samanta [21] defined a fuzzy soft point on a fuzzy soft topological space. In 2018, Ibedou and Abbas [17] redefined this concept. Recently, Gao and Wu [7] studied the properties of fuzzy soft points introduced in [17] deeply and pointed that the fuzzy soft point given in [17] was more effective than that given in [21]. They also gave the definitions of a fuzzy soft net consisting of fuzzy soft points and its convergence. On these bases, they characterized the continuity of fuzzy soft mappings by the net approach.

This paper aims to further the study of [7]. In Section 2, some preliminaries will be recalled. In Section 3, the characterizations of some important results involving closure, separation, and compactness will be obtained by means of fuzzy soft nets.

## 2. Preliminaries

Throughout this paper,  $U$  refers to an initial universe and  $E$  is the set of all parameters for  $U$ . In this case,  $\mathcal{I}^U$  is also denoted by  $(U, E)$ .  $I^U$  is the set of all fuzzy subsets over  $U$ , where  $I \in [0, 1]$ . The elements  $0, 1 \in I^U$ , respectively, refer to the functions  $0(x) = 0$  and  $1(x) = 1$  for all  $x \in U$ . For an element  $A \in I^U$ , if there exists an  $x \in U$  such that  $A(x) > 0$  and  $A(y) = 0, \forall y \in (U \setminus \{x\})$ , then  $A$  is called a fuzzy point over  $U$  and is denoted by  $x_\lambda$ ,  $x$  and  $\lambda$  are its support and height, respectively.

The definitions in this section are all sourced from the existing literature [7, 17, 21, 22].

*Definition 1.* Let  $A \subseteq E$ . A mapping  $F_A: E \rightarrow I^U$ , is called a fuzzy soft set over  $(U, E)$ , where  $F_A(e) = 0$  if  $e \in (E \setminus A)$  and  $F_A(e) \neq 0$  if  $e \in A$ .

The set of all fuzzy soft sets over  $(U, E)$  is denoted by  $FS(U, E)$ .

The fuzzy soft set  $F_\phi \in FS(U, E)$  is called the null fuzzy soft set and is denoted by  $\Phi$ . Here,  $F_\phi(e) = 0$  for every  $e \in E$ .

For  $F_E \in FS(U, E)$ , if  $F_E(e) = 1$  for all  $e \in E$ , then  $F_E$  is called the absolute fuzzy soft set and is denoted by  $E$ .



# Online Smart Voting System Support through Face Recognition

Dr.S.Prem Kumar

Professor, Department of Computer Science and Engineering  
G.Pullaiah College of Engineering and Technology  
Kurnool, India  
Email id:premkumar@gpcet.ac.in

A. Muhammad Marzooq

Department of Information Technology  
SRM Valliammai Engineering College  
Chennai, India  
Email id: muhammed@srm.ac.in

U. Ranjithkumar

Department of Information Technology  
SRM Valliammai Engineering College  
Chennai, India  
Email id: ranjith@srm.ac.in

S. Romario

Department of Information Technology  
SRM Valliammai Engineering College  
Chennai, India  
Email id: romaria@srm.ac.in

P. Surya

Department of Information Technology  
SRM Valliammai Engineering College  
Chennai, India  
Email id: surya@srm.ac.in

**Abstract:-** An online voting system using face recognition is a digital platform designed to enhance the security and accuracy of the voting process. The system utilizes facial recognition technology to verify the identity of voters, ensuring that only eligible voters can participate in the election. This system eliminates the need for physical polling stations, reducing costs and increasing accessibility for voters. The abstract of this system would detail its features, including its ability to authenticate voter identities, securely store votes, and prevent fraud. It would also discuss the benefits of using such a system, such as increased voter turnout and improved transparency in the electoral process. Object Detection using Haar feature-based cascade classifiers is an effective object detection method. Local Binary Pattern (LBP) is a simple yet very efficient texture operator which labels the pixels of an image. Then the server checks for the data from the database and compares that data which is already existing in database. If the data matches with the already stored information, the person is allowed to poll the vote. If not, a message is displayed on the screen and therefore the person is not allowed to poll the vote. Overall, an online voting system using face recognition technology has the potential to revolutionize the way we conduct elections, making the process more efficient, secure, and accessible for all.

**Keywords:-** Face Recognition, Haar Cascade, LBPH, User Authentication.

## I. INTRODUCTION

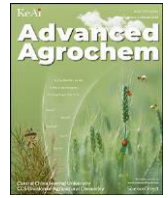
As per the records of TOI 24 Jan 2009 11 lakhs fake votes were observed in Delhi. Then according to India News June 2013: 30000 illegal voters were found in election commission IJSRT23MAR742

under Sheila Dikshit constituency. Another news which was alleged by LJP.(Lok Janshakti Party) Chief, Ram Vilas Paswan saying that Bihar election were having 30% fake voter- cards. Election involves both public or private vote which depends on the position. Local, state, and federal governments are some of the most important positions. In paper based on election, Voters cast their votes by simply depositing their ballots in sealed boxes distributed across the electoral circuits around a given country. After ending of election period, the boxes which contain ballot control unit are opened and votes are counted manually in presence of the certified officials appointed by election commission.

So, it is a time-consuming process and requires a lot of resources to conduct voting process. In this paper we have proposed an online voting system to cast the vote using face recognition. The information about the Face is passed to the server unit for further verification. Then the server checks for the data from the database and compares that data which is already existing in database.

If the data matches with the already stored information, the person is allowed to poll the vote. If not, a message is displayed on the screen and therefore the person is not allowed to poll the vote. For voting representatives are appointed by electorates. In current scenario voter needs to show his/her voter ID card to cast the vote on the booth. So, this process is time consuming as the voter ID card needs to be get verified by the officials.

Thus, to speed up the voting process and avoid such type of problems, we have proposed the new system.



# The Role of Artificial Intelligence in Modern agriculture

Dr.S.Prem Kumar <sup>1</sup>, Abid Haleem <sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology, India

Email id: [premkumar@gpct.ac.in](mailto:premkumar@gpct.ac.in)

<sup>2</sup>College of Engineering, Northeastern University, Boston, MA, USA

Email id: [abid@boston](mailto:abid@boston)

## ARTICLE INFO

### Keywords:

Artificial intelligence  
Application  
Agriculture  
Farming  
Information  
Machine learning

## ABSTRACT

Artificial Intelligence (AI) has been extensively applied in farming recently. To cultivate healthier crops, manage pests, monitor soil and growing conditions, analyse data for farmers, and enhance other management activities of the food supply chain, the agriculture sector is turning to AI technology. It makes it challenging for farmers to choose the ideal time to plant seeds. AI helps farmers choose the optimum seed for a particular weather scenario. It also offers data on weather forecasts. AI-powered solutions will help farmers produce more with fewer re- sources, increase crop quality, and hasten product time to reach the market. AI aids in understanding soil qualities. AI helps farmers by suggesting the nutrients they should apply to increase the quality of the soil. AI can help farmers choose the optimal time to plant their seeds. Intelligent equipment can calculate the spacing between seeds and the maximum planting depth. An AI-powered system known as a health monitoring system provides farmers with information on the health of their crops and the nutrients that need to be given to enhance yield quality and quantity. This study identifies and analyses relevant articles on AI for Agriculture. Using AI, farmers can now access advanced data and analytics tools that will foster better farming, improve efficiencies, and reduce waste in biofuel and food production while minimising the negative environmental impacts. AI and Machine Learning (ML) have transformed various industries, and the AI wave has now reached the agriculture sector. Companies are developing several technologies to make monitoring farmers' crop and soil health easier. Hyperspectral imaging and 3D laser scanning are the leading AI-based technologies that can help ensure crop health. These AI-powered technologies collect precise data on the health of the crops in greater volume for analysis. This paper studied AI and its need in Agriculture. The process of AI in Agriculture and some Agriculture parameters monitored by AI are briefed. Finally, we identified and discussed the significant applications of AI in agriculture.

## 1. Introduction

Agriculture is one of the world's oldest and most important industries. The world's population is rapidly growing, increasing the demand for food and employment. As a result, new automated methods are being introduced to meet food requirements because traditional methods used by farmers are insufficient to meet these requirements while also providing employment opportunities to billions of people worldwide.<sup>1,2</sup> Farmers are forced to seek new solutions due to a labour shortage, stricter legislation, an increasing global population, and a declining number of farmers. Technologies such as the Internet of Things, Big Data & Analytics, Artificial Intelligence (AI), and Machine Learning (ML)

make inroads into almost every industry. Efforts and research are underway to improve the quality and quantity of agricultural products by making them "connected" and "intelligent" through "smart farming."<sup>3-5</sup>

Pesticides are sprayed over cropping areas in open-air or greenhouse settings to improve yield. Farmers can also use ML as part of precision agriculture management, in which agrichemicals are applied based on time, place, and affected crops. Farmers must accurately detect and classify crop quality features to increase product prices and reduce waste. Machines can use data to detect and reveal new traits that contribute significantly to crop quality. Agriculture's water management significantly impacts the agronomic, climatological, and hydrological balance. ML-based applications can estimate evapotranspiration daily,

\* Corresponding author.

E-mail addresses: [mjavid@jmi.ac.in](mailto:mjavid@jmi.ac.in) (M. Javid), [ahaleem@jmi.ac.in](mailto:ahaleem@jmi.ac.in) (A. Haleem), [haleemkhan.i@northeastern.edu](mailto:haleemkhan.i@northeastern.edu) (I.H. Khan), [dr.r.suman@gbpuat-tech.ac.in](mailto:dr.r.suman@gbpuat-tech.ac.in) (R. Suman).

<https://doi.org/10.1016/j.aac.2022.10.001>

Received 6 September 2022; Received in revised form 17 October 2022; Accepted 24 October 2022

Available online 28 October 2022

2773-2371/© 2022 The Authors. Publishing services by Elsevier B.V. on behalf of KeAi Communications Co. Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

1. Artificial intelligence in agriculture. *NJAS: Impact. Agric. Life Sci.* 2021;93(1):172–196.
2. Liu J, Xiang J, Jin Y, Liu R, Yan J, Wang L. Boost precision agriculture with unmanned aerial vehicle remote sensing and edge intelligence: a survey. *Rem Sens.*

# Machine Learning Based SVM Classifier for Copy Create Video Forgery Detection Techniques Using Frame Correlation Difference

Dr.K.Sheshadri Ramana

*Professor*

*Department of Computer Science and Engineering  
G.Pulliah College of Engineering and Technology  
Kurnool, AndhraPradesh, India*

Email: [shesadriramana@gpcet.ac.in](mailto:shesadriramana@gpcet.ac.in)

Srilakshmi Aluri

*Assistant Professor*

*Department of Information Technology  
Gokaraju Rangaraju Institute of Engg. and Tech.  
Hyderabad, Telangana, India*

Email: [alurisrilaxmi@gmail.com](mailto:alurisrilaxmi@gmail.com)

S. Velliangiri

*Associate Professor*

*Department of Computer Science and Engineering  
B V Raju Institute of Technology*

*Narasapur, Medak, Telangana*

Email: [veliangingiris@gmail.com](mailto:veliangingiris@gmail.com)

R. Cristin

*Assistant Professor*

*Department of Computer Science and Engineering  
GMR Institute of Technology*

*Rajam, AndhraPradesh, India*

Email: [cristin.r@gmrit.edu.in](mailto:cristin.r@gmrit.edu.in)

**Abstract**— Digital multimedia applications have greatly increased in recent years as a result of improvements in network technology, low-cost multimedia devices, intelligent image or video editing software, and widespread acceptance of digital multimedia coding standards. One of the most difficult aspects of video forensics is establishing whether a video is authenticated or not. When videos are used as fundamental evidence to affect judgments, such as in a court of law, this can be a critical duty. This paper proposes using the statistical feature of noise remnant to detect passive forgeries in a digital video. To find the revamped section of a video by analyzing the temporal correlation of block-level noise remnants. Significant simulation findings are given to show that the approach can accurately identify the altered region and predict alteration parameters with high reliability.

**Keywords**— Video Forgery Detection, Noise Remnants, Weiner Filter, Pegasos Algorithm

## I. INTRODUCTION

The major focus of the project is to detect forged region in a video using correlation of noise remnants and to locate the major revamped area particularly in the investigating image. In any case, the advanced idea of the media's records, they would now be able to be effortlessly controlled, combined, and altered from multiple points of view without leaving noticeable pieces of information. Accordingly, the honesty of an image /video content can presently don't be underestimated and various legal, related issues emerge. Besides in news sources, logical diaries, political missions, courts, and photograph lay that land in our email boxes, produced images are showing up more often in an interesting manner unfit to distinguish the phony image with the required complexity. Realness and uprightness of the computerized images are thoroughly examining to be critical to beat these issues in light of the manufacturing in fields like forensic, clinical imaging, web -based business, modern photography, and so on.

The efficacy confirmation check of an image is prominently utilized where an images are considered to supporting confirmations, chronicled records, protection claims, and so forth Alternately, with consolations of the present PC innovation, more refined programming

resembles Adobe Photoshop, Corel Draw, or Gimp are accessible for the change of the first images, bringing about an image altering. This venture utilizes an artificial neural network to store the separated information from image streams to totally and precisely recognize altered areas especially.

The methodology is AI based and requires negligible client collaboration. The procedure is appropriate to an image containing at least two individuals and requires no master interaction for the altering choice. The ostensible progression from the film photography to computerized photography is practical aid, however it's not dependable. Customary film photos can't be altered while the computerized images can be altered and changed, get-togethers catch. The image altering in the point of view of computerized works can be considered as an imaginative work, yet there are a few situations where the altered images are in effect malignantly mishandled. Such basic condition emerges where images are by all accounts the confirmation for the clinical reports, crime locations, and so on where the fashioned images bring about patients' demise and departure of the criminal individually. The producing of the first image prompts unlawful circulation, which raises the information starvation issue.

Computerized wrongdoing, along with continually arising programming advancements, is developing at a rate that far outperforms safeguarding strategies. Here and there an advanced image or a video are indisputable proof of a wrongdoing or the evidence of a malicious activity. By viewing at a computerized content as an advanced hint, mixed media criminology intends to acquaint novel systems with help piece of information examination and to give a guide to making a choice about a wrongdoing. Sight and sound legal a science manage to create mechanical instruments working without watermarks or marks embedded in the image. Indeed, not quite the same as advanced watermarking, criminology implies are characterized as "inactive" on the grounds that they can define an evaluation on a computerized record by turning just to the advanced resource itself.

These methods fundamentally permit the client to decide whether a specific substance has been altered with

# Precocious ATM System Using Iris Scanner

DR. K. Seshadri Ramana<sup>1</sup>, R. Ankit Jain<sup>2</sup>, U. Jayarama Krishna<sup>3</sup>

*\*1Assistant Professor, GPCET (affiliated to JNTUA, Anantapur) Kurnool, India <sup>2</sup>B.Tech Student, CSE Department, GPCET(affiliated to JNTUA, Anantapur),Kurnool, India <sup>3</sup>B.Tech Student, CSE Department, GPCET(affiliated to JNTUA, Anantapur),Kurnool, India*

\*\*\*

**Abstract:** Nowadays we are experiencing an intensive increase in skimming within the Automated Teller Machine (ATM) systems. So, actuation in development and safety of the ATM machines is required. An automated teller machine (ATM) is an digital telecommunications tool that enables customers of banking departments in transactions and transfer of cash in their debts. The patron enters their precise private identity wide variety (PIN), i.e. Stored inside the chip of the card. Due to an increase inside the set up of ATM and the number of ATM cardholders, the range of cases of fraudulence has also improved significantly. The development in generation has ended in an boom in various skimming activities. So, trends are incorporated within the present structures to make it greater comfortable, handy and reliable. The hired secured gadget need to have excessive velocity and have to be long lasting. The supplied design is unique due to biometric scanners which includes Iris scanner and the two-manner check with fingerprint scanner makes it greater reliable. The iris scanner being the number one safety test lets the system get admission to the further steps for transaction. Fingerprint scanner embedded in the ATM card acts as the secondary security take a look at for the gadget. The transaction system is a success best if the enter information by means of the card holder matches with the database. It consumes much less electricity that makes it appropriate for use. The counseled changed device is pragmatic moreover economical when correlating to the opportunity current category and confirmation procedures of ATMs.

## I. INTRODUCTION

Transaction system has seen a certain improvement for the reason that early age. Previously barter gadget turned into used for the transaction. Then came steel coins and notes. As on this twenty first century, nobody incorporates liquid cash of their wallet. The traditional use of metal cash and paper notes have now been replaced with the aid of plastic forex in the shape of diverse transaction cards used in ATMs. This led to the discovery of the Automated Teller Machine (ATM). The number of ATM card holders has also elevated. The quantity of ATM card customers has accelerated considerably as distinctive banks everywhere in the world have installed a massive wide variety of Automated Teller Machines (ATMs). As development in technology has also elevated the variety of illegal pursuit and cyber-crimes like ATM card skimming. In spite of continuous caution with the aid of the bank authorities, clients have a tendency to disclose their personal information to the fraudsters and for this reason come to be their victims. The fraudsters victimize the customers with the aid of intercepting their PIN thru fraud textual content messages and emails.

The purchaser's account turns into easily handy once they share their account's PIN through these emails or messages.

Advancements in era have additionally been a boon to the fraudsters as they have get entry to technology along with thermal cameras. Thermal imaging attachments are used to retrieve the consumer's PIN. When a button is pressed, thermal signatures are left at the back of on the keypad. The time lapse among the pressings of the buttons makes it very convenient to the fraudsters to understand the PINs. ATM- set up card skimming gadgets are fabricated as a way to healthy the actual ATM it is hooked up on. This makes it tough for the consumer to apprehend the devices. Keypad overlays are also a sort of ATM-established skimmer that stores the patron's PIN once they enter it. The fraudsters then make fake ATM cards with the identical PIN to withdraw the cash from the person's account. Both the banks and the clients are affected similarly via this act of fraudulence. So, precautions need to be taken from both the sides, else the banks may incur massive losses. Thus, the need of advancements in technology and ATM systems are had to enforce if you want to stop such skimming sports. Many of the banks are starting to put in force a 2nd stage of authentication device. Further advancements are to be implemented to be at par with the skimming technology.

## II. PROPOSED SYSTEM

We are augmenting a fingerprint sensor of FIM3030 collection to the RFID card with a small energy supply linked to the card. This acts as our degree one protection test. The fingerprint given as input to the cardboard is move confirmed with the database created through the financial institution. A message is sent to the registered card holder if there is a mismatch among the input fingerprint and the fingerprint in the database. If the safety test has a clearance, the gadget in addition is going on with the level-2 safety check i.e. The IRIS scanner. IRIS is the most effective a part of our body which doesn't trade from birth until our dying. So IRIS being the most secured biometric device that we have utilized in our proposed gadget. The banks need to layout a database which include the records of the IRIS of the customers, that is to be demonstrated at

## Sixth Sense Technology

Dr.K.Sheshadri Ramana<sup>1</sup>, Prof. Sudeshna Roy<sup>2</sup>

<sup>1</sup>Professor, Dept of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology, Kurnool, India

Email id: seshadriramana@gpcet.ac.in

<sup>2</sup>Professor, Dept. of Master of Computer Application Bharati Vidyapeeth's Institute of Management and Information Technology, Maharashtra, India

Email id: sudheshna@vidyapeeth.ac.in

\*\*\*

**Abstract** - Every day we encounter new objects around us hence we become curious about that particular object. This makes us surf through the Internet or ask any expert in that field. Instead Sixth Sense Technology can be used to get the information as soon as you see that object. Sixth Sense Technology gives us the feeling that we are dealing with real world objects. Thus making the entire world your computer integrating information into our daily life to reduce the gap between the physical and digital world and the goal is to bring part of the physical world to the digital world. Natural Hand Gestures are used to communicate with the Sixth Sense Device. This paper explains the working of Sixth Sense Technology, its components, history. This paper also focuses on the security issues of the Sixth Sense Technology and how the effects of these issues can be minimized, the usefulness of Sixth Sense Technology to disabled human beings, its advantages, future vision and conclusion.

**Key Words:** Digital World, Natural Hand Gestures, Sixth Sense Technology, Sixth Sense Device, Security Issues.

### 1. INTRODUCTION

We all know that sixth sense is a simple wearable gestural interface device but it can also interact with the world using our five senses. Sixth sense technology is an extra sense to human beings. Sixth sense technology bridges the gap between the physical and digital world with the help of hand gestures.

It is a pendant-like device which has a projector, camera, and cell phone. Every new device is almost a touch screen device hence Sixth Sense Technology also accepts the input in touch only which makes ease of operation and saves utilization time, using simple hand gestures, touch screens can be obtained from any surface for various applications.

The inception of this concept of wearable devices was first done by Steve Mann in 1990. Pranav Mistry, further took this idea of sixth sense technology which was developed at Media Labs in MIT and it was called as Wear Ur World (WUW).

The various applications can be performed such as drawing with index finger, reading newspaper, mapping, checking time by drawing a wrist watch etc.

### 2. OBJECTIVES OF BLUE EYES

The main objectives of the research paper are as follows:

- [1] The basic objective is to understand the Sixth Sense Technology's working and its all components. This includes study of what all devices are required to use this Sixth Sense Technology. The work of individual devices.
- [2] The main objective is to focus on the security issues of the Sixth Sense Technology. We all know that Sixth Sense Technology is being for a while but not been used in daily usage because of its security issues. The security issues will be taken into consideration.
- [3] As there are security issues in Sixth Sense Technology, it is required to minimize those issues so that it can be used in our daily lives.
- [4] We are human beings and the technology needs to be in such a way that is useful for all people. Here it is discussed how this Sixth Sense Technology is useful for disabled people.
- [5] The advantages are also mentioned further.

### 3. LITERATURE OVERVIEW

As mentioned earlier Steve Mann invented a wearable device in 1990's. Firstly this device was worn on the head with a helmet but later designed the device to wear around the neck.

The mind behind Sixth Sense technology was started late in 1990's by Steve Mann at MIT who actually proposed the first wearable computer.

In 1994, he came up with the idea to put a projector on the head and camera. He is also known as "father of emergence Sixth Sense" technology. It was not an easy design to wear and use it daily hence modified the design and made it a neck-wear device. Further, an Indian scientist Pranav Mistry took the

# Different Types of ML Methods for Network Intrusion Detection

Dr.K.Sheshadri Ramana

*Professor*

*Department of Computer Science and Engineering  
G.Pullaiah College of Engineering and Technology  
Kurnool, AndhraPradesh, India*

Email: [shesadriramana@gpcet.ac.in](mailto:shesadriramana@gpcet.ac.in)

Srilakshmi Aluri

*Assistant Professor*

*Department of Information Technology  
Gokaraju Rangaraju Institute of Engg. and Tech.  
Hyderabad, Telangana, India*

Email: [aluririlaxmi@gmail.com](mailto:aluririlaxmi@gmail.com)

S. Velliangiri

*Associate Professor*

*Department of Computer Science and Engineering  
B V Raju Institute of Technology  
Narasapur, Medak, Telangana*

Email: [veliangiris@gmail.com](mailto:veliangiris@gmail.com)

R. Cristin

*Assistant Professor*

*Department of Computer Science and Engineering  
GMR Institute of Technology  
Rajam, AndhraPradesh, India*

Email: [cristin.r@gmrit.edu.in](mailto:cristin.r@gmrit.edu.in)

## Abstract

The rapid advances in the internet and communication fields have resulted in a huge increase in the network size and the corresponding data. As a result, many novel attacks are being generated and have posed challenges for network security to accurately detect intrusions. Furthermore, the presence of the intruders with the aim to launch various attacks within the network cannot be ignored. An intrusion detection system (IDS) is one such tool that prevents the network from possible intrusions by inspecting the network traffic, to ensure its confidentiality, integrity, and availability. Despite enormous efforts by the researchers, IDS still faces challenges in improving detection accuracy while reducing false alarm rates and in detecting novel intrusions. Recently, machine learning (ML) and deep learning (DL)-based IDS systems are being deployed as potential solutions to detect intrusions across the network in an efficient manner. This article first clarifies the concept of IDS and then provides the taxonomy based on the notable ML and DL techniques adopted in designing network-based IDS (NIDS) systems. A comprehensive review of the recent NIDS-based articles is provided by discussing the strengths and limitations of the proposed solutions. Then, recent trends and advancements of ML and DL-based NIDS are provided in terms of the proposed methodology, evaluation metrics, and dataset selection. Using the shortcomings of the proposed methods, we highlighted various research challenges and provided the future scope for the research in improving ML and DL-based NIDS.

## KEYWORDS

Deep learning, Machine learning, Network anomaly detection, Network intrusion detection system, Network security

---

## SHORT COMMUNICATION

# MATLAB TECHNOLOGY

Dr.K.Sheshadri Ramana<sup>1</sup>, Prof. Sudeshna Roy<sup>2</sup>

<sup>1</sup>Professor, Dept of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology, Kurnool, India

Email id: seshadriramana@gpcet.ac.in

<sup>2</sup>Professor, Dept. of Master of Computer Application Bharati Vidyapeeth's Institute of Management and Information Technology, Maharashtra, India

Email id: sudheshna@vidyapeeth.ac.in

---

## Abstract

MATLAB is a software package used by engineers for design, optimisation, visualisation of data, and to simulate and control hardware. There are many important skills that engineering students develop through learning to use MATLAB – the most significant of which is the ability to distil a problem so that it can be solved using a computer algorithm quickly and efficiently. This research is presented as a short case study focusing on the process of transforming a course from a traditional lecture/tutorial-based format to a blended learning experience. Changes to the course structure, learning and teaching methods, and assessment are deconstructed and analysed. Consistent with dual coding and cognitive load theory of multimedia learning, new course materials were developed around a series of screencasts. The blended course design allowed the students to learn MATLAB in an interactive way, at their own pace, and through hands-on experience. Although student performance from before and after the move to blended learning has not yet been formally evaluated, comments made in end-of-course questionnaires and through conversations with academics indicate the new course has been very well received.

**Keywords:** blended learning, interactive, MATLAB, self-study, flexible

## Introduction

MATLAB (<http://www.mathworks.co.uk/products/matlab/>) is produced by MathWorks (Natick, MA), and is one of a number of commercially available software packages for numerical computing and programming. MATLAB is widely-used in many different fields of engineering and science, and provides an interactive environment for algorithm development, data visualisation, data analysis, and numerical computation. The ability to use tools such as MATLAB is increasingly required by employers of graduate engineers, with many job adverts specifically mentioning knowledge of MATLAB as an essential skill. In addition, the professional engineering institutions such as the Institution of Mechanical Engineers (IMechE), the Institution of Civil Engineers (ICE), and the Institution of Engineering Technology (IET) are demanding that, within accredited engineering degrees, students must learn to use industry-standard software. There is therefore a great deal of





# Underwater Wireless Communication

Dr.K.Sreenivasulu\*, Dushantha Nalin K. Jayakody<sup>†</sup>, Tharindu D. Ponnimbaduge Perera\*,Kathiravan Srinivasan<sup>‡</sup>, Abhishek Sharma<sup>§</sup> and Ioannis Krikidis<sup>¶</sup>

\*Professor, Dept of Computer Science and Engineering, G.Pulliah Engineering College, Kurnool, India

<sup>†</sup>School of Postgraduate Studies, Sri Lanka Technological Campus, Sri Lanka

<sup>‡</sup> School of Information Technology and Engineering, Vellore Institute of Technology, INDIA

<sup>§</sup>Department of Electronics Communication Engineering, The LNM Institute of Information Technology, INDIA

<sup>¶</sup>Department of Electrical and Computer Engineering, University of Cyprus, Cyprus

Email:[ali89,ponnimbaduage,nalin]@tpu.ru, kathiravan.srinivasan@vit.ac.in, abhisheksharma@lnmiit.ac.in.

**Abstract**—Our earth the only planet where water could be found and covered more than seventy percent with it. Monitoring different phenomenal activities in an underwater environment, such as environmental impact surveillance, marine life, oil and gas exploration is essential in underwater. In this regard, underwater wireless communication (UWC) has become a significant field. Optical, acoustic and electromagnetic waves have been widely used for data transmission in UWC. Investigation of possible UWC techniques has an influential impact on wireless communications. Nowadays, UWC is being used for experimental observation, oceanographic data collection and analysis, underwater navigation, disaster prevention and early detection warning of a tsunami. This work presents an overview, main initiatives and up-to-date contributions of the most widely used UWC techniques, i.e, underwater wireless optical, acoustic and electromagnetic communications. In addition, we summarize emerging technologies in the UWC, future research directions and recommendations using fifth generation (5G) communication techniques.

**Index Terms**—Underwater wireless acoustic communication, Underwater electromagnetic communication, Underwater optical communication, 5G wireless communication.

## I. INTRODUCTION

Global warming has become an issue for several decades. In rising of global warming, the polar ice caps melt gradually cause of rising sea level. Hence, the importance of observing ocean environmental activities such as oceanographic data collection, water sampling, etc., has gradually increased with time variation. Underwater Wireless Communication (UWC) supports surveillance of coastal securities, especially for military purposes and commercially for investigation of natural resources in underwater environment. Moreover, it also helps for mapping and discovering the unknown regions of underwater. Nowadays, UWC is being used for experimental observation, data collection, and analysis, underwater navigation, disaster prevention and early detection warning of tsunami [1]. Optical, acoustic and electromagnetic (EM) wireless carriers are considered to envisage UWC in underwater applications. Deploying UWC techniques in an unexplored water medium are highly challenging as compared to terrestrial wireless communication [2]. However, the quality and reliability of data transmission in shallow and deep water are dependent on the physical characteristics of the water channel [3]. The Quality

of Service (QoS) of UWC, depends on the physicochemical properties of water medium and physical characteristic of optical, acoustic and EM waves. UWC plays a significant role in deployed underwater applications, which has an influential impact on the wireless network. The deployment of communication network setup in underwater systems consist of fixed and anchored sensor nodes with the seabed, floating unmanned underwater vehicle nodes (UUVs) or autonomous underwater vehicle (AUVs), signal receiver processing towers, floating devices (buoy), submarines, ships and onshore base stations [4].

EM waves in radio frequency (RF), 3Hz to 3 kHz frequency range is capable for high data acquisition and transmission in shallow water over short distances and usually attenuated easily by seawater [4]. On the other side, acoustic waves are affected by different propagation factors due to ambient noise, external interference, water-surface geometrical expansion, attenuation, multi-path effects, and Doppler spreading. Optical waves have high bandwidth, but affected by absorption, scattering and different level of temperature in underwater. Underwater wireless optical communication (UWOC) has less explored and somewhat challenging to deploy than acoustic propagation in underwater [5]. The existing Underwater wireless acoustic communication (UWAC) has the limited performance of low bandwidth, latency and multi-path propagation in an underwater medium. The maximum data acquisition in UWAC is roughly 100 kbps for short distances while 10 kbps over long distances. The possible bandwidth with respect to propagation distance in UWAC are listed down in Table I.

The main purpose of this survey is to understand the main characteristics and existing features of UWC. This work has an overview of possible UWC techniques and up-to date literature. The remaining structure of this paper as follows: In section II, we discuss the main deployable techniques of UWC towards the next generation of wireless network. Underwater wireless RF communication (UWRFC) and related issues are described in section III. Underwater wireless optical communication (UWOC) has been widely discussed in section IV. In section V, underwater wireless acoustic communication (UWAC) and it's issues are discussed. The paper contributes



INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES &amp; RESEARCH TECHNOLOGY

## Expert System

Dr. K. Sreenivasulu

Professor, Dept of Computer  
Science and Engineering,  
G. Pullaiah College of Engineering  
and Technology, Kurnool, India

### Abstract

One of the largest area of applications of artificial intelligence is in expert systems, or knowledge based systems as they are often known. This type of system seeks to exploit the specialised skills or information held by group of people on specific areas. It can be thought of as a computerised consulting service. It can also be called an information guidance system. Such systems are used for prospecting medical diagnosis or as educational aids. They are also used in engineering and manufacture in the control of robots where they inter-relate with vision systems.

In this paper I have discussed the number of researches carried out in the area of expert system. It also describes the future of expert system.

**Keywords:** Artificial Intelligence, Expert System, Rule-based system

### Introduction

Expert systems are an offspring of the more general area of study known as artificial intelligence (AI). In the simplest sense, AI is the study of developing computer programs which exhibit human-like intelligence. Early AI researchers focused on such problems as game theory, robotic control, and vision systems. Common to each of these problems was research into ways of representing and reasoning with knowledge, in a computer, in a fashion similar to humans. The early studies in AI provided the insight needed to develop expert systems. In particular, these studies showed that reasoning alone is not a sufficient measurement of intelligent behaviour, but rather, one had to have a rich set of knowledge with which to reason. It was also determined that the problem needed to be well-focused, using only the knowledge relevant to a specific problem. These two requirements led AI researchers to use human experts for their source of problem-solving knowledge. By virtue of being an expert, the human possesses unique talents, made possible by the human's knowledge and problem solving skills on a particular subject. Because of the nature of these intelligent computer programs, they were aptly called expert systems. An expert system is a computer program designed to model the problem-solving ability of a human expert. The program models the following characteristics of the human expert:

- Knowledge
- Reasoning
- Conclusions
- Explanations

The expert system models the knowledge of the human expert, both in terms of content and structure. Reasoning is modelled by using procedures and control structures which process the knowledge in a manner similar to the expert. Conclusions given by the system must be consistent with the findings of the human expert. The expert system also provides explanations similar to the human expert. The system can explain "why" various questions are being asked, and "how" a given was obtained. One of the principal attractions of expert systems is that they enable computers to assist humans in many fields. These systems are rule-based systems are used as a way to store and manipulate knowledge to interpret .A rule consists of two parts: condition (antecedent) part and conclusion (action, consequent) part, i.e:

IF (conditions) THEN (actions)

Antecedent part of the rule describes the facts or conditions that must exist for the rule to fire. Consequent describes the facts that will be established, or the action that will be taken or conclusion that will be made. Information in a useful way. They are often used in artificial intelligence applications and research.

### Conventional Programs Versus Expert Systems

- Use a heuristic search [implicit steps] rather than an algorithmic search [explicit steps] – this speeds up the process of finding a “good enough solution” when an exhaustive search is impractical
- Satisfactory answers are usually acceptable,



# CYBER FORENSICS

Dr.K.Sreenivasulu<sup>1</sup>, Prof. Sudeshna Roy<sup>2</sup>

<sup>1</sup>Professor, Dept of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology, Kurnool, India

Email id:sreenivasulu@gpcet.ac.in

<sup>2</sup>Professor, Dept. of Master of Computer Application Bharati Vidyapeeth's Institute of Management and Information Technology, Maharashtra, India

Email id:sudheshna@vidyapeet.ac.in

**Abstract:** The Cyber Forensics Behavioral Analysis (CFBA) model merges Cyber Behavioral Sciences and Digital Forensics to improve the prediction and effectiveness of cyber threats from Autonomous System Numbers (ASNs). Traditional cybersecurity strategies, focused mainly on technical aspects, must be revised for the complex cyber threat landscape. This research proposes an approach combining technical expertise with cybercriminal behavior insights. The study utilizes a mixed-methods approach and integrates various disciplines, including digital forensics, cybersecurity, computer science, and forensic psychology. Central to the model are four key concepts: forensic cyberpsychology, digital forensics, predictive modeling, and the Cyber Behavioral Analysis Metric (CBAM) and Score (CBS) for evaluating ASNs. The CFBA model addresses initial challenges in traditional cyber defense methods and emphasizes the need for an interdisciplinary, comprehensive approach. This research offers practical tools and frameworks for accurately predicting cyber threats, advocating for ongoing collaboration in the ever-evolving field of cybersecurity.

**Keywords:** behavioral analysis; behavioral threat intelligence; cyber behavioral analysis; cyber defense; cyber forensics; cyberpsychology; forensic cyberpsychology; predictive analytics; Prophet model; time-series analysis



**Citation:** Rich, M.S.; Aiken, M.P. An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics. *Forensic Sci.* **2024**, *4*, 110–151. <https://doi.org/10.3390/forensicsci4010008>

Academic Editors: Ricardo Jorge Dinis-Oliveira and Marcus Rogers

Received: 5 December 2023

Revised: 3 February 2024

Accepted: 24 February 2024

Published: 4 March 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

The fields of cyber behavioral sciences, integrating psychology, cyberpsychology, IT, cybersecurity, and digital forensics are pivotal for understanding human aspects in cyber interactions. Together they shed light on behavioral patterns, motivations, and intentions in cyberspace, contributing significantly to comprehending the human factors influencing cybersecurity [1–3].

This study is dedicated to developing and implementing a real-world integrated predictive model. This model will synergistically fuse the insights of cyber behavioral sciences with the technical rigor of digital forensics. Its primary aim is to significantly improve the accuracy of cyber threat predictions linked to specific Autonomous System Numbers (ASNs).

This study's approach, which leverages live data from Internet Service Provider (ISP) customers to assess ASN predictive models, is a pivotal aspect, underscoring its substantial real-world applicability. The criticality of ASNs in the efficient routing of internet traffic and the overall management of the global internet infrastructure cannot be overstated, making this an essential point in substantiating the study's significance.

### 1.1. Problem Overview

Traditional cybersecurity strategies, predominantly grounded in technical methodologies, face significant challenges in accurately predicting these threats. The increasing sophistication of cybercriminal activities necessitates an approach that not only relies

# Detecting Unconventional Attacks in Virtualized Infrastructures in Cloud Computing Using big Data Analytics

<sup>1</sup>M.Srilakhmi, <sup>2</sup>Dayakar Suddala

<sup>1</sup>Assistant Professor, <sup>2</sup>M.Tech( CSE ) Scholor

<sup>1</sup>Department of Computer Science and Engineering

<sup>1</sup>G.Pullaiah College of Engineering and Technology, Kurnool, India

**Abstract-** Virtualized infrastructure in cloud computing has turned into an appealing focus for cyber aggressors to dispatch propelled attacks. This paper proposes a novel enormous information based security examination way to deal with recognizing propelled attacks in virtualized infrastructures. System logs and in addition client application logs gathered intermittently from the visitor virtual machines (VMs) are put away in the Hadoop Distributed File System (HDFS). At that point, extraction of assault highlights is performed through diagram based occasion relationship and Map Reduce parser based ID of potential assault ways. Next, assurance of assault nearness is performed through two-advance machine learning, namely: strategic relapse is connected to ascertain assault's restrictive probabilities as for the qualities, and conviction spread is connected to figure the faith in presence of an assault in light of them.

**Index Terms-** Virtualized infrastructure, virtualization security, malware detection and security analytics.

## I. INTRODUCTION

Virtual Environment is taking administrations ("cloud services") and moving them outside an associations firewall on shared systems. Applications and administrations are gotten to by means of the Web, rather than your hard drive. The administrations are conveyed and utilized over the Internet and are paid for by cloud client (your business), regularly on an "as-required, pay-per-utilize" plan of action. The cloud infrastructure is kept up by the cloud supplier, not the individual cloud client. A virtualized infrastructure comprises of virtual machines (VMs) that depend upon the product characterized multi-case assets of the facilitating equipment. The virtual machine screen, likewise called hypervisor, maintains, directs and deals with the product characterized multi-case engineering. The capacity to pool diverse computing assets and in addition empower on-request asset scaling has prompted the far reaching sending of virtualized infrastructures as an imperative provisioning to cloud computing administrations.

Security examination applies investigation on the different logs which are acquired at various indicates inside the system decide assault nearness.

The primary purpose behind doing this undertaking is to maintain a strategic distance from attacks in virtualized infrastructures. Albeit one can't keep away from totally, so we are giving our best in distinguishing the propelled attacks. By and large, a virtualized infrastructure comprises of virtual machines (VMs) that depend upon the product characterized multi-case assets of the facilitating equipment. The virtual machine screen, additionally called hypervisor, maintains, controls and deals with the product characterized multi-case engineering. The capacity to pool diverse computing assets and in addition empower on-request asset scaling has prompted the far reaching arrangement of virtualized infrastructures as a critical provisioning to cloud computing administrations. This has influenced virtualized infrastructures to end up an appealing focus for cyber assailants to dispatch attacks for unlawful access. Abusing the product vulnerabilities inside the hypervisor source code, modern attacks, for example, VENOM (Virtualized Environment Neglected Operations Manipulation) have been performed which enable an assailant to break out of a visitor VM and access the hidden hypervisor.

Likewise, attacks, for example, Heart drain and Shellshock which abuse the vulnerabilities inside the working system can likewise be utilized against the virtualized infrastructure to acquire login points of interest of the visitor VMs and perform attacks extending from benefit acceleration to Distributed Denial of Service (DDoS).

To dispense with all these we are going for novel enormous information based security examination way to deal with identifying propelled attacks in virtualized infrastructures. To beat these constraints, in this paper we propose a novel huge information based security examination (BDSA) way to deal with ensuring virtualized infrastructures against cutting edge attacks. By making utilization of the system logs and also the client application logs gathered from the visitor VMs which are put away in a Hadoop Distributed File System (HDFS), our BDSA approach first concentrates assault includes through diagram based occasion relationship, a MapReduce parser based distinguishing proof of potential assault ways and afterward determines assault nearness through two-advance machine learning, namely calculated relapse and conviction proliferation.

## Multi-factor Authentication Approach for Secure Access Cloud Services

M.Srilakshmi<sup>\*</sup>, Vijay Ghorpade<sup>2</sup>, Madhuri Dhange<sup>3</sup>

<sup>1</sup>Department of Computer Science & Engg., G. Pullaiah College of Engineering and Technology, Kurnool, India

Email id: msrilakhmi@gpcet.ac.in

<sup>2</sup>Department of Computer Science & Engg., D.Y.Patil college of Engg., Shivaji University, Kolhapur, Maharashtra, India

Email id: vijay@patil.ac.in

<sup>3</sup>Department of Computer Science & Engg., VVPIET, Solapur University, Solapur, Maharashtra, India

Email id: madhuri@vpiet.ac.in

Available online at: [www.ijcseonline.org](http://www.ijcseonline.org)

Received: May/26/2016

Revised: Jun/02/2016

Accepted: Jun/12/2016

Published: Jun/30/2016

**Abstract**—Cloud computing is a one of the emerging technology in IT industries nowadays. Cloud computing offers a wide range of services to its users. It delivers on demand services over internet with low cost investments. One of the service provided by cloud is data storage. But security and privacy of cloud data are main issues as cloud does not ensure the security aspects like confidentiality, integrity, identification etc. The cloud computing also enables users to access data from the cloud servers. To protect data access by unauthorized users, authentication plays an important role. Authentication is a first step for data security, through which user can establish proof of identities prior data access from system. In cloud computing environment, conventional authentication methods do not provide strong security against today's most modern means of attacks. So cloud needs a dynamic approach for user authentication which should include more than one credentials for authentication. In this paper, we propose a data security architecture with a robust, dynamic and feasible *Multi-Factor Authentication (MFA)* scheme which integrates more than one factors like knowledge, possession, location and time, for cloud user authentication.

**Keywords**-cloud computing; data security; multi-factor authentication; one time password

### I. INTRODUCTION

Cloud computing offers several services to its customers over Internet. Users can access the shared computing resources from anywhere, at any time with pay per use basis. People are fascinated towards the cloud because it delivers resources on demand. In previous generations, people used to store data in Hard Disks, DVDs, CDs, and Pen Drives etc. But today, they prefer to store data on cloud. Nowadays many companies are offering cloud data storage services such as *Google Drobox, AWS S3, and IBM Blue Cloud* etc. The companies which offers cloud services are called as, *Cloud Service Provider (CSP)*. To avail the services from cloud, *Service Level Agreement (SLA)* has to agree between data owner and *CSP*.

*NIST (National Institute of Standards and Technology)*, defines cloud computing as, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[1]. Cloud offers three types of cloud service models such as *Software as a Service (SaaS)*, *Platform as a Service (PaaS)*, and *Infrastructure as a Service (IaaS)*. *SaaS* offers application

# Rain Technology

**K. Lakshmi**  
 Assistant professor,  
 Dept of Computer Science and Engineering,  
 G. Pullaiah College of Engineering and Technology,  
 Kurnool, India  
 Email id: klakshmi@gpcet.ac.in

**Abstract:** New emerging technology coming to the expansion of the internet named Reliable array of independent nodes. Before this rain technology we can use the cluster technology in which we have number of nodes and it is not easy to maintain the connection of all these nodes but in rain technology we are capable of providing the solution by reducing the number of nodes in the chain linking the client and server in addition to making the current nodes more robust and more autonomous. One implementation done for this was RAIN-Reliable Array Of Independent Nodes developed by the California Institute of Technology, in collaboration with NASA Jet Propulsion Laboratory and the Defense Advanced Research Projects Agency (DARPA). The technology is implemented in a distributed computing architecture, built with inexpensive off-the-shelf components. The RAIN platform involves heterogeneous cluster of nodes linked using many interfaces to networks configured in fault-tolerant topologies.

**Keywords:** RAIN, NASA, SNOW, RAINWALL

## I. INTRODUCTION

RAIN technology originated in a research project at the California Institute of Technology (Caltech), in collaboration with NASA's Jet Propulsion Laboratory and the Defense Advanced Research Projects Agency (DARPA). The name of the original research project was RAIN, which stands for Reliable Array of Independent Nodes. The objective of the RAIN is to recognize and make key building blocks for reliable distributed systems built using reasonably priced off-the-shelf components. RAIN technology also offers the new feature of reinstating an out of order node by a new one thus keeping away from the break in information flow [1][2]. The main purpose of the RAIN project was to identify key software building blocks for creating reliable distributed applications using off-the-shelf hardware. The focus of the research was on high-performance, fault-tolerant and portable clustering technology for space-borne computing. RAIN Technology (Redundant/reliable array of inexpensive/independent nodes) is a heterogeneous collection of nodes called clusters linked through numerous interfaces to networks configured in fault-tolerant topologies. The RAIN technology concentrates on developing high - performance, fault-tolerant, portable clustering technology. RAIN technology was capable to proffer the solution by lessening the number of nodes in the chain connecting the client and server. Apart from this it also facilitates in making the current nodes of client-server architecture more robust [3].

## II. WHY WE APPLY RAIN TECHNOLOGY?

RAIN technology is implemented to increase fault tolerance in a cluster. The storage clusters can be managed through a centralized management interface. The management software builds a virtual pool of storage devices without requiring the physical presence of network and storage administrators. The RAIN management software automatically detects any new RAIN nodes and allows them to communicate with each other. In case of a node failure, the lost data is replicated among other RAIN nodes in a cluster to avoid immediate replacement of the failed node. RAIN-based grids are more resilient to application workload changes through effective load-balancing features [4].

## III. GOALS OF RAIN TECHNOLOGY

The goal of the RAIN project was to identify key software building blocks for creating reliable distributed applications using off-the-shelf hardware.

The focus of the research was on high-performance, fault-tolerant and portable clustering technology for space-borne computing. Two important assumptions were made, and these two assumptions reflect the differentiations between RAIN and a number of existing solutions both in the industry and in academia[5]:

1. The most general share-nothing model is assumed. There is no shared storage accessible from all computing nodes. The only way for the computing nodes to share state is to communicate via a network.

2. The distributed application is not an isolated system. The distributed protocols interact closely with existing networking protocols so that a RAIN cluster is able to interact with the environment.

In short, the RAIN project intended to marry distributed computing with networking protocols. It became obvious that RAIN technology was well-suited for Internet applications. During the RAIN project, key components were built to fulfill this vision.

## IV. ADVANTAGES OF RAIN TECHNOLOGY

[6][7] RAIN technology offers various benefits as listed below:

**Fault tolerance:** RAIN achieves fault tolerance through software implementation. The system tolerates multiple node, link, and switch failures, with no single point of failure. A RAIN cluster is a true distributed computing system that is durable to faults, it works on the principle of graceful degradation[8][9].

**Simple to deploy and manage:** It is very easy to deploy and administer a RAIN cluster. RAIN technology deals with the scalability problem on the layer where it is happening, without the need to create additional layers in the front. The management software allows the user to monitor and configure the entire cluster by connecting to any one of the nodes. **Open and portable:** The technology used is open and highly portable. It is compatible with a variety of hardware and software environments. Currently it has been ported to Solaris, NT and Linux.

**Supports for heterogeneous environment:** It supports a

# ML KIT IN FIREBASE FOR APP DEVELOPMENT

K.LAKSHMI<sup>1</sup>, ATMAKUR VANI<sup>2</sup>, BANDA SRINIVASULU<sup>3</sup>, KADAPA SHAIKSHAVALI<sup>4</sup>

<sup>1</sup>Assistant Professor, GPCET (Autonomous)(Affiliated to JNTUA, Anantapur), Kurnool, India

<sup>2,3</sup>B.Tech Student, CSE Department, GPCET(Autonomous)(Affiliated to JNTUA, Anantapur), Kurnool, India

\*\*\*

**ABSTRACT:-** ML Kit or Machine Learning Kit is a mobile Software Development Kit(SDK) that brings Google's machine learning expertise to Android and iOS apps in a powerful yet easy-to-use library. Whether you are new or experienced in machine learning, you can implement the operations you need in clear and easy manner. No deep knowledge of neural networks or model optimization to get started. On the other hand, if you are an experienced Machine Learning developer, ML Kit provides convenient API's that help you use your custom TensorFlow Lite models in your mobile applications.

**Key words:** App development; platform; API; Frameworks;TensorFlow;Neural Networks;

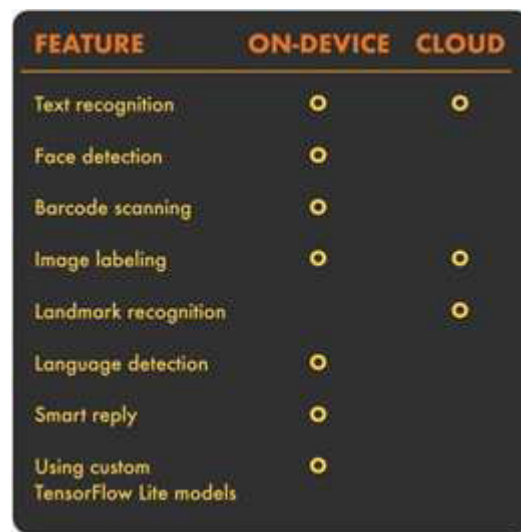
## 1. INTRODUCTION

Machine Learning for a beginner can be very tricky to understand the concepts and then implement them at the same time and it's also very time consuming so Google has come with an interesting,exciting and ready to go solution for Machine Learning which is ML Kit.It is a mobile SDK that brings Google's machine learning expertise to Android and iOS apps in a powerful yet easy-to-use library. Whether you are new or experienced in machine learning, you can implement the operations you need in clear way. No deep knowledge of neural networks or model optimization to get started.Where as if you are an experienced ML and AI developer, ML Kit provides convenient APIs that help you use your custom TensorFlow Lite models in your mobile applications.

## 2. FEATURES

- [1] **TEXT RECOGNITION:-**Text recognition can automate tedious data entry for credit cards, receipts, and business cards of various organizations. With the Google Cloud-based API, you can extract text from pictures of documents of various formats, which you can use to increase accessibility or translate documents.
- [2] **FACE DETECTION:-** The Machine Learning Kit's face detection API, you can detect faces in an image, identify key facial features of a human in a more interactive way and get the contours of detected faces.
- [3] **SMART REPLY:-** The Machine Learning Kit's Smart Reply API, you can automatically generate relevant replies to messages. Smart Reply helps the broad range of users respond to messages quickly, and makes it easier to reply to messages on devices with limited input capabilities.

Some of the features of ML Kit are shown in Figure 1.



FEATURE	ON-DEVICE	CLOUD
Text recognition	<input type="radio"/>	<input type="radio"/>
Face detection	<input type="radio"/>	<input type="radio"/>
Barcode scanning	<input type="radio"/>	<input type="radio"/>
Image labeling	<input type="radio"/>	<input type="radio"/>
Landmark recognition	<input type="radio"/>	<input type="radio"/>
Language detection	<input type="radio"/>	<input type="radio"/>
Smart reply	<input type="radio"/>	<input type="radio"/>
Using custom TensorFlow Lite models	<input type="radio"/>	<input type="radio"/>

Fig-1:ML Kit Features



# Unity 3-d Game Integration in Native Android Application

K.Lakshmi<sup>1</sup>, Vijay Ghorpade<sup>2</sup>, Madhuri Dhange<sup>3</sup>

<sup>1</sup>Dept of Computer Science & Engg., G. Pullaiah College of Engineering and Technology, Kurnool,  
Email id: [klakhmi@gpcet.ac.in](mailto:klakhmi@gpcet.ac.in)

<sup>2</sup>Dept of Computer Science & Engg., D.Y.Patil college of Engg., Shivaji University, Kolhapur,  
Maharashtra, India

Email id: [vijay@patil.ac.in](mailto:vijay@patil.ac.in)

<sup>3</sup>Dept of Computer Science & Engg., VVPIET, Solapur University, Solapur, Maharashtra, India  
Email id: [madhuri@vpnet.ac.in](mailto:madhuri@vpnet.ac.in)

**Abstract:** Paper aims to develop relevant understanding and knowledge about the Unity game development engine for the better conception of the people allied with the IT sector. The main audience targeted in this paper are those who are from a non-technical and technical background and due to the augmentation of technology, they want to pursue their careers in game development. Moreover, in this paper, qualitative research methods have been adopted. It is found that Unity is a smart and active game development platform that is playing an operative role nowadays. Different industries are inspired by Unity that may impact positively such as in career growth, job opportunities, and in other regards. Unity comes with many benefits; it is an easy and simple platform to learn game development and is a powerful tool that is preferred by professionals.

**Keywords:** Unity, Information Technology, Benefits, Game Development, and Challenges.

## I. INTRODUCTION

Unity has been developed under the umbrella of Unity-Technologies that is a cross-platform game engine released in 2005 June at World Wide Apple Inc's Conference as an exclusive game engine (Mac OS X). In 2018, the engine was extended and facilitated more than 20 platforms. This game engine can be used to develop the augmented reality, virtual reality, two-dimensional, and three-dimensional, games along with simulations and for other practices. This game engine in the 21<sup>st</sup> Century has been adopted by businesses outside video gaming like film, architecture, automotive, construction, and engineering [1]. This paper is presenting survey on the Unity as in the current epoch amid the IT (Information Technology) sector the surge of gaming and its development has emerged enormously; however, Unity is playing actively in game development and thus, the researchers of this paper deem that there must be some comprehensive survey that supports the people working in IT sector to connect with the benefits, challenges, and appropriate solutions of those challenges that emerged in the Unity. This ultimately helps the readers and the people allied with the IT sector in the development of relevant knowledge and understanding of Unity.

### A. Research Paper Aim

To develop relevant understanding and knowledge about Unity for the better comprehension of the people allied with the IT sector. To attain the aim, three objectives and questions are developed that are depicted below.

### B. Research Paper Objectives

1. To examine the benefits of Unity game development engine.
2. To inspect the challenges that may emerge in Unity.
3. To outline the best approaches of Unity for enhancing the skills of Unity developers

### C. Research Paper Questions

1. What are the benefits of Unity game development engine?
2. To what extent the challenges of Unity affect the people working in the game development domain?
3. What are the best approaches to Unity skills for enhancing the skills of Unity developers?

### D. Research Paper Layout

To achieve the aim and objectives the research paper has been segregated into five sections. Section 1 covers the introduction, section 2 comprised of the literature review, section 3 depicts the methods and material adopt to conduct the study, section 4 covers the discussion. Section 5 covers the conclusion and future recommendations.

## II. LITERATURE REVIEW

In this section of the proposed paper, the literature review has been conducted. The documentation of relevant works and examination of the collected sources fundamentally is demonstrated in Fig 1. Moreover, Fig 1 is constructed with the help of a technique named as PRISMA, depicted below. Therefore, the literature review has been considered as one of the vital aspects of the research paper as its supports authors as well the readers in understanding and examining several



## Speed Control Using GPS

K.Lakshmi<sup>1</sup>, Shaik Subhani<sup>2</sup>

<sup>1</sup>Dept. of Computer Science and Engineering, G. Pullaiah College of Engineering and Technology, Kurnool, India

Email id: klakshmi@gpcet.aac.in

<sup>2</sup>Dept. of Computer Science and Engineering, G. Pullareddy College of Engineering and Technology, Kurnool, India

Email id: subhani@gprec.ac.in

Available online at: [www.isroset.org](http://www.isroset.org)

Received: 15/Oct/2019, Accepted: 25/Oct/2019, Online: 31/Oct/2019

**Abstract--** The GPS signals got from cell phone gadget will be utilized to screen the individual when he is driving .The directions got from the GPS is put away in the Database. This information is additionally used to screen the speed at which the individual is driving. Data is kept up about every individual and if the individual crosses a limit speed he is ordered as a driver. These way engine insurance agencies can possibly give modified answers for their customers.

**Keywords--** Firebase, GPS, Android Studio, Speed calculation

### I. INTRODUCTION

Use the data collected by the Smartphone application to categorize the driver whether he is eligible or not eligible for motor insurance. Following driver conduct brings down upkeep costs, diminishes your vehicle's risk, and encourages you remunerate the correct drivers for their protected driving strategies. It likewise causes you center you're driving instructing endeavors around the drivers who need it most; notwithstanding pinpointing what zones they explicitly need to work on. No all the more pulling great drivers off the street for superfluous exercises; you know precisely who should be there and who could be out making conveyances.

Utilizing observing framework, chiefs can screen their vehicles and increment the wellbeing of their drivers. Alarms can be set for over speeding, cruel driving and it will educate the directors when a worker drives recklessly. Directors can respond to these circumstances and can keep mishaps from happening. The checking framework additionally gives the drivers intend to raise a caution on the off chance that they end up in any risk. GPS vehicle observing framework can help insurance agencies to improve their client administration. For instance: Office staff can educate directors about the driver if the vehicle is going quick. Likewise, they can react to client inquiries viably. As the representatives present in the workplace have the office to see constant information of driver vehicles, they can distinguish rapidly which vehicle will be most appropriate to go to a client. They are additionally ready to give quick answer and better support of the clients. GPS vehicle checking framework diminishes the measure of administrative work that drivers need to round out. As the checking framework gives point by point data on the

whereabouts of the vehicle, drivers need not enter it on records. This framework builds the exactness of records.

### II. VEHICLE SPEED CONTROL SYSTEM USING GSM/GPRS

The work is an undertaking to control the speed of the vehicle arranged with PC programming to engage the untouchable or owner to get the region, speed and activity of the driver. To achieve this, the structure can transmit the information logically. The usage of GSM/GPRS advancements allows the framework to follow the articles and give the state-of-the-art information. This information is endorsed to unequivocal customers over the web as the server gets the information. It is the tele-checking structure to transmit data to the remote customer. As needs be the applications are used persistently traffic surveillance. This paper proposes a model for territory following using Geographical Positioning Global System for Mobile Communication System and Global System for Communicate) development. The progression relies upon the windows phone 8 application by techniques it can give flexibility and transportability to the customer to get the information from wherever. As these GPS propels having progressively significant extent of frequencies, the customer can get the information as speedier as would be reasonable. This structure is useful to speed control at express traffic roads.

### III. LITERARY SURVEY

In this section of the related work we describe the existing system, the limitation of the existing system, the earlier version, current version, proposed version, and expected

## Article

# An Efficient and Secure Modified privacy data access control Scheme for Multi-Authority Cloud Storage

M.Sri Lakshmi<sup>1</sup>, Priyesh Kanungo<sup>1</sup>, Nirmal Dagdee<sup>2</sup>, Golla Madhu<sup>3</sup>

<sup>1</sup> Assistant professor, Dept of Computer Science and Engineering, G. Pullaiah College of Engineering and Technology, Kurnool, India

Email id: srilakshmi@gpcet.ac.in

<sup>2</sup> Department of Information Technology, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad 500090, India

Email id: privesh@vnr.ac.in

<sup>3</sup> Department of CSE, SRM University, Amaravati 522240, India

Email id: nirmal@srm.ac.in

**Abstract:** With continuous advancements in Internet technology and the increased use of cryptographic techniques, the cloud has become the obvious choice for data sharing. Generally, the data are outsourced to cloud storage servers in encrypted form. Access control methods can be used on encrypted outsourced data to facilitate and regulate access. Multi-authority attribute-based encryption is a propitious technique to control who can access encrypted data in inter-domain applications such as sharing data between organizations, sharing data in healthcare, etc. The data owner may require the flexibility to share the data with known and unknown users. The known or closed-domain users may be internal employees of the organization, and unknown or open-domain users may be outside agencies, third-party users, etc. In the case of closed-domain users, the data owner becomes the key issuing authority, and in the case of open-domain users, various established attribute authorities perform the task of key issuance. Privacy preservation is also a crucial requirement in cloud-based data-sharing systems. This work proposes the SP-MAACS scheme, a secure and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing. Both open and closed domain users are considered, and policy privacy is ensured by only disclosing the names of policy attributes. The values of the attributes are kept hidden. Characteristic comparison with similar existing schemes shows that our scheme simultaneously provides features such as multi-authority setting, expressive and flexible access policy structure, privacy preservation, and scalability. The performance analysis carried out by us shows that the decryption cost is reasonable enough. Furthermore, the scheme is demonstrated to be adaptively secure under the standard model.

**Keywords:** electronic health records; access control; cloud storage; attribute-based encryption; multiple authorities; privacy preservation



**Citation:** Gupta, R.; Kanungo, P.; Dagdee, N.; Madhu, G.; Sahoo, K.S.; Jhanjhi, N.Z.; Masud, M.; Almalki, N.S.; AlZain, M.A. Secured and Privacy-Preserving Multi-Authority Access Control System for Cloud-Based Healthcare Data Sharing. *Sensors* **2023**, *23*, 2617. <https://doi.org/10.3390/s23052617>

Academic Editor: Paul Davidsson

Received: 28 November 2022

Revised: 14 February 2023

Accepted: 21 February 2023

Published: 27 February 2023



**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

The modern health industry is adopting Internet of Things (IoT) technology for providing advanced healthcare services [1]. A wide range of IoT devices and applications are designed for healthcare needs, e.g., sensors, remote healthcare monitoring applications, telemedicine consultation applications, etc. Healthcare organizations can collect, record, and monitor patient data regularly, providing them with adequate treatment in every situation. Patients can be treated well in emergencies by making use of their electronic



## Secure Data Deduplication in Cloud

<sup>1</sup>M.Sri Lakshmi .R, <sup>2</sup>Pavithra G. S

*Assistant Professor, Dept of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology, Kurnool, India*

<sup>2</sup>Department of CSE, SJBIT,

[srilakshmi@gpct.ac.in](mailto:srilakshmi@gpct.ac.in),

[pavi.pgs@gmail.com](mailto:pavi.pgs@gmail.com)

### ABSTRACT

*Deduplication is a process that eliminates redundant copies of data and reduces storage overhead. Data deduplication becomes more and more a necessity for cloud storage providers because of the continuous and exponential increase in the number of users and the size of their data. Storage and data transfer costs will be reduced by their cloud providers by storing a unique copy of duplicate data. Cloud computing offers a new way of service provision by re-arranging various resources over the Internet. The most often known, important and popular cloud service is data storage. The privacy of data holders are more important, so in order to preserve the privacy of the data holders, data is often stored in the cloud in an encrypted form. In cloud data deduplication, encrypted data will introduce new challenges, which becomes crucial for data storage and processing in the cloud. There are some of the traditional schemes for deduplication that cannot work on encrypted data. Some of the Existing solutions are present for encrypted data deduplication which suffers from security weakness i.e. brute force attacks means they cannot flexibly support data access control and revocation. Therefore, few of them can be readily deployed in practice. In this paper, we propose a scheme to deduplicate the encrypted data which is stored in the cloud. And also we use RAS and AES algorithm for encryption and hash code generation the results show the sequence diagram over deduplication process and test cases for login purpose, especially for data deduplication in cloud storage.*

**Keywords:** *Deduplication, Encryption Technique, Decryption Technique.*

---

### I. INTRODUCTION

Cloud providers offer potentially infinite storage space, where users can use as much space as they can and vendors constantly look for techniques which aimed to minimize redundant data (multiple copies) and maximize space savings. To minimize redundant data that is the elimination of multiple copies, we make use of deduplication technique. The most widely adopted technique is Cross-user deduplication. The simple idea behind deduplication is to store duplicate Data only once.

Therefore, if a user wants to upload a data which is already stored in the cloud, the cloud provider will show deduplication not allowed. Deduplication can reduce storage needs by up to 90-95% for backup applications [11] and up to 68% in standard file systems [23]. Users require the protection of their data and confidentiality along with low ownership costs and flexibility which guarantees through encryption. Unfortunately, deduplication and encryption are two conflicting technologies. While the aim of deduplication is to detect duplicate data and store them only once, the result of encryption is to make two identical data indistinguishable after being encrypted. This means that if data are encrypted by users in a standard way, the cloud storage provider cannot apply deduplication since two identical data will be different after encryption. On the other hand, confidentiality cannot be guaranteed and data are not protected against attackers in cloud storage providers if data are not encrypted by users. convergent encryption.

Convergent encryption is a technique which has been proposed to meet these two conflicting requirements [18], [25], [26] whereby the encryption key is usually the result of the hash of the data. If we want to achieve confidentiality and deduplication at the same time, convergent encryption seems to be a good candidate but unfortunately, it suffers from various well-known weaknesses [15], [24]. Here we mainly focus on deduplication and cloud storage. Cloud computing offers a new way of Information Technology services by re-arranging various resources (e.g., storage, computing) and providing them to users based on their demand





## Train Bot: Chatbot for Railways

R.VaraPrasad\*, Kameshwar S\*\*,

\*Assistant Professor, Department of Computer Science and Engineering, G.Pulliah Engineering College,  
Kurnool, India.

Email id: rvaraprasad@gpcet.ac.in

\*\* (Assistant Professor, Department of Information Technology, Sri Manakula Vinayagar Engineering College,  
Madagadipet, Puducherry.

Email id: kameshwar@manakula.ac.in

### ABSTRACT

In all forms of on-line communications, so far noticed that no bots can imitate what a human can do. Chatbot is a program that provides an interaction with the chat services to automate tasks for the humans, Chatbot can provide 24X7 service to user. Chatbot acts like routing agent that can be used to classify user's context in conversation. Chatbots are aided with Natural Language Processing (NLP) which is used to examine the request and draw out some keyword information's based on the keywords that the Chatbot provides, thus the Railway reservation bot gives details such as number of seats available each class, source and destination with time. Chatbot also provides word suggestion which can be used to find train name, source and destination name etc..., which aids the user for better conversation.

**Keywords** - : Artificial Intelligence, chatbot, NLP, Railway reservation, SQL.

Date of Submission: 20-03-2020

Date Of Acceptance: 06-04-2020

### I. INTRODUCTION

In the current survey , the chatbot are utilized by many humans's . In that what are the blessings and downsides and disadvantages, we will see this inside the survey. In the chatbot Artificial Intelligence is used, and strategies are mentioned on this survey. Chat bots or Virtual Assistants have been designed to simplify the interplay among computer systems and humans and feature hit the market.

We can note that through now Chatbots discover software in all types of on-line verbal exchange and to automate the human procedure. The generation is changed and advanced. Computers are quicker and smart telephones are to be had to each person. Numerous net offerings provide ubiquitous connections amongst human beings, information and software program. Large quantities of human understanding are gathered and available. Due to the growing amount of information, techniques for automatic reading that information has end up an essential studies subject matter. While examine modern-day chat-bots and nation that any system, gadget or application (chat-

bot) showing a few, however now not all basics of intelligence are a Partially Intelligent System. Therefore, chat-bots are Partially Intelligent Systems. Moreover, nowadays's device intelligence is significantly confined to the limits of Partial Intelligence.

In order to achieve the automation procedure for railway ticket reservation. The consumer performs the booking operation through the communicate or with voice enter to the bot. The bot offers the word notion the usage of N-gram module. Then the bot performs tokenization Chatbot splits the check enter into numerous small tokens or key-word consistent with the key-word the Chatbot executes the unique handler. After the reservation process then it performs price movement the usage of the fee APIs and additionally in FAQ mode the chat bot replies for the user queries using the IE (Information Extraction) approach.

### II. RELATED WORKS

#### A. Anatomy and Utilities of an Artificial Intelligence Conversational Entity

In this paper, we going to look approximately the SARANG Bot and FUTURE

# Explorations of Data Visualization Techniques for Business Analytics

R.VaraPrasad<sup>1</sup>

C.K.Indira<sup>2</sup>

V.VenuGopal<sup>3</sup>

<sup>1</sup>Dept of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology,  
Kurnool, India

Email id: rvaraprasad.@gpcet.ac.in@,

<sup>2</sup>Department of CSE, SJBIT, Bengaluru, India

Email id: [indusmiles09@gmail.com](mailto:indusmiles09@gmail.com)

<sup>3</sup>Department of CSE, RGM College of Engineering and Technology, Nandyal, Kurnool,India

Email id: venugopal17@gmail.com

The Big Data era has realized the availability of a great amount and variety of datasets for analysis by non-corporate data analysts, such as research scientists, data journalists, policy makers, SMEs and individuals. They are characterized by high volumes which make traditional database and system infrastructure incapable of efficiently storing and processing them; they are accessible in very different, usually raw formats (e.g., plain text, json, rdf); they are generated or modified in high rates, and they exhibit different levels of data quality and schema representations. The level of difficulty in transforming a data-curious user into someone who can access and analyze that data is even more burdensome now for a great number of users with little or no support and expertise on the data processing part. The goal of visual data exploration and analysis is to facilitate information perception and manipulation, knowledge extraction and inference by non- expert users. The visualization techniques, used in a variety of modern systems, provide users with intuitive means to interactively explore the content of the data, identify interesting patterns, infer correlations and causalities, and supports sense-making activities that are not always possible with traditional data traditional data analysis techniques.

Several challenges arise in the field of information visualization and data management, due to the new Big Data characteristics. First, the modern exploration and visualization systems should offer scalable data management techniques in order to efficiently handle billion objects datasets, limiting the system response in a few milliseconds. Nowadays systems must, also, address the challenge of on-the-fly scalable visualizations over

---

\* Special Issue on “*Big Data Exploration, Visualization and Analytics*”, Big Data Research, Elsevier, 2019

Review

# A Survey on Video Surveillance Using Artificial Intelligence

<sup>1</sup>R.Vara Prasad, <sup>2</sup>Aakanksha Ramesh Jadhav, <sup>3</sup>Aditya Ramesh Jadhav<sup>1</sup>Assistant Professor, Dept of Computer Science and Engineering, G. Pullaiah Engineering College, Kurnool, India

Email id: varaprasad@gpcet.ac.in

<sup>2</sup>Assistant Professor, Dept of Computer Science and Engineering, G.Pullareddy Engineering College, Kurnool, India

Email id: ramesh@gprec.ac.in

<sup>3</sup>Assistant Professor, Dept of Computer Science and Engineering, RGM Engineering College, Kurnool, India

Email id: adithya@rgm.ac.in

**Abstract:** Surveillance cameras have recently been utilized to provide physical security services globally in diverse private and public spaces. The number of cameras has been increasing rapidly due to the need for monitoring and recording abnormal events. This process can be difficult and time-consuming when detecting anomalies using human power to monitor them for special security purposes. Abnormal events deviate from normal patterns and are considered rare. Furthermore, collecting or producing data on these rare events and modeling abnormal data are difficult. Therefore, there is a need to develop an intelligent approach to overcome this challenge. Many research studies have been conducted on detecting abnormal events using machine learning and deep learning techniques. This study focused on abnormal event detection, particularly for video surveillance applications, and included an up-to-date state-of-the-art that extends previous related works. The major objective of this survey was to examine the existing machine learning and deep learning techniques in the literature and the datasets used to detect abnormal events in surveillance videos to show their advantages and disadvantages and summarize the literature studies, highlighting the major challenges.

**Keywords:** video surveillance; abnormal events; anomaly detection; artificial intelligence



**Citation:** S, engönül, E.; Samet, R.; Abu Al-Haija, Q.; Alqahtani, A.; Alturki, B.; Alsulami, A.A. An Analysis of Artificial Intelligence Techniques in Surveillance Video Anomaly Detection: A Comprehensive Survey. *Appl. Sci.* **2023**, *13*, 4956. <https://doi.org/10.3390/app13084956>

Academic Editor: Ke Gu

Received: 2 March 2023

Revised: 5 April 2023

Accepted: 12 April 2023

Published: 14 April 2023



**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

The use of surveillance cameras in private and public spaces has become increasingly prevalent in recent years for various purposes, including tracking, monitoring, and preventing violations. An anomaly, as defined in the surveillance field, refers to a deviation from common rules, types, arrangements, or forms and can be characterized as an uncommon event that deviates from “normal” behavior.

Detecting anomalies in surveillance videos is crucial to maintaining security in various applications, such as crime detection, accident detection, abandoned object detection, illegal activity detection, and parking area monitoring. However, the manual detection of anomalies in surveillance videos is a tedious and labor-intensive task for humans. This is due to the large amount of data generated by critical systems in security applications, making manual analysis an impractical solution.

In recent years, there has been a significant increase in the demand for automated systems for detecting video anomalies. These systems include biometric identification of individuals, alarm-based monitoring of Closed-Circuit Television (CCTV) scenes, automatic detection of traffic violations, and video-based detection of abnormal behavior [1].



# **Sanskrit: A Platform for Computer Programming Languages and AI**

**P.RamaRao<sup>1</sup> and Raghav Agrawal<sup>2</sup>**

*Assistant Professor, Dept of Computer Science and Engineering, G. Pullaiah College of Engineering and Technology, Kurnool*

*Email id: pramarao@gpcet.ac.in.*

*Assistant Professor, Dept of CSE, RGM College of Engineering and Technology, Nandyal, Kurnool*

*Email id: raghav@rgm.ac.in.*

## **Abstract**

In this paper represents the work toward developing a dependency parser for Sanskrit language and also represents the efforts in developing a NLU(Natural Language Understanding) and NLP(Natural Language Processing) systems. Here, we use ashtadhayayi (a book of Sanskrit grammar) to implement this idea. We use this concept because the Sanskrit is an unambiguous language. In this paper, we are presenting our work towards building a dependency parser for Sanskrit language that uses deterministic finite automata(DFA) for morphological analysis and 'utsarga apavaada' approach for relation analysis. The importance of astadhayayi is it provide a grammatical framework which is general enough to analyze other language as well therefore it is uses for language analysis.

**Keyword:** Panani Ashtadhayayi, Vibhakti, Karaka, NLP, Sandhi.

## **1. Introduction**

Parsing is the process of analyzing a string of symbols either in natural language or computer languages according to the rule of formal grammar. Determine the functions of words in the input sentence. Getting an efficient and unambiguous parse of natural languages has been a subject of wide interest in the field of artificial intelligence over past 50 years. Most of the research have been done for English sentences but English has ambiguous grammar so we need a strong and unambiguous grammar which is provided by maharishi Panini in the form of astadhayayi. Briggs(Briggs, 1985) demonstrated in his article the silent feature of Sanskrit language that can make it serve as an artificial language. The computational grammar described here takes the concept of vibhakti and karaka relations from Panini framework and uses them to get an

## **The Creative Idea of Replicating the Human Brain as a Virtual Brain-Blue Brain**

<sup>1</sup>C. Praveen, <sup>2</sup>Aakanksha Ramesh Jadhav, <sup>3</sup>Aditya Ramesh Jadhav

<sup>1</sup>Assistant Professor, Dept of Computer Science and Engineering, G. Pullaiah Engineering College, Kurnool, India

Email id: praveen@gpcet.ac.in

<sup>2</sup>Assistant Professor, Dept of Computer Science and Engineering, G.Pullareddy Engineering College, Kurnool, India

Email id: ramesh@gprec.ac.in

<sup>3</sup>Assistant Professor, Dept of Computer Science and Engineering, RGM Engineering College, Kurnool, India

Email id: adithya@rgm.ac.in

---

### **ABSTRACT:**

Technology is progressing at an unprecedented pace, and one notable endeavor is IBM's pursuit of the Blue Brain project, aiming to create a virtual brain. Blue Brain stands as the world's first virtual brain, a revolutionary concept seeking to replicate the cognitive abilities of the human brain through artificial intelligence. The essence of the Blue Brain project lies in the creation of a virtual brain that continues to function even after an individual's physical demise. This virtual brain will preserve and harness a person's information, intelligence, personality, emotions, and memories, contributing to the advancement of human society. The ultimate objective of this research is to enable the uploading of the human brain into a machine. The initial strategy for achieving this ambitious goal involves reverse-engineering the mammalian brain.. The outcome will be a functional, three-dimensional model capable of replicating the rapid electrochemical exchanges occurring within the brain. This modeling encompasses various aspects of brain functionality, including the understanding of brain dysfunctions such as mental conditions like depression and autism, as well as cognitive abilities like language, learning, perception, and memory. Subsequently, the scope of modeling will extend to cover additional brain regions.

**Keywords:** *Supercomputer, Blue Gene, Nanotechnology, Robotics, Virtual Machine, Brain Simulation*

### **1. Introduction:**

The human brain stands as a testament to the exquisite marvels of creation, often deemed as God's most precious gift to humanity. It is this remarkable organ that distinguishes humans as intelligent beings, enabling them to decode and respond to the intricate web of impulses that carry information. However, a profound dilemma arises upon the demise of the human body, as the wisdom and knowledge contained within the brain are irretrievably lost. One cannot help but ponder the potential benefits that this reservoir of knowledge could have bestowed upon the growth and progress of

# Mitigate Cloud Threats: Step-by-Step Process of Threat Modeling

P. Kiran Rao

*Abstract*—Cloud infrastructure presents new paradigms in efficiency and economy, but also bring along a new threat surface for cyber defenders to contend with. Each unique cloud computing model varies the characteristics of the cloud platform when compared to the traditional on-premise computing network. Characteristics such as shared security responsibility between the cloud provider and tenant, reduced levels of cyber visibility and response capability, on-demand computing resources, cloud-based and more complex identity and access management, and various other characteristics impact the results of applying a threat model to the cloud computing platform. Thus, the threat modeling of cloud platforms must consider a new model of shared responsibility. The threat model should recognize an approach that requires the end user to explicitly trust the cloud service provider in their respective areas of responsibility, and must consider new or modified threats. Organizations migrating their computer network from a more traditional on-premise system to cloud-based services must consider the classes of threats that any computer network faces, but also the impacts resulting from cloud unique characteristics. In this paper, we select and apply a threat model to a cloud platform. Specific cloud unique characteristics are identified, and discussions on their impact to the threat model results are described.

*Keywords*—cloud computing, cyber security, cyber threat

## I. INTRODUCTION

The ongoing trend in government, defense, and industry is one that sees the migration of enterprise services to cloud-space. In enterprise networks, visibility into the information system is granted through touch-points owned and operated by the organization and their network defenders. As a tried-and-true paradigm, this approach may produce vast swaths of host/network data, coupled with trending and threat feeds, to provide granular visibility and context about the state of the network, its users, and extant maliciousness. With cloud computing, the underlying infrastructure is removed from the lens, leading to blind spots for which the user or responder may have no visibility of breaches [1][2]. This addition of cloud devices/ architecture into a network, adds a new threat surface and increases the amount of information and data to monitor for maliciousness.

---

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

We opine that security systems meant to protect infrastructure and data should be specified based on *threat profiles*. By quantifying threat and risk, we can show how attacks are ranked (via analysis/visualization), and what/how defenses protect the system or increase the work-factor for an adversary.

So, as organizations migrate either all or a part of their computing applications to the public cloud, they face different and additional security challenges when compared to their on-premise computing network system. Additional threats the organization faces when migrating to the cloud can be discovered by applying a threat model to the cloud computing environment.

In Section II, we discuss the differences in cloud computing versus on-premises computing, with regard to the nuances that prohibit traditional enterprise security from being adequately used on a cloud platform. In Section III, we build the discussion points from Section II to define a threat model for the cloud. We then conclude the paper in Section IV.

## II. CLOUD COMPUTING VS. ON-PREMISE COMPUTING

In this section we discuss key cloud computing characteristics that differentiate cloud computing from traditional on-premise computer networks. This group of cloud characteristics is not exhaustive; however, their generality is sufficient to encompass many other security concerns for cloud computing—all of which should be considered when applying a threat model.

### A. Shared Responsibility Model for Cloud Security

A public cloud is comprised of similar computing resources that an on-premises data center is comprised of, including computing hardware (e.g., processors and storage), operating systems, and software, all of which have vulnerabilities. With the cloud location being remote, the tenant cannot be expected to handle all security roles and responsibilities. Additionally, the cloud compute resources are shared among multiple tenants. Thus the cloud service provider (CSP) must provide security of the compute resources, and also must secure the software components shared among different tenants. The CSP must secure cloud tenant data from an attacker, but also protect data from being exposed to other users and tenants. Depending on the cloud model used, the CSP security responsibility may include more layers of the software stack. Data and identify protection and, in cases, application software are the responsibility of the tenant. Thus in cloud computing,



# HOSTEL MANAGEMENT SYSTEM USING ENSEMBLE LEARNING

P Kiran Rao

<sup>1,2,3</sup>CSE Department, GPCET (affiliated to JNTUA, Anantapur), Kurnool, India

Abstract - There is an unprecedented increase in the no. of educational institutions founded throughout the world in particular during the last decade. The growth has taken education to people's doorstep. As a result, it is increasing education and helped to create the number of educated citizens who can easily accept rules of society which is civilized and make a meaningful contribution. However, the majority of newly established educational institutions use the old traditional techniques to manage their properties, particularly hostel facilities. Such old techniques with their inherent limitations have had a negative impact on this educational system's overall operational performance. This paper proposes the creation of an integrated system for managing hostel accommodation. The algorithms for the automated system is developed using Visual Basic, and the underlying database was developed with Microsoft Access. It also has authentication algorithm built in to prevent unauthorized access. The developed framework overcomes the drawbacks of conventional hostel management methods; with access control systems, it is more user-friendly, graphical-user-oriented, robust, efficient, and safe.

Keywords - Video, Surveillance, A.I, Footages, Machine Learning, Programs, Humans.

## 1. INTRODUCTION

Basic economic theories argue that an organization's success depends on how well it will harness and optimizes the production factors to achieve its organizational goals. We say the logical resources by the means of money. Physical resources are property, labor / machine, money, and entrepreneurship while knowledge is the intellectual tool. Regardless of the amount of fund that could has gone to a project, if efforts / resources are not properly orchestrated, the whole investment will be wasted and the dream of the people will not be accomplished. Thus management is one of the major factors evaluating an organization's performance index in its attempt to achieve its corporate goals. Furthermore, research has shown that the standard of initiative implemented in management is what matters. Through programs we meet the models, theories, scientifically validated.

Keywords: Hostel management visual basic context level DFD access management mechanism approach or algorithm applied to the management of resources. Once applied to physical and logical resources allocation and management, appropriate, programming rule etc have well-tried terribly helpful. Our analysis work mentioned here is proscribed to academic establishments. In an endeavor to satisfy the

challenges facing the growing population in countries round the world, government and personal investors have joined the academic sector to line up higher learning establishments.

An integral part of facility created on the market in such establishments area unit hostel accommodation areas for college students to form an educational community which is able to facilitate efficient refinement and development of scholars.

Clearly, the normal method of running and maintaining host el in institution is not successful as it looks due to the followi ng challenges: difficulty in record keeping data retention, diff iculty in data updating; diffiulty in data recovery; difficulty in producing information about the students who left the hoste l, to manipulation / human error; difficulty in manipulation / data recovery. The entire exercise is time-consuming and a waste of resources, both human and material. The system proposed provides a solution to the traditional method of handling the hostel facilities. The system is trying to develop the hostel facilities of institutions for stakeholders the hostel administrator, management and students. This automates the administrative processes and reduces the stress associated with finding information in a set of registers about a student / facility. It is designed specifically for centrally allocating and controlling accommodation spaces in a complex student hostel. The device owner has the details of students who left the hostel and search from the database of all the current students within few seconds. At the time of room allocation, the student staying in the hostel will be identified by the SID number given to him. This program will calculate the bills and issues updates automatically to the students. It also keeps records and produce letters to discipline the students who do not follow regulations and rules.

The program has a special approach to information collection that is critical. That makes the system proposed more stable, more effective and more efficient. The system's entire range includes multiple modules, transport scheduling and other administrative tasks.

Tracking output in the application of hostel accommodation framework may be well described. The program uses a mono central database to address the complexities of management of the student hostels and all admin functions.

The hostel management facility software is a user-friendly



## Cross Entropy Based Long Short Term Memory Recurrent Neural Network Model for Analyzing the Time Series on Stock Market Price

D. Jayanarayana

<sup>1</sup>*G Pullaiah College of Engineering and Technology (Autonomous),  
Department of Computer Science and Engineering, Kurnool, India*  
\* Corresponding author's Email: [djnreddy@gmail.com](mailto:djnreddy@gmail.com)

---

**Abstract:** In the financial stock market, a sequence of prices obtained from the share market with respect to the time series is usually examined. Generally, time series in finance, particularly shows importance in predicting investment in today's share market. Since there are too many factors such as public opinions, general economic conditions, or political events, vulnerability in the economy are directly or indirectly reflects on the evolution of financial time series. The desire of the investor is to predict the future stock prices neglecting whether the investor is a long-term investor or a day-trader. A major challenge is to develop and design an efficient predictive model that guides investors to make appropriate decisions. In this research work, Long Short Term Memory-Recurrent Neural Network (LSTM-RNN) is developed to overcome such disputes and contributing an efficient technique for predicting the future stock prices financially. In addition to the model, cross entropy is calculated using a Mutual Information feature selection model to minimize the optimization problems that create the time complexity in the system. The proposed LSTM-RNN has achieved best accuracy of 61.33% of prediction accuracy compared to state-of-the-art techniques.

**Keywords:** Cross entropy, Global financial crisis, Long short term model, Recurrent neural network, Stock market.

---

### 1. Introduction

The stock market is a place where the aggregation of both buyers and sellers happens in a single platform for offering shares to the general public. Meanwhile, the capital is raised on products needed for expansion of new operations [1]. During the past two decades, the stock market has been advanced as the main form of investment in numerous organizations as well as individuals for arranging huge investment funds [2]. As a result, many companies have been listed in stock markets around the world and investing a huge amount of their capital regularly. The time series analysis and topic modelling have been used in various applications such as the environment, the economy, health, and politics, even the social media. An overview of time series analysis of social media in different settings and focus areas were provided [3]. The traditional financial theory is a foundation for deciding the

effective market system that shows the investors are fully rational. The stock price in turn reflects all available information precisely at any time. The mood factors affect the judgment of investors and behaviour of investors that impact on the stock price in great demand. The investors sometimes overreact to good news when they are in a good mood or for bad news. Thus, investors tend to buy more or sell less stocks when they are in a good mood than they are in a bad mood, which causes the abnormal change in stock price [4]. In order to reduce the dimensionality of time series in univariate data, an Asynchronism Principal Component Analysis (APCA) was developed based on Dynamic Time Warping (DTW). ARIMA (Auto Regressive Integrated Moving Average) model was developed for the prediction of stock market movement. The Univariate time series models reduce the range of economical phenomena through the historical behaviour of a dependent variable. The accuracy



# Fake Profile Identification using Machine Learning

D. Jayanarayana Reddy

Mahatma Gandhi Institute of Technology, Computer Science and Engineering, Hyderabad, Telangana, India

\*\*\*

**Abstract** - In the present generation, the social life of everyone has become associated with online social networks. These sites have made a drastic change in the way we pursue our social life. Making friends and keeping in contact with them and their updates has become easier. But with their rapid growth, many problems like fake profiles, online impersonation have also grown. There are no feasible solutions exist to control these problems. In this paper, I came up with a framework with which the automatic identification of fake profiles is possible and is efficient. This framework uses classification techniques like Random Forest Classifier to classify the profiles into fake or genuine classes. As this is an automatic detection method, it can be applied easily by online social networks that have millions of profiles whose profiles cannot be examined manually.

**Key Words:** Social Media, Facebook, Random Forest Classifier, Classification, Framework, and Dataset.

## 1. INTRODUCTION

Social networking site is a website where each user has a profile and can keep in contact with friends, share their updates, meet new people who have the same interests. These Online Social Networks (OSN) use web2.0 technology, which allows users to interact with each other. Social networking sites are growing rapidly and changing the way people keep in contact with each other. The online communities bring people with the same interests together which makes users easier to make new friends.

### 1.1. History

These social networking sites starting with <http://www.sixdegrees.com> in 1997 then came <http://www.makeoutclub.com> in 2000. Sixdegrees.com couldn't survive much and closed very soon but new sites like myspace, LinkedIn, Bebo became successful and Facebook was launched in 2004 and presently it is the largest social networking site in the world.

### 1.2. Social Impact

In the present generation, the social life of everyone has become associated with online social networks. These sites have made a drastic change in the way we pursue our social life. Adding new friends and keeping in contact with them and their updates has become easier. Online social networks have an impact on science, education, grassroots organizing, employment, business, etc. Researchers have been studying these online social networks to see the impact they make on

the people. Teachers can teach the students easily through this making a friendly environment for the students to study, teachers nowadays teachers are getting themselves familiar with these sites bringing online classroom pages, giving homework, making discussions, etc. which improves education a lot. The employers can use these social networking sites to employ the people who are talented and interested in the work, their background check can be done easily using this. Most of the OSN is free but some charge the membership fee and uses this for business purposes and the rest of them raise money by using the advertising. This can be used by the government to get the opinions of the public quickly. The examples of these social networking sites are sixdegrees.com, The Sphere, Nexopia which is used in Canada, Bebo, Hi5, Facebook, MySpace, Twitter, LinkedIn, Google+, Orkut, Tuenti used in Spain, Nasza-Klasa in Poland, Cyworld mostly used in Asia, etc. are some of the popular social networking sites.

## 2. Objective

In today's online social networks there have been a lot of problems like fake profiles, online impersonation, etc. To date, no one has come up with a feasible solution to these problems. In this project, I intend to give a framework with which the automatic detection of fake profiles can be done so that the social life of people become secured and by using this automatic detection technique we can make it easier for the sites to manage the huge number of profiles, which can't be done manually.

## 3. LITERATURE SURVEY

Various fake record recognition methodologies depend on the investigation of individual interpersonal organization profiles, with the point of distinguishing the qualities or a combination thereof that help in recognizing the legitimate and the fake records. In particular, various features are extracted from the profiles and posts, and after that Machine learning algorithms are used so as to construct a classifier equipped for recognizing fake records.

For instance, Nazir et al. (2010) [1] describes recognizing and describing phantom profiles in online social gaming applications. The article analyses a Facebook application, the online game "Fighters club", known to provide incentives and gaming advantage to those users who invite their peers into the game. The authors contend that by giving such impetuses





# IoT: Distributed Data Service Functionalities

D. Jayanarayana Reddy

Received: 23 January 2021 / Accepted: 3 May 2021 / Published online: 19 May 2021  
© The Author(s) 2021

## Abstract

Widespread adoption of smart IoT devices is accelerating research for new techniques to make IoT applications secure, scalable, energy-efficient, and capable of working in mission-critical use cases, which require an ability to function offline. In this context, the novel combination of distributed ledger technology (DLT) and distributed intelligence (DI) is seen as a practical route towards the decentralisation of IoT architectures. This paper surveys DI techniques in IoT and commences by briefly explaining the need for DI, by proposing a comprehensive taxonomy of DI in IoT. This taxonomy is then used to review existing techniques and to investigate current challenges that require careful attention and consideration. Based on the taxonomy, IoT DI techniques can be classified into five categories based on the factors that support distributed functionality and data acquisition: cloud-computing, mist-computing, distributed-ledger-technology, service-oriented-computing and hybrid. Existing techniques are compared and categorized mainly based on related challenges, and the level of intelligence supported. We evaluate more than thirty current research efforts in this area. We define many significant functionalities that should be supported by DI frameworks and solutions. Our work assists system architects and developers to select the correct low-level communication techniques in an integrated IoT-to-DLT-to-cloud system architecture. The benefits and shortcomings of different DI approaches are presented, which will inspire future work into automatic hybridization and adaptation of DI mechanisms. Finally, open research issues for distributed intelligence in IoT are discussed.

**Keywords** Internet of Things (IoT) · Distributed intelligence (DI) · Cloud-computing · Mist-computing · Distributed-ledger technology · Service-oriented-computing · Hybrid

## Introduction

The Internet of Things or the IoT, is an emerging worldwide network of interconnected physical-heterogeneous smart objects (e.g., wearable-sensors, environmental sensors and connected devices) that are uniquely addressable, and are available through networking technologies such as WiFi, Bluetooth and others. By 2030, the study predicts that

IoT will rise exponentially, for example, by about 125 billion connected devices to the internet [1–3]. As a result, this poses several challenges in terms of providing timely delivery, data volume, speed, confidentiality and scalability [4, 5].

There are several features available for IoT applications: First, *sensing* the environment; Second, *communication* between objects for efficient data transfer; and Third, *computation* typically carried out to produce necessary raw data information.

The advent of the IoT enables a new paradigm that binds the physical objects on the Internet to form pervasive networks that allow sensing and medicating environments to respond to dynamic stimuli [6], often known as cyber-physical systems (CPS) [7]. IoT was also demonstrated by the Auto-ID centre that immediately recognises physical objects in the supply chain via radio-frequency identification RFID technology and electronic goods codes (EBC). These systems have shown the ability to improve the way of living by



# Cloud-Based Multimedia Content Protection System

**D. Jayanarayana Reddy**

## Abstract

In day to day life so many multimedia contents are created and uploaded in the Internet. It is easy to duplicate copyrighted multimedia materials. The paper presents a novel system for multimedia content protection on cloud infrastructures. These duplicated multimedia contents are illegally distributed over the Internet can result in significant loss of revenues for content creators. It is difficult to find out the illegally made multimedia contents copies made over the internet. In this paper a novel system for protection of multimedia contents on cloud infrastructures is presented. This system helps to protect different types of multimedia contents such as 2-D/3-D videos, audios, images etc., This system is based on cloud infrastructure which provides quick access to computing hardware and software resources. The components that are mainly included in this system are creating signatures of 3-D videos and the distributed index which is used to match multimedia objects.

**Keywords:** Copyright, Cloud Infrastructures, Internet, Index Multimedia, Signatures.

## 1. Introduction

Advances in processing and recording equipment of multimedia content as well as the availability of free online hosting sites have made it relatively easy to duplicate copyrighted materials such as videos, images, and music clips. Illegally redistributing multimedia content over the Internet can result in significant loss of revenues for content creators. Finding illegally-made copies over the Internet is a complex and computationally expensive operation, because of the sheer volume of the available multimedia content over the Internet and the complexity of comparing content to identify copies.

The system can be used to protect various multimedia content types, including regular 2-D videos, new 3-D videos, images, audio clips, songs, and music clips. The system can run on private clouds, public clouds, or any combination of public-private clouds. Our design achieves rapid deployment of content protection systems, because it is based on cloud infrastructures that can quickly provide computing hardware and software resources. The design is cost effective because it uses the computing resources on demand. The design can be scaled up and down to support varying amounts of multimedia content being protected. The proposed system is fairly complex with multiple components, including: (i) crawler to download thousands of multimedia objects from online hosting sites, (ii) signature method to create representative fingerprints from multimedia objects, and (iii) distributed matching engine to store signatures of original objects and match them against query objects.

The problem of protecting various types of multimedia content has attracted significant attention from academia and industry. One approach to this problem is using watermarking, in which some distinctive information is embedded in the content itself and a method is used to search for this information in order to verify the authenticity of the content.



All content following this page was uploaded by [Boddu Thirumala Rao](#) on 17 January 2021.

The user has requested enhancement of the downloaded file.

# Big Data based Security Analytics Approach for Finding the Advanced in Virtualized Infrastructures

M. Janardhan

**Abstract**—Cloud computing has Virtualized infrastructure become a target for cyber attackers to launch advanced attacks. This Project proposes a big data based security analytics approach to detecting advanced attacks in virtualized infrastructures. Network logs and user application logs collected periodically from the guest virtual machines (VMs) are stored in the Hadoop Distributed File System (HDFS). Then, extraction of attack features is performed through graph-based event correlation and Map Reduce parser based identification of potential attack paths. Next, determination of attack presence is performed through two-step machine learning, namely logistic regression is applied to calculate attack's conditional probabilities with respect to the attributes, and belief propagation is applied to calculate the belief in existence of an attack based on them.

**Index Terms**—Virtualized infrastructure, virtualization security, cloud security, malware detection, security analytics, event correlation, logistic regression, belief propagation

## 1. Introduction

A virtualized infrastructure consists of multiple virtual machines (VMs) that are depend upon the software-defined multi-instance resources of the hosting hardware. The virtual machine monitor, also called hypervisor, sustains, regulates and manages the software-defined multi-instance architecture. The ability to pool different computing resources as well as enable on-demand resource scaling has led to the widespread deployment of virtualized infrastructures as an important provisioning to cloud computing services.

Existing security approaches to protecting virtualized infrastructures generally include two types, namely malware detection and security analytics. Malware detection usually involves two steps, first, monitoring hooks are placed at different points within the virtualized infrastructure, then a regularly-updated attack signature database is used to determine attack presence. While this allows for a real-time detection of attacks, the use of a dedicated signature database makes it vulnerable to zero-day attacks for which it has no attack signatures.

Security analytics applies analytics on the various logs which are obtained at different points within the network to determine attack presence. By leveraging the huge amounts of logs generated by various security systems (e.g., intrusion detection systems (IDS), security information and event management (SIEM), etc.), applying big data analytics will be able to detect attacks which are not discovered through signature- or rule-based detection methods. While security analytics removes the need for signature database by using event correlation to detect previously undiscovered attacks, this is often not carried out in real-time and current implementations are intrinsically non-scalable.

To overcome these limitations, in this paper we propose a novel big data based security analytics (BDSA) approach to protecting virtualized infrastructures against advanced attacks. By making use of the network logs as well as the user application logs collected from the guest VMs which are stored in a Hadoop Distributed File System (HDFS), our BDSA approach first extracts attack features through graph-based event correlation, a MapReduce parser based identification of potential attack paths and then ascertains attack presence through two-step machine learning, namely logistic regression and belief propagation.

The remainder of the paper is arranged as follows. Section 2 presents a review upon the existing security approaches. Section 3 proposes our big data based security analytics (BDSA) approach. Experimental evaluations are presented in Section 4, while Section 5 discusses our BDSA approach in contrast with the related work. Section 6 draws the conclusion.

## 2. Literature Review

### 2.1 Malware detection in virtualised infrastructure

Malware refers to any executable which is designed to compromise the integrity of the system on which it is run. There are two prominent approaches to malware detection in cloud computing, namely in-VM and outside-VM inter-working approach and hypervisor-assisted malware detection.



**International Journal of Research**  
Available at <https://edupediapublications.org/journals>

e-ISSN: 2348-6848  
p-ISSN: 2348-795X  
Volume 05 Issue 17  
July 2018

---





# Sensor-based datasets for Human Activity Affirmation

M. Srilakshmi

**ABSTRACT** The research area of Ambient Assisted Living (AAL) has led to the development of Activity Recognition Systems (ARS) based on Human Activity Recognition (HAR). These systems improve the quality of life and the health care of the elderly and dependent people. However, before making them available to end users, it is necessary to evaluate their performance in recognising Activities of Daily Living (ADL), using dataset benchmarks in experimental scenarios. For that reason, the scientific community has developed and provided a huge amount of datasets for HAR. Therefore, identifying which ones to use in the evaluation process and which techniques are the most appropriate for prediction of HAR in a specific context is not a trivial task and is key to further progress in this area of research. This work presents a Systematic Review of Literature (SRL) of the sensor-based datasets used to evaluate ARS. On the one hand, an analysis of different variables taken from indexed publications related to this field was performed. The sources of information are journals, proceedings and books located in specialised databases. The analysed variables characterise publications by year, database, type, quartile, country of origin and destination, using scientometrics, which allowed identification of the dataset most used by researchers. On the other hand, descriptive and functional variables were analysed for each of the identified datasets: occupation, annotation, approach, segmentation, representation, feature selection, balancing and addition of instances, and classifier used for recognition. This paper provides an analysis of the sensor-based datasets used in HAR to date, identifying the most appropriate dataset to evaluate ARS and the classification techniques that generate better results.

**INDEX TERMS** Ambient Assisted Living – AAL, Human Activity Recognition – HAR, Activities of Daily Living – ADL, Activity Recognition Systems – ARS, dataset.

## I. INTRODUCTION

The care of elderly dependent people who have difficulties to effectively develop ADL requires a lot of attention and dedication, because both the lifestyle and the health state of these people are affected. The proliferation of problems associated with dementia in older adults between 74 and 84 years of age [1] constitutes one of the main public health challenges worldwide. Due to this fact, secondary problems are generated that affect mental, physical and mobility capabilities [2-4]. In addition, there is a decline in basic

communication skills, such as writing, speaking and performing simple and complex motor activities (cooking, taking medications and paying bills, among others) [5].

Nowadays, there has been a growing need for society to take care of their health integrating the use of technology. HAR enables monitoring of people's quality of life and more features and functionalities arise in this area over time, relying on a wide repertoire of hardware and software components. The research area of AAL has influenced the generation of reminder solutions, as a support for people

Article

# Multi-Factor Authentication Approach for Secure Access Cloud Services

K. Lakshmi



- <sup>1</sup> Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakaka 72388, Saudi Arabia; mkelfaki@ju.edu.sa
- <sup>2</sup> Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka 72388, Saudi Arabia; maismail@ju.edu.sa (M.E.); mfalruily@ju.edu.sa (M.A.); ehamouda@ju.edu.sa (E.H.); 431100004@ju.edu.sa (M.A.)
- <sup>3</sup> Computer Science Department, Faculty of Computers and Informatics, Zagazig University, Zagazig 44511, Egypt; wmohamed@taibahu.edu.sa
- <sup>4</sup> Computer Science Department, College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia
- \* Correspondence: amhassane@ju.edu.sa

**Abstract:** Cloud multi-factor authentication is a critical security measure that helps strengthen cloud security from unauthorized access and data breaches. Multi-factor authentication verifies that authentic cloud users are only authorized to access cloud apps, data, services, and resources, making it more secure for enterprises and less inconvenient for users. The number of authentication factors varies based on the security framework's architecture and the required security level. Therefore, implementing a secured multi-factor authentication framework in a cloud platform is a challenging process. In this paper, we developed an adaptive multi-factor multi-layer authentication framework that embeds an access control and intrusion detection mechanisms with an automated selection of authentication methods. The core objective is to enhance a secured cloud platform with low false positive alarms that makes it more difficult for intruders to access the cloud system. To enhance the authentication mechanism and reduce false alarms, multiple authentication factors that include the length, validity, and value of the user factor is implemented with a user's geolocation and user's browser confirmation method that increase the identity verification of cloud users. An additional AES-based encryption component is applied to data, which are protected from being disclosed. The AES encryption mechanism is implemented to conceal the login information on the directory provider of the cloud. The proposed framework demonstrated excellent performance in identifying potentially malicious users and intruders, thereby effectively preventing any intentional attacks on the cloud services and data.

**Keywords:** cloud authentication; multi-factor authentication; authentication factors; cloud intrusion detection; user behavior

## 1. Introduction

Cloud authentication verifies user identities across a cloud platform to determine whether the user is trusted to access cloud applications, data, services, and resources by ensuring access rights and privileges. The lack of strong and appropriate cloud authentication techniques leads to the occurrence of some cloud security threats and attacks. Some of the most common cloud threats are information disclosure, Denial-of-Service (DoS), spoofing identity, data tampering, repudiation, account hijacking, and the elevation of privilege [1,2]. Cloud-based authentication attacks include DoS attacks, Man-in-the-Middle (MITM) attacks, Replay attacks, Cloud Malware Injection attacks, Password Discovery



# Rain Technology

D. K. Sreenivasulu

**Abstract:** New emerging technology coming to the expansion of the internet named Reliable array of independent nodes. Before this rain technology we can use the cluster technology in which we have number of nodes and it is not easy to maintain the connection of all these nodes but in rain technology we are capable of providing the solution by reducing the number of nodes in the chain linking the client and server in addition to making the current nodes more robust and more autonomous. One implementation done for this was RAIN-Reliable Array Of Independent Nodes developed by the California Institute of Technology, in collaboration with NASA Jet Propulsion Laboratory and the Defense Advanced Research Projects Agency (DARPA).The technology is implemented in a distributed computing architecture, built with inexpensive off-the-shelf components. The RAIN platform involves heterogeneous cluster of nodes linked using many interfaces to networks configured in fault-tolerant topologies.

**Keywords:** RAIN, NASA, SNOW, RAINWALL

## I. INTRODUCTION

RAIN technology originated in a research project at the California Institute of Technology (Caltech), in collaboration with NASA's Jet Propulsion Laboratory and the Defense Advanced Research Projects Agency (DARPA). The name of the original research project was RAIN, which stands for Reliable Array of Independent Nodes. The objective of the RAIN is to recognize and make key building blocks for reliable distributed systems built using reasonably priced off-the-shelf components .RAIN technology also offers the new feature of reinstating an out of order node by a new one thus keeping away from the break in information flow [1][2]. The main purpose of the RAIN project was to identify key software building blocks for creating reliable distributed applications using off-the-shelf hardware. The focus of the research was on high-performance, fault-tolerant and portable clustering technology for space-borne computing. RAIN Technology (Redundant/reliable array of inexpensive/independent nodes) is a heterogeneous collection of nodes called clusters linked through numerous interfaces to networks configured in fault-tolerant topologies. The RAIN technology concentrates on developing high - performance, fault-tolerant, portable clustering technology .RAIN technology was capable to proffer the solution by lessening the number of nodes in the chain connecting the client and server .apart from this it also facilitates in making the current nodes of client-server architecture more robust [3].

## II. WHY WE APPLY RAIN TECHNOLOGY?

RAIN technology is implemented to increase fault tolerance in a cluster. The storage clusters can be managed through a centralized management interface. The management software builds a virtual pool of storage devices without requiring the physical presence of network and storage administrators. The RAIN management software automatically detects any new RAIN nodes and allows them to communicate with each other. In case of a node failure, the lost data is replicated among other RAIN nodes in a cluster to avoid immediate replacement of the failed node. RAIN-based grids are more resilient to application workload changes through effective load-balancing features [4].

## III. GOALS OF RAIN TECHNOLOGY

The goal of the RAIN project was to identify key software building blocks for creating reliable distributed applications using off-the-shelf hardware.

The focus of the research was on high-performance, fault-tolerant and portable clustering technology for space-borne computing. Two important assumptions were made, and these two assumptions reflect the differentiations between RAIN and a number of existing solutions both in the industry and in academia[5]:

1. The most general share-nothing model is assumed. There is no shared storage accessible from all computing nodes. The only way for the computing nodes to share state is to communicate via a network.
2. The distributed application is not an isolated system. The distributed protocols interact closely with existing networking protocols so that a RAIN cluster is able to interact with the environment.

In short, the RAIN project intended to marry distributed computing with networking protocols. It became obvious that RAIN technology was well-suited for Internet applications. During the RAIN project, key components were built to fulfill this vision.

## IV. ADVANTAGES OF RAIN TECHNOLOGY

[6][7] RAIN technology offers various benefits as listed below:

**Fault tolerance:** RAIN achieves fault tolerance through software implementation. The system tolerates multiple node, link, and switch failures, with no single point of failure .A RAIN cluster is a true distributed computing system that is durable to faults, it works on the principle of graceful degradation[8][9].

**Simple to deploy and manage:** It is very easy to deploy and administer a RAIN cluster. RAIN technology deals with the scalability problem on the layer where it is happening, without the need to create additional layers in the front. The management software allows the user to monitor and configure the entire cluster by connecting to any one of the nodes. **Open and portable:** The technology used is open and highly portable. It is compatible with a variety of hardware and software environments. Currently it has been ported to Solaris, NT and Linux.

**Supports for heterogeneous environment:** It supports a heterogeneous environment as well, where the cluster can

[3] nsive\_Nodes



Article

# Cyber Forensics

N. Parsuram

**Abstract:** The Cyber Forensics Behavioral Analysis (CFBA) model merges Cyber Behavioral Sciences and Digital Forensics to improve the prediction and effectiveness of cyber threats from Autonomous System Numbers (ASNs). Traditional cybersecurity strategies, focused mainly on technical aspects, must be revised for the complex cyber threat landscape. This research proposes an approach combining technical expertise with cybercriminal behavior insights. The study utilizes a mixed-methods approach and integrates various disciplines, including digital forensics, cybersecurity, computer science, and forensic psychology. Central to the model are four key concepts: forensic cyberpsychology, digital forensics, predictive modeling, and the Cyber Behavioral Analysis Metric (CBAM) and Score (CBS) for evaluating ASNs. The CFBA model addresses initial challenges in traditional cyber defense methods and emphasizes the need for an interdisciplinary, comprehensive approach. This research offers practical tools and frameworks for accurately predicting cyber threats, advocating for ongoing collaboration in the ever-evolving field of cybersecurity.

**Keywords:** behavioral analysis; behavioral threat intelligence; cyber behavioral analysis; cyber defense; cyber forensics; cyberpsychology; forensic cyberpsychology; predictive analytics; Prophet model; time-series analysis

## 1. Introduction

The fields of cyber behavioral sciences, integrating psychology, cyberpsychology, IT, cybersecurity, and digital forensics are pivotal for understanding human aspects in cyber interactions. Together they shed light on behavioral patterns, motivations, and intentions in cyberspace, contributing significantly to comprehending the human factors influencing cybersecurity [1–3].

This study is dedicated to developing and implementing a real-world integrated predictive model. This model will synergistically fuse the insights of cyber behavioral sciences with the technical rigor of digital forensics. Its primary aim is to significantly improve the accuracy of cyber threat predictions linked to specific Autonomous System Numbers (ASNs).

This study's approach, which leverages live data from Internet Service Provider (ISP) customers to assess ASN predictive models, is a pivotal aspect, underscoring its substantial real-world applicability. The criticality of ASNs in the efficient routing of internet traffic and the overall management of the global internet infrastructure cannot be overstated, making this an essential point in substantiating the study's significance.

### 1.1. Problem Overview

Traditional cybersecurity strategies, predominantly grounded in technical methodologies, face significant challenges in accurately predicting these threats. The increasing sophistication of cybercriminal activities necessitates an approach that not only relies



# A Survey on Video Surveillance Using Artificial Intelligence

<sup>1</sup>Dr. K. SheshadriRamana

**Abstract** – In surveillance and security field, the technology plays a vital role in capturing the images and videos every second. But understanding and analyzing them is a hectic task but has a lot of importance. So as a improvised solution to this problem, surveillance can be implemented through artificial intelligence. This uses computer programs that analyze the surveillance cameras for recognizing humans, objects or vehicles. These programs functions by using machine vision technology. This computer vision uses a series of procedures, algorithms which follows a series of questions for comparing the seen object with predefined postures, movements and positions. These type of artificial intelligence programs are known as “rule-based” programs because humans set some rules and the program works based on this rule.

**Keywords** – Video, Surveillance, A.I, Footages, Machine Learning, Programs, Humans.

## I. INTRODUCTION

Upon the application of the A.I programs for the video cameras, the programs check for the object that is observed in the camera some of the metrics which are earlier set by the programmer. They include

1. Is the size of the object is like the predefined object?
2. Do the color of the observed object matches with the predefined object?
3. If the observed object is moving, then what is its speed and is that identical to the speed stated in rules?
4. In which direction the object is moving?
5. Is the object just moving or vibrating too?

Combining and considering all these observations, the result is deduced which is whether the observed object is a human or not or it is like some other stated class.

Humans cannot always monitor the video surveillance footages which are mostly live and hence there comes the demand of artificial intelligence. Humans can not focus on the observation for a longer time and the quality of vigilance looses there. For example, for not more than thirty minutes, they can not keep watching continually with attention. Most of the time, the location where the surveillance system is installed is idle without and creature in it. Like in the factories or garages at night time or some empty rooms and halls. So obviously one loses his attention. But there is a huge overwhelming demand for the video surveillance. Even in forensic department these footages are used but can't be used effectively due to the earlier stated reasons.

## II. EARLIER SOLUTION ATTEMPTS

Motion detection cameras and advanced video motion detection are the most proposed solutions. In reaction to the shortcomings of human guards to watch surveillance video display units long-time period, the first solution become to add

motion detectors to cameras. The hassle was that during an out of doors surroundings there is constant movement or changes of pixels that incorporate the whole regarded image on screen. The motion of leaves on trees blowing within the wind, clutter alongside the floor, bugs, birds, dogs, shadows, headlights, sunbeams and so on all contain movement. This triggered hundreds or maybe lots of fake signals consistent with day, rendering this answer inoperable besides in indoor environments at some point of times of non-operating hours.

The subsequent evolution decreased false alerts to a point however on the cost of complex and time-eating guide calibration. here, changes of a target inclusive of a person or car relative to a fixed heritage are detected. wherein the history adjustments seasonally or because of other modifications, the reliability deteriorates through the years. The economics of responding to too many fake indicators once more proved to be an obstacle and this answer become insufficient.

## III. APPLICATION–REALTIME PREVENTATIVE ACTION

The detection of intruders using video surveillance has boundaries based on economics and the character of video cameras. commonly, cameras outside are set to a huge attitude view and yet look out over a long distance. frame rate consistent with 2nd and dynamic variety to deal with brightly lit regions and dimly lit ones further assignment the camera to surely be good enough to look a moving human intruder. At night time, even in illuminated out of doors regions, a transferring situation does not acquire enough light per body according to 2d and so, unless pretty near the digital camera, will appear as a thin wisp or slightly discernible ghost or completely invisible. situations of glare, partial obscuration, rain, snow, fog, and darkness all compound the trouble. even when a human is directed to observe the actual vicinity on a screen of a subject in these situations, the concern will normally no longer be detected. The A.I. is capable of impartially study the entire picture and all cameras' pictures simultaneously. using statistical models of degrees of deviation from its learned pattern of what constitutes the human form it will locate an intruder with high reliability and a low false alert rate even in unfavorable conditions. Its getting to know is primarily based on approximately 1 / 4 million images of human beings in diverse positions, angles, postures, and so forth.

The one-megapixel VideoIQ digicam with the onboard video analytics became capable of hit upon a human at a distance of about 350' and an perspective of view of about 30 tiers in non-ideal conditions. guidelines could be set for a "digital fence" or intrusion into a pre-defined location. policies may be set for directional journey, item left in the back of, crowd formation and some other conditions.





# Sanskrit: A Platform for Computer Programming Languages and AI

<sup>1</sup>R. Vara Prasad

**Abstract**— Language is a structured logical expression of thought, may be in sounds, gestures, arrangements or words spoken or written or otherwise. Every language is a logical system but every logical system is not a language. So what qualifies a logical system to become a language? Sanskrit Daivbhasha tradition is not new rather developed over centuries by diverse talents like thinkers, analysts, sculptors, grammarians and the like. The language traditions are very deep in the logical hearts of people of India for generations over several millennia, so much so that western world has also believing that the logical structure of Computer programming language can be matched with only Sanskrit. Almost all oriental languages have words from Sanskrit origin and very clear and logical structure based on Aastik philosophy which goes to the root of communication, i.e., the “thought” or “Idea” itself which is desired to be communicated. In 1985 Rickk Briggs highlighted comparison of Data Representation in Sanskrit and Artificial Intelligence. The discussion continued for decades that Sanskrit language could be one of best option for computers. Sanskrit is logical and clear with laws of its grammar but the present situation of both Computer programming and Sanskrit in present framework is not ready for Handshake for further development and expansion of the former. Sanskrit Vyakaran is based on only fourteen sutras called Mahesh war (Shiva) sutra, Grammarian Panini created 4000 sutras on which the system of modern day sanskrit is based. Computer as machine learning requires such language to perform better and faster with less programming. Sanskrit can play important role in making computer programming language flexible, logical and compact. This paper is focused on analysis of current status of research done on Sanskrit as a programming language the opportunity, scope and challenges.

**Index Terms**—Sanskrit, Language, Logic, Computer Programming, Computer, Natural Processing Language, Programming Language, AI- Artificial Intelligence

## I. INTRODUCTION

Language starts from the domain of Creation of Idea though it is often understood as Exchange of Idea. Till the time we don't create an idea we don't need to exchange it with anyone. But this fact was never brought to us through any means of education. But in Vedic Language (VedBhasha) it always starts from Thought<sup>1</sup>. This information was never important till the time cognition and neuroscience came into existence as a means for scientific exploration of man & machines. As Vedas were considered Religious books of Hindu religion with no relation with Science, this aspect remained buried. Hence, till now the dialogue was considered between 2 humans with different language origin and different language families were observed on that premise. Problem which emerged in last a few decades since 1980 was Dialogue between 2 persons with with the interface of machines. Thus we started to have Machine language, Artificial Intelligence and computer programming languages. In last few decades it was only computer language but now machine is equipped with intelligence. So a thinking structure is also needed for Machines. This created a huge Chaos as different languages have different language structures and none can be taken as a standard structure which could be applied over different language structures. Whether Sanskrit may form the base of a standard language structure which may be applied on all languages Human or Machine is our subject of study. In other words whether standard language structure applicable both to human and machine language may be based on or developed through Sanskrit as Vedas - Tantra - Tarka texts in Sanskrit has the key to all. Specially Tantra (System) have all three components for machine communication, i.e., Tantra (Sytems)+ Mantra(softwares) + Yantra (machines) all three integrated or knit into one. However, this process also needs many clarifications as the commentaries done by many have really confused the audience. Our effort in this paper is to remove those confusions and to create a meaningful system where everything is defined.

### Aims and Objectives:

To review the literature related to the concept of structure of Sanskrit language which can be easily moulded into Computer Programming Language. The objectives of this research paper are twofold, i.e., to dig out the ancient knowledge about Sanskrit and its connection with Computer Programming Logic that is used in translation over different Languages and to reduce (or minimize) the confusion about the meaning and connotation of origin of Logic of Language.

### Methodology:

Reviews of Vedas , Vyakaran & Tarka texts, electronic data base, and published researches have been carried out. Collection, compilation and deep analysis of the concept have been done.

### Review of Literature:

A language is a structured system of communication. John Peters argues that the difficulty of defining communication emerges from the fact that communication is both a universal phenomenon (because everyone communicates) and a specific discipline of institutional academic study<sup>ii</sup>. Language was mostly considered as exchange of thoughts between two or more, but how can we exchange thoughts without even having created them. So, Language starts from creation of thoughts to exchange of thoughts





# **MATLAB Technology**

**R. VaraPrasad**

**Abstract:** *Matlab has become a popular choice for researchers across various fields due to its versatility, ease of use, and powerful analytical capabilities. In this paper, we explore the role of Matlab as the ultimate solution for research challenges. We first discuss the benefits of using Matlab in research, including its ability to handle complex mathematical computations, data visualization, and simulation of complex systems.*

**Keywords:** Matlab, Research, Analytical capabilities, Modeling, Simulation

## **I. INTRODUCTION**

Matlab has become a widely recognized tool in the research community for its ability to facilitate a broad range of analytical tasks, from data visualization and analysis to modeling and simulation. Matlab is an abbreviation for "Matrix Laboratory," and it is a multi-paradigm numerical computing environment and programming language.

Over the years, Matlab has continued to evolve, providing an expanding range of functionalities and features that cater to researchers' needs in different fields. This evolution has made it a reliable tool for addressing a wide range of research challenges in various fields, including engineering, finance, biology, and physics.

This paper aims to explore the role of Matlab as the ultimate solution for research challenges. We will discuss the benefits of using Matlab in research, such as its ease of use, versatility, and powerful analytical capabilities. Additionally, we will showcase how Matlab can be used in different research fields and its applications in solving research challenges.

Furthermore, we will highlight the importance of Matlab in facilitating reproducible research, enabling researchers to share their code and data, and make their research transparent and verifiable. We will also touch on the availability of a vast library of prebuilt tools and add-ons that can save researchers time and effort while providing advanced functionalities.

This paper aims to demonstrate that Matlab is the ultimate solution for research challenges, offering a range of powerful tools and functionalities that enable researchers to tackle complex problems and drive innovation across various fields. We hope this paper will inspire researchers to leverage Matlab's capabilities to gain a competitive advantage in their research and advance their respective fields.

## **II. MATLAB**

Matlab is a numerical computing environment and programming language that is widely used in scientific research, engineering, and other related fields. It was initially developed in the late 1970s by Cleve Moler, a professor of computer science at the University of New Mexico. Since then, it has grown to become one of the most widely used computational tools in research and industry.

Matlab provides a flexible and powerful platform for performing complex mathematical computations, analyzing data, visualizing data, and building models and simulations. Its popularity stems from its ease of use and the fact that it is a highly efficient programming language for numerical calculations. Moreover, Matlab has an extensive library of functions and toolboxes that can be used to perform a wide range of tasks, such as image processing, signal analysis, optimization, control system design, and more.

Matlab is also highly customizable and can be used to build user interfaces, create interactive graphics, and develop algorithms for specific applications. Additionally, it provides a robust development environment, including debugging



Impact Factor: **7.301**

**IJARSCT**

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 3, Issue 1, April 2023

## Train Bot: Chatbot for Railways

R. VaraPrasad

### ABSTRACT

In all forms of on-line communications, so far noticed that no bots can imitate what a human can do. Chatbot is a program that provides an interaction with the chat services to automate tasks for the humans, Chatbot can provide 24X7 service to user. Chatbot acts like routing agent that can be used to classify user's context in conversation. Chatbots are aided with Natural Language Processing (NLP) which is used to examine the request and draw out some keyword information's based on the keywords that the Chatbot provides, thus the Railway reservation bot gives details such as number of seats available each class, source and destination with time. Chatbot also provides word suggestion which can be used to find train name, source and destination name etc., which aids the user for better conversation.

**Keywords** - : Artificial Intelligence, chatbot, NLP, Railway reservation, SQL.

Date of Submission: 20-03-2020

Date Of Acceptance: 06-04-2020

### I. INTRODUCTION

In the current survey , the chatbot are utilized by many humans's . In that what are the blessings and downsides and disadvantages, we will see this inside the survey. In the chatbot Artificial Intelligence is used, and strategies are mentioned on this survey. Chat bots or Virtual Assistants have been designed to simplify the interplay among computer systems and humans and feature hit the market.

We can note that through now Chatbots discover software in all types of on-line verbal exchange and to automate the human procedure. The generation is changed and advanced. Computers are quicker and smart telephones are to be had to each person. Numerous net offerings provide ubiquitous connections amongst human beings, information and software program. Large quantities of human understanding are gathered and available. Due to the growing amount of information, techniques for automatic reading that information has end up an essential studies subject matter. While examine modern-day chat-bots and nation that any system, gadget or application (chat-

bot) showing a few, however now not all basics of intelligence are a Partially Intelligent System. Therefore, chat-bots are Partially Intelligent Systems. Moreover, nowadays's device intelligence is significantly confined to the limits of Partial Intelligence.

In order to achieve the automation procedure for railway ticket reservation. The consumer performs the booking operation through the communicate or with voice enter to the bot. The bot offers the word notion the usage of N-gram module. Then the bot performs tokenization Chatbot splits the check enter into numerous small tokens or key-word consistent with the key-word the Chatbot executes the unique handler. After the reservation process then it performs price movement the usage of the fee APIs and additionally in FAQ mode the chat bot replies for the user queries using the IE (Information Extraction) approach.

### II. RELATED WORKS

#### A. Anatomy and Utilities of an Artificial Intelligence Conversational Entity

In this paper, we going to look approximately the SARANG Bot and FUTURE

