(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :15/07/2023

(21) Application No.202341047816 A

(43) Publication Date : 01/09/2023

(54) Title of the invention : SYNTHESIS OF TWO DIMENSIONAL INORGANIC MATERIALS FOR OPTOELECTRONICS

(51) International classification	:B82Y0030000000, H01L0021020000, B82Y0020000000, H01L0029240000, B82Y0040000000
(86) International Application No Filing Date	:PCT// :01/01/1900
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**

1)Dr.N.Kotilingaiah

Address of Applicant :PDF Scholar, Department of Chemistry, Srinivas University, Mangalore, Karnataka, -574146 ----------- ----------

2)Dr.J.Venkateshwarlu

3)Dr. Gajula Kiran

4)Dr. J. Sandhya

5)B.M Praveen

Name of Applicant : NA

Address of Applicant : NA

(72)**Name of Inventor :**

1)Dr.N.Kotilingaiah

Address of Applicant :PDF Scholar, Department of Chemistry, Srinivas University, Mangalore, Karnataka, -574146 ----------- ----------

2)Dr.J.Venkateshwarlu

Address of Applicant :Assistant Professor, Guru Nanak Institute of Technology, Ibrahimpatnam, Ranga Reddy, Telangana - 501506 ----------- -----------

3)Dr. Gajula Kiran

Address of Applicant :Assistant Professor, TKR College of Engineering, Meerpet, (D) Rangareddy, Hyderabad, Telangana ---------- -----------

4)Dr. J. Sandhya

Address of Applicant :Assistant professor, Vaageswari College of Engineering, Thimmapur, Karimnagar Telangana ----------- ----------

5)B.M Praveen

Address of Applicant :Director, Research and Innovation Council, Srinivas University, Mangalore, Karnataka - 574146 ----------- ----------

(57) Abstract :

The layered crystalline solids that make up two-dimensional materials have strong bonding in the crystal plane but weak vander-Waals forces between the neighbouring atomic layers. The unique structure of 2D materials gives them a variety of amazing capabilities. First, compared to their bulk parent materials, 2D materials exhibit several new optical and electrical properties as a result of quantum confinement in the direction perpendicular to the 2D plane. The integration of 2D materials with photonic structures is made easier by the surfaces of these materials being naturally passivated and lacking dangling bonds. Additionally, by creating vertical heterostructures with a variety of 2D materials, the problem of lattice mismatch may be avoided since the various layers are joined together by van der Waals forces.

No. of Pages : 13 No. of Claims : 3

Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 07 (July -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i07.pp163- 168*

A Hybrid Framework For Travel Advice System Using Big Data And AI

Nusrath Zeeshan[1] | Dr.V.Bapuji[2]

[1]Department of MCA, Vaageswari College of Engineering,Karimnagar.
[2]Professor & HoD, Department of MCA, Vaageswari College of Engineering,Karimnagar.

To Cite this Article
Nusrath Zeeshan | Dr.V.Bapuji, "A Hybrid Framework For Travel Advice System Using Big Data And AI " *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp163-168*
Article Info
Received: 06-06-2023 Revised: 06-07-2023 Accepted: 17-07-2023 Published: 27-07-2023

ABSTRACT

In recent years, with the development of the internet and technology, the tourism industry has seen a significant increase in tourist numbers. The growing demand for personalized travel experiences has led to the development of travel advice systems for tourism. This helps travel agents find suitable travel destinations for clients, especially those unfamiliar with the location. Advisory systems are becoming more common in everyday activities like social networking and online buying. A hybrid framework for a travel advice system is proposed based on big data and artificial intelligence. The main aim of the system is to provide tourists with personalized travel planning based on user preferences and historical data. This allows the user to quickly locate what they are seeking for without wasting time or effort. It combines the strength of a content-based and collaborative filtering approach. To improve user affinity relationships and the quality of recommendations in the travel industry, a common recommendation filtering algorithm based on designations and user preferences has been proposed. Context-aware advice systems combine software computing and data mining to incorporate user profiles, social media history, and POI (points of interest) data. Suggestion system for a list of tourist attractions adapted to the preferences of tourists. Also acts as a travel planner by developing a detailed program that includes a multi-level framework for the travel advice system. Based on the traveler's experiences, the ratings (reviews) were also collected and analyzed to make better decisions for new travelers that advise tourist travel locations based on their previously rated venues. The algorithm searches the database for travel opportunities and uses text-mining techniques to find places of interest. the application of intelligent e-tourism consultation in tourism, focusing on interfaces, consultation algorithms, characteristics, and techniques of artificial intelligence. The goal aims to develop a hybrid travel advisory system that leverages intelligent e-tourism advice in the travel industry, focusing on interfaces and recommendations based on big data and artificial intelligence techniques.

KEYWORDS: Hybrid Advice system; Content-based Filtering; Collaborative Filtering; Context-aware system; e-Tourism; user preferences; trip planner.

1. INTRODUCTION

Tourism is a captivating domain. As it offers numerous destinations and attractions such as adventure, business, cultural/historical, etc. throughout the world for someone wishing to travel[1]. With such a large volume of options, travelers often need advice about where to go and what to see, Commonly, the tourist is helped by the travel agents who provide advice to tourists, but human factors like lack of memory and limited knowledge about the place can limit their ability to match their requirements against available options. However, the increasing number of choices and difficulties in locating services make it difficult for users to find what they are looking for[2], with the increasing demand for travel due to advancements in information and communication technology.

Factors such as availability of activities, affordability, popularity, and safety, influence a tourist's choice of vacation destination[3]. However, the efficiency of using the World Wide Web for finding a destination is questionable due to the lack of personalized information and can be complex and time-consuming for tourists. To address these issues, advice systems have been

Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 07 (July -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i07.pp124 - 132*

Suspicious Account Detection Using Machine Learning Techniques

Afshan Anjum[1] | B.Anvesh kumar[2] |Dr.V.Bapuji[3]

[1]Department of MCA, Vaageswari College of Engineering, Karimnagar,
[2] Assistant Professor,Department of MCA,Vaageswari College of Engineering, Karimnagar,
[3] Professor & HoD,Department of MCA, Vaageswari College of Engineering, Karimnagar,

To Cite this Article
. Afshan Anjum, B.Anvesh kumar, Dr.V.Bapuji, "**Suspicious Account Detection Using Machine Learning Techniques**" *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp124-132*
Article Info
Received: 04-06-2023 Revised: 09-07-2023 Accepted: 17-07-2023 Published: 27-07-2023

ABSTRACT

In the current generation, social networking sites have become an integral part of life for most people. On social networking sites such as Facebook, Instagram, and Twitter, thousands of people create their profiles daily, interacting with each based on the classification for detecting Suspicious accounts on social networks. Here the traditionally way has been used for different classification methods in this paper.

The implementation of machine learning and natural language processor (NLP) techniques are done to enhance the accuracy of others regardless of location and time. Our goal is to understand who encourages threats in social networking profiles. To determine which social network profiles are genuine and which ones are Suspicious profiles, The support vector machine (SVM) and Naves bays algorithm technique can also be applied to achieve this strategy.

KEYWORDS: *Online Social network, Classification, Natural language processing (NLP), Facebook, Support vector machine (SVM).*

INTRODUCTION

Millions of participants and billions of minutes of usage make social networking a well-liked online network. However, there are many security issues and protection concerns, particularly with the threat of identity theft. The privacy regulations imposed by social networking service providers tend to be inadequate, making them vulnerable to manipulation and misuse. The advance in technology has led to an evolution of knowledge. Machine learning algorithms have emerged, emphasizing analyzing obstacles as well as data. Although handheld devices and social media outlets revolutionize communication and improve decision-making, they tend to be prone to violation of privacy. To identify users who conceal their identities. Research has focused on trained and untrained machine learning algorithms, with the vast majority accomplishing a precision of 50%- 96%. The techniques in use have become effective at ensuring personal information about users from harmful behavior.

In addition to the impact of the increasing popularity of social networking sites on the web, individuals are becoming more susceptible to increasing security dangers and weaknesses including being subjected to violations of privacy, fraud identities, unsafe programs, suspicious profiles, and harassment based on gender. To resolve those problems, security providers provide protective systems and surveillance technologies. Online interaction monitoring tools like those offered by monitoring make it easy to identify users and address security issues. as open social network (OSN) usage increases, it will become critical to address such problems by developing feasible solutions.

Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 07 (July -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i07.pp133- 139*

Detection Of Cyber Attack In Network Using Machine Learning Techniques

Annam Pranitha[1] | Polu Satish[2] | Dr.V.Bapuji[3]

[1]Department Of MCA Vaageswari College Of Enginnering, Karimnagar
[2]Professor,Department Of MCA. Vaageswari College Of Engineering, Kraimnagar
[3]HoD, Department, Of MCA, Vaageswari College Of Engineering, Karimnagar

To Cite this Article
. **Annam Pranitha | Polu Satish| Dr.V.Bapuji**, "**Detection Of Cyber Attack In Network Using Machine Learning Techniques**" *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp133-139*
Article Info
Received: 04-06-2023 Revised: 08-07-2023 Accepted: 17-07-2023 Published: 27-07-2023

ABSTRACT

Improvements in computer and communication technologies have produced significant developments that are standing put from the past. Utilising new technologies offers governments, associations, and people incredible benefits, but some people are opposed to them. For instance, the security of designated data stages, the availability of data, and the assurance of important information. Dependent on these problems, advanced anxiety-based abuse may be the current big problem. Computerised dread, which caused many problems for foundations and individuals, has manifested at a level where it might be used to undermine national and open security by a variety of social entities, such as criminal association, intelligent people, and skilled activists. In order to maintain a crucial distance from sophisticated attacks, intrusion detection systems (IDS) have been developed.

Learning to reinforce support is now taking place with accuracy rates pf 97.80% and 69.79%, respectively, vector machine (SVM) estimations were developed independently to recognise port compass attempts based on the new CICID2017 dataset. Perhaps instead of SVM, we can present some alternative calculations like CNN, ANN, and Random Forest 99.33, and ANN 99.11. To disrupt, disable, damage, or maliciously control a computing environment or infrastructure, to compromise the integrity of data, or to steal controlled information, a cyber-attack attacks an enterprise's usage of cyberspace's via cyberspace. Cyberspace's current state foretells uncertainty for the internet's future and its rising user base. With big data obtained by gadget sensors disclosing enormous amounts of information, new paradigms because they might be exploited for targeted attacks. Cyber security is currently dealing with new difficulties as a result of the expansion of cloud services, the rise in users of web applications, and changes to the network infrastructure that links devices with different operating systems. So by detecting the cyberattacks we can solve this problem.

KEYWORDS:
Intrusion detection system (IDS); CICID2017 dataset; ANN; CNN; Random Forest; Cyber space; Cybersecurity

INTRODUCTION

The world has recently witnessed a significant evolution in the numerous fields of related technologies like dazzling matrices, the internet of vehicles, long-distance improvement, and 5G communication. According to CISCO [1], it is expected that by 2022, there will be several times as many IP-connected devices as people on the planet. These devices will generate 4.8zb of IP traffic annually. This accelerated development

Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 07 (July -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i07.pp140- 145*

Secure Mobile Cloud Storage

Bodasu Manisha[1] | Dr.V.Bapuji[2]

[1]Departmen of MCA, Vaageswari College of Engineering,
[2]Professor & HoD,Department of MCA, Vaageswari College of Engineering,

To Cite this Article
. **Bodasu Manisha | Dr.V.Bapuji** , "**Secure Mobile Cloud Storage** " *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp140-145*
Article Info
Received: 04-06-2023 Revised: 08-07-2023 Accepted: 18-07-2023 Published: 27-07-2023

ABSTRACT

Data may be stored on a cloud and accessible from anywhere using mobile devices thanks to mobile cloud storage (MCS). MCS services are provided for commercial use by sizable firms like Apple I Cloud, Dropbox, Microsoft One Drive, and Google Drive. Since customers may not fully trust clouds, data security may be achieved using encryption techniques. However, sensitive data, including location data, is frequently included in location-based apps. This exposed data can be used to deduce the client's behavior and encrypted data. For instance, 80% of search queries may be recognized by a searchable encryption system using a generic inference attack with access pattern leaking and little prior knowledge. The activity of the client can also be inferred via oblivious technologies, such as oblivious transfer and oblivious storage.This study presents a mobile cloud storage system that simultaneously safeguards data confidentiality and privacy while being effective, secure, and privacy-preserving. An oblivious selection and update (OSU) protocol built on onion additive homo morphic encryption with constant encryption layers serves as the underlying primitive. This dramatically lowers computation and transmission costs by enabling clients to covertly retrieve encrypted data items from the cloud and update them with new information. The suggested approach is more appropriate for MCS situations because it has beneficial characteristics such a fine-grained data structure, minimal client-side processing, and constant communication overhead. The "verification chunks" technique also confirms that the strategy is resistant to malicious cloud assaults. According to the comparison and assessment, the suggested plan is more effective than currently available oblivious storage options in terms of client .A valuable tool for distant storage, akin to cloud storage, is remote data integrity checking.

KEYWORDS: *Cloud computing, third-party verify, data, remote storage, cloud storage, CSP schema.*

INTRODUCTION

Cloud computing is gaining popularity in the business community due to its scalable,pay-on-demand,location-independent storage services. However, it also presents new security challenges, such as Data Loss & Leakage. To ensure data integrity, protocols must be developed that allow data owners to verify their data storage in the cloud. Cloud service providers (CSP) have become increasingly popular due to their ability to share data and process it efficiently at a low cost. However, the integrity of outsourced data is difficult to guarantee due to lack of transparency and the reputation of CSP. To design a secure and efficient audit mechanism for dynamic shared data in cloud storage, several challenges must be efficiently addressed. The traditional method of data integrity verification is to download all data from the data owner directly from the CSP and check the integrity of the data locally. However, this method wastes network transmission resources and local storage resources, weakening the advantages of cloud service.

The proposed scheme meets provable data possession, avoids certificate management problems, and achieves data privacy preservation without leaks of the data owner's identity information. As information

Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 07 (July -2023)
www.jst.org.in DOI:https://doi.org/10.46243/jst.2023.v8.i07.pp152- 157

An Efficient Single Instance Scheme With User Authentication To Cloud Data

Boini Vandana[1] |P.Sathish[2] | Dr.V.Bapuji[3]

[1]Department of MCA, Vaageswari College of Engineering, Karimnagar.
[2] Assistant Professor, Department of MCA, Vaageswari College of Engineering, Karimnagar.
[3] Professor & HoD, Department of MCA, Vaageswari College of Engineering, Karimnagar.

To Cite this Article

Boini Vandana |P.Sathish | Dr.V.Bapuji , "**An Efficient Single Instance Scheme With User Authentication To Cloud Data** " *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp152-157*

Article Info

Received: 06-06-2023 Revised: 07-07-2023 Accepted: 16-07-2023 Published: 27-07-2023

ABSTRACT

Cloud Storage is a computer data storage method where digital data is stored on servers in off-site locations, managed by a third-party provider. This enables organizations to store, access, and maintain data without owning and operating their own data centers. Cloud storage is scalable, allowing organizations to expand or reduce their data footprint depending on their needs. Users upload data to servers via internet, which is saved on a virtual machine on a physical server. Cloud providers often spread data to multiple virtual machines in global data centers to maintain availability and redundancy. Google Cloud offers various scalable options for organizations to store their data in the cloud. The widespread use of cloud computing has made data sharing and storage more accessible, but concerns about data integrity, efficiency, and privacy remain. Duplication, a popular method of data compression, is used to reduce duplicate copies of data in cloud storage.

However, data duplication also raises security and privacy concerns, as users' confidential data is vulnerable to attacks from insiders and outsiders. Traditional solutions for duplication, based on convergent encryption, provide confidentiality but do not maintain duplicate checks based on differential permissions. This paper proposes an approved data duplication plan that counts the number of users with differential privileges in the duplicate check.Users with differential privileges are added to the duplicate check, and files are encrypted with differential privilege keys to maintain stronger security. Users can only access files marked with matching privileges for copy checks.

A third-party auditor can confirm file occurrence after duplication in the cloud, ensuring timely uploads. This paper offers advantages for both storage providers and users through duplication systems and auditing methods.

KEYWORDS: *Cloud storage, Dropbox, Mozy, Perfect Hashing, Storage, Encryption, Attacks, Privacy*

1.INTRODUCTION

There will be 4 billion digital files stored in the cloud by 2020. Costs associated with management, upkeep, and handling are substantial. By keeping redundant information only once, information duplication techniques try to get rid of duplicate data. However, outsourcing sensitive data necessitates its encryption, which makes duplication attempts more difficult. Numerous solutions have been put out to deal with this problem, however they are hindered by things like brute-force attacks and the storage capacity limitations of the cloud.

Effective And Efficient Detection Of Phishing Emails Using Machine Learning

Moola.Akshitha[1] | Dr.D.Srinivas Reddy[2] | Dr.V.Bapuji[3]

[1]Department of MCA, Vaageswari college of Engineering,Karimnagar
[2] Professor,Department of MCA, Vaageswari college of Engineering,Karimnagar
[3] HoD,Department, of MCA, Vaageswari college of Engineering,Karimnagar

To Cite this Article
Moola.Akshitha| Dr.D.Srinivas Reddy| Dr.V.Bapuji, "Effective And Efficient Detection Of Phishing Emails Using Machine Learning" *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp158-162*
Article Info
Received: 06-06-2023 Revised: 07-07-2023 Accepted: 16-07-2023 Published: 27-07-2023

ABSTRACT

Emails are widely used for personal and professional communication,often involving the transmission of sensitive information like banking details,credit reports,and login data.Consequently,these emails become valuable targets for cyber criminals who seek to exploit such knowledge for their own malicious purposes.Phishing, a deceptive technique employed by these individuals,involves impersonating well-known sources to deceive and extract sensitive information from unsuspecting individuals.The sender of a phishing email uses false pretenses to persuade recipients into disclosed personal information.In this work,the detection of phishing emails is learning methods to categorize emails as either genuine or phishing attempts.LMT classifiers have proven highly effective in accurately classifying emails,achieving optimal accuracy in email classification tasks.

KEYWORDS: Phishing,Emails,Efficient,Detection,Effective,Transmission.

INTRODUCTION

Phishing stands as the most prevalent form of cybercrime, involving the manipulation of victims to disclose sensitive information like account numbers, passwords,and bank details. Cyber-attacks commonly exploit email,instant messages,and phone calls[1,2].Despite ongoing efforts to update preventive measures,the outcomes have proven insufficient.Conversely,there has been a significant increase in phishing emails in recent years, underscoring need for more effective and modern countermeasures[3,4].Numerous approaches have been developed to filter phishing emails,but a comprehensive solution to the problem is still required.This study represents the first known survey focusing on the application of Machine Learning[ML] algorithms currently employed to detect the phishing emails at different stages of an attack[5].

It includes a comparative assessment and analysis of these methodologies ,offering an overview of the topic,its immediate solution space,and potential future research directions[6-8]The rapid advancement of internet technologies has transformed online interactions while introducing new security risks .Despite phishing being extensively referenced in scientific papers receiving press coverage and drawing attention from banks and law enforcement agencies the question of what phishing truly entails arises[10].

A Machine Learning Framework For Data Poisoning Attacks

Priyanka Narsingoju[1] | Dr.D.Srinivas Reddy[2] |Dr.V.Bapuji[3]

[1]Department of MCA,Vaageswari College Of Engineering, Karimnagar.
[2]Associate Professor,Department of MCA,Vaageswari College Of Engineering, Karimnagar.
[3]Professor & HoD, Department of MCA,Vaageswari College Of Engineering, Karimnagar.

To Cite this Article
Priyanka Narsingoju, Dr.D.Srinivas Reddy ,Dr.V.Bapuji , "A Machine Learning Framework For Data Poisoning Attacks " *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp169-176*
Article Info
Received: 06-06-2023 Revised: 06-07-2023 Accepted: 17-07-2023 Published: 27-07-2023

ABSTRACT

Federated models are built by collecting model changes from participants. To maintain the secrecy of the training data, the aggregator has no visibility into how these updates are made by design.. This paper aims to explore the vulnerability of federated machine learning, focusing on attacking a federated multitasking learning framework. The framework enables resource-constrained node devices, such as mobile phones and IOT devices, to learn a shared model while keeping the training However, the communication protocol among attackers may take advantage of various nodes to conduct data poisoning assaults, which has been shown to pose a serious danger to the majority of machine learning models. The paper formulates the problem of computing optimal poisoning attacks on federated multitask learning as a bi-level program that is adaptive to arbitrary choice of target nodes and source attacking nodes.The authors propose a novel systems-aware optimization method, Attack confederated Learning(AT2FL), which is efficiency to derive the implicit gradients for poisoned data and further compute optimal attack strategies in the federated machine learning.

KEYWORDS: *Federated machine learning, Vulnerability,Arbitrary, Attack on federated machine learning(AT2FL), Gradients.*

INTRODUCTION

Machine learning has been widely applied in various applications, such as spam filtering and natural gas price prediction[1]. However, the reliability and security of these systems have been a concern, including adversaries. Researchers can rely on public crowd sourcing platforms or Private teams to collect training datasets, but both have the potential to be injected corrupted or poisoned data by attackers. It is crucial to research how well machine learning operates under poisoning it attempts in order to increase the resilience of real-world machine learning systems. Exploratory attacks and causal assaults are two categories of attack tactics. The n nodes in this federated learning system are shown by distinct colors. Corrupted or poisoned data is injected into certain nodes, whereas clean data is the sole data present in other nodes. The fundamental idea behind federated machine learning is to develop machine learning models based on data sets dispersed across numerous devices, while limiting data loss.

Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 07 (July -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i07.pp177- 183*

Secured And Efficient Data Duplication With Re-Encryption Techniques

Amirishetti Sukanya[1] | P.Sathish[2] | Dr.V.Bapuji[3]

[1]Department of MCA, Vaageswari College of Engineering,Karimnagar.
[2]Assistant Professor, Department of MCA, Vaageswari College of Engineering, Karimnagar.
[3]Professor & HOD Department of MCA, Vaageswari College of Engineering, Karimnagar.

To Cite this Article
Amirishetti Sukanya | P.Sathish | Dr.V.Bapuji, "Secured And Efficient Data Duplication With Re-Encryption Techniques " *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp177-183*
Article Info
Received: 04-06-2023 Revised: 05-07-2023 Accepted: 15-07-2023 Published: 27-07-2023

ABSTRACT

To get rid of duplicate copies and conserve bandwidth, data duplication is a vital approach in cloud storage. A convergent encryption strategy is suggested to encrypt data before outsourcing to maintain sensitive data confidentially. This work considers varied user privileges in duplicate checks to address authorized data duplication. In a hybrid cloud architecture, it introduces novel duplication structures that facilitate authorized duplicate checking. The proposed authorized duplicate check technique is constructed and tested, and security analysis proves the scheme's security. When compared to standard operations, the proposed system has a low overhead. Before outsourcing data into the cloud, encryption measures are frequently employed to ensure secrecy, however, commercial storage providers are hesitant to utilize encryption due to the possibility of different cipher texts. Convergent encryption, which protects data secrecy while permitting duplication, has been offered as a solution to these problems. Systems for cloud storage have difficulty maintaining duplication, dependability, and confidentiality. Duplication is a method for maximizing the use of storage resources by preventing the creation of duplicate copies of the same material. Both single-cloud duplication architecture and multi-cloud duplication architecture are categories for it.

KEYWORDS: Encryption, Storage, Authorized, Architecture, Duplication, Secrecy, Security.

I INTRODUCTION

Cloud technology allows for data access from any location with an internet connection, it improves data security and collaboration. It is essential to offer user-related data access as flexible and remote working grow increasingly common[2]. Based on the convergent all-or-nothing transform (CAONT) and randomly selected bits from the

Bloom filter, a safe data duplication strategy is suggested. This system can withstand stub-reserved assaults and guarantee data owners' privacy. Data owners just need to re-encrypt a tiny portion of the package instead of the complete package, which reduces the computational burden on the system.

Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 07 (July -2023)
www.jst.org.in DOI:https://doi.org/10.46243/jst.2023.v8.i07.pp184- 192

IDENTIFYING AND PREVENTING THE DISSEMINATION OF FAKE NEWS

Syed Salman Hussain[1] | Boddupalli Anvesh[2] | Dr. V. Bapuji[3]

[1]Department of MCA, Vaageswari College of Engineering,
[2]Asst Professor, Department of MCA, Vaageswari of Engineering,
[3]Professor and Hod, Department of MCA, Vaageswari College of Engineering,

To Cite this Article
Syed Salman Hussain | Boddupalli Anvesh | Dr. V. Bapuji, **"IDENTIFYING AND PREVENTING THE DISSEMINATION OF FAKE NEWS "** *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp184-192*
Article Info
Received: 04-06-2023 Revised: 05-07-2023 Accepted: 15-07-2023 Published: 27-07-2023

ABSTRACT

Misinformation poses a significant threat to democratic societies, particularly in today's interconnected digital world, as it has the potential to shape public opinion. Researchers from various disciplines, including computer science, political science, information science, and linguistics, have been investigating the spread of fake news, methods for detecting it, and strategies to mitigate its impact. However, effectively identifying and preventing the dissemination of false information remains a complex endeavor. Given the increasing role of Artificial Intelligence (AI) systems, it is vital to offer clear and user – ,bfriendly explanations for the decisions made by fake news detectors, particularly on social media platforms. Therefore, this paper conducts a systematic analysis of the latest approaches employed to detect and combat the spread of fake news. By examining these approaches, we uncover key challenges and propose potential future research directions, with a particular emphasis on integrating AI explain ability into fake news credibility systems.

KEYWORDS: *AI explainability, fabricated news, synthetic media, misleading content, dishonest information, fake profiles, online platforms, biased information, block – chain powered identification.*

INTRODUCTION

Numerous solutions[1] have been suggested to tackle various security and privacy issues, whether they are related to the Internet of Things(IoT)[2], user authentication problems[3], enhancing road traffic safety or other cyber-crime threats. However, as people and organizations increasingly rely on real-time information from diverse sources such as user- generated content and social media platforms there is a new risk emerging: the abuse of these sources and dissemination methods through the spread of fake news.

Currently, research in the field of fake news is still in its preliminary stages. We define fake news as content intentionally created to deceive users, aiming to mislead[4], deceive or defame individuals, groups, organizations, and governments. Fake news can have various consequences on our society, as illustrated in figure 1.

A Protection System For Securing Multimedia Content In The Cloud

Venkata Sivaram Kumpati[1] |Polu Sathish[2] |Dr.V.Bapuji[3]

[1]Department of MCA, Vaageswari College Of Engineering, Karimnagar
[2]Assistant Professor, Department of MCA, Vaageswari College Of Engineering, Karimnagar.
[3]Professor& HoD, Department of MCA, Vaageswari College Of Engineering, Karimnagar.

To Cite this Article
Venkata Sivaram Kumpati |Polu Sathish |Dr.V.Bapuji, **"A Protection System For Securing Multimedia Content In The Cloud "** *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp193-197*
Article Info
Received: 04-06-2023 Revised: 05-07-2023 Accepted: 15-07-2023 Published: 27-07-2023

ABSTRACT

Every day, a vast amount of multimedia content is generated and shared on the internet. Unfortunately, it has become all too easy to duplicate copyrighted materials. To address this issue, in this work to introduces an innovative system for safeguarding multimedia content on cloud infrastructures. When these duplicated multimedia materials are illicitly distributed online, Content creators suffer significant revenue losses. Detecting these unauthorized copies of multimedia content is a challenging task. This paper presents a pioneering system designed to protect various types of multimedia content, including 2-D/ 3-D videos, audios, images, and more. Built upon cloud infrastructure, this system offers rapid access to computing hardware and software resources. Its key components involve generating signatures for 3-D videos and utilizing a distributed index to match multimedia object.

KEYWORDS: *Multimedia, Cloud computing, Protection, Copyrighted ,images,videos,*

1. INTRODUCTION

The advancement of multimedia processing and recording equipment, combined with the proliferation of free online hosting platforms, has greatly facilitated the unauthorized replication of copyrighted materials such as videos, images, and music clips. This illicit distribution of content is a

challenging and computationally intensive task, requiring complex comparisons to identify duplicates. To handle this issue, a comprehensive system has been developed to safeguard various type of multimedia content, including 2D and 3D videos, images, audio clips, songs.

The system is designed to operate seamlessly on private clouds, public clouds, or a combination of both. Leveraging cloud infrastructure enables rapid deployment of content protection system by

providing instant access to necessary computing hardware and software resources. This design is

SECURE AND EFFICIENT BIOMETRIC BASED SAFE ACCESSMECHANISM FOR CLOUD SERVICES DEVELOPMENT

Kondapalukula, Abhishek Rao[1] | Dr. V. Bapuji[2] | Dr. V. Bapuji[3]

[1]Department of MCA, Vaageswari College of Engineering,
[2]Professor, Department of MCA, Vaageswari of Engineering,
[3]Professor and HoD, Department of MCA, Vaageswari College of Engineering,

To Cite this Article

Kondapalukula Abhishek Rao, Dr. V. Bapuji, Dr. V. Bapuji, "SECURE AND EFFICIENT BIOMETRIC BASED SAFE ACCESS MECHANISM FOR CLOUD SERVICES DEVELOPMENT" *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp198-202*

Article Info

Received: 04-06-2023 Revised: 04-07-2023 Accepted: 14-07-2023 Published: 27-07-2023

ABSTRACT

User authentication with unlink capability is one of the corner gravestone services for numerous security and separateness services which are needed to protect dispatches in wireless detector nets (WSNs). This document describes SESAME (guard European network for operations in a Multivendor Environment), a security framework for public assigned networks evolved by Bull, ICL and Siemens Nixdorf. The generalities behind the infrastructure, what parcels it has and what features it provides are carried. Particular emphasis has been given away to inflexibility, administration and directness. A figure of the system of the SESAME factors is also carried, displaying its effectiveness with regard to performance and authority and its defense rates. A particularized Real- Or- Random (ROR) design predicated regular protection anatomy, irregular(non-mathematical) shield assay and alike routine safeguard verification utilizing the astronomically- accepted Automated proof of Internet Security Protocols and Applications (AVISPA) device expose that the offered approach can oppose several given attempts against (unresistant/alive) adversary. hence, the suggested scheme not only specifics its shield defects but similarly improves its version. It's further capable for functional operations of WSNs device.

KEYWORDS: Authentication, biometric-based security, cloud service access, session key.

. I. INTRODUCTION

The guard of resource in assigned computing surround is primarily achieved by direct logon to each end- system penetrated [1], using watchwords [2], with druggies transmitting the word in a clear and vulnerable form. This has a number of downsides first, it isn't veritably secure [3], as anyone equipped to hear to the network could learn a stoner's vulnerable word and so be suitable to impersonate that stoner; second, it isn't accessible for a stoner to have to flashback several watchwords and to have to enter a different one each time he accesses a different end system; and third, the user isn't known as a single stoner to the distributed system as awhole [4], there's no collaboration of hisuse of the distributed system across thedifferent system waiters. These are some of the access control issues in a distributed computing context.protection and isolation are certifiably hypercritical for the going deployment of a WSN [5]. Due to the public and energetic nature of wireless message media in WSNs, they're subject to varied attempts, similar as bugging, revision, interception, insertion, and omission.

SOCIAL MEDIA ANALYSIS WITH ACTIVE ONLINE LEARNING TO SUPPORT CRISIS MANAGEMENT

MEDISHATTI RAMYASREE, H.no:20S41D5814,Mtech (CSE), Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,

Karimnagar, Telangana, INDIA, Email-id: ramya.medishatti@gmail.com.

DR.CHANDRA MOULI, HOD, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,

Karimnagar, Telangana, INDIA, Email-id: cmnarsingoju@gmail.com.

ABSTRACT

People express and discuss various circumstances they are involved in, such as crises, via social media (SM). Therefore, it makes sense to employ SM contents to aid crisis management, particularly by disseminating important and little-known information about the crises in real-time. As a result, we suggest the AOMPC, a brand-new active online multiple-prototype classifier. It finds pertinent information about a crisis. AOMPC is a data stream-operating online learning algorithm that has active learning mechanisms to actively query the label of ambiguous unlabeled data. A fixed budget technique is employed to limit the amount of inquiries. AOMPC typically accepts data streams with partial labelling. Two types of data were used to assess AOMPC: (1) synthetic data and (2) SM data from Twitter connected to two crises, the Australia Bushfires and the Colorado Floods. An extensive analysis of the outcomes' quality was conducted using a variety of established indicators. Additionally, a sensitivity analysis was performed to demonstrate the impact of the AOMPC's parameters on the reliability of the outcomes. AOMPC was compared to various online learning algorithms that are currently available. The trials demonstrated that AOMPC behaves very well while handling changing, partially labelled data streams.

Index Terms:—Online learning, multiple-prototype classifier, active learning, social media.

Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 07 (July -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i07.pp146- 151*

PROTECTION FOR YOUR PURCHASE PREFERENCES WITH DIFFERENTIAL PRIVACY

Dumpeti Saikumar[1] | DR. G.S. Chowhan[2] | Dr. V. Bapuji[3]

[1]Department of MCA, Vaageswari College of Engineering,
[2]Professor, Department of MCA, Vaageswari of Engineering,
[3]Professor and HoD, Department of MCA, Vaageswari College of Engineering,

To Cite this Article

Dumpeti Saikumar | DR. G.S. Chowhan | Dr. V. Bapuji, "PROTECTION FOR YOUR PURCHASE PREFERENCES WITH DIFFERENTIAL PRIVACY " *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp146-151*
Article Info
Received: 04-06-2023 Revised: 08-07-2023 Accepted: 18-07-2023 Published: 27-07-2023

ABSTRACT

Internet banking can be done to uncover customers' buying habits as the conclusion to various attempts. Before actually transferring it on-line, monetary institutions with contrasting statutes of darkness. Every buyer can disrupt their local business connection before transferring it to online banks, due to divergent security. However, the adoption of differential security in web-based foundations will be problematic because popular differential protection plans do not involve the issue of the concussion limit. Similarly, we manage an academic test above and below to show that our projects are able to meet the standard of differentialprotection. Finally, in order to decide on sustainability, we place our diets on trial in the mobile initiation trial. The importance of aggregate usage and online banking. Total amount decreased significantly, and the protection errors for common data are less than 0.5, which is consistent with the test findings.

KEYWORDS: *Differential Privacy, Noise Boundary, Online Bank, Shopping Preference Protection.*

INTRODUCTION

Online banks have precisely the new growth popularized for the distribution of financial services [1]. Online banks, in their separate phase, are defenseless in the face of outside and intermediary attempts. Brutal violations of the commandments are contained in violations for shipwrecked persons [2], social phishing and transferred violations. Data improperly processed by persons with authorized access shall be treated as an intermediate offence. Clients' financial data may exist collected by foreign aggressors in order to conclude individual buying preferences [3], operational designs, or credit collection. Shoppers can accept advice [4],

DIABETES PREDICTION USING MACHINE LEARNING ALGORITHMS

CHIPPA NARESH KUMAR, H.no: 20S41D5828,Mtech (CSE), Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,Karimnagar, Telangana, INDIA, Email-id: sunnynaresh189@gmail.com.

MD.SIRAJUDDIN,Professor, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,Karimnagar, Telangana, INDIA, Email-id: mohdsiraj569@gmail.com.

ABSTRACT

Numerous people suffer from diabetes mellitus, one of the most serious diseases. Age, obesity, inactivity, genetic diabetes, a poor diet, high blood pressure, and other factors can all contribute to diabetes mellitus. Diabetes increases a person's chance of developing several illnesses, including heart disease, renal disease, stroke, vision problems, nerve damage, etc. A variety of tests are currently used in hospitals to get the data needed to diagnose diabetes, and depending on that diagnosis, the proper therapy is given. The healthcare sector greatly benefits from big data analytics. Databases in the healthcare sector are very vast. By analysing large datasets using big data analytics, one may learn from the data and make accurate predictions about the future by uncovering hidden patterns and information. The categorization and prediction accuracy of the current approach is not very good. In this study, we suggested a diabetes prediction model that combines a few extrinsic variables that cause diabetes in addition to more common parameters like glucose, body mass index (BMI), age, insulin, etc. Compared to the old dataset, the new dataset improves classification accuracy. Additionally, a pipeline model for diabetes prediction was imposed with the goal of enhancing classification accuracy.

Index Terms:-Diabetes mellitus ,Diabetes prediction, healthcare sector, body mass index (BMI), classification accuracy.

ENABLING IDENTITY BASED INTEGRITY AUDITING AND DATA SHARING WITH SENSITIVE INFORMATION HIDING FOR SECURE CLOUD STORAGE

FAREEDA SULTANA, H.no: 20S41D5808,Mtech (CSE), Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,

Karimnagar, Telangana, INDIA,Email-id: fareedasultana04@gmail.com.

DR. E.SRIKANTH REDDY,Associate Professor, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,

Karimnagar, Telangana, INDIA,Email-id: srikanth574@gmail.com.

ABSTRACT

Users can remotely store their data to the cloud and enable data sharing with others via cloud storage services. To ensure the integrity of the data saved in the cloud, remote data integrity auditing is suggested. The cloud file may include potentially sensitive data in some popular cloud storage systems, such as the Electronic Health Records (EHRs) system. When the cloud file is shared, the sensitive information shouldn't be made available to others. The sensitive information can be realised by encrypting the entire shared file, but it will prevent others from using it. It has not yet been determined how to implement data sharing with sensitive information concealed in remote data integrity audits. We provide a remote data integrity auditing approach that realises data sharing with sensitive information hidden in this study to solve this issue. A sanitizer is employed in this method to turn the data blocks' signatures into valid ones for the sanitised file while also sanitising the data blocks that correspond to the file's sensitive information. During the integrity auditing process, these signatures are used to confirm the accuracy of the sanitised file. As a consequence, our method enables the cloud-stored file to be shared and utilised by others under the condition that the sensitive data is masked, while retaining the ability to effectively carry out remote data integrity audits. While this is going on, the suggested approach uses identity-based cryptography to streamline the challenging certificate administration. The suggested method is efficient and secure, according to the performance analysis and security analysis.

Index Terms:- Data sharing, Electronic Health Records , sensitive information, data integrity, identity-based cryptography.

MOVIE RECOMMENDATION SYSTEM USING SENTIMENT ANALYSIS FROM MICROBLOGGING DATA

NANDAGIRI MANOGNYA, H.no: 20S41D5816,Mtech (CSE), Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,

Karimnagar, Telangana, INDIA, Email-id:manognyamanu4@gmail.com.

DR.DINESH KUMAR, Associate professor, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,

Karimnagar, Telangana, INDIA.

ABSTRACT

For use in e-commerce and digital media, recommendation systems (RSs) have attracted a great deal of interest. Collaborative filtering (CF) and content-based filtering (CBF) are examples of traditional methodologies used in RSs. However, these approaches have several drawbacks, such as the requirement of past user history and habits in order to accomplish the work of suggestion. This article suggests a hybrid RS for films that incorporates the finest ideas from CF and CBF as well as sentiment analysis of tweets from microblogging sites in order to lessen the impact of such limitations. The goal of using movie tweets is to comprehend the prevailing patterns, general consensus, and audience reaction to the film. Promising findings have come from experiments performed using the public database.

Index Terms:-Collaborative filtering, content-based filtering, recommendation system (RS), sentiment analysis, Twitter

SECURE KEYWORD SEARCH AND DATA SHARING MECHANISM FOR CLOUD COMPUTING

SHAFIA SHAHREEN, H.no: 20S41D5818, Mtech (CSE), Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,

Karimnagar, Telangana, INDIA, Email-id: Shahareen16595@gmail.com.

K.SRIDHER REDDY, Associate Professor,Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,

Karimnagar, Telangana, INDIA, Email-id: sridhark529reddy@gmail.com.

ABSTRACT

The cost of hardware and software resources in computer infrastructure has drastically decreased with the rise of cloud infrastructure. Before being sent to the cloud, the data is often encrypted to protect security. It is difficult to look for and distribute data that has been encrypted, as contrast to plain data. However, it is a crucial responsibility for the cloud service provider since customers depend on the cloud to quickly search for their data and provide the results without jeopardizing the secrecy of their data. We suggest a ciphertext-policy attribute-based approach with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data to address these issues. Contrary to existing systems, which only offer one of two aspects, the suggested approach not only permits attribute-based data exchange but also provides attribute-based keyword search. Furthermore, our technique allows for the updating of the keyword without interacting with the PKG during the sharing phase. In this study, the concept of CPAB-KSDS and its security model are discussed. Additionally, we provide a specific technique and demonstrate that it is safe in the random oracle model and resistant to selected ciphertext and chosen keyword attacks. Finally, the performance and property comparison shows how feasible and effective the suggested building is.

Index Terms:-Distribute data, Data sharing, searchable attribute-based encryption, attribute-based , ciphertext. security model.

TRUST-BASED PHOTO SHARING IN ONLINE SOCIAL NETWORKS WITH PRIVACY PRESERVING

TARANNUM FATHIMA, H.no: 20S41D5820,Mtech (CSE), Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,

Karimnagar, Telangana, INDIA, Email -Id:tarannumfathima789@gmail.com.

S. SATEESH REDDY, Associate Professor, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, Email -Id:sateesh.singireddy@gmail.com.

ABSTRACT

Sharing images in online social networks has grown in popularity as a result of the advancement of social media technology as a means of preserving social ties. However, a photo's wealth of details makes it simpler for a hostile observer to deduce private information about persons who are depicted in the picture. In recent years, there has been a great lot of discussion on how to solve the privacy disclosure issue brought on by photo sharing. The publisher of the photo should consider all linked users' privacy while publishing a photo that involves numerous users. In this research, we provide a privacy-preserving sharing method based on trust for these types of co-owned images. The main concept is to anonymize the original image in order to prevent people who would significantly lose privacy due to the sharing of the image from being recognised from the anonymized image. Depending on how much a user trusts the recipient of the photo, there will be a privacy loss. And privacy loss has an impact on the user's faith in the publication. A threshold that the publisher has set controls how an image is anonymized. To strike a balance between the privacy protected by anonymization and the information shared with others, we provide a greedy approach for the publisher to adjust the threshold. The results of the simulations show how the trust-based photo sharing mechanism helps to minimise privacy loss and how the proposed threshold tweaking approach might benefit the user.

Index Terms:- online social networks,privacy-preserving sharing, anonymized image, trust-based photo, information shared ,threshold.

WIRELESS INTRUSION DETECTION SYSTEM

ALLI ANILKUMAR, H.no: 20S41D5801,Mtech (CSE), Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA.

DR D.SRINIVAS REDDY,Associate Professor, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA.

ABSTRACT

The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The recent denial of service attacks on major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. The IDS engine is the control unit of the intrusion detection system. Its main purpose is to manage the system, i.e., supervise all operations of the intrusion detection system. Its duty depends on the intrusion detection method used. Wireless has opened a new and exciting world for many of us. Its technology is advancing and changing every day and its popularity is increasing. The biggest concern with wireless, however, has been security. The traditional wired IDS is a great system, but unfortunately it does little for the wireless world. Implementing WIDS systems is definitely a step in the right direction. If you have wireless and are concerned about attacks and intruders, a WIDS may be a great idea.

Index Terms:-Intrusion Detection System (IDS), wireless networks, mobile computing attacks,intruders.

Designing of Delay Approximation Model for Prime Speed Interconnects in Current Mode

Dr. Udutha Rajender
Assistant Professor
Electronics & Communication Engineering
Vaageswari College of Engineering
Karimnagar, Telangana-505 527

Abstract:

There is enormous demand for high speed VLSI networks in present days. The coupling capacitance and interconnect delay play a major role in judging the behavior of onchip interconnects. There is an on chip inductance effect as we switch to low technology that leads to delay in interconnecting. In this paper we are attempting to apply second order transfer function designed with finite difference equation and transform Laplace at the ends of the source and load termination. Analysis shows that the current signaling mode in VLSI interconnects provide better time delay than the voltage mode.

IndexTerms*: VLSI ,Interconnect, Current mode, feedbackscheme.*

I. INTRODUCTION

As the number of transistors on a chip keeps increasing, on-chip communications will become a more crucial aspect of architectural design. Conventional electrical wires, normally driven by digital components using simplistic virtual signals have problems to address inside the scaling chip multiprocessor marketplace, in particular latency and strength. Worldwide cord latency remains highly constant, translating to a bigger relative latency for even reasonably-sized structures. In an effort to make sure sign pleasant, virtual repeaters and packet-switching routers need to be added to facilitate the transmission of lengthy distance communications, contributing further to the latency and power problems. As delivered in the references, signal is transmitting to a modern change signaling to 3 times more than the voltage mode signaling.

Change display close to speed of light electric signaling the use of the reality that the signaling pace may expanded using punishing to energy spectrum destiny to indicators of high level frequency uses at modulations methods. However at strength intake turns into acceptable high of at which cases to max schemes desires to huge wiring on the top Meta metallic layers. The on-chip interconnect network's speed

Designing of Synthetic Aperture Radar Based Control Algorithms for the Autonomous Vehicles

Dr.Udutha Rajender
Department of ECE
Vaageswari College of Engineering, Karimnagar, India

***Abstract*— The rise in popularity of self-driving cars can be attributed to advancements in modern technology. The surge in interest in self-driving cars has led to an increase in their development, but this has also brought some challenges. A large part of the solution to these problems is satellite remote sensing and GIS technology. Optical data remote sensing technologies alone have limited potential for long-term forest management sustainability. Active Synthetic Aperture Radar (SAR) remote sensing technology has grown in importance in forestry because of its uniqueness and rapid advancement. For example, SAR has an all-weather capability that is sun light independent, cloud and rain-resistant, and highly penetrating. SAR and optical, SAR and LiDAR, optical and LiDAR remote sensing have all been shown to be useful for accurate forest AGB estimation when compared to single sensor data. These types of sensor data integrations are becoming increasingly common. This is made possible by the fact that the scattering process heavily influences the polarimetric signatures that can be observed. The inclusion of SAR polarimetry improves classification and segmentation quality compared to conventional SAR with a single channel. Decomposition products' outputs have been classified.**

Keywords*— Synthetic Aperture Radar, LiDAR, Autonomous Vehicles,

I. INTRODUCTION

Because it makes use of microwaves, imaging RADAR technology known as Synthetic Aperture Radar (SAR) creates images with a high resolution and is able to capture RADAR images regardless of the weather. The speckle effect, which is induced by the coherent processing of backscattered signals, is to blame for the noisy appearance of SAR images. Speckles are a type of background noise that are present in every single SAR image. Before utilising the photographs, remove the background noise. The elimination of noise is one method for improving the appearance of digital photographs. The objective of the method is to lessen the amount of noise while maintaining the integrity of small details like edges. Soft computing methods are being more and more frequently used for the purpose of reducing noise in SAR images [1]. We have conducted research into a variety of methods for filtering speckle noise in SAR images, and we have presented speckle noise filters that are based on soft computing. A device that can detect and find things is known as a RADAR, which stands for radio detection and ranging. Vision in humans can be improved so that it works better in low light, rain, and other adverse conditions. The foundation of a RADAR system is comprised of the antennas for both the transmitter and the receiver. The transmitter is responsible for emitting electromagnetic waves into space so that they can be used to pinpoint the target. The energy that was diverted by the target is brought into the receiving antenna so that it can be processed. The quantity of energy that an item reflects can be affected by a number of factors, including its physical properties, its structural properties, and its chemical properties [2]. There is a correlation between the radiation's strength, wavelength, and angle of incidence. [3] The receiver is responsible for processing the reflected energy, also known as echoes, in order to retrieve target identifying parameters such as range, velocity, and angular location. It wasn't until the early 1920s that RADAR was first put to use to spot ships and aero planes in the sky.

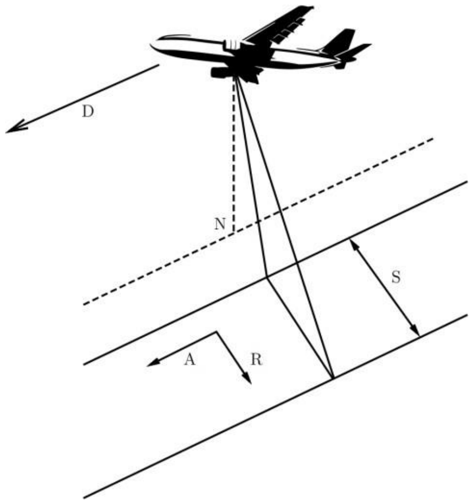


Fig. 1. Geometry of SAR viewing

In the 1970s, search and rescue (SAR) technology was made accessible to the general population. The majority of the time, a SAR system will be mounted on either a spaceship or an aero plane [4]. It illuminates the surface being scanned in a direction perpendicular to its plane by means of a beam of coherent electromagnetic pulses. When the illuminated surface sends back an echo, the SAR receiver is able to pick it up, file it away in its memory, and then use it as input for image processing to produce an image of the target surface. Because it is impractical for a spaceship to carry a very large

Forensic Accounting – A Tool for Encountering Bank Frauds (An Opinion Survey)

Dr. E. Hari Prasad[1], S. Sridhar Reddy[2]
[1]Vaageswari College of Engineering, Karimnagar, Telangana, India
[2]Assistant Professor, Dept. of Business Management, Vaageswari College of Engineering, Karimnagar, Telangana, India

ABSTRACT

A country's development directly depends on the economic health of that country. It is not exaggerated to say that the economic progression of a nation is vital to keep the nation rolling on its wheels. An efficient and strong banking system is the backbone of the country's economy. But, in recent years Indian economy experienced various bank frauds and scams that pulled the economic system into the stake. But the failures in the Indian banking system pushed the economy at stake and adversely affected investors' investment behavior. This led to financial distress and funds were divorced and improperly drain off many banks collapsed. As per the recent records, a total of 9,103 fraud cases in banks were recorded during the financial year 2021-22. Therefore, the present study aims to study the appropriateness of forensic accounting in mitigating financial fraud in banks.

Key Words: Economic progression, Banking system, Forensic Accounting, Financial frauds, Financial crimes, white-collar crimes, detection and prevention of frauds.

INTRODUCTION

Forensic accounting is an emerging tool for detecting and preventing financial fraud and provides justice by providing crucial information related to financial crime. Most organizations like banks, insurance companies, and police have well recognized the importance of this forensic accounting and started taking help for their investigations. The increasing rate of white-collar crimes and difficulties faced by investigation agencies in detecting frauds has also been the reason for the emerging and increasing importance of forensic accounting.

According to the Journal of Forensic Accounting, "Forensic accounting is sufficiently thorough and complete so that an accountant, in his/ her considered independent professional judgment, can deliver a finding as to accounts, inventories, or the presentation thereof that is of such quality

that it would be sustainable in some adversarial legal proceeding, or within some judicial or administrative review". (*Fraud, the unmanaged Risk.* Earnest and Young 2003). It is a specific area of accounting which investigates fraud and analyze financial information which can be utilized in legal trials. Forensic accounting is a judicious mix of accounting, auditing, and investigative skills to perform investigations of financial fraud. It is helpful for legal action and analytical accounting.

Bank Frauds in India: "A bank fraud means and includes any of the following acts committed by any person with the connivance or by his agent including a banker with an intention to cheat or actually cheat or conceal or falsify or forge documents, accounts or indulge in misappropriation which results in wrongful gains to any person with or without monetary loss in the course of banking transactions" (Mohan, 2002). Due to advancements in technology, now, frauds relating to digital payments are also taking place. The RBI categorized these digital payment frauds into 10 types. They include phishing, hacking, pharming, smishing, vishing frauds, frauds using online sales platforms, frauds due to unverified mobile phones, frauds using screen sharing apps, ATM card skimming, SIM swaps/cloning, frauds by compromising credentials on results through search engines, fraud through QR code scan and impersonation on social media (The Times

BioGecko

Vol 12 Issue 03 2023

ISSN NO: 2230-5807

ROLE OF STAKEHOLDERS IN DELIVERING QUALITYMANAGEMENT EDUCATION FOR SUSTAINABLE DEVELOPMENT

Dr. E. Hari Prasad Sharma
Associate Professor, Departmentof Business Management
Vaageswari College of Engineering – Karimnagar

Abstract:
Dynamism of business environment is throwing different challenges to higher educational institutions to meet the industry requirements and the same to prepare the students by enhancing their competencies required to instrument decision making strategies. It is very difficult to the management of management institutions to offer quality management education. Innovative activities are to be introduced in a rapid way to meet the requirements. At present, institutions are facing a lot of problems to achieve the desired level of effectiveness of quality management education. The present paper attempts to find out the role of stakeholders who are involve in delivering quality management education and characteristics those are required to a management students and fundamentals that are essential to impart the qualitative management education at emerging scenario.

Key Words: *Quality management education, Higher educational institutions, Stake holders, Faculty, Educational system, Students, Sustainable development.*

Introduction

The expansion of education in management area can be found back to 18th century. Since 18th century, there are tremendous changes are found in management education. In India, though, management education was derived from the western management thought and practice, Indian management scholars and practitioners are drawing some extrapolations from epics like, Maha Bharatha, Ramayana, Bhagavad Geetha and other Puranas and Shastras. Management education was evaluated with emerging trends in industrial engineering and closely related with the disciplines like psychology, philosophy, sociology, economics, accounting, statistics and mathematics.In India, management education is seen as special and superior discipline. Students select management education, not because for sake but for personal exposure and experience, to create something innovative which useful to the society and inspired by the magnitudes associated with management education.

The government of India (GoI) announced its New Industrial Policy in 1991 and had introduced the process of Liberalization, Privatization and Globalization (LPG). These reforms in economy led to replace the traditional approach of education to more efficient professional education and introduced advance courses in education to bond with the industry requirement which have greater economic value in the present competition world. Management education got a special recognition with the changing of time. Along with the traditional courses like financial management, marketing management and human resource management, new functional areas like OperationsManagement, Supply Chain Management, Rural Management, International Business Management, Digital Marketing, Data Analytics, Financial Analytics and HR Analytics are also covered in management education to meet the industry demand for highly efficient management people. As a result of this, management education became one of the most trending courses which provide a good career to the youth. With this, in India, private eduprenuers are entering in management education and investing an enormous amount of funds by establishing business schools.

PEER-TO-PEER CLOUD: ANONYMOUS AUTHENTICATION AND KEY AGREEMENT

[#1]BONGONI MADHURI,
[#2]P.SATHISH, ***Assistant Professor,***
[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

Abstract: Cross-cloud data migration is a typical issue for mobile consumers, and it is a required step when customers transfer mobile phone providers. Customers frequently find it difficult to backup all data from the original cloud servers to their mobile phones before migrating the downloaded data to the new cloud provider due to smart phones' limited local storage and computing capabilities. To solve this issue, we present an efficient data transit model among cloud providers, as well as an elliptic curve certificate-free mutual authentication and key agreement technique for peer-to-peer cloud. The proposed technique builds trust among cloud providers and lays the groundwork for cross-cloud data transfer deployment. The mathematical veracity and security correctness of our technique are compared to important current data migration strategies, demonstrating that our proposed scheme surpasses other state-of-the-art schemes in terms of both computational and communication cost reduction.

Index Terms**—**Cloud computing, data migration, elliptic curve, authentication, key agreement.

1. INTRODUCTION

Data must be transferred from the cloud server of the current smart device provider to the cloud server of the new smart device provider if a customer decides to switch to a different smart device made by a different firm. It is normal practice to access the primary cloud server, transfer the data to intelligent terminal devices, access the secondary cloud server, and then transfer the data to the secondary cloud server.

In order to accomplish this, it is necessary to devise a safer and more streamlined method of transferring data between different cloud services. The most efficient method for transferring user data from one cloud server to another. The term for this process is "data migration." Implementing this ideal data migration strategy is complicated by the wide variety of cloud service providers available. This is due to issues with compatibility, lack of trust, and potential security breaches during data transfer.

Data migration research has been demonstrated to have significant practical ramifications. It can be challenging to move data from one cloud to another for a variety of reasons. There are currently a number of issues that make data migration to the cloud less efficient. To make it simpler and quicker for consumers to transfer their data between cloud servers when they switch phones, additional research is needed on the context of cloud data mobility. Multicloud setups make it challenging to establish trust, which is especially problematic for apps that transfer sensitive data and must adhere to stringent security protocols. Mutual authentication, secure communication keys, and uncompromised data transfer are all crucial considerations. These

MACHINE LEARNING-BASED ANALYSIS AND FINANCIAL RISK MANAGEMENT IN CRYPTOCURRENCY MARKET

#1GUNDA SAI NIKHIL,

#2B.ANVESH KUMAR, ***Assistant Professor,***

#3Dr.V.BAPUJI, ***Associate Professor& HOD,***

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR,TELANGANA

ABSTRACT: For daily bitcoin market forecasting and trading, we deploy and analyze a range of machine learning algorithms. The algorithms have been trained to forecast the binary relative daily price movements of the top 100 cryptocurrencies. All of the models we tested produced statistically plausible estimates, with average accuracy values ranging from 52.9% to 54.1% across all cryptocurrencies. Based on the subset of predictions with the 10% greatest model confidences per class and day, these accuracy results range from 57.5% to 59.5%. We find that after transaction costs, a long-short portfolio strategy based on the forecasts of the deployed LSTM and GRU ensemble models yields annualized out-of-sample Sharpe ratios of 3.23 and 3.12, respectively. In comparison, the benchmark buy-and-hold market portfolio strategy has a Sharpe ratio of only 1.33. These findings point to a threat to the efficiency of the bitcoin market, albeit the impact of certain arbitrage constraints cannot be completely ruled out.

Keywords: Financial market prediction; Market efficiency; Statistical arbitrage; Machine learning; GRU; LSTM; Neural network; Random forest;Gradient boosting; Temporal convolutional neural network

1. INTRODUCTION

In 2008, Nakamoto1 officially introduced the Bitcoin peer-to-peer currency system. Since then, numerous other cryptocurrencies have been developed, each with its own set of technological characteristics and possible uses, all of which can trace their origins back to Bitcoin. As the cryptocurrency market has grown exponentially during the past decade, individual digital currencies' prices have fluctuated widely.There isn't enough space in the user's text to rewrite it scholarly. Different market participants have different opinions on whether or not Bitcoin and similar cryptocurrencies are effective.The user entered a three-four-five number sequence. Auto-regressive statistical approaches, which explicitly represent any non-linear interactions, are frequently used in such investigations. Due to their ability to understand the malleable functional relationship between features and targets, machine learning algorithms have been successfully used in the past to forecast the cryptocurrency market, including Bitcoin.Seven, eight, and nine are mentioned. Thus, these methods can detect and capitalize on intricate linkages among several variables in high-dimensional areas, including but not limited to those not specifically discussed in studies of market performance. The purpose of this research was to compare and contrast the performance of various machine learning models for use in financial market prediction. Accordingly, the primary inquiry driving this work is as follows: Can statistical arbitrage be

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 01 | January - 2023 Impact Factor: 7.185 ISSN: 2582-3930

Designing of Synthetic Aperture Radar Based Control Algorithms for the Autonomous Vehicles

Dr.Udutha Rajender
Department of ECE
Vaageswari College of Engineering, Karimnagar, India

***Abstract*— The rise in popularity of self-driving cars can be attributed to advancements in modern technology. The surge in interest in self-driving cars has led to an increase in their development, but this has also brought some challenges. A large part of the solution to these problems is satellite remote sensing and GIS technology. Optical data remote sensing technologies alone have limited potential for long-term forest management sustainability. Active Synthetic Aperture Radar (SAR) remote sensing technology has grown in importance in forestry because of its uniqueness and rapid advancement. For example, SAR has an all-weather capability that is sun light independent, cloud and rain-resistant, and highly penetrating. SAR and optical, SAR and LiDAR, optical and LiDAR remote sensing have all been shown to be useful for accurate forest AGB estimation when compared to single sensor data. These types of sensor data integrations are becoming increasingly common. This is made possible by the fact that the scattering process heavily influences the polarimetric signatures that can be observed. The inclusion of SAR polarimetry improves classification and segmentation quality compared to conventional SAR with a single channel. Decomposition products' outputs have been classified.**

Keywords*— *Synthetic Aperture Radar, LiDAR, Autonomous Vehicles,

I. Introduction

Because it makes use of microwaves, imaging RADAR technology known as Synthetic Aperture Radar (SAR) creates images with a high resolution and is able to capture RADAR images regardless of the weather. The speckle effect, which is induced by the coherent processing of backscattered signals, is to blame for the noisy appearance of SAR images. Speckles are a type of background noise that are present in every single SAR image. Before utilising the photographs, remove the background noise. The elimination of noise is one method for improving the appearance of digital photographs. The objective of the method is to lessen the amount of noise while maintaining the integrity of small details like edges. Soft computing methods are being more and more frequently used for the purpose of reducing noise in SAR images [1]. We have conducted research into a variety of methods for filtering speckle noise in SAR images, and we have presented speckle noise filters that are based on soft computing. A device that can detect and find things is known as a RADAR, which stands for radio detection and ranging. Vision in humans can be improved so that it works better in low light, rain, and other adverse conditions. The foundation of a RADAR system is comprised of the antennas for both the transmitter and the receiver. The transmitter is responsible for emitting electromagnetic waves into space so that they can be used to pinpoint the target. The energy that was diverted by the target is brought into the receiving antenna so that it can be processed. The quantity of energy that an item reflects can be affected by a number of factors, including its physical properties, its structural properties, and its chemical properties [2]. There is a correlation between the radiation's strength, wavelength, and angle of incidence. [3] The receiver is responsible for processing the reflected energy, also known as echoes, in order to retrieve target identifying parameters such as range, velocity, and angular location. It wasn't until the early 1920s that RADAR was first put to use to spot ships and aero planes in the sky.

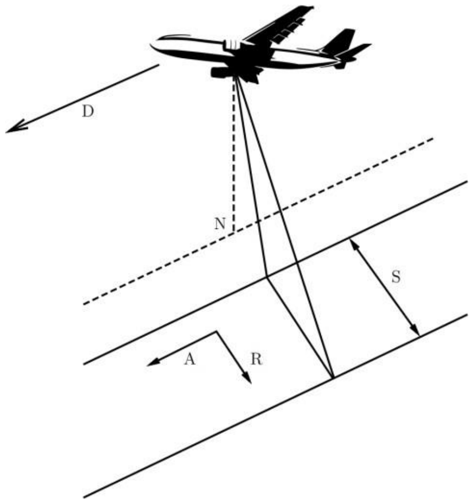


Fig. 1. Geometry of SAR viewing

In the 1970s, search and rescue (SAR) technology was made accessible to the general population. The majority of the time, a SAR system will be mounted on either a spaceship or an aero plane [4]. It illuminates the surface being scanned in a direction perpendicular to its plane by means of a beam of coherent electromagnetic pulses. When the illuminated surface sends back an echo, the SAR receiver is able to pick it up, file it away in its memory, and then use it as input for image processing to produce an image of the target surface. Because it is impractical for a spaceship to carry a very large

Forensic Accounting – A Tool for Encountering Bank Frauds (An Opinion Survey)

Dr. E. Hari Prasad[1], S. Sridhar Reddy[2]
[1]Vaageswari College of Engineering, Karimnagar, Telangana, India
[2]Assistant Professor, Dept. of Business Management, Vaageswari College of Engineering, Karimnagar, Telangana, India

ABSTRACT

A country's development directly depends on the economic health of that country. It is not exaggerated to say that the economic progression of a nation is vital to keep the nation rolling on its wheels. An efficient and strong banking system is the backbone of the country's economy. But, in recent years Indian economy experienced various bank frauds and scams that pulled the economic system into the stake. But the failures in the Indian banking system pushed the economy at stake and adversely affected investors' investment behavior. This led to financial distress and funds were divorced and improperly drain off many banks collapsed. As per the recent records, a total of 9,103 fraud cases in banks were recorded during the financial year 2021-22. Therefore, the present study aims to study the appropriateness of forensic accounting in mitigating financial fraud in banks.

Key Words: Economic progression, Banking system, Forensic Accounting, Financial frauds, Financial crimes, white-collar crimes, detection and prevention of frauds.

INTRODUCTION

Forensic accounting is an emerging tool for detecting and preventing financial fraud and provides justice by providing crucial information related to financial crime. Most organizations like banks, insurance companies, and police have well recognized the importance of this forensic accounting and started taking help for their investigations. The increasing rate of white-collar crimes and difficulties faced by investigation agencies in detecting frauds has also been the reason for the emerging and increasing importance of forensic accounting.

According to the Journal of Forensic Accounting, "Forensic accounting is sufficiently thorough and complete so that an accountant, in his/ her considered independent professional judgment, can deliver a finding as to accounts, inventories, or the presentation thereof that is of such quality

that it would be sustainable in some adversarial legal proceeding, or within some judicial or administrative review". (*Fraud, the unmanaged Risk.* Earnest and Young 2003). It is a specific area of accounting which investigates fraud and analyze financial information which can be utilized in legal trials. Forensic accounting is a judicious mix of accounting, auditing, and investigative skills to perform investigations of financial fraud. It is helpful for legal action and analytical accounting.

Bank Frauds in India: "A bank fraud means and includes any of the following acts committed by any person with the connivance or by his agent including a banker with an intention to cheat or actually cheat or conceal or falsify or forge documents, accounts or indulge in misappropriation which results in wrongful gains to any person with or without monetary loss in the course of banking transactions" (Mohan, 2002). Due to advancements in technology, now, frauds relating to digital payments are also taking place. The RBI categorized these digital payment frauds into 10 types. They include phishing, hacking, pharming, smishing, vishing frauds, frauds using online sales platforms, frauds due to unverified mobile phones, frauds using screen sharing apps, ATM card skimming, SIM swaps/cloning, frauds by compromising credentials on results through search engines, fraud through QR code scan and impersonation on social media (The Times

BioGecko

Vol 12 Issue 03 2023

ISSN NO: 2230-5807

ROLE OF STAKEHOLDERS IN DELIVERING QUALITYMANAGEMENT EDUCATION FOR SUSTAINABLE DEVELOPMENT

Dr. E. Hari Prasad Sharma
Associate Professor, Departmentof Business Management
Vaageswari College of Engineering – Karimnagar

Abstract:
Dynamism of business environment is throwing different challenges to higher educational institutions to meet the industry requirements and the same to prepare the students by enhancing their competencies required to instrument decision making strategies. It is very difficult to the management of management institutions to offer quality management education. Innovative activities are to be introduced in a rapid way to meet the requirements. At present, institutions are facing a lot of problems to achieve the desired level of effectiveness of quality management education. The present paper attempts to find out the role of stakeholders who are involve in delivering quality management education and characteristics those are required to a management students and fundamentals that are essential to impart the qualitative management education at emerging scenario.

Key Words: *Quality management education, Higher educational institutions, Stake holders, Faculty, Educational system, Students, Sustainable development.*

Introduction

The expansion of education in management area can be found back to 18th century. Since 18th century, there are tremendous changes are found in management education. In India, though, management education was derived from the western management thought and practice, Indian management scholars and practitioners are drawing some extrapolations from epics like, Maha Bharatha, Ramayana, Bhagavad Geetha and other Puranas and Shastras. Management education was evaluated with emerging trends in industrial engineering and closely related with the disciplines like psychology, philosophy, sociology, economics, accounting, statistics and mathematics.In India, management education is seen as special and superior discipline. Students select management education, not because for sake but for personal exposure and experience, to create something innovative which useful to the society and inspired by the magnitudes associated with management education.

The government of India (GoI) announced its New Industrial Policy in 1991 and had introduced the process of Liberalization, Privatization and Globalization (LPG). These reforms in economy led to replace the traditional approach of education to more efficient professional education and introduced advance courses in education to bond with the industry requirement which have greater economic value in the present competition world. Management education got a special recognition with the changing of time. Along with the traditional courses like financial management, marketing management and human resource management, new functional areas like OperationsManagement, Supply Chain Management, Rural Management, International Business Management, Digital Marketing, Data Analytics, Financial Analytics and HR Analytics are also covered in management education to meet the industry demand for highly efficient management people. As a result of this, management education became one of the most trending courses which provide a good career to the youth. With this, in India, private eduprenuers are entering in management education and investing an enormous amount of funds by establishing business schools.

PEER-TO-PEER CLOUD: ANONYMOUS AUTHENTICATION AND KEY AGREEMENT

[#1]BONGONI MADHURI,

[#2]P.SATHISH, ***Assistant Professor,***

[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

Abstract: Cross-cloud data migration is a typical issue for mobile consumers, and it is a required step when customers transfer mobile phone providers. Customers frequently find it difficult to backup all data from the original cloud servers to their mobile phones before migrating the downloaded data to the new cloud provider due to smart phones' limited local storage and computing capabilities. To solve this issue, we present an efficient data transit model among cloud providers, as well as an elliptic curve certificate-free mutual authentication and key agreement technique for peer-to-peer cloud. The proposed technique builds trust among cloud providers and lays the groundwork for cross-cloud data transfer deployment. The mathematical veracity and security correctness of our technique are compared to important current data migration strategies, demonstrating that our proposed scheme surpasses other state-of-the-art schemes in terms of both computational and communication cost reduction.

Index Terms—Cloud computing, data migration, elliptic curve, authentication, key agreement.

1. INTRODUCTION

Data must be transferred from the cloud server of the current smart device provider to the cloud server of the new smart device provider if a customer decides to switch to a different smart device made by a different firm. It is normal practice to access the primary cloud server, transfer the data to intelligent terminal devices, access the secondary cloud server, and then transfer the data to the secondary cloud server.

In order to accomplish this, it is necessary to devise a safer and more streamlined method of transferring data between different cloud services. The most efficient method for transferring user data from one cloud server to another. The term for this process is "data migration." Implementing this ideal data migration strategy is complicated by the wide variety of cloud service providers available. This is due to issues with compatibility, lack of trust, and potential security breaches during data transfer.

Data migration research has been demonstrated to have significant practical ramifications. It can be challenging to move data from one cloud to another for a variety of reasons. There are currently a number of issues that make data migration to the cloud less efficient. To make it simpler and quicker for consumers to transfer their data between cloud servers when they switch phones, additional research is needed on the context of cloud data mobility. Multicloud setups make it challenging to establish trust, which is especially problematic for apps that transfer sensitive data and must adhere to stringent security protocols. Mutual authentication, secure communication keys, and uncompromised data transfer are all crucial considerations. These

MACHINE LEARNING-BASED ANALYSIS AND FINANCIAL RISK MANAGEMENT IN CRYPTOCURRENCY MARKET

[#1]GUNDA SAI NIKHIL,

[#2]B.ANVESH KUMAR, ***Assistant Professor,***

[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR,TELANGANA

ABSTRACT: For daily bitcoin market forecasting and trading, we deploy and analyze a range of machine learning algorithms. The algorithms have been trained to forecast the binary relative daily price movements of the top 100 cryptocurrencies. All of the models we tested produced statistically plausible estimates, with average accuracy values ranging from 52.9% to 54.1% across all cryptocurrencies. Based on the subset of predictions with the 10% greatest model confidences per class and day, these accuracy results range from 57.5% to 59.5%. We find that after transaction costs, a long-short portfolio strategy based on the forecasts of the deployed LSTM and GRU ensemble models yields annualized out-of-sample Sharpe ratios of 3.23 and 3.12, respectively. In comparison, the benchmark buy-and-hold market portfolio strategy has a Sharpe ratio of only 1.33. These findings point to a threat to the efficiency of the bitcoin market, albeit the impact of certain arbitrage constraints cannot be completely ruled out.

Keywords: Financial market prediction; Market efficiency; Statistical arbitrage; Machine learning; GRU; LSTM; Neural network; Random forest; Gradient boosting; Temporal convolutional neural network

1. INTRODUCTION

In 2008, Nakamoto1 officially introduced the Bitcoin peer-to-peer currency system. Since then, numerous other cryptocurrencies have been developed, each with its own set of technological characteristics and possible uses, all of which can trace their origins back to Bitcoin. As the cryptocurrency market has grown exponentially during the past decade, individual digital currencies' prices have fluctuated widely.There isn't enough space in the user's text to rewrite it scholarly. Different market participants have different opinions on whether or not Bitcoin and similar cryptocurrencies are effective.The user entered a three-four-five number sequence. Auto-regressive statistical approaches, which explicitly represent any non-linear interactions, are frequently used in such investigations. Due to their ability to understand the malleable functional relationship between features and targets, machine learning algorithms have been successfully used in the past to forecast the cryptocurrency market, including Bitcoin.Seven, eight, and nine are mentioned. Thus, these methods can detect and capitalize on intricate linkages among several variables in high-dimensional areas, including but not limited to those not specifically discussed in studies of market performance. The purpose of this research was to compare and contrast the performance of various machine learning models for use in financial market prediction. Accordingly, the primary inquiry driving this work is as follows: Can statistical arbitrage be

MACHINE LEARNING ALGORITHMS FOR PREDICTING CRIMINAL ACTIVITY NATURE AND FREQUENCY

[#1]PEDDI RAMYA,
[#2]Y.SUSHEELA, ***Assistant Professor,***
[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

Abstract: The problem of crime is one of the most pressing issues facing modern society. It is the single most pervasive and powerful force in today's society. And it's a widespread social problem. As a result, crime prevention must be given top importance. Analysis of criminal cases needs to be done methodically. The analysis is essential in spotting and stopping illicit acts. The investigational patterns and crime trends are easier to spot after conducting this research. The primary purpose of this study is to analyze the efficiency of police work in solving crimes. The software was developed with the express purpose of discovering patterns in criminal activity. A criminal's prognosis is presented in the study based on the inferences drawn from the crime scene. In this work, we describe the approach taken to make predictions about the age and gender of perpetrators. Two major components of crime forecasting are presented in this study. The perpetrator's age and gender should be taken into account. In unsolved cases, the parameters used include study of multiple elements such year, month, and weapon used. The objective of the study's quantitative section is to count the number of open criminal cases. The task of prediction requires the generation of a detailed description of the offender's and victim's ages, sexes, and relationship dynamics. Kaggle provided the dataset used for this study. Predictions are made using a combination of multi-linear regression, KNeighbor's classifier, and neural networks. Machine learning techniques were used in the building and evaluation of the model.

Keywords: *Crime Prediction, KNN, Decision Tree. Multilinear Regression; K-Neighbors Classifier, Artificia l Neural Networks.*

1. INTRODUCTION

It is the act itself that defines a crime. There has been a breach of trust. The behavior in question is illegal. Law enforcement faces formidable obstacles when tasked with uncovering and evaluating underground criminal activity. Furthermore, a wealth of data pertaining to the occurrence is accessible. Therefore, specific methods ought to be able to aid the probe. Therefore, the recommended methodology should help bring about a positive outcome to the criminal incidence.

The application of machine learning methods can improve crime analysis and forecasting. Regression strategies are available via the machine learning methodology. The use of classification strategies aids in accomplishing the study's primary goal. Regression methods, particularly multilinear regression, are a type of statistical instrument frequently used in data analysis. Using this method, you can easily evaluate the connection between any two numbers. The dependent variable values are predicted from the independent variable values using this method. Classifiers can be developed using a wide variety of approaches, such as the K-Nearest Neighbor classifier. Multiclass target variables are classified using classifiers. When

MACHINE LEARNING ALGORITHM FOR PREDICTING AIR POLLUTION

[#1]SANGEM AJAY,

[#2]Dr.V.BAPUJI, ***Associate Professor& HOD,***

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

Abstract: The air quality monitoring system collects information on contaminants from multiple sites to maintain optimal air quality. It is currently the most pressing issue. The release of hazardous chemicals from industrial sources, as well as car emissions, damage the atmosphere. Today's main cities have dangerously high levels of air pollution that exceed the government-mandated air quality index standard. It has a tremendous impact on a person's health. Air pollution predictions can be made using Machine Learning (ML) techniques. Machine learning (ML) combines statistics and computer science to improve prediction accuracy. Machine learning (ML) is used to calculate the Air Quality Index. A variety of sensors and a microcontroller known as an Arduino Uno are used to collect the data. The K-Nearest Neighbor (KNN) approach is then used to anticipate air quality.

Keywords: Machine Learning, KNN, AQI, Arduino, sensors.

1. INTRODUCTION

One of the most pressing problems humanity faces today is air pollution. Industry activity is picking up speed as a result of the brisk economic expansion. Because of this, levels of air pollution are rapidly increasing. contamination from industry is a major contributor to environmental contamination, which is bad for humans and all other forms of life. Solids and gases, such as dust, pollen, and bacteria, contribute to air pollution. Burning natural gas, coal, or wood creates carbon monoxide, carbon dioxide, nitrogen dioxide, sulfur oxide, chlorofluorocarbons, particulate matter, and other air pollutants. Major health issues, including lung and breathing disorders, have been linked to prolonged exposure to dirty air. About 3.8 million people each year are killed by exposure to gasoline fumes in their houses. Air pollution is responsible for the premature deaths of 4,2 million people worldwide every year. The air quality in which 90% of the world's population resides is below the standards set by the World Health Organization. According to the Southeast Asia Analysis of IQAir conducted by Greenpeace, approximately 120,000 people in India will be killed by air pollution and related ailments in 2020.The study found that air pollution cost India's GDP 2 trillion rupees.

This highlights the significance of maintaining a vigilant vigilance on air quality. Primary pollutants and secondary pollutants are the two most common forms of air pollution. Primary pollutants are those that enter the environment unfiltered. When two main pollutants combine or react with one another or with other components of their environment, a secondary pollutant is produced. Air pollution is just one effect that pollutants have on their environments. Other issues that have worsened in recent years include acid rain, global warming, aerosol generation, and photochemical smog.

Predicting the weather is a crucial step in reducing air pollution. Machine Learning (ML) models can be used for this purpose. In order to educate a computer to create models, machine learning is used. It is a subfield of AI that trains computers to anticipate future events with increasing accuracy. In order to identify patterns and tendencies, ML may examine a wide variety of data. Statistics and advanced mathematics are employed for this purpose.

Air quality has been difficult to monitor due to its steady decline. The frequency with which air quality is measured can be used to estimate the level of pollution present. According to the data gathered by the sensors, we can see exactly where and how much pollution is there. The ML model and this information can be used to develop strategies for reducing pollution. A MQ-135 air quality sensor, a MQ-5 sensor, and an optical dust sensor make up the hardware device. These three sensors, which are linked to an Arduino uno

MACHINE LEARNING ALGORITHM FOR PREDICTING AIR POLLUTION

[#1]**SANGEM AJAY,**

[#2]**Dr.V.BAPUJI,** ***Associate Professor& HOD,***

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

Abstract: The air quality monitoring system collects information on contaminants from multiple sites to maintain optimal air quality. It is currently the most pressing issue. The release of hazardous chemicals from industrial sources, as well as car emissions, damage the atmosphere. Today's main cities have dangerously high levels of air pollution that exceed the government-mandated air quality index standard. It has a tremendous impact on a person's health. Air pollution predictions can be made using Machine Learning (ML) techniques. Machine learning (ML) combines statistics and computer science to improve prediction accuracy. Machine learning (ML) is used to calculate the Air Quality Index. A variety of sensors and a microcontroller known as an Arduino Uno are used to collect the data. The K-Nearest Neighbor (KNN) approach is then used to anticipate air quality.

Keywords: Machine Learning, KNN, AQI, Arduino, sensors.

1. INTRODUCTION

One of the most pressing problems humanity faces today is air pollution. Industry activity is picking up speed as a result of the brisk economic expansion. Because of this, levels of air pollution are rapidly increasing. contamination from industry is a major contributor to environmental contamination, which is bad for humans and all other forms of life. Solids and gases, such as dust, pollen, and bacteria, contribute to air pollution. Burning natural gas, coal, or wood creates carbon monoxide, carbon dioxide, nitrogen dioxide, sulfur oxide, chlorofluorocarbons, particulate matter, and other air pollutants. Major health issues, including lung and breathing disorders, have been linked to prolonged exposure to dirty air. About 3.8 million people each year are killed by exposure to gasoline fumes in their houses. Air pollution is responsible for the premature deaths of 4,2 million people worldwide every year. The air quality in which 90% of the world's population resides is below the standards set by the World Health Organization. According to the Southeast Asia Analysis of IQAir conducted by Greenpeace, approximately 120,000 people in India will be killed by air pollution and related ailments in 2020.The study found that air pollution cost India's GDP 2 trillion rupees.

This highlights the significance of maintaining a vigilant vigilance on air quality. Primary pollutants and secondary pollutants are the two most common forms of air pollution. Primary pollutants are those that enter the environment unfiltered. When two main pollutants combine or react with one another or with other components of their environment, a secondary pollutant is produced. Air pollution is just one effect that pollutants have on their environments. Other issues that have worsened in recent years include acid rain, global warming, aerosol generation, and photochemical smog.

Predicting the weather is a crucial step in reducing air pollution. Machine Learning (ML) models can be used for this purpose. In order to educate a computer to create models, machine learning is used. It is a subfield of AI that trains computers to anticipate future events with increasing accuracy. In order to identify patterns and tendencies, ML may examine a wide variety of data. Statistics and advanced mathematics are employed for this purpose.

Air quality has been difficult to monitor due to its steady decline. The frequency with which air quality is measured can be used to estimate the level of pollution present. According to the data gathered by the sensors, we can see exactly where and how much pollution is there. The ML model and this information can be used to develop strategies for reducing pollution. A MQ-135 air quality sensor, a MQ-5 sensor, and an optical dust sensor make up the hardware device. These three sensors, which are linked to an Arduino uno

SECURE AND PRIVATE DATA STORAGE IN IOT USING BLOCKCHAIN TECHNOLOGY

[#1]PEDDI GANGAIAH,
[#2]B.ANVESH KUMAR, ***Assistant Professor,***
[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT

The Internet of Things (IoTs) is a network of sensing devices with diverse capabilities that can be used for a number of tasks. Due to limited data management abilities, limited storage, and security issues, it is extremely difficult to protect networks from unauthorized information access and effectively utilize storage in such settings. Few of the data storage and security options investigated by researchers are suitable for WSN-enabled IoTs. For secure communication in Internet of Things (IoT) devices employing wireless sensor networks (WSN), a blockchain-based decentralized architecture with authentication and privacy-preserving mechanisms is being developed. A cloud computing system communicates with sensor nodes and base stations via protocols for registration, certification, and revocation. The cluster heads use this method to deliver the accumulated data to the BS. As a result, BS keeps all vital data on a decentralized blockchain and sends large amounts of data to the cloud. BS removes all certificates revoked by rogue nodes from the blockchain. The effectiveness of the proposed method is evaluated using detection precision, certification latency, computational and communicational overheads. Simulation, comparison analysis, and security validation results reveal that the proposed technique outperforms existing solutions.

1. INTRODUCTION

One of the most well-known, useful, and preeminent technologies of the present day, the Internet of Things (IoTs) has revolutionized wireless communication and information processing [1]. Internet-enabled "things" (or "IoTs") are those that can be recognized, analyzed, controlled, and localized online. Since the internet is capable of both communication and processing, it can be used to link nearly all IoT devices already in use, enabling the development of new and better uses for these devices [2]. The Internet of Things relies on a vast network of sensor nodes for its monitoring, sensing, and automation capabilities. Together, these nodes form Wireless Sensor Networks (WSNs), which are essential to the IoT [3] due to their ability to detect and track any objects in their immediate vicinity.

Sensor nodes, sometimes known as "motes," are inexpensive, easy to deploy, can communicate with one another, and may cover large regions [4]. By combining sensing, processing, and communication capabilities in a wireless medium, sensor nodes in WSNs allow for real-time tracking and identification of physical events. WSNs are used for a variety of purposes, including but not limited to monitoring, sensing, broadcasting, and data processing [5] [6]. The information volume, however, is enormous and expanding at an unprecedented rate, thus this challenge must be met.

Now, in the information era. WSNs are used in many fields and industries, from the military and business to smart homes and healthcare to surveillance and environmental monitoring and agriculture. [7] [8]. The sensor nodes that make up a WSN have finite resources, including time, memory, processing speed, and communication speed. Thus, as the Internet of Things raises demand for WSNs, new difficulties in effectively implementing them arise. Additionally, security is

SECURE GROUP MANAGEMENT FOR CLOUD-BASED SHARED DATA ENABLES PUBLIC AUDITING AND PROTECTS USER PRIVACY

[#1]**PADIGELA SUSMITHA,**
[#2]**Dr.D.SRINIVAS REDDY,** ***Associate Professor,***
[#3]**Dr.V.BAPUJI,** ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT: Cloud storage enables users to store their data remotely and access high-quality apps and services on demand from a shared pool of reconfigurable computing resources, eliminating the need to manage and retain their data locally. However, because users no longer physically control the outsourced data, ensuring its integrity in cloud computing is difficult, especially for users with low computational capacity. Furthermore, users should not have to worry about cloud storage integrity; rather, they should be able to access it as if it were local. As a result, providing public auditability for cloud storage is critical so that users may rely on a third party auditor (TPA) to check the accuracy of outsourced data while feeling secure. The auditing technique should not generate any additional online constraints for users or vulnerabilities affecting user data privacy in order to appropriately and successfully construct a TPA. We present a private public auditing mechanism for a secure cloud storage system in this research. We broaden our investigation so that the TPA can audit multiple consumers effectively and concurrently. The recommended solutions are both provably secure and exceptionally effective, according to a rigorous security and performance assessment.

Index Terms—Data storage, privacy-preserving, public auditability, cryptographic protocols, cloud computing.

1. INTRODUCTION

Cloud computing has been conceptualized as the forthcoming enterprise information technology (IT) framework, owing to its extensive array of unparalleled benefits in the history of IT. These advantages include on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid resource elasticity, usage-based pricing, and risk transference. The advent of cloud computing has brought about significant disruptions, leading to a comprehensive revolution in the manner in which enterprises employ information technology. The process of centralizing data or outsourcing it to the cloud is a fundamental element of this paradigm shift. From the standpoint of users, encompassing both individuals and IT companies, the practice of remotely storing data in a flexible and on-demand manner through cloud technology presents appealing benefits.

These advantages include alleviating the burden of storage management, enabling universal data access across different geographical locations, and eliminating the need for capital expenditures associated with hardware, software, and personnel maintenance, among various other advantages. The advent of cloud computing has rendered these advantages increasingly enticing, yet it has also unveiled novel and formidable security risks to users' outsourced data. As cloud service providers (CSPs) are separate administrative organizations, the act of data outsourcing involves relinquishing full authority over the fate of the user's data. The accuracy of cloud-based data is degraded as a result of the considerations outlined below.

Cloud infrastructures are subject to a diverse range of internal and external data integrity concerns, however they are notably more robust and reliable compared to personal PCs. Allegations have been made regarding instances of service disruptions and security breaches that have impacted prominent cloud providers. Furthermore, cloud service providers (CSPs) have the potential to deceive cloud customers in regards to the actual whereabouts of their outsourced data due to many factors. For example, a Cloud Service Provider (CSP) may opt to remove data that has remained inactive for an extended period in order to reduce costs. Alternatively, the CSP can choose to conceal occurrences of data loss as

A HYBRID DEEP LEARNING APPROACH FOR DETECTING CYBER BULLYING IN THE TWITTER SOCIAL MEDIA PLATFORM

#1**SANNAPURI GAYATHRIRANI,**
#2**Dr.V.BAPUJI,** ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

ABSTRACT: Cyberbullying (CB) is becoming more common in online entertainment situations. Given the popularity of social media and its widespread use by people of all ages, it is critical to keep the platforms safe from cyberbullying. DEA-RNN, a hybrid deep learning model for CB identification on Twitter, is introduced in this study. The proposed DEA-RNN model combines an improved Dolphin Echolocation Algorithm (DEA) with Elman-type recurrent neural networks (RNNs) to reduce training time and fine-tune the Elman RNNs' parameters. Using a dataset of 10,000 tweets, we fully evaluated DEA-RNN and compared its performance to that of cutting-edge algorithms such as Bi-LSTM, RNN, SVM, Multinomial Naive Bayes (MNB), and Random Forests (RF). The results of the experiments demonstrate that DEA-RNN was superior in every situation. In terms of detecting CB on the Twitter site, it outperformed previously considered strategies. In scenario 3, DEA-RNN fared better, with an average accuracy of 90.45%, precision of 89.52, recall of 88.98, F1-score of 89.25, and specificity of 90.94%.

Index terms: cyber bullying, social media, Recurrent Neural Network, Deep Learning.

1. INTRODUCTION

The most common locations for people of all ages to interact online are social media platforms like Facebook, Twitter, Flickr, and Instagram. In addition to facilitating hitherto impossible types of communication and connection, these platforms have facilitated negative phenomena like stalking. Cyberbullying is a sort of psychological abuse with far-reaching implications for our culture. Young individuals who spend a lot of time switching between different social media sites are particularly vulnerable to cyberbullying. Because of the widespread usage of social media sites like Twitter and Facebook and the anonymity they provide, these platforms are particularly susceptible to CB. Facebook and Twitter account for 14% of all abuse in India, with 37% of that coming from teenagers [1]. When it comes to your mental health, cyberbullying may be harmful and could lead to more severe issues. Anxiety, sadness, stress, and social and emotional problems associated with cyberbullying are major contributors to suicide. Therefore, it is important to have a system in place for identifying instances of cyberbullying in online content such as posts, tweets, and comments.

How Twitter identifies abusive content is the primary topic of this piece. Finding instances of cyberbullying in tweets and taking preventative measures are crucial given the growing prevalence of the issue on Twitter [5]. As a result, there's an increasing demand for research on cyberbullying on social networks to better understand the issue and provide solutions [6]. Handling trolling on Twitter is a full-time job in and of itself [7]. Furthermore, it is laborious to go through social media posts in search of cyberbullying. For instance, tweets tend to be succinct, rife with slang, and peppered with emojis and gifs. Therefore, it is not possible to infer someone's motivations or values from their social media activity alone. Covert forms of bullying, such as passive aggression or sarcasm, can sometimes be difficult to identify. Despite the fact that cyberbullying can be difficult to detect

AN EFFICIENT PRICING SCHEME FOR DATA MARKETS IN REAL TIME ENVIRONMENT

#1**RIMSHA TAHREEM,** *M.Tech Student,*

#2***Dr. E.SRIKANTH REDDY***, *Associate Professor,*

#3***Dr. N.CHANDRAMOULI***, *Associate Professor &HOD,*

Department of Computer Science and Engineering

VAAGESWARI COLLEGE OF ENGINEERING, KARIMANGAR, TELANAGANA.

ABSTRACT: *The society's insatiable appetites for personal data are driving the emergence of data markets, allowing data consumers to launch customized queries over the datasets collected by a data broker from data owners. In this paper, we study how the data broker can maximize its cumulative revenue by posting reasonable prices for sequential queries. We thus propose a contextual dynamic pricing mechanism with the reserve price constraint, which features the properties of ellipsoid for efficient online optimization and can support linear and non-linear market value models with uncertainty. In particular, under low uncertainty, the proposed pricing mechanism attains a worst-case cumulative regret logarithmic in the number of queries. We further extend our approach to support other similar application scenarios, including hospitality service and online advertising, and extensively evaluate all three use casesover MovieLens 20M dataset, Airbnb listings in U.S. major cities, and Avazu mobile ad click dataset, respectively. The analysis and evaluation results reveal that: (1) our pricing mechanism incurs low practical regret, while the latency and memory overhead incurred is low enough for online applications; and (2) the existence of reserve price can mitigate the cold-start problem in a posted price mechanism, thereby reducing the cumulative regret.*

1. INTRODUCTION

Nowadays, tremendous volumes of diverse data are collected to seamlessly monitor human behaviors, such as product ratings, electrical usages, social media data, web cookies, health records, and driving trajectories.

However, for the sake of security, privacy, or business competition, most of data owners are reluctant to share their data, resulting in a large number of data islands. Because of data isolation, potential data consumers (e.g., commercial companies, financial institutions, medical practitioners, and researchers) cannot benefit from private data. To facilitate personal data circulation, more and more data brokers have emerged to build bridges between the data owners and the data consumers. Typical data brokers in industry include Factual [2], DataSift [3],

Datacoup [4], CitizenMe [5], and CoverUS [6]. On the one hand, a data broker needs to adequately compensate the data owners for the breach of their privacy caused by using their data to answer any data consumer's query, thereby incentivizing active data sharing. On the

IDENTIFYING PHISHING WEBSITES AND URLS A REAL-WORLD EXAMPLE UTILIZING DIFFERENT LOGIN URLS

#1MADUPU RAHUL,

#2P.SATHISH, *Assistant Professor,*

#3Dr.V.BAPUJI, *Associate Professor& HOD,*

Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

ABSTRACT: A web service is required for Internet communication software to function. The use of deceptive ways to steal personal information is on the rise. While convenient, it introduces numerous security flaws into the Internet's private infrastructure. One of several security concerns to web services is web phishing. Experienced users can detect phishing attacks, however novice users frequently prioritize security. Phishing is the practice of impersonating respectable website operators in order to steal sensitive user data. Phishing poses a significant risk to web security. Violent websites encourage internet crime and stifle the expansion of web services. As a result, there has been a significant effort to develop a comprehensive solution to ban the websites. Our idea is a literacy-focused strategy to categorizing webpages as benign, spam, or harmful. Our system only looks at URLs, not web page content. As a result, program stalling and drug users' web surfing dangers are reduced. Due to learning methodologies, our solution beats blacklisting services in generality and substance.

Keywords: Security; Web Services; URL; Vulnerabilities

1. INTRODUCTION

During the day, our primary concentration is on online work. Using a system and an internet connection in many ways simplifies both professional and personal life. This platform improves sales and operations in the commercial, medical, academic, information, financial, aeronautics, exploration, infrastructure, entertainment, and welfare sectors. Because of the advancement of mobile and wireless technology, drug users can now connect to a network and surf the internet 24 hours a day, seven days a week. Despite its ease, this system has revealed information security problems. As a result, online drug users must secure their computers. Data theft and other crimes can be committed by cybercriminals, hackers, and fair-limited users. The purpose is to access the system or its data in multiple methods, or to get specific data. Bushwhackers communicate with a variety of drug traffickers in order to gather knowledge and profit. According to Kaspersky, an attacker will cost between $108,000 and $1.4 billion by 2019, depending on the intensity of the attack. The billionaire spent $124 billion on global security products and services. Phishing is the most prevalent cybersecurity attack, and its perpetrators are cyber threats. Most victims are vulnerable to phishing attempts due to their lack of expertise about web operations, computer networks, and associated technology. It is easier to target drug addicts with fake websites and incentives to click on them than it is to breach the information security system. A malicious website imitates the original site's visual aesthetics and user experience by using copyrighted content such as the association's logos and other visual elements. Individuals and businesses have suffered considerable financial and reputational harm as a result of drug users unintentionally browsing phishing website URLs. The most dangerous cyberattack in this category was phishing. For this attack, cybercriminals use dispatch or other social media networks. Bushwhackers entice drug users

USING MACHINE LEARNING TO DETERMINE BLOCKED URLS

[#1]ANDRI BHAVANI,

[#2]Dr.V.BAPUJI, ***Associate Professor& HOD,***

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT: A malicious URL, often known as a malicious website, is a common mechanism for storing unwelcome content such as spam, malicious ads, phishing, and drive-by vulnerabilities, to mention a few. It is critical to identify harmful URLs as soon as possible. Techniques such as blacklisting, regular expression, and signature matching have already been employed in research. These methods are useless for detecting versions of existing malicious URLs or wholly new URLs. To address this issue, a machine learning-based solution might be proposed. This type of solution necessitates extensive research in the fields of feature engineering and feature representation of security objects such as URLs. Furthermore, feature engineering and feature representation resources must be regularly updated to handle both versions of current URLs and whole new URLs. Deep learning has enabled AI systems to achieve human-level performance in a range of disciplines, even outperforming human vision in a number of computer vision applications. They can automatically extract the best feature representation from raw inputs. Deep URL Detect (DUD) encrypts raw URLs using character level embedding for use and translation in the cyber security arena. Character level embedding is a cutting-edge method for encoding characters in numeric form in natural language processing (NLP). Hidden layers in deep learning architectures take properties from character level embedding and then apply a non-linear activation function to determine whether the URL is potentially dangerous. We compare and contrast different cutting-edge deep learning-based character level embedding approaches for detecting counterfeit URLs in this paper. Several trials are carried out in order to determine the most effective deep learning-based character level em- bedding model. All experiments employing various deep learning-based character level embedding models are carried out for 500 epochs at a learning rate of 0.001. In all test instances, DUD beats all comparable deep learning-based character level embedding algorithms in terms of performance and computing cost. Furthermore, character level embedding models-based deep learning architectures outperformed n-gram representation. This is because the embedding records the sequence and interrelationship of all the characters in the URL.

Keywords: Cyber security, Cybercrime, Malicious URL, Machine learning, Deep learning, Character embedding

1. INTRODUCTION

Malicious Uniform Resource Locators (URLs) are frequently used by threat actors to host and transmit malicious content. They are crucial to the success of many cyberattacks. Harmful URLs are commonly spread through email and social media, and are often shared using Facebook, Twitter, WhatsApp, Orkut, and other social media apps. Users understand that the information found here has not been vetted or approved. Hackers can gain access to the hosting platform if an unsuspecting user accesses the website via the URL. The user is then vulnerable to frauds that attempt to steal

SAFELY STORING AND DELIVERING INFORMATION FROM INTERNET OF THINGS DEVICES

#1SAMEENA KOUSAR, ***MCA Student,***
#2B.ANVESH KUMAR, ***Assistant Professor,***
#3Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

Abstract: Data sharing among intelligence communities is critical for expediting data analysis and supporting decision-making in order to guarantee the security of the nation. If an internet-safe data exchange channel is available, data sharing inside an intelligence community may become more possible. However, transporting data between many parties is problematic due to the issue of confidentiality and the possibility of being exposed to unauthorized users and attackers. As a result, this study offers a blockchain-based secure data-sharing architecture for intelligence agencies. This document goes into great detail on the procedure, rules, and policies involved. To assess the intention to implement the proposed paradigm, the technology readiness and acceptance model (TRAM) was applied. The optimism, innovativeness, discomfort, and insecurity characteristics were investigated in this study to determine their link with the technical Acceptance Model (TAM). According to the study, personality traits and feelings can influence the adoption process and intention to use a blockchain-based data-sharing model for system integration inside the intelligence community. This study discovered that blockchain technology might be used in a data-sharing architecture created expressly for the intelligence community based on the established dimensions.

Index Terms: *Blockchain, secure data sharing, Technology Acceptance Model, Technology Readiness Index.*

I. INTRODUCTION

Innovations in digital technology are essential for sharing information throughout a society. The intelligence community had abandoned its reliance on HUMINT in favor of Signal Intelligence (SIGINT) and open source information (OSINT) for its investigations. In order to make choices and formulate plans for the nation's security, the intelligence agency must collect precise and accurate data.

Researchers have proposed integrating blockchain as an extra technology to increase data security after various investigations demonstrated blockchain's remarkable performance. [1], [2]. To make sure that the technology, methods, procedures, and policies associated with blockchain adoption within the intelligence community are thoroughly evaluated before implementation, a comprehensive research on the topic is required.

In this research, we investigate how blockchain technology might be applied to the formulation of secure information exchange protocols. For the intelligence community, this article proposed a conceptual secure blockchain-based data-sharing paradigm based on the requirements, norms, and rules. The technology readiness and acceptance model (TRAM) was developed with the proposed model as its basis. The proposed dimension is a direct result of the selected variables. This study is the first to our knowledge to examine the adoption of a blockchain-based data-sharing paradigm within the intelligence community, and it is also the first to do so using TRAM theory.

ONLINE REVIEW FRAUD DETECTION: SUPERVISED AND SEMI-SUPERVISED LEARNING

[#1]**NEHA YASMEEN,** ***MCA Student,***
[#2]**B.SHARAN,** ***Assistant Professor,***
[#3]**Dr.V.BAPUJI,** ***Associate Professor& HOD,***
Department of Master of Computer Application,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

ABSTRACT: With more and more people keeping an eye on social media, it's important to look at social data to figure out how people act. So, sentiment analysis is used to look at social data, especially Twitter Tweets, to see if the user's opinion about movie reviews is accurate. This study uses relevant keywords taken from social media and web reviews to build a full vocabulary and find hidden patterns of relationships. In recent years, there has been a big rise in the number of people who shop online. Online reviews have a big effect on how people decide what to buy when they shop online. Many people look at product or store reviews before deciding where to shop or what to buy. Because there are a lot of benefits to making fake reviews and doing other kinds of fraud, there has been a noticeable rise in the number of fake spam reviews on digital platforms that are used to review goods and services. Reviews that aren't true include those that are made up, reviews that aren't asked for, and reviews that aren't very good. Positive reviews of the product under consideration have the potential to attract more customers and boost sales, while negative reviews have the potential to lower demand and hurt sales. The above review is dishonest or fraudulent because it was written with the aim of tricking people or hurting the company's reputation by giving potential customers false information. The goal of our study is to find out how true the review is. In our work, we used three different classification algorithms: the Naive Bayes Classifier, the Logistic Regression, and the Support Vector Machines.'

Keywords: e-commerce, product recommender, product demographic, microblogs, recurrent neural

1. INTRODUCTION

Every day, there are new technological developments and advancements. Newer technology are always replacing older ones. People are able to do their jobs better with the help of this cutting-edge technology. One prominent manifestation of this technical development is the emergence of online markets. The internet marketplace allows us to make bookings and purchases at our convenience. Almost everyone reads product reviews before deciding whether or not to buy a given product or item. Because of this, it's possible that these reviews will have a major effect on the brands' reputations. The advertising and promotion of goods and services are also profoundly affected by these assessments. Therefore, there are more and more examples of fraudulent reviews on the web. People can post phony reviews to boost the reputation of their own items, which is harmful to the interests of legitimate businesses and consumers. Competitors' firms might also suffer damage to their reputations from fake bad reviews. Researchers looked explored several methods for identifying fabricated reviews on the web. Some depend on the nature of the review itself, while others are set by the author's choices and input during the review's creation. The text-based approach places more weight on the review's actual text or language than does the User behavior-based approach, which looks at factors like the reviewer's number of posts, location, and

DEPENDABLE AND ACCURATE SPAM DETECTION THROUGH SUPERVISED LEARNING

#1BONGONI SANDHYA, ***Department of MCA,***
#2B.ANVESH KUMAR, ***Assistant Professor,***
#3Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT: A collection of millions of devices with sensors and actuators that are linked via wired or wireless channels for data transmission. Over the last decade, it has grown rapidly, with more than 25 billion devices expected to be connected by 2020. The amount of data released by these devices will multiply many times over in the coming years. In addition to increased volume, the device generates a large amount of data in a variety of modalities A network of millions of sensors and actuators linked for data transfer via wired or wireless channels. It has expanded substantially in the last decade, with over 25 billion devices expected to be connected by 2020. The volume of data released by these devices will increase in the coming years. The gadget creates a large amount of data in a variety of modalities, with data quality varying based on its speed in terms of time and location. In such a setting, machine learning algorithms can play a critical role in ensuring biotechnology-based security and authorisation, as well as anomaly detection to improve usability and security. Attackers, on the other hand, frequently employ learning algorithms to exploit system weaknesses. As a result of these factors, we propose that machine learning be used to detect spam on devices to improve device security. The Spam Detection Using Machine Learning Framework is proposed to accomplish this goal. Using a number of metrics and input feature sets, this system analyzes four machine learning models. Based on the modified input attributes, each model computes a spam score. This score reflects the device's dependability based on a number of factors. According to the data, the proposed technique is more effective than other current options.

Keywords: *Collection of data, Authorization, Anomalous detection, Support Vector Machine, K-nearest neighbour, Spam.*

1. INTRODUCTION

As a result of advancements in communication and computing technologies, it is now much simpler and faster to transfer data from one location to another. Users from all over the world can exchange data on a variety of platforms. Many people consider email to be the most convenient, inexpensive, and rapid method of international communication. However, there are other methods that can be used to assault an email, the most frequent and potentially harmful of which is spam. Getting pointless emails is annoying because it costs time and energy. Keep in mind that these emails could contain malicious material that is disguised as an attachment or a URL. Because of this, system security may be jeopardized. Spam occurs when bad actors use electronic communication channels to transmit numerous irrelevant messages to a large number of recipients. As a result, ensuring the safety of email systems is crucial. Malicious software including viruses, worms, and Trojan horses can

ANALYZING EMOTIONAL SIMILARITY IN ONLINE STORE REVIEWS TO BUILD USER TRUST IN MINING

#1JELLA ANUHYA, ***Department of MCA,***

#2B.ANVESH KUMAR, ***Assistant Professor,***

#3Dr.V.BAPUJI, ***Associate Professor& HOD,***

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

Abstract- - Electronic commerce is the activity of exchanging goods and services over a computer network. Aside from purchasing and selling, many people utilize the internet for research purposes, such as seeing what's new in the market or comparing prices before making a purchase. E-commerce platforms are generally seen as valuable resources that provide users with an experience, feelings, and desire in purchasing things based on consumer evaluations. This form of data includes consumer opinions on products that can show interest, attitudes, and expressions. Several research theories suggest that people who have similar sentiments toward similar topics are more likely to trust one another. We suggest in this paper that asking and accepting recommendations and feelings in e-commerce networks is a form of reciprocal trust. A scientific observer studied consumers while they were shopping. To explore user trust and similarity, a sentiment similarity analysis approach oriented toward E-commerce system reviews is provided. In essence, trust may be separated into two types: direct trust and trust propagation, which results in a trust connection between two people. We present an entity-sentiment word pair mining approach for extracting similarity features. Sentiment similarity is used to calculate the direct trust degree. The transitivity feature is utilized to compute the trust spread. The proposed trust model is used to calculate the shortest path and to present an improved shortest path algorithm to determine the propagation trust relationship between users. A large dataset of E-commerce reviews is gathered to evaluate the efficacy of the algorithms and the viability of the models. Sentiment similarity analysis, according to the experimental data, can be a beneficial tool for generating user confidence in E-commerce systems.

I. INTRODUCTION

The same behavior might also be referred to as "business." However, the phrase is more commonly used to describe how the Internet is influencing fields like marketing, logistics, and communication within enterprises. E-commerce is defined here as the action of transacting business online. Business-to-Business (or B2B) The proliferation of information and communication technologies (ICTs), notably the Internet, has led to the widespread adoption of electronic commerce (e-Commerce) in the commercial sector. Consumers who have access to the global market via the Internet have a distinct advantage because of their ability to shop around, learn about items, and see if order fragmentation influences prices. Customers have easy access to comparing the offerings of various e-commerce businesses due to the transparency of the industry. For instance, when making an online purchase, the purchaser's rivals are literally a mouse click away. Customers have much greater leeway to cancel an online purchase than they would in a physical store if they are dissatisfied with the website's items, prices, or services. As far as the Vendors are concerned, a

EFFICIENT MESSAGE AUTHENTICATION FOR PRIVACY PRESERVING INTERNET OF THINGS

[#1]MUPPU SANDHYARANI, Department of *MCA*,

[#2]Dr.V.BAPUJI, *Associate Professor& HOD,*

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT: In recent years, the Internet of Things (IoT) has evolved fast as a key component of the next generation Internet. IoT devices generate/collect massive amounts of data that machine learning and big data analytics can use for a variety of purposes, including improving people's lives. Because IoT relies on machine-to-machine (M2M) communication, data security and privacy are critical challenges that must be addressed in order to prevent various cyber assaults (such as impersonation and data pollution/poisoning). Nonetheless, building lightweight and diverse IoT security solutions is a difficult challenge due to limited processing power and the diversity of IoT devices. We present an efficient, safe, and privacy-preserving message authentication mechanism for IoT in this work. Our technique is more versatile and efficient than prior systems since it supports IoT devices with varied cryptography settings and enables for offline/online computing.

Index Terms—Internet of Things, hop-by-hop authentication, integrity, source privacy.

1. INTRODUCTION

The Internet of Things (IoT) makes it possible to build a system out of many disparate parts, each of which contributes to the whole in some way. With machine learning, data may be easily shared and retrieved among programs with little to no human intervention required. After the development of computers and the Internet, this innovation is the third most important in the field of information technology. Interactions between the IoT and various sectors of society and the economy pave the way for the development of a pervasive online existence. That way, people can talk to things and, more crucially, to other people and things that are connected to them. Several new fields of study have emerged thanks to the Internet of Things (IoT), such as smart home systems (SHSs), intelligent transportation systems (ITSs), machine learning, big data, and others.

Machine-to-machine (M2M) communication, specifically between a massive number of IoT devices, will be the main form of network traffic in the future. Machine learning and big data analytics, to name just two examples, rely heavily on the authenticity and reliability of the massive amounts of data collected and transmitted by IoT devices. Data that has been intentionally introduced or manipulated can result in incorrect forecasts and choices. Therefore, it is crucial to maintain the validity and integrity of the gathered data to ensure the veracity and precision of machine learning and big data analysis.

Both a public-key based strategy and a symmetric-key approach have emerged to guarantee safe message delivery in the IoT domain. Since symmetric-key operations are more efficient than public-key operations, the computational cost of the symmetric-key methodology is lower than that of the public-key method. However, in the context of symmetric-key based techniques inside a heterogeneous and extensive IoT network, the management of cryptographic keys presents a considerable difficulty. Furthermore, the intermediate

ENHANCED SECURITY PROVISION FOR EFFICIENT AND SECURE DYNAMIC ID-BASED AUTHENTICATION KEY AGREEMENT SYSTEM

[#1]NAKATI SUSMITHA, ***Department of MCA,***
[#2]P.SATHISH, ***Assistant Professor,***
[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

Abstract: A realistic two factor (2f) authentication is used for smart card password verification. As a result, the two variables are "dynamic ID-based" or "anonymous". To preserve user privacy, smart cards have a tamper-resistant security feature. Reverse engineering and power analysis approaches were used to obtain certain private data from the smart card memory. Rather than relying on a vulnerable database, smart card verification is securely implemented in memory. Daily applications such as e-banking, e-health, and e-governance store password tables on a server. Throughout the login process, the user's identity is sent in clear across public networks. Many non-tamper-resistant OTP solutions have been developed, all with ambitious design processes. A 2f system can ensure that a user with a valid OTP and password will be approved by the server.

IndexTerms:*2fauthentication,EMV,AKE,DA2localsecure*

1. INTRODUCTION

Using cloud computing, files and data may be stored on a scalable network that can be made public or private on the fly. As this technology advanced, the cost of several services, including app hosting, data storage, computation, and content distribution, decreased significantly. Forrester [1] defines cloud computing as an elastic computing model that provides on-demand or subscription-based service to end users. The design of a computer should prioritize bandwidth, data processing, and storage.

2. RELATED WORKS

The security of cloud storage can be managed with an optional two-factor login method. The data is encrypted before being sent from the sender to the recipient via a server in the cloud. The sender must know the recipient's name; all other details are irrelevant. Both the sender and the recipient need to know two things for the message to be deciphered. The first is the lock and key to the storage chest.

A connected gadget that serves to safeguard the machine. You can't find out what's concealed unless you have all the pieces. If you lose your device or it gets stolen, the first thing you should do is disable the security features. Data stored in the cloud is encrypted using the procedures in the security device. The buddy is briefed on the process. Cloud servers are not able to decipher encrypted data. It appears that this strategy will be effective and can be implemented. Accessing data stored in the cloud requires a security device, a secret key, and knowledge of the encrypted data. When the device is turned off, the cloud server immediately and secretly replaces the matching cipher text, making the data even more secure.

The EMV protocol and its implementation were found to have serious flaws by the author. The fundamental issue is that nonces for EMV cards were generated using counters, secret algorithms, and time stamps, which is not secure. There is now public knowledge of a scam "pre-play" attack involving counterfeit cards. Proof-of-concept assaults on automated teller machine and terminal equipment, along with their breadth and potential weak points, are mapped as part of a vulnerability discovery methodology. Issues were discovered in widely deployed ATMs utilized by major corporations. Banks refused to compensate the customer since EMV cards cannot be duplicated and the customer committed a mistake. The card's

CLOUD-BASED UPLOADING AND DELETION OF COUNTING BLOOM FILTER DATA

#1RAGI SARITHA, ***Department of MCA,***
#2P.SATHISH, ***Assistant Professor,***
#3Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR,TELANGANA

ABSTRACT: Because of the rapid expansion of cloud storage, which may substantially reduce local storage overhead, an increasing number of data owners are preferring to outsource their data to a cloud server. Data owners who want to move cloud service providers must now use cloud data transfer since different cloud service providers provide varying levels of data storage service, including security, reliability, access speed, and pricing. As a result, the key problem that data owners confront is figuring out how to safely migrate data from one cloud to another while also removing the data from the original cloud. To address this issue, we present a novel counting Bloom filter-based technique in this paper. In addition to safe data transport, the proposed approach can provide permanent data deletion. Furthermore, the proposed system may be able to meet the requirements for public verifiability without the involvement of a trustworthy third party. Finally, we provide a simulated implementation to demonstrate the viability and effectiveness of our proposal.

Key words *— Cloud storage, Data deletion, Data transfer, Counting Bloom filter, Public verifiability.*

1. INTRODUCTION

The cloud computing model includes the ever-evolving concepts of parallel computing, distributed computing, and grid computing. Cloud storage has become one of the most widely used applications of cloud computing. A vast number of storage devices can be linked together in a network, simplifying data storage and access for both individuals and organizations. Customers can save significantly on on-premises hardware, software, and man-hours by storing their data in the cloud. The convenience and versatility of cloud storage have led to its widespread adoption in both private and professional contexts. This is why a growing number of individuals and organizations with restricted means are opting for cloud storage solutions. Data privacy, data integrity, data availability, and data erasure are just some of the additional security challenges that cloud storage must address because of the division of data custody and management that occurs when data is outsourced. The widespread adoption of cloud storage could be slowed if these concerns, especially those related to data deletion, are not adequately addressed. Deleting data at the end of its useful life affects how successfully the entire data life cycle may conclude. This is crucial for protecting confidentiality and anonymity in stored information. There has been a lot of focus on data encryption and protection, but far less on data deletion. There are a few challenges and bottlenecks that need to be fixed immediately, despite the fact that there have been a number of established ways to remove outsourced data in the

Published in the year: **2023**

Published By:
Prof. Bholanath Dutta
President: MTC Global ®

MTC Global
Educate, Empower, Elevate

MTC Global Trust ®
A Global Think Tank in Higher Education
Bangalore, India
www.mtcglobal.org I president@mtcglobal.org

Title: Education in Sustainable Development
ISBN: **978-93-5810-911-5**

Price: Rs. 500/-
US $ 30
Brought to you by

Research & Publications

MTC Global Research and Publication Wing
MTC Global®, Bangalore, India

ROLE OF STAKEHOLDERS IN DELIVERING QUALITY MANAGEMENT EDUCATION FOR SUSTAINABLE DEVELOPMENT

Dr. E. Hari Prasad Sharma
Associate Professor, Dept. of Business Management
Vaageswari College of Engineering - Karimnagar

Introduction

The development of management education can be traced back to 18th century. Since 18th century, there are tremendous changes are found in management education. In India, though, management education was derived from the western management thought and practice, Indian management scholars and practitioners are drawing some extrapolations from epics like, Maha Bharatha, Ramayana, Bhagavad Geetha and other Puranas and Shastras. Management education was evaluated with emerging trends in industrial engineering and closely related with the disciplines like psychology, philosophy, sociology, economics, accounting, statistics and mathematics. In India, management education is seen as special and superior discipline. Students select management education not because for sake but for exposure, experience to create something innovative which useful to the society and motivated by the consequences associated with management education.

In India, the government announced its New Industrial Policy in 1991 with the process of Liberalization, Privatization and Globalization (LPG). These reforms in the economy led to replace the traditional approach of education to more efficient professional education and introduced advance courses in education to bond with the industry requirement which have more economic value in present time. Management education got a special recognition with the changing of time. Along with the traditional courses like financial management, marketing management and human resource management, new functional areas like Operations Management, Supply Chain Management, Rural Management, International Business Management, Digital Marketing, Data Analytics, Financial Analytics and HR Analytics are also covered in management education to meet the industry demand for highly efficient management people. As a result of this, management education became one of the most trending courses which provide a good career to the youth. With this, in India, private eduprenuers are entering in management education and investing an enormous amount of funds by establishing business schools.

Management Education in India

GCS PUBLISHERS

A Msme Registered Company Udyam-ap-04-0018434

Gst No 97isepk7907q1zs

Website Www.gcspublishers.com/email Id:info@gcspublishers.com

ISBN 978-93-94304-09-3

CERTIFICATE OF PUBLICATION

This is to certify that the book entitled

VLSI DESIGN

ISBN: 978-93-94304-09-3

Authored by

Dr. UDUTHA RAJENDER

from

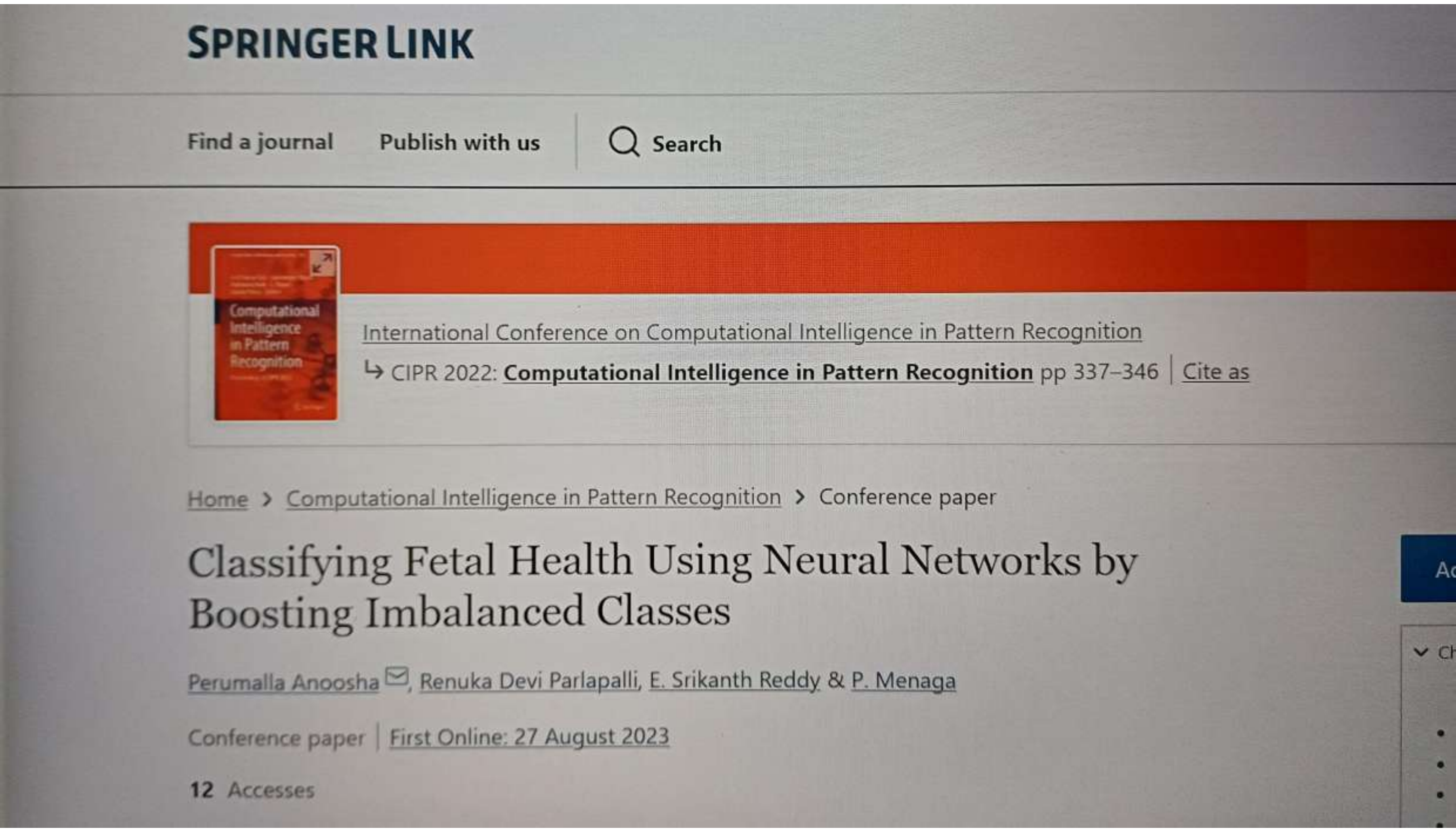
Assistant Professor,Department of Electronics and Communication Engineering,
Vaageswari College of Engineering, Beside L.M.D Police Station, Ramakrishna Colony,
Karimnagar, Telangana, India - 505 527.

has been published in

GCS PUBLISHERS, INDIA

K. Dhana Lakshmi

Editor Chiff



International Conference on Computational Intelligence in Pattern Recognition

↳ CIPR 2022: **Computational Intelligence in Pattern Recognition** pp 337–346 | Cite as

Home > Computational Intelligence in Pattern Recognition > Conference paper

Classifying Fetal Health Using Neural Networks by Boosting Imbalanced Classes

Perumalla Anoosha, Renuka Devi Parlapalli, E. Srikanth Reddy & P. Menaga

Conference paper | First Online: 27 August 2023

12 Accesses

2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) | 979-8-3503-9737-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICACCS57279.2023.10112842

Monitoring Indoor and Outdoor Air Quality Using Raspberry PI Processor

Vijayakumar Sajjan
Malla Reddy University,
Hyderabad, India.
vijay.sajjan26@gmail.com

Srikanth Reddy E
Vaageswari College of Engineering,
Karimnagar, India.
srikanth574@gmail.com

C P Pavan Kumar Hota
Anil Neerukonda Institute of Technology and Sciences,
Visakhapatnam, India.
hcppavankumar@gmail.com

B Kiran Kumar
Marri Laxman Reddy Institute of Technology,
Hyderabad, India.
kiranbadhavat@gmail.com

Abstract—**The parameters of the environment to be monitored are selected as temperature, humidity, extent of CO, quantity of CO2, detection of leakage of any fuel - smoke, alcohol, LPG. The values of these parameters are transmitted by the use of Zigbee Pro (S-2) to a base station in which they will be being monitored. In order to display tremendous of air, a Wireless sensor community (WSN) based totally new framework is proposed that is based totally on statistics acquisition and transmission. The charge of temperature and humidity are transmitted over Bluetooth also simply so absolutely everyone within the kind of the machine can check it over their clever telephones and laptops as those parameters maintain importance to anyone. CO, a risky parameter is monitored with a further precaution. A textual content message is despatched to the bottom station thru GSM module whenever its extent exceeds a selected secure restrict meant for a specific software. As humans usually spend greater than 90 % in their time in indoor environments. This artwork describes the system (IAQ), a low-rate indoor air exquisite tracking wireless sensor community system, superior the use of Raspberry pi Processor, XBee modules and micro sensors, for storage and availability of tracking facts on an internet portal. Other sensors can be brought for tracking precise pollutants. The outcomes reveal that the machine can offer an powerful indoor air quality assessment to prevent exposure chance. In fact, the indoor air tremendous can be extremely particular compared to what is anticipated for a first-rate dwelling surroundings.**

Keywords—IOT, Wireless sensor community, IAQ, Raspberry PI, GSM, Etc.

I. Introduction

Internet-of-Things(IoT) has emerge as very attractive inside the contemporary wi-fi communications context. The improvement in embedded system has proved to a reliable answer in monitoring and controlling the surroundings monitoring machine. The task goals at constructing a machine which can be used on universally at any scale to screen the parameters in a given environment. With the evolution of miniaturized sensor devices coupled with wi-fi technologies it's miles feasible to remotely monitor the parameters such as temperature, Gas(co2) in air and lots of greater. In this context, integration of WSN with gasoline sensors will provide powerful approach to observe, screen and manage the diverse vital gadgets in AQMS. We will be the use of raspberry-pi as our fundamental board and sensors will acquire all the real time data from environment and this actual time information will be fetched by way of the web server and show it.

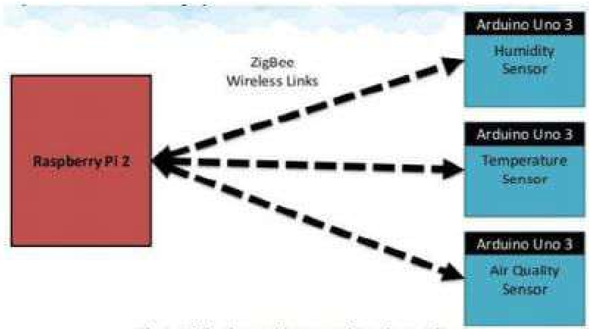


Fig 1: Utilization architecture of Raspberry Pi2 processor

User can get entry to this records from everywhere thru Internet. As proven in fig. 1: utilization architecture of Raspberry Pi2 processor can be very use full in industries on this gadget we have a temperature sensor and gas sensor's while any sensor's reaches the edge limits it will send a notification to Twitter and also photograph will seize by using the camera and sent alert mail to person can reveal.

- This utility is very use complete in industries.
- One of the primary motive for international warming is carbon dioxide emission into the atmosphere.

979-8-3503-9737-6/23/$31.00 ©2023 IEEE

(12) PATENT APPLICATION PUBLICATION (21) Application No.202341047816 A
(19) INDIA
(22) Date of filing of Application :15/07/2023 (43) Publication Date : 01/09/2023

(54) Title of the invention : SYNTHESIS OF TWO DIMENSIONAL INORGANIC MATERIALS FOR OPTOELECTRONICS

(51) International classification	:B82Y0030000000, H01L0021020000, B82Y0020000000, H01L0029240000, B82Y0040000000
(86) International Application No Filing Date	:PCT// :01/01/1900
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Dr.N.Kotilingaiah
Address of Applicant :PDF Scholar, Department of Chemistry, Srinivas University, Mangalore, Karnataka, -574146 ----------- ----------
2)Dr.J.Venkateshwarlu
3)Dr. Gajula Kiran
4)Dr. J. Sandhya
5)B.M Praveen
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr.N.Kotilingaiah
Address of Applicant :PDF Scholar, Department of Chemistry, Srinivas University, Mangalore, Karnataka, -574146 ----------- ----------
2)Dr.J.Venkateshwarlu
Address of Applicant :Assistant Professor, Guru Nanak Institute of Technology, Ibrahimpatnam, Ranga Reddy, Telangana - 501506 ----------- -----------
3)Dr. Gajula Kiran
Address of Applicant :Assistant Professor, TKR College of Engineering, Meerpet, (D) Rangareddy, Hyderabad, Telangana ---------- -----------
4)Dr. J. Sandhya
Address of Applicant :Assistant professor, Vaageswari College of Engineering, Thimmapur, Karimnagar Telangana ----------- ----------
5)B.M Praveen
Address of Applicant :Director, Research and Innovation Council, Srinivas University, Mangalore, Karnataka - 574146 ----------- ----------

(57) Abstract :
The layered crystalline solids that make up two-dimensional materials have strong bonding in the crystal plane but weak vander-Waals forces between the neighbouring atomic layers. The unique structure of 2D materials gives them a variety of amazing capabilities. First, compared to their bulk parent materials, 2D materials exhibit several new optical and electrical properties as a result of quantum confinement in the direction perpendicular to the 2D plane. The integration of 2D materials with photonic structures is made easier by the surfaces of these materials being naturally passivated and lacking dangling bonds. Additionally, by creating vertical heterostructures with a variety of 2D materials, the problem of lattice mismatch may be avoided since the various layers are joined together by van der Waals forces.

No. of Pages : 13 No. of Claims : 3