© FEB 2024 | IRE Journals | Volume 7 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV7I8-1712448

AI Techniques for Web-Based Fraud Detection: A Review

R. PRASANTH REDDY[1], NAGAVELLI YOGENDER NATH[2], GATTU RAMYA[3], SYED ABDUL HAQ[4]

[1]*Assistant Professor, Department of Computer Science & Engineering, RSR Engineering College*
[2]*Assistant Professor, Department of Computer Science & Engineering (AI&ML), Sumathi Reddy Institute of Technology for Women, Hyderabad.*
[3]*Assistant Professor, Department of Computer Science & Engineering, Vignan Institute of Management and Technology for Women, Hyderabad.*
[4]*Assistant Professor, Department of Computer Science & Engineering, Malla Reddy Engineering College, Hyderabad.*

Abstract- ***Web-based frauds pose significant challenges due to their evolving nature, sophisticated methods, and the vast amount of data involved. However, advancements in AI and machine learning offer promising possibilities for effective detection and prevention. By continuously updating detection models and employing robust measures, it is possible to mitigate the risks associated with online frauds and protect individuals and organizations from its adverse effects. This paper review establishes a foundation for future advancements in AI-driven fraud detection, contributing to the ongoing efforts to safeguard individuals and organizations against fraudulent activities. This paper presents machine learning approaches for web-based fraud detection, addressing the limitations of traditional methods and offering robust solutions for identifying and preventing web-based frauds. The proposed frameworks demonstrate high accuracy and precision in detecting various types of web-based fraud, highlighting their potential for practical applications.***

Index Terms—Deep Learning, Web-based Fraud, Fraud Detection, Intelligent Approaches Web-based

I. INTRODUCTION

Fraud is a deliberate misrepresentation or concealment of information with the intent to deceive or manipulate someone into making decisions that result in harm or financial loss. When fraud occurs, it erodes people's confidence in financial, governmental, or social institutions, leading to reduced trust in systems designed to protect and serve the public. Beyond monetary losses, the impact of frauds extends to reputation damage, legal consequences, and operational disruption, which can be devastating for individuals, businesses, and governments. Its impact on the economy is profound, making it challenging for the government and private entities to implement effective policies and practices [1]. The Association of Certified Fraud Examiners (ACFE) defines fraud as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets" (ACFE, 2002).

Frauds can be further considered into offline frauds and online frauds [2]. While Offline frauds occur through traditional means, online frauds occur through digital channels. Both offline and online frauds pose significant threats, causing considerable damage to victims. Therefore, understanding the different types of frauds and the methods used by fraudsters is essential for developing effective prevention and detection strategies.

Offline Frauds: These are traditional, physical frauds that occur without the internet or digital platforms. These frauds involve face-to-face interactions or manipulation of physical documents. Common examples include identity theft , check fraud, insurance fraud, credit card skimming, investment scams, and counterfeiting. Identity theft involves stealing personal information, such as social security numbers or credit card details. Check fraud involves illegally using checks to pay for goods or services, often involving altering or forging checks. Insurance fraud involves false claims to receive unwarranted

© FEB 2024 | IRE Journals | Volume 7 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV7I8-1712448

payouts from insurance companies. Credit card skimming involves capturing information from legitimate transactions, often at ATMs or point-of-sale terminals. Investment scams involve persuading individuals to invest in fraudulent schemes or businesses, often involving Ponzi schemes or "too good to be true" opportunities.

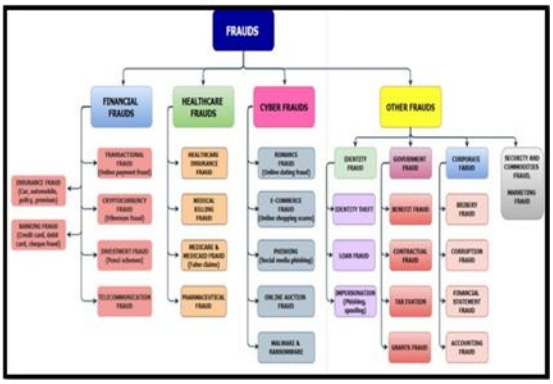

Figure 1: Taxonomy of the most common areas of frauds and their types

Online Frauds: Increasingly prevalent and sophisticated, online frauds exploit individuals and organizations through the Internet and digital technologies. Examples include phishing, malware, online shopping frauds, credit card frauds, social engineering, advance fee scams, auction and retail schemes, and cyber extortion. Phishing involves sending fraudulent emails or messages to trick recipients into providing personal information, while malware distributes malicious software to infiltrate, damage, or disable computers and networks. Online shopping frauds involve setting up fake e-commerce websites to deceive consumers into paying for goods or services that do not exist, while credit card frauds involve using stolen or hacked information for unauthorized transactions. Social engineering involves manipulating individuals into divulging confidential information through online interactions, while advance fee scams promise large sums of money or valuable items in exchange for an upfront fee. Auction and retail schemes deceive buyers by misrepresenting products or failing to deliver items after payment. Further, cyber extortion threatens to damage, disclose, or withhold access to data or systems unless a ransom is paid, with ransom ware attacks being a common [3].

II. WEB-BASED FRAUDS AND THEIR TYPES

The widespread use of the Internet has become integral to daily activities, resulting in the generation of massive amounts of user-generated data. This data explosion offers numerous benefits, such as personalized services, enhanced user experiences, and improved decision-making processes. However, it also poses significant challenges, notably the rise of web-based frauds [4]. Online and web-based frauds are often used interchangeably, but they have distinct meanings depending on the context. Online frauds involve various digital activities, including email phishing, social media scams, online banking, and mobile app frauds. In contrast, web-based frauds are more specific to websites and applications, such as e-commerce frauds, phishing websites, online auction frauds, etc. Online frauds involve any digital interaction, not just web-based ones. Thus, online frauds can be considered as superset of web-based frauds.

A recent report by the Indian Cybercrime Coordination Centre revealed that digital financial frauds accounted for a staggering 1.25 lakh crore rs over the last three years. According to the National Cybercrime Reporting Portal (NCRP), in 2023, at least 10,319 crore rs was reported to be lost by victims of digital financial frauds. Due to the increasing reliance on digital platforms for commerce, communication, and transactions, the detection and prevention of web-based frauds have become a critical concern. Web-based frauds can be broadly categorized into:

Financial Frauds: These refer to intentional deception or manipulation used to gain financial benefits unlawfully. They typically involve deceitful practices that trick individuals or institutions into giving up money or assets. Financial frauds are split into cryptocurrency, transactional, insurance, telecommunication, online banking frauds, etc.

Healthcare Frauds: They refer to deceptive practices aimed at charging for more expensive services or procedures than those provided. These types of frauds exploit healthcare systems, services, and financial transactions to gain an undue advantage. They encompass a range of illicit activities that undermine

© FEB 2024 | IRE Journals | Volume 7 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV7I8-1712448

the integrity of healthcare delivery and billing processes. Healthcare frauds can be further distinguished into insurance frauds, medical billing frauds, and pharmaceutical frauds, among others [5].

Cyber Frauds: They refer to fraudulent activities conducted through digital means, involving the use of technology and the Internet to deceive individuals for monetary benefits by fabricated romantic relationships to build trust. Cyber frauds encompass various schemes and tactics that target victims by manipulating online systems and data for financial gain. Cyber frauds can be further distinguished into Online Social Network (OSN) based dating frauds, romance frauds, e-commerce frauds, and phishing, etc. [6]

III. LITERATURE WORK

The rapid expansion of digital technologies has significantly increased the complexity and frequency of fraud, posing substantial challenges to individuals, businesses, and financial institutions. Traditional fraud detection methods, which rely heavily on rule-based systems and manual inspections, have proven inadequate in dealing with the dynamic and complex nature of modern fraudulent activities. These conventional methods often fail to adapt to new fraud patterns and are limited in their ability to process large volumes of data efficiently. In contrast, Artificial Intelligence (AI) has emerged as a powerful solution, offering enhanced accuracy, efficiency, and adaptability in fraud detection tasks.

Fraud has been a persistent issue for centuries, evolving with human society and economic systems. Early detection methods used human intuition and manual checks, such as signature verification and cross-checking physical documents, but often failed to identify new or sophisticated fraudulent activities. The need for advanced detection techniques became apparent as the volume and complexity of online data increased. During the early 2000s, various techniques were commonly used in fraud detection, including rule-based systems, anomaly detection, statistical analysis, association rules, and manual reviews [6-7]. Early digital fraud detection methods were primarily extensions of traditional techniques, implemented through rule-based systems. These systems used predefined rules to flag suspicious activities but had limitations such as being static, inflexible, and prone to high false positive rates. Researchers began employing statistical methods, such as regression analysis, clustering, and Bayesian networks, to address these limitations. Although statistical methods were more sophisticated than rule-based systems, they still had limitations in adapting to rapidly changing fraud tactics and the need for significant human oversight. These methods, however, had limitations such as high operational costs, limited adaptability, high false positives, and inability to handle large data sets effectively. They often allowed fraud to occur before it was identified, leading to disruptions and customer dissatisfaction.

AI-based techniques for web-based fraud detection, encompassing machine learning, network-based, and hybrid methodologies, As the digital landscape evolves, fraud detection approaches are advancing in parallel, with researchers and practitioners adopting cutting-edge techniques to outpace fraudsters and safeguard digital environments [8]. This shift from traditional methods to AI-driven techniques marks a significant evolution in the field of fraud detection.

Machine learning has become a cornerstone of modern fraud detection systems due to its ability to learn from data and identify intricate fraud patterns. It involves learning features and fraudulent patterns from a training dataset and applying this knowledge to detect similar patterns in unseen datasets. [9].

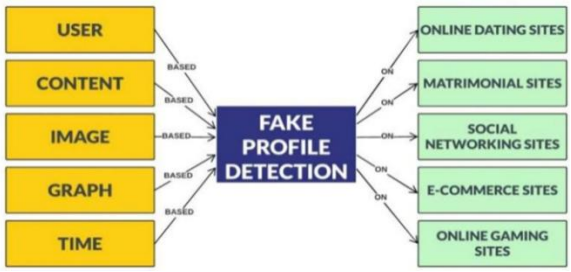

Figure 2: Features for fake profile detection on online social networks

A study performed by [9] focused on identifying fake accounts on Facebook. Their study identified 17 features describing user behavior and constructed learning models using 12 supervised machine learning classification algorithms including k-NN, NB,

Decision Tree, RF, Decision Rule-Based, SVM, and Sequential Minimal Optimization using Weka . Their work achieved a classification accuracy of 79%. Further, [10] focused on detecting malicious accounts on Twitter. They gathered 16 Twitter API attributes such as description, length, followers_count, friends_count, and hashtags_average to employ the Naive Bayes classifier, reporting an accuracy of 90.41%. [11] identified malicious accounts in 82 Arabic and English languages from the Twitter dataset. To categorize the data into fraudulent and actual profiles, they used classifiers such as NB, Multi-Layer Perceptron (MLP), DT, k-NN, and C4.5, with NB obtaining the best results with 95.70% accuracy, 94% precision, and 96% recall. Similarly, [12] developed a "content-based fraudulent website detection method" using sentiment analysis, natural language processing, and supervised machine learning techniques. They used six classifiers viz Bernoulli, LR, NB, Stochastic Gradient Descent, Multinomial Naïve Bayes, and SVM to construct the ensemble classifier using a voting scheme. Their proposed model, consisting of data acquisition, preprocessing, feature extraction, and classification, achieved 97.67% crossvalidated accuracy with a 3.49% false positive rate [13].

The state-of-the-art techniques for web-based fraud detection using various AI approaches, focusing on different datasets feature selection techniques, and MLbased models employed by researchers to combat frauds. The literature survey reveals that various research efforts use imbalanced datasets related to transactional and users' profile datasets, leading to biased model formation [14].

IV. ROLE OF ARTIFICIAL INTELLIGENCE IN FRAUD DETECTION

As fraudulent activities have become more sophisticated and complicated, traditional rulebased fraud detection techniques, which often rely on rule-based systems and statistical methods [15] have demonstrated limitations in effectively identifying or combating frauds. The emergence of new technologies and digital platforms has provided fraudsters with innovative ways to exploit system vulnerabilities.

As a result, there is a growing demand for innovative solutions that take advantage of cutting-edge technologies including Artificial Intelligence (AI), which simulates human intellect in machines, allowing them to think and learn like humans [16]. Data mining techniques help uncover hidden patterns indicative of fraudulent behavior, such as unusual spending patterns or anomalies in transaction frequencies, aiding in the early detection and prevention of financial frauds. It provides the foundational data that AI and other models use to learn and make predictions. Predictive models based on historical data help predict the likelihood of fraudulent activities. These models are built using data mining results and are continuously updated and refined through AI techniques to improve accuracy. Natural Language Processing (NLP) is a field of AI and computational linguistics that aims to enable machines to understand, interpret, and generate human language [17].

In fraud detection, NLP techniques analyze textual data such as user profile descriptions, emails, and chat messages to detect fraudulent content. Text mining, (aka, text analytics) is an AI technique that transforms unstructured data into structured formats by leveraging Natural Language Processing (NLP) to improve analysis. Text mining uses information retrieval, classification, entity recognition, sentiment analysis, and topic modeling to extract meaningful information and patterns from unstructured textual data. It helps identify fraudulent texts in user profiles by classifying them based on keywords and analyzing sentiment and emotional tone, thereby enhancing fraud detection capabilities [18].

Machine Learning

A branch of AI, which uses complex algorithms and data analytics to detect fraudulent actions [19], ML is emerging as a promising approach to enhance accuracy and adaptability in web-based fraud detection. It can be seen as a significant tool because it can learn from previous or recent fraud trends and spot them in future transactions. Thus, ML-based AI systems can analyze large amounts of transactional data, uncover patterns, and identify anomalies that may indicate fraudulent activity. Figure 3 illustrates the ML work-flow framework. ML models require explicit feature extraction and selection, they are less computationally intensive and can run on standard CPUs, offering interpretability and faster training

© FEB 2024 | IRE Journals | Volume 7 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV7I8-1712448

times. ML methods can be broadly categorized into supervised and unsupervised learning.

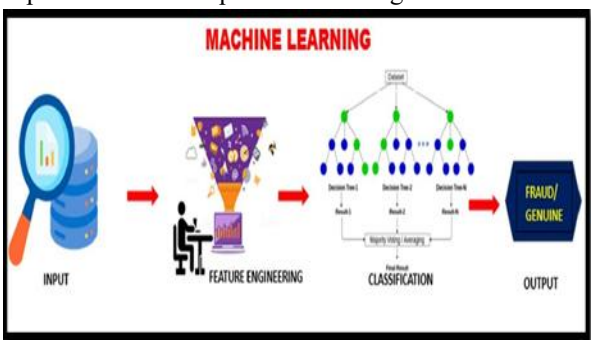

Figure 3: Different types of chest disease

Supervised Machine Learning: Supervised ML involves training a model on labeled data, where the desired output is known. This approach allows the model to learn the relationship between input and target variables [20]. In ML classification, classifiers are broadly categorized into individual and ensemble classifiers as illustrated in Figure 4.

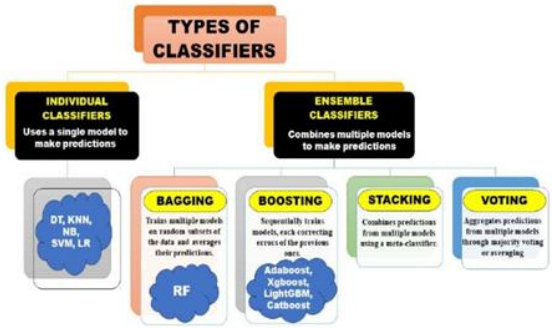

Figure 4: Individual versus ensemble classifiers [21]

Unsupervised Machine Learning: It involves training models on unlabeled data to uncover hidden patterns or structures from large data collection. Common unsupervised ML approaches include clustering, anomaly detection, dimensionality reduction, etc. The clustering techniques for grouping similar objects or users together, enabling the discovery of outliers and unusual clusters that may signify fraudulent users.

Ensemble Learning

Ensemble learning is a meta-method that combines projections from various models to improve predictive performance. It is effective for classification issues as it reduces errors of a single base classifier by combining several weak classifiers. This results in superior accuracy with lower errors and greater consistency, avoiding over-fitting and decreasing bias and variance errors. Bagging and boosting is popular ensemble machine-learning techniques due to their powerful experimental results and theoretical performance guarantees [22].

Bagging: It is a bootstrap aggregation technique that learns homogeneous weak classifiers with high variance and combines their predicted results using regression and majority voting. It increases stability and accuracy while reducing variance.

Boosting: It is a technique that adapts the training set's distribution based on the accuracy of previously constructed classifiers. It aims to create new classifiers that can better categorize rigid samples for earlier ensemble members. Boosting is significant for small sample sizes and high-dimensional samples, and is quick, easy to program, highly adaptable, and accurate.

Deep Learning

A subset of ML that uses deep neural networks with multiple layers to learn hierarchical representations of data, these models effectively process large volumes of complex data, such as images and texts, and can automatically extract intricate fraud patterns from unstructured data sources. DL models are scalable, suitable for big data applications, and can learn directly from raw data to output predictions, requiring less manual feature engineering than traditional ML models. However, DL models require significant time to train and are highly computationally intensive, often needing GPUs or TPUs. They are often considered "black boxes" and are harder to interpret [23].

V. THE PROBLEM OF WEB-BASED FRAUD DETECTION

According to various studies in this field of research, an ideal fraud detection model should be capable of processing a set of user interactions or transactions, identifying and categorizing them into fraudulent or non-fraudulent activities or behaviors. The term "Web-based fraud detection" has recently broadened to include various techniques that go beyond traditional rule-based and statistical approaches, incorporating advanced machine learning methods to

analyze user behaviors and transaction patterns on web resources. Extensive research has focused on improving the accuracy and reliability of fraud detection systems by exploring various aspects such as data collection strategies, data types, preprocessing techniques, feature engineering, and building effective classification models.

Further, it has been observed that the traditional methods for detecting fraudulent profiles rely on supervised machine-learning techniques that use labeled data for training purposes. Such methods detect fake and genuine profiles focusing on account- and content-based features, and semantic analysis of text or a combination of these approaches [24]. On the other side, handling unlabeled data presents a significant challenge in fake profile detection, particularly on online dating platforms where the lack of ground truth labels hampers supervised techniques. Labeling these accounts manually is impractical, making it imperative to explore unsupervised machinelearning methods that can recognize fake profiles without prior labeling.

In healthcare insurance, frauds can take various forms, including rebilling, readmission, unbundling, kickback practices, billing for services that were not rendered or are unnecessary, and the willful omission of information essential to determining the benefits to be paid [25]. In such situations, establishing relationships and interactions among the participating entities through network formation is critical for developing effective healthcare fraud detection methods. A network among these entities can be utilized to extract network-based features, such as centrality measures and community structures, which enhance the detection of patterns indicative of fraudulent activities.

In general, fraudulent activities can occur in any online environment, including e-commerce platforms for financial transactions, the insurance sector, social networks, or any web-based applications. The generic term object or user account is used to denote the entity representing an individual, account, transaction or profile, etc. that interacts with the system and whose behavior is analyzed for potential frauds.

VI. CHALLENGES IN WEB-BASED FRAUD DETECTION

Web-based fraud detection is a crucial field that aims to protect online users and services from fraudulent activities. Despite advancements, the field still faces significant challenges due to the complexity of fraud tactics and the volume of data involved. Research gaps are evident, particularly in applying AI-based techniques for real-time fraud detection [26]. This part discusses some of the most significant challenges associated with web-based fraud detection:

Unavailability of ground-truth data and need for diverse datasets: Fraud detection faces challenges due to the lack of ground-truth data, which is crucial for accurately labeling fraudulent and legitimate transactions. Acquiring this data is often difficult and resource-intensive. Efficient data harvesting tools are essential for gathering comprehensive datasets, but lacking these can hinder effective fraud detection. Further, collecting instances of fake profiles for model training is also a significant challenge. Many unlabeled datasets exist but are not considered due to in-depth analysis and labeling time. Therefore, unsupervised machine learning techniques are useful to identify suspicious users and alert relevant agencies. Imbalanced datasets: Handling imbalanced datasets remains a significant challenge in web-based fraud detection. Many datasets contain a disproportionate number of legitimate transactions compared to fraudulent ones, complicating the training of accurate models. This imbalance can lead to model biases towards the majority class.

Effective feature engineering for finding the best discriminators: The web-based fraud dataset, organized at various granularities, requires extensive subject expertise and time to identify and extract crucial features. Furthermore, the dynamic nature of fraud behaviors needs frequent modifications to feature sets. Different methodologies are necessary for each domain to determine the most discriminating traits, which is typically difficult.

Lack of standard framework for Web-based fraud detection: Data mining frameworks like CRISP-DM and OSEMN offer detailed guidelines for planning and implementing projects, enhancing data analysis,

model development, and result interpretation. However, the lack of standard frameworks in fraud detection systems presents a significant challenge in developing reliable and accurate models.

Selection of efficient classification model: Fraudulent operations can be quite sophisticated and diverse, encompassing a variety of techniques such as identity theft, phishing, intricate financial frauds, and many more. Detecting such a diverse set of fraudulent actions necessitates complex classification approaches and models capable of comprehending and identifying subtle patterns and anomalies. Very few studies have looked into the collaborative impacts of combining supervised, unsupervised, and network-based learning. Such combinations could potentially overcome the limits of utilizing a single approach while improving overall detection performance. A major concern in fraud detection is the high rate of false positives, where legitimate transactions are incorrectly flagged as fraudulent. False positives can lead to stakeholders' dissatisfaction, loss of trust, and unnecessary operational costs as legitimate transactions are scrutinized or blocked [27]. Selecting an effective classification model remains a significant challenge in terms of reducing false positives while maintaining high detection accuracy.

Lack of network-based approach: It has been found that important information regarding fraud detection and its transmission throughout interconnected networks can be obtained using network analytics. The use of network-based techniques in fraud detection is rare, although it can be helpful in situations where entities and their interactions are involved.

VII. CONCLUSION

Despite significant advancements in AI for fraud detection, several research gaps remain. One of the primary challenges identified is the need to handle large datasets to efficiently train DL models. High-performance computing resources are essential for training complex DL models, especially when dealing with large-scale data.

In the domain of web-based fraud detection, particularly with AI-driven approaches, several challenges arise that can impact the accuracy and reliability of detection systems. Fraudulent content or actions on the web are often complex, evolving, and diverse, making it difficult to achieve perfect classification accuracy. User behavior can be inconsistent, with fraudulent user's constantly changing tactics to avoid detection. Moreover, the data used for training AI models often contains class imbalance, incomplete records, or non-representative samples, which complicates the learning process. Fraud detection is dynamic, and continuous learning and adaptation are necessary to maintain accuracy over time. Comprehensive, diverse training repositories and an iterative approach to model development can help overcome these challenges and improve overall system performance.

REFERENCES

[1] Abdo, A. A., Alhajri, K., Alyami, A., Alkhalaf, A., Allail, B., Alyami, E., & Baaqeel, H. (2023). AI-based Spam Detection Techniques for Online Social Networks: Challenges and Opportunities. Journal of Internet Services and Information Security, 13(3), 78-103.

[2] Baxter, G. J., Dorogovtsev, S. N., Goltsev, A. V., & Mendes, J. F. F. (2012). K-core organization in complex networks. Handbook of Optimization in Complex Networks: Theory and Applications, 57, 229-252.

[3] Adikari, S., & Dutta, K. (2020). Identifying fake profiles on LinkedIn. arXiv preprint arXiv:2006.01381.

[4] Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. Journal of Big Data, 8, 1-21.

[5] Akyon, F. C., & Kalfaoglu, M. E. (2019). Instagram fake and automated account detection. In 2019 Innovations in intelligent systems and applications conference (ASYU), IEEE, 1-7.

[6] Isabona, J., Imoize, A. L., & Kim, Y. (2022). Machine Learning-Based Boosted Regression Ensemble Combined with Hyperparameter Tuning for Optimal Adaptive Learning. Sensors, 22(10), 3776.

[7] Johnson, J. M., & Khoshgoftaar, T. M. (2019). Medicare fraud detection using neural networks. Journal of Big Data, 6(1), 63.

[8] Alam, M. N., Sarma, D., Lima, F. F., Saha, I., & Hossain, S. (2020). Phishing attacks detection using machine learning approach. In 2020 third international conference on smart systems and inventive technology (ICSSIT), IEEE, 1173–1179.

[9] Kerrysa, N. G., & Utami, I. Q. (2023). Fake account detection in social media using machine learning methods: literature review. Bulletin of Electrical Engineering and Informatics, 12(6), 3790-3797.

[10] Liu, Q., & Vasarhelyi, M. (2013). Healthcare fraud detection: A survey and a clustering model incorporating geo-location information. In 29th world continuous auditing and reporting symposium (29WCARS), Brisbane, Australia, 1-10.

[11] Kontsewaya, Y., Antonov, E., & Artamonov, A. (2021). Evaluating the effectiveness of machine learning methods for spam detection. Procedia Computer Science, 190, 479-486.

[12] Kovács, F., Legány, C., & Babos, A. (2005). Cluster validity measurement techniques. In 6th International symposium of hungarian researchers on computational intelligence, 35, 1-11

[13] Usman, M., Zubair, M., Hussein, H. S., Wajid, M., Farrag, M., Ali, S. J., ... & Habeeb, M. S. (2021). Empirical mode decomposition for analysis and filtering of speech signals. IEEE Canadian Journal of Electrical and Computer Engineering, 44(3), 343-349.

[14] Naveen Sai Bommina, Nandipati Sai Akash, Uppu Lokesh, Dr. Hussain Syed, Dr. Syed Umar, "A Hybrid Optimization Framework for Enhancing IoT Security via AI-based Anomaly Detection", International Journal on Recent and Innovation Trends in Computing and Communication, (2023) ISSN: 2321-8169 Volume: 11 Issue: 3.

[15] Uppu Lokesh , Naveen Sai Bommina , Nandipati Sai Akash , Dr. Hussain Syed , Dr. Syed Umar. (2021). Deep Reinforcement Learning with Genetic Algorithm Tuning for Intrusion Detection in IoT Systems. International Journal of Communication Networks and Information Security (IJCNIS), 13(3), 582–595.

[16] Mr DD Sarpate, "Design of Dual Band Microstrip for satellite Applications", 2nd International Conference on Recent Innovations in Engineering & Technology 2020

[17] Singh, A., Gupta, M., Raj, A., Gupta, S. K., & Habeeb, M. S. (2020, December). TWDM-PON: The Enhanced PON for Triple Play Services. In 2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE) (pp. 1-5). IEEE.

[18] Uppu Lokesh, Naveen Sai Bommina, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Designing Energy-Efficient and Secure IoT Architectures Using Evolutionary Optimization Algorithms", International Journal of Applied Engineering & Technology, Vol. 4 No.2, September, 2022.

[19] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Multi-Objective Genetic Algorithms for Secure Routing and Data Privacy in IoT Networks", International Journal of Communication Networks and Information Security (IJCNIS), (2020), 12(3), 632–643.

[20] M. Mukhedkar, D. Rohatgi, V.A. Vuyyuru, K.V.S.S. Ramakrishna, Y.A. Baker El-Ebiary, V.A. Asir Daniel, "Feline wolf net: A hybrid lion-grey wolf optimization deep learning model for ovarian cancer detection", Int. J. Adv. Comput. Sci. Appl., 14 (9) (2023)

[21] Nandipati Sai Akash, Naveen Sai Bommina, Uppu Lokesh, Hussain Syed, Syed Umar, "Optimized Block Chain-Enabled Security Mechanism for IoT Using Ant Colony Optimization", International Journal on Recent and Innovation Trends in Computing and Communication, (2023), 11(10), 1226–1233.

[22] Mr. Dikshendra Daulat Sarpate, and Dr. B.G Nagaraja, "CONVOLUTION NEURAL NETWORK-BASED SPEECH EMOTION RECOGNITION USING MFCCS", International Journal of Communication Networks and Information Security, 2023/12/10

[23] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Privacy-Preserving Federated Learning for IoT Devices with Secure Model Optimization", International Journal of Communication Networks and Information Security (IJCNIS), (2021), 13(2), 396–405.

[24] Naveen Sai Bommina, Uppu Lokesh, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Optimized AI Models for Real-Time Cyberattack Detection in Smart Homes and Cities", International Journal of Applied Engineering & Technology, Vol. 4 No.1, June, 2022.

[25] Divya Rohatgi, Dr. Tulika Pandey, "Regression Test Selection Framework for Web Services", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 03, MARCH 2020.

[26] Umar, Syed, Bommina Naveen Sai, Nagineni Sai Lasya,Doppalapudi Asutosh, and LohithaRani. "Machine Learning based Sentiment Analysis of Product Reviews Using DeepEmbedding." Journal of Optoelectronics Laser 41, no. 6(2022): 108-113.

[27] K. Kartheeban, K. Kalyani, S. K. Bommavaram, D. Rohatgi, M. N. Kathiravan, and S. Saravanan, “Intelligent Deep Residual Network based Brain Tumor Detection and Classification,” in 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Dec. 2022, pp. 785–790. doi:10.1109/ICACRS55517.2022.10029146.