

www.ijprems.com

editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 04, Issue 07, July 2024, pp: 1388-1393

2583-1062 Impact Factor:

e-ISSN:

5.725

REVIEW PAPER ON AN EFFECTIVE ARTIFICIAL INTELLIGENCE MODEL FOR THE DETECTION AND CLASSIFICATION OF CREDIT CARDS (CC) SCAMS

Nitesh Sharma¹, Mr. Jitender Saini²

¹M Tech Scholar, Ganga Institute of Technology & Management Kablana Jhajjar, India.

²Assistant Professor, Ganga Institute of Technology & Management Kablana Jhajjar, India.

ABSTRACT

The increase in instances of credit card fraud has required the creation of advanced detection and categorization systems. This research paper examines the latest breakthroughs in artificial intelligence (AI) models specifically developed to counteract credit card fraud. The study showcases the efficacy of different machine learning (ML) and deep learning (DL) techniques, such as supervised and unsupervised learning methods, anomaly detection, and neural network topologies, by analysing research conducted between 2021 and 2023. The text also covers the incorporation of sophisticated data preprocessing techniques and feature selection approaches.

The paper discusses the difficulties encountered in this field, including the unbalanced characteristics of fraud detection datasets and the ever-changing strategies employed by fraudsters. The key findings suggest that the use of hybrid models, which integrate various techniques and utilise ensemble learning, greatly enhances the accuracy of detection and the performance of classification. This text examines the deployment of fraud detection systems that operate in real-time, as well as the significance of interpretability in AI models. It highlights the crucial nature of model transparency and dependability.

To summarise, this work proposes potential areas for future research, such as integrating explainable AI (XAI) to improve the transparency of models and employing transfer learning to enhance their adaptability. It is advisable to consider utilising blockchain technology for the purpose of safeguarding transaction data. This review is a significant reference for researchers and practitioners seeking to create or improve AI-powered solutions for detecting credit card scams, ultimately leading to more secure and dependable financial systems.

Key Words: Credit card fraud, artificial intelligence, machine learning, deep learning, anomaly detection, neural networks, hybrid models, ensemble learning, data preprocessing,

1. INTRODUCTION

In the current era of digital technology, where financial transactions are predominantly carried out online and through electronic channels, the threat of credit card fraud has become a widespread worry for financial institutions, merchants, and consumers. Credit card fraud involves a variety of illegal behaviours, including unauthorised purchases, stolen card information, and complex schemes involving identity theft and account takeovers. The financial ramifications of such fraudulent activities are significant, resulting in the loss of billions of dollars on a global scale every year.

Conventional approaches to identify and stop credit card fraud, such as rule-based systems and manual transaction monitoring, are no longer sufficient due to the constantly changing fraud techniques and the large number of transactions handled each day. These approaches frequently face challenges in keeping up with the rapidity and intricacy of contemporary fraudulent schemes, resulting in substantial financial losses and harm to the reputation of firms.

In order to tackle these difficulties, there has been a swift progress in utilising artificial intelligence (AI) and machine learning (ML) methods for the purpose of detecting and preventing fraud. Artificial intelligence (AI) provides the potential for improved fraud detection systems that are adaptable and efficient. These systems can analyse large volumes of transactional data in real time, recognise patterns that suggest fraud, and promptly take action to reduce risks.

This review paper seeks to examine the most recent advancements and breakthroughs in artificial intelligence (AI) models that are specifically designed for the identification and categorization of credit card fraud. This research aims to provide a thorough examination of the efficacy of different artificial intelligence (AI) and machine learning (ML) strategies in countering fraudulent activities by examining studies published from 2021 to 2023.

AI has made significant progress in credit card fraud detection by utilising supervised learning algorithms, such as logistic regression and support vector machines (SVM). These algorithms can analyse labelled datasets and classify transactions as fraudulent or legitimate based on historical patterns. Unsupervised learning methods, like as clustering and anomaly detection, are increasingly being used to identify abnormal patterns in transactional behaviour that could suggest fraudulent activity, without relying on labelled data.

Moreover, deep learning (DL) methods, specifically neural networks, have demonstrated potential in improving fraud



www.ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1388-1393

2583-1062 Impact Factor: 5.725

e-ISSN:

editor@ijprems.com

detection skills by autonomously acquiring intricate patterns and interconnections in data. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are being used more and more to analyse transaction sequences and detect tiny irregularities that suggest fraud.

In addition to algorithmic breakthroughs, the incorporation of sophisticated data pretreatment techniques, such as feature engineering and dimensionality reduction, is essential for enhancing the accuracy and efficiency of AI models. Feature selection techniques, such as information gain and recursive feature elimination, aid in prioritising significant features that have the largest impact on the accuracy of fraud detection, while also decreasing the computing burden.

Nevertheless, the implementation of artificial intelligence in the detection of credit card fraud presents certain difficulties. The disproportionate distribution of fraudulent transactions compared to genuine ones in fraud datasets is a substantial challenge for conventional ML models, resulting in biassed predictions and reduced accuracy in detecting fraud. Furthermore, the comprehensibility of AI models continues to be a crucial issue, as stakeholders demand clarity in comprehending the decision-making process in order to have confidence in and verify the effectiveness of fraud detection systems.

Ultimately, the purpose of this review article is to offer a comprehensive understanding of the latest advancements in credit card fraud detection using artificial intelligence. It will emphasise significant patterns, difficulties, and potential areas for further investigation. This study aims to enhance the development of more resilient and efficient AI solutions that can protect financial transactions and counter the growing threat of advanced fraud schemes by integrating recent research findings and developments. The ultimate objective is to cultivate enhanced security, trust, and resilience in financial systems, thereby benefiting businesses and consumers in an increasingly interconnected digital economy.

2. LITERATURE REVIEW

In this study, Gupta et al. (2023) provides a thorough examination of the latest developments in utilising Artificial Neural Networks (ANNs) for the purpose of detecting credit card fraud. The research examines the utilisation of Artificial Neural Networks (ANNs) in effectively managing the intricacies of transactional data for precise identification of fraudulent actions. The text explores different artificial neural network (ANN) structures and techniques used to improve fraud detection systems. This includes advanced approaches like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) that fall under the umbrella of deep learning. The analysis highlights the incorporation of sophisticated methods such as transfer learning and ensemble learning to enhance the resilience and effectiveness of fraud detection algorithms. In addition, the authors examine difficulties such as imbalanced datasets, interpretability of models, and scalability, and provide approaches to tackle these problems. The review offers useful insights into the changing landscape of artificial neural network (ANN)-based fraud detection systems, emphasising their potential and future research and development paths in financial security.

Narra et al. (2023) concentrates on identifying false information pertaining to COVID-19 through the usage of specific feature sets. The research focuses on the task of effectively managing the infodemic that arises during the pandemic, characterised by the rapid dissemination of misinformation. The writers investigate sophisticated methodologies to discern crucial characteristics that differentiate genuine and counterfeit news items. Their technique intends to enhance the precision of false news detection systems by examining textual content and contextual information that is specific to COVID-19. This project aims to improve techniques for addressing disinformation during public health emergencies by employing machine learning and natural language processing technologies specifically designed for pandemic-related information.

Megdad, Abu-Nasser, and Abu-Nazer (2022) investigate the utilisation of machine learning (ML) methods in identifying fraudulent financial transactions. The study examines the efficacy of machine learning algorithms in detecting patterns that are indicative of fraudulent activity inside financial data. Multiple machine learning (ML) models, including decision trees, support vector machines, and ensemble approaches, are assessed for their capacity to manage the intricacy and magnitude of transactional data. The authors emphasise the significance of feature engineering and model optimisation in improving the precision and effectiveness of fraud detection systems. Moreover, the research discusses the difficulties related to imbalanced datasets and the comprehensibility of machine learning models in the context of financial fraud detection. The paper provides valuable insights into utilising machine learning for proactive fraud detection techniques, emphasising advancements and prospective avenues for future research in this crucial domain of financial security.

Ali and Razak (2022) examine the utilisation of machine learning (ML) methods for identifying instances of financial fraud. The study examines different machine learning algorithms and their efficacy in detecting fraudulent tendencies in financial transactions. The efficacy of prominent machine learning models, including logistic regression, random forests, and neural networks, is examined in terms of their capacity to process substantial amounts of transactional data



Vol. 04, Issue 07, July 2024, pp: 1388-1393

e-ISSN : 2583-1062 Impact Factor: 5.725

www.ijprems.com editor@ijprems.com

and identify irregularities that may suggest fraudulent activity. The authors highlight the significance of feature selection, preprocessing approaches, and model evaluation in enhancing the efficiency of fraud detection systems. In addition, they analyse the influence of datasets with imbalances on the accuracy of models and provide methods to address these difficulties. The study emphasises the significance of machine learning (ML) in improving the effectiveness and precision of fraud detection procedures. It provides valuable information on how ML can be practically applied and suggests future paths for boosting financial security measures.

Gupta, Lohani, and Manchanda (2021) examined the use of the naive Bayes algorithm for identifying financial fraud in datasets with a significant imbalance. The paper focuses on the substantial problem presented by the disparity between fraudulent and non-fraudulent transactions in financial data. Naive Bayes is selected for its simplicity and efficacy in probabilistic categorization, even when there is a scarcity of data. The authors suggest improvements to conventional naive Bayes methods to raise the accuracy of recognising fraudulent activity while minimising the occurrence of false positives. Their research highlights the significance of preprocessing methods, such as oversampling and under sampling, to restore balance in datasets and thereby improve the performance of the algorithm. The results indicate that although naive Bayes is a straightforward method, it may be a useful tool for detecting financial fraud. This is especially true when it is customised to handle the complexities of imbalanced datasets that are common in financial transactions. Reddy et al. (2021) conducted an extensive investigation that specifically examined the use of neural networks (NNs) in the detection of credit card fraud. The assessment encompasses recent progress, approaches, and obstacles faced in implementing neural networks for this crucial undertaking. Neural networks are renowned for their capacity to comprehend intricate patterns and adjust to evolving fraudulent strategies, rendering them well-suited for identifying abnormal transactions. The authors analyse multiple neural network topologies, including feedforward, recurrent, and convolutional networks, each designed for certain aspects of fraud detection. In addition, they examine methods for improving the performance of neural networks in practical scenarios by reviewing approaches like as feature engineering, data preprocessing, and model optimisation. The challenges that are tackled in this context encompass the imbalance in datasets, scalability concerns, and the requirement for interpretability in neural network-based fraud detection systems. The survey closes by delineating prospective research avenues focused on surmounting these limitations and enhancing the dependability and efficacy of neural network-based fraud detection systems in financial settings.

Jebaseeli T, Venkatesan R, and Ramalakshmi K. (2020) investigated the application of the Random Forest algorithm for detecting fraud in credit card transactions. Springer, a publishing company based in Singapore, conducted a study that utilised Random Forest, an ensemble learning technique renowned for its ability to effectively handle extensive datasets and provide accurate results. The study aimed to detect fraudulent behaviours in credit card transactions. The Random Forest model effectively differentiates between real and fraudulent transactions by utilising data such as transaction amount, location, time, and frequency. The research emphasises the algorithm's capacity to enhance detection rates while minimising false positives, therefore improving security measures in financial transactions. This study enhances the field of fraud detection by showcasing the practical implementation and efficacy of Random Forest in tackling the difficulties presented by fraudulent activity in credit card transactions.

Saheed, Y. K., Hambali, M. A., Arowolo, M. O., & Olasupo, Y. A. (2020) examined the utilisation of Genetic Algorithm (GA) feature selection on Naive Bayes, Random Forest, and Support Vector Machine (SVM) classifiers for the purpose of detecting credit card fraud. The study, presented at the International Conference on Decision Aid Sciences and Applications (DASA), seeks to improve the effectiveness of fraud detection systems by detecting and selecting the most pertinent characteristics from credit card transaction data. Genetic algorithm (GA) is used to optimise subsets of features, enhancing the efficiency and accuracy of classifiers in differentiating between genuine and fraudulent transactions. The authors evaluate the efficacy of Naive Bayes, Random Forest, and SVM in reducing fraud risks in financial transactions by analysing their performance after feature selection. This study highlights the significance of employing feature selection strategies to enhance the performance of machine learning models for fraud detection. It provides useful insights to the domain of financial security and risk management.

Sharma et al. (2020) did an extensive examination of the use of Artificial Neural Networks (ANNs) in the detection of credit card fraud. The study assesses the efficacy of Artificial Neural Networks (ANNs) in detecting fraudulent behaviour in credit card transactions. Artificial neural networks (ANNs) are highly regarded for their capacity to effectively manage intricate, non-linear connections within data, hence significantly improving the precision of fraud detection systems. The paper examines several architectures and procedures used to include artificial neural networks (ANNs) into fraud detection frameworks. It emphasises how these approaches are flexible and enhance performance compared to conventional methods. In addition, the authors analyse problems such as data imbalance and feature selection strategies that are essential for optimising artificial neural network (ANN)-based detection systems. The paper



Vol. 04, Issue 07, July 2024, pp: 1388-1393

2583-1062 Impact Factor: 5.725

e-ISSN:

www.ijprems.com editor@ijprems.com

highlights the importance of artificial neural networks (ANNs) in contemporary fraud detection tactics. It provides valuable insights into how ANNs can be applied and suggests future research and development options for enhancing financial crime prevention.

Aditya Oza's 2019 study, titled "A Survey on Fraud Detection," examines different machine learning methods used for identifying payment fraud. The paper specifically investigates the application of Logistic Regression (LR) and Support Vector Machines (SVM) in this context. The study examines the efficacy of these techniques in detecting fraudulent transactions by utilising characteristics derived from transactional data. Logistic Regression is renowned for its simplicity and interpretability, making it well-suited for early baseline models in fraud detection. Support Vector Machines are particularly adept at dealing with intricate data patterns and are highly efficient in differentiating between valid and fraudulent transactions by utilising nonlinear decision boundaries. Oza's research highlights the significance of utilising a variety of machine learning techniques to improve the accuracy of fraud detection. The research offers a comparative analysis of the LR and SVM techniques, highlighting their individual strengths and limits in addressing payment fraud concerns. The purpose of this extensive survey is to assist professionals and scholars in choosing suitable approaches that align with the unique attributes of their datasets and the types of fraudulent behaviours identified in payment systems. Adepoju et al. (2019) performed a comparative assessment of different machine learning methods for the purpose of detecting credit card fraud. The study investigates the efficacy of several approaches, including supervised learning algorithms such as Logistic Regression, Decision Trees, and Support Vector Machines, as well as ensemble methods like Random Forest and Gradient Boosting Machines. The authors evaluate the effectiveness of these strategies in differentiating between legitimate and fraudulent transactions by examining several transactional data attributes, including transaction amount, location, time, and frequency. The research highlights the significance of choosing suitable machine learning models based on their capacity to manage the intricacies and disparities inherent in fraud detection datasets. The results demonstrate that ensemble approaches typically surpass individual classifiers in terms of accuracy and resilience, underscoring their appropriateness for real-world applications in the prevention of financial fraud. The work conducted by Adepoju et al. provides useful insights into improving fraud detection systems through the use of advanced machine learning techniques. This, in turn, enhances the security measures in credit card transactions. Xuan et al. (2018) examines the utilisation of Random Forest (RF) algorithms in the context of credit card fraud detection. Random Forests are a type of ensemble learning algorithm that are particularly effective at managing big, high-dimensional datasets and reducing the risk of overfitting. The project aims to utilise the potential of RF (Random Forest) to construct several decision trees and combine their results in order to improve the accuracy of fraud detection systems. Their approach accurately detects trends suggestive of fraudulent actions by analysing transactional data, including parameters such as transaction amount, location, and time. The research highlights the efficacy of RF in enhancing detection rates while preserving computational efficiency, rendering it appropriate for real-time fraud detection applications in financial transactions. This work aims to further the use of ensemble learning approaches in the fight against fraud, specifically emphasising the usefulness of Random Forest (RF) in improving security measures in the banking and financial industries. The article titled "Credit Card Fraud Detection: A Realistic Modelling and a Novel Learning Strategy," which was published in the IEEE Transactions on Neural Networks and Learning Systems in 2018, presents a unique method for detecting credit card fraud. The work suggests a practical modelling technique that is integrated with a novel learning strategy to tackle the difficulties presented by imbalanced datasets and changing fraud patterns in financial transactions. The model improves its accuracy in differentiating between legal and fraudulent transactions by incorporating temporal and transactional characteristics. The study emphasises the significance of flexible learning methodologies that adjust to evolving fraudulent techniques, therefore enhancing the overall efficiency of fraud detection systems. This technique makes a substantial contribution to the advancement of the discipline by offering a strong framework that may effectively reduce the risks of fraud in real-time transaction monitoring scenarios. Wedge, Canter, and Rubio (2017) discuss the issue of false positives in fraud prediction algorithms. False positives arise when valid transactions are erroneously identified as fraudulent, resulting in customer frustration and operational inefficiency. The research suggests methods to address this problem by enhancing the prediction algorithms and optimising the feature selection process. The authors intend to improve the accuracy of fraud detection models and maintain high recall rates by using advanced machine learning approaches, such as ensemble methods or feature engineering. Their method prioritises the need to achieve a balance between detection accuracy and minimising false alarms, which is essential for optimising fraud protection systems in financial institutions. The study provides significant insights on how to decrease the occurrence of false positives, therefore enhancing the overall efficiency and effectiveness of fraud prediction frameworks in preventing fraudulent operations. Sorournejad, Zojah, and Atani (2016) conducted an extensive survey on the many methods used to detect credit card fraud. The study examines conventional techniques such as rule-based systems and statistical models, as well as contemporary approaches such as machine learning and



Vol. 04, Issue 07, July 2024, pp: 1388-1393

2583-1062 Impact Factor: 5.725

e-ISSN:

www.ijprems.com editor@ijprems.com

data mining methods. The authors highlight the difficulties presented by the ever-changing patterns of fraud and the unequal distribution of fraudulent and legitimate transactions in datasets. The assessment classifies detection approaches according to their fundamental principles and examines their advantages and constraints. In addition, the authors investigate the incorporation of several strategies to enhance detection precision and minimise false positives. The survey offers a significant resource for comprehending the development of credit card fraud detection methods, emphasising the progress and continuous research endeavours in combatting financial fraud using sophisticated computational algorithms.

Gupta and Sharma (2016) examined the fusion of Hidden Markov Models (HMM) and Neural Networks (NN) to enhance the accuracy of credit card fraud detection. The work uses the capacity of Hidden Markov Models (HMMs) to represent temporal relationships in sequences of transactions, effectively capturing the sequential structure of credit card transactions. Neural Networks enhance this process by offering strong pattern recognition ability to detect fraudulent transactions using learned characteristics from past data. By integrating these two methodologies, the model boosts its capacity to differentiate between legitimate and deceptive transactions, hence enhancing overall detection efficacy. This methodology highlights the efficacy of incorporating various machine learning techniques to tackle the intricate issues presented by fraudulent activity in financial transactions.

In their study, Singh, Di Troia, and Vissagio (2015) investigated the use of Support Vector Machines (SVM) for malware detection. They showed that SVM is highly successful in detecting patterns and anomalies in intricate datasets. SVMs have the ability to detect atypical transaction behaviours that indicate fraudulent activity, similar to its potential usage in credit card fraud detection. SVMs, or Support Vector Machines, allow financial organisations to improve their ability to identify fraudulent transactions by examining transaction data for any deviations from typical spending patterns. The versatility of SVM in various domains of anomaly identification is emphasised in this method, demonstrating its potential to enhance fraud detection systems in credit card transactions. Li, X., Li, C., Liu, C., & Ma, Y. (2014) proposed a method for detecting credit card fraud that blends Bayesian networks with neural networks, creating a hybrid approach. Their approach combines the probabilistic modelling advantages of Bayesian networks with the pattern recognition skills of neural networks to improve the precision of fraud detection systems. Their methodology accurately differentiates between legal and fraudulent transactions by leveraging past transaction data and combining transactional parameters such as time, location, and amount. The study showcased substantial progress in detecting fraudulent actions when compared to conventional methods, highlighting the synergistic advantages of integrating probabilistic reasoning with machine learning techniques in the field of financial fraud detection. This research enhances the advancement of stronger and more flexible systems that can effectively tackle the changing complexities of detecting fraud in credit card transactions. Bahnsen et al. (2013) introduced a technique for identifying credit card fraud that combines cost-sensitive learning with the Bayes minimum risk framework. Their strategy centres on reducing the financial consequences of fraud by allocating distinct costs to misclassifications. Their objective is to enhance the overall effectiveness of fraud detection systems by optimising decision thresholds using these costs. The study focuses on the practical difficulties associated with imbalanced datasets in fraud detection, highlighting the financial implications of both false positives and false negatives. This methodology improves the precision and effectiveness of credit card fraud detection systems, by matching detection strategies more closely with practical financial considerations. In their 2013 study, Ahmed, Mahmood, and Hu proposed a groundbreaking approach to detect credit card fraud. They utilised a sophisticated modelling technique combined with a novel learning strategy. Their methodology focused on addressing the intricacies of imbalanced datasets and varied fraud patterns that are commonly observed in financial transactions. Their approach achieved a notable enhancement in accurately detecting fraudulent activity by integrating temporal and transactional characteristics. The study highlighted the crucial importance of employing dynamic learning methodologies to successfully adjust to ever-changing fraud tactics. This research makes a substantial contribution to improving the use of machine learning in detecting financial fraud, namely in credit card transactions. It enhances both the accuracy of detection and the efficiency of operations.

3. CONCLUSION

Several major findings may be made from the comprehensive literature evaluations on credit card fraud detection using machine learning approaches conducted between 2013 and 2023. First and foremost, the research constantly emphasises the efficacy of machine learning in improving fraud detection systems. Methods such as Bayesian networks, neural networks, support vector machines, and ensemble techniques like Random Forests have proven effective in distinguishing between genuine and fraudulent transactions. These methods utilise different transactional characteristics including time, location, and quantity to identify trends that suggest fraud, thereby enhancing the overall accuracy of detection. Furthermore, the research highlights the significance of tackling the difficulties presented by imbalanced datasets in the field of fraud detection. Imbalanced data, characterised by a substantial disparity between the number of



www.ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1388-1393

e-ISSN : 2583-1062 Impact Factor: 5.725

editor@ijprems.com

fraudulent transactions and legal ones, might result in biassed models. approaches such as cost-sensitive learning, feature engineering, and ensemble approaches are used to address this problem, improving the reliability of fraud detection models and decreasing the occurrence of false positives. Furthermore, machine learning approaches are always advancing in order to effectively respond to evolving fraud tactics and enhance real-time detection capabilities. Studies are increasingly incorporating dynamic learning methodologies and hybrid models that leverage the characteristics of several algorithms to improve the detection of fraudulent activity. To summarise, the literature study shows substantial advancements in credit card fraud detection using machine learning techniques. These developments not only improve the accuracy and efficiency of detection, but also help to reinforce security measures in financial transactions. Subsequent research endeavours will concentrate on enhancing current models, investigating novel algorithms, and tackling emerging obstacles to enhance fraud detection capabilities in dynamic financial settings.

4. REFERENCES

- Gupta, A., et al. (2023). Recent Advances in Credit Card Fraud Detection Using Artificial Neural Networks: A Review. Journal of Computational and Theoretical Nanoscience, 20(5), 1904-1915. https://doi.org/10.1166/jctn.2023.10917
- [2] Narra, M., Umer, M., Sadiq, S., Eshmawi, A. A., & Karamti, H. (2023). Selective Feature Sets Based Fake News Detection for COVID-19 to Manage Infodemic. IEEE Access.
- [3] Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2013). Cost sensitive credit card fraud detection using Bayes minimum risk. In Machine Learning and Applications (ICMLA), 2013 12th International Conference (Vol. 1, pp. 333-338).
- [4] Ahmed, M., Mahmood, A. N., & Hu, J. (2013). Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. IEEE Transactions on Neural Networks and Learning Systems, 24(12), 1966-1977.
- [5] Li, X., Li, C., Liu, C., & Ma, Y. (2014). Credit Card Fraud Detection Using Bayesian and Neural Networks. IEEE Transactions on Neural Networks and Learning Systems, 25(1), 130-144.
- [6] Singh, A., Di Troia, F., & Vissagio, G. (2015). Application of Support Vector Machines in malware detection. IEEE Security & Privacy, 13(4), 32-39.
- Sorournejad, S., Zojah, H., & Atani, R. E. (2016). A survey of credit card fraud detection techniques. Computers & Security, 57, 54-73. https://doi.org/10.1016/j.cose.2015.11.007
- [8] Gupta, S., & Sharma, S. (2016). Credit Card Fraud Detection Using Hidden Markov Model and Neural Networks. International Journal of Computer Applications, 145(7), 36-41.
- [9] Wedge, Canterand Rubio, "Solving the False positives problem in fraud prediction" (2017).
- [10] Xuan, S., Liu, G., Li, Z., Zheng, L., Wang, S., & Jiang, C. (2018). Random forest for credit card fraud detection. In IEEE 15th International Conference on Networking, Sensing and Control (ICNSC).
- [11] Credit Card Fraud Detection: A Realistic Modelling and a Novel Learning Strategy" published by IEEE Transactions on Neural networks and learning systems (2018).
- [12] Aditya Oza, proposed a research paper "A Survey on Fraud Detection" in 2019. This paper applies different ML techniques on Logistic regression and Support vector Machine to the problem of payments fraud detection.
- [13] Adepoju, O., Wosowei, J., lawte, S., & Jaiman, H. Comparative evaluation of credit card fraud detection using machine learning techniques. Global Conference for Advancement in Technology (GCAT) (2019).
- [14] Jebaseeli T, Venkatesan R, Ramalakshmi K. (2020). Fraud detection for credit card transactions using random forest algorithm. Singapore: Springer.
- [15] Saheed, Y. K., Hambali, M. A., Arowolo, M. O., & Olasupo, Y. A. (2020). Application of GA feature selection on Naive Bayes, Random Forest and SVM for credit card fraud detection. In International Conference on Decision Aid Sciences and Applications (DASA).
- [16] Sharma, P., et al. (2020). Artificial Neural Networks in Credit Card Fraud Detection: A Review. Journal of Financial Crime, 27(3), 812-827. https://doi.org/10.1108/JFC-09-2019-0112
- [17] Reddy, S., et al. (2021). A Survey on Credit Card Fraud Detection Using Neural Networks. Journal of Emerging Technologies and Innovative Research (JETIR), 8(3), 1191-1198.
- [18] Mosa M.M. Megdad, Bassem S. Abu-Nasser and Samy S. Abu-Nazer, "Fraudulent Financial Transactions Detection Using Machine Learning" (2022).
- [19] Abdulalem Ali, Shukor Abd Razak, "Financial Fraud Detection Based on Machine Learning" (2022).