INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 6, June 2026 | ISSN: 2456-4184 | IJNRD.ORG

FRAUD DETRCTION IN PAYMENTS USING ARTIFICIAL INTELLIGENCE

Anushka Shukla (Student Galgotias University)
Pratika Raj (Student Galgotias University)
Ms. Nidhi Sharma (Assistant Professor Galgotias University)

Abstract: In today's time, owing to rapid development and changes in the digital ecosystem, there has been an increase in the number of digital transactions. With exponential increases in digital payment transactions, various security threats emerge that pose great challenges for both enterprises as well as consumers. Due to digital payments, a huge amount of fraudulent activities are happening causing financial loss to consumers. To cope with these kinds of security issues, one needs to leverage traditional techniques along with AI to detect any kind of fraud. This research paper provides a thorough analysis of how artificial intelligence can be used in fraud detection in digital payment system.

Keyords: Financial Fraud Detection, Machine Learning, Deep Learning, Imbalanced Datasets, Privacy and Compliance, LSTM, Random Forest, Explainable

AI.

I] INTRODUCTION

The fast-changing environment within the realm of digital payments has ensured immense benefits for both consumers and businesses. Nevertheless, in addition to its benefits, the rise in digital payment activities also presents the risk of fraud. Not only can such activities result in substantial financial losses, but they can also affect the credibility of digital payments. To tackle the issue, firms are now incorporating also involves integrating machine learning algorithms.

There is increasing reliance on advanced computer programs for identifying any fraud attempts made via online payments systems thereby serving as digital detectives in the world of digital payments. Most applications have an inherent ability to consume large volumes of historic transactional data that includes fields like transactional value, frequency of transactions, location where transaction occurred and even behavioral analysis. As digitization gains momentum within the finance sector, the forms in which transaction frauds can occur are rapidly becoming complicated and diverse, posing serious threats to individual users, enterprises and the entire finance sector as well. Given this situation, conventional forms of transaction fraud detection are increasingly unable to combat these new fraud types owing to the limitations imposed by them. Machine learning, on the other hand, which entails high volume data handling, complex pattern recognition and self-adaptation capabilities, is viewed as a potent antidote to transaction fraud.

II] FINANCIAL FRAUD IN DIGITAL PAYMENTS

Several types of payment systems exist in the digital payment system. Every payment system has been attacked by the digital criminals through several approaches for the purpose of executing frauds. Few of the important payment systems in digital payment systems are mobile wallets and payments, Peer to Peer payment and transaction through online shopping platforms. In every payment system, fraudsters continuously find new ways to exploit weaknesses in the payment system.

Following are few instances of financial frauds in the digital payment system-

Stolen Card Fraud (Payment card fraud): It is one of the fraudulent practices where fraudsters employ stolen or replicated card data to carry out unauthorized transactions. Both credit card and debit card information can be cloned using high

technology equipment that skims or replicates card data of cardholders. An instance of this practice is that in point-of- sale terminals, consumer card information can be stolen through various phishing emails or SMS messages directing consumers to phishing sites. The classification of types and forms of fraudulent interference, its consequences, and methods of combating them while considering user interests havebeen developed. Aim and objectives. The factors that cause payment card fraud, the various forms and types of fraudulent transactions in the use of payment cards have been classified and analyzed. Research findings.

Account Takeover: This form of fraud entails illegal access to digital payment accounts/banking of the consumer. This can

either be through the consumer's mobile wallets or mobile banking online. The fraud occurs through hacking or exploitation of any loopholes present in the security system used in the system. After gaining access to such an account, the digital fraudsters engage in fraudulent activities including alteration of the account settings in order to carry out the fraud process. Account takeover fraud is categorized as identity fraud since it entails gaining access to one's digital account. These actions can have serious implications for the consumer, the company in charge of operating the system, and all others who use such systems. The fraudster does not engage in unauthorized transactions through multiple login but rather through a few login attempts.

Identity Theft: A digital fraud technique whereby a fraudster attempts to use someone's personal information such as name, address, and nationality, and may include banking information as well.

By applying this information, digital criminals attempt to purchase different financial products such as loans and credit cards, and then proceed to conduct financial transactions by using their acquired identity authority, which means the use of some form of authority to identify another individual in order to perpetrate, or attempt to perpetrate, or assist in or aid or abet, or in connection with, any offense against Federal law, or any felony against any State or local "Means of identification" is described as being "any name or number that may be used, either alone or with any other information, to identify a specific individual." Since identity theft requires two distinct components — the stealing of the information and then its fraudulent use

— the plans for carrying out such thefts can be both simplistic and complicated, can be undertaken solo or with accomplices, and involve many types of individuals, from employees of legitimate companies through to typical street criminals. In addition, even though identity fraud depends upon identity theft, this does not mean that there will always be identity fraud once there has been identity theft.

Phishing and Spoofing: This is one of the most common forms of exploitation carried out by cybercriminals, whereby victims are made to offer their financial details to the hackers. These kinds of cyberattacks usually start in websites that resemble legitimate business sites and require users to enter personal information ranging from names and email addresses to sensitive information such as credit/debit card details.Such websites usually appear in form of links sent in spam emails or SMS that offer rewards to users.
Phishing is the most widespread form of cyber attack available today. In this research paper, the purpose is to conduct a brief survey of phishing. Phishing involves carrying out an attack for the purpose of accessing the personal data of an individual over the Internet, through fake websites. It also includes ways to prevent such attacks from taking place. Usually, such an attack uses methods like emails, messages, or websites from which the victim can be misled into providing personal information.. Phished links should be identified, and the users should be kept safe from such attacks. In order to help enterprises detect and mitigate phishing threats, several industry

solutions have been developed to identify phishing links. These include email security gateway, endpoint protection, URL filtering, and cyber suites, among others. The most common forms of phishing include email phishing, SMS phishing, and many more. As discussed earlier, there are several solutions available to help mitigate such phishing threats, however, most of them focus on email phishing, whereas SMS phishing requires some attention. The advent of mobile banking services has made SMS phishing very popular in recent years. Fraud detection within the digital payment environment requires an approach which not only uses traditional approaches but integrates technology for better results. Some of the methods used to detect fraud within digital payment systems include real-time monitoring, various layers of protection, and educating users on how to

avoid being victims of fraud. For businesses, it is vital to deploy additional security measures, such as multi-factor authentication (MFA), secure encryption, and effective detection techniques.

III] WHAT IS ARTIFICIAL INTELLIGENCE

Artificial intelligence, more popularly known as AI, involves the replication of human intelligence processes using machines, particularly computer programs. This can be through a number of methods, including but not limited to learning where one acquires knowledge that includes rules, and reasoning based on acquired knowledge that may be approximate or definite. The first trend is the use of artificial intelligence in payments. Artificial Intelligence is used for detecting and preventing frauds. It involves the use of algorithms that analyze transaction data and detect any fraudulent transactions. Another aspect of the use of artificial intelligence in payments is personalization of customer experience using algorithms that analyze customer data and behavior. Payment automation is one other benefit that results from AI in payments in that it speeds up the process of payments for businesses. Cross- border payments is another key trend. The use of emerging technology like blockchain and stablecoins has simplified cross-border payments by making the process easier and faster. Lower charges and shorter

processing periods further improve the effectiveness of cross-border transactions. The emergence of peer-to-peer (P2P) transactions has seen tremendous growth, offering people easy and fast payment methods. P2P transactions incorporate social elements that allow users to link up with their friends and pay them using messaging applications or social networking sites. Data protection and privacy have become critical aspects for online payments. Strict data privacy policies, such as GDPR, safeguard sensitive financial and personal details. Techniques such as encryption and tokenization provide better protection for transaction data, ensuring its confidentiality and accuracy. The trade-off between security and convenience is It is vital to ensure that

users' trust and use of digital payments remain intact. In summary, organizations and consumers need to be up to date with the latest trends in digital payments in order to exploit them. Trends such as the use of artificial intelligence to detect fraud, ease of cross-border transactions, the rise of peer- to-peer transactions, and strong security measures for data protection have greatly impacted digital payments. Machine Learning is a major technology in the realm of artificial intelligence. This article offers a fairly systematic introduction to machine learning. In the first place, the history of the evolution of machine learning is briefly introduced, and then an emphasis is placed on discussing the classic machine learning algorithms. Key concepts in artificial intelligence (AI) include:

Machine Learning:

Understanding ML techniques is very important for AI and the algorithmic techniques that enable the software to analyze and learn from data, improving on its abilities without any explicit instructions given by a programmer. Several algorithms can be used to improve accuracy.

Deep Learning:

The type of ML that is characterized by the presence of several layers of neural networks to generate data representations. In the course of time, the applications of Deep Learning have resulted in some amazing achievements. The following are some applications of Deep Learning.

- Image Recognition
- Natural Language Processing
- Speech Recognition
-

Neural Networks:

In light of the architecture of the brain of humans, neural networks are considered to be a key part of deep learning systems. They are composed of neurons arranged in layers and can learn intricate patterns. **Natural Language Processing (NLP)**: Natural Language Processing centers on how computers interact with human languages. It allows computers to analyze human languages and even generate them in response, thus enabling activities like language translation and chatbots.

Computer Vision:

Computer vision is an ability for computers to understand the visual world. This includes things like detecting objects within images, classifying images, and segmenting images. Computer vision has been vastly improved by deep learning.

IV] WHAT IS DATA MINING

Data mining is one of the most crucial elements of Artificial Intelligence. This includes finding out data patterns, correlation lookup, and dataset creation for insight. Some significant activities that come under data mining include data cleaning, preprocessing, pattern identification, and knowledge discovery, leading to revealing

insights in data that might be highly valuable. One of the most innovative ways of handling huge amounts of data coming from databases is data mining. Information is very common these days in any kind of business or industry. For different business purposes, fields select data mining techniques, and data mining enables the field to find the best customer base line and create a relationship that will last. Statistical analysis, machine learning, predictive modeling, and Data mining techniques have been proven beneficial for businesses for several reasons. Nowadays, there has been an increasing trend among companies that have started to make use of historical data after analyzing them deeply, and they are even making use of real-time analytics to analyze the data stream as it is being created or collected. Effective data mining can help companies in many ways in the process of developing strategies for their business and managing their operations. They include customer-oriented activities such asmarketing, advertising, selling, customer support, production, logistics and transportation, finances, and human resources. Key techniques used in data mining include:

Association Rule Learning: Relationship discovery refers to finding associations and relationships between variables in a data collection. In financial services and online payment systems, for example, data mining can be used to identify connections between financial transactions. Association rules are conditional statements that aid in finding relationships between unrelated variables contained in a database, relational database, or other information storage system. They are used to determine the relationship among those objects which are used frequently together. Some applications of association rules include basket data analysis, classification, cross marketing, clustering, catalog design, and loss leader analysis.

Clustering : Clustering is an approach in which data sets are clustered or classified based on their inherent attributes. The Clustering approach assists in identifying natural groups within a data set in data mining. Clustering and classification are two fundamental approaches to data mining tasks. Classification is typically used in supervised learning tasks, while clustering is employed in unsupervised learning. The objective of classification is to predict while that of clustering is descriptive (Veyssieres and Plant, 1998). Because the clustering technique attempts to find new clusters, evaluation of the clusters themselves is intrinsic.

Classification: It is yet another method used in data mining where certain predetermined tags are assigned to the data according to their attributes. The procedure involved in data mining aids the process of extracting knowledge fromlarge amounts of data. The main areas of data mining are clustering/classification, association rules, and sequence analysis. According to simple definition, in clustering/classification, one analyzes a collection of data and formulates a set of classification rules that can then be applied to future sets of data.

Regression: It is the task of predicting the numerical value using the independent variables. There has been extensive use of regression in understanding the relation between the independent and dependent variables.
As the number of customers increases along with the increase in companies using credit cards for the completion of financial transactions, the incidence of fraud cases has seen an enormous rise. The problem has been further accentuated by the presence of noisy and imbalanced data as well as the presence of outliers. The proposed study involves a method for detecting frauds using artificial intelligence. The proposed system uses logistic regression to develop a classifier to prevent frauds associated with credit card transactions. The pre-processing technique used for cleaning the dirty data to achieve a higher level of accuracy is included. Two innovative approaches have been used for data cleaning in the pre- processing step - the mean-based method and clustering-based method.

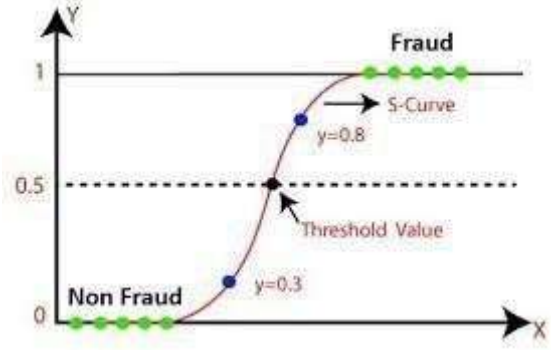
V] TYPES OF ARTIFICIAL INTELLIGENCE ALGORITHMS USED FRAUD DETECTION

Detection of fraud in digital payment ecosystem requires not just one but multiple approaches to be applied in the process. The combination of various AI algorithms is adopted in order to ensure that the process is more accurate. One of the key methodologies adopted for this purpose is machine learning which analyzes a huge volume of data to identify any suspicious behavior and anomalies.

Following are the some of the most common algorithms used for fraud detection in digital payments:

Logistic Regression:
It is an algorithm used for prediction of binary

values in a given set of independent variables (1 / 0, Yes / No, True / False). Logistic regression method is used for binary classification problems. In case of fraud detection in digital payments ecosystem, logistic regression model could be employed in order to classify a transaction as legitimate or illegitimate. Logistic regression is widely preferred due to its simplicity & effectiveness. In case of a simple correlation of input variable and log-odds of target variable, this method works effectively. On the other hand, logistic regression fails to capture the complex non-linear relationship as compared to decision trees & neural networks. Results show that the logistic regression model can achieve an accuracy of detecting"0" as seen in figure 1.

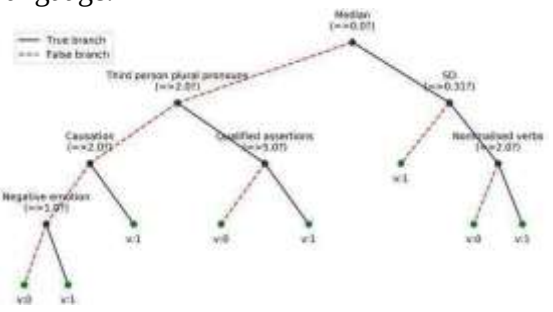


Decision Trees:

One of the most frequently applied AI algorithms is the one that works efficiently when establishing decision boundaries using vectors like the amount of the transaction, its place, date, and time. A new decision tree algorithm which aims at minimizing the summation of the misclassification costs when deciding upon which attribute to split in every non- terminal node of the tree is designed, and its classification performance is evaluatedagainst traditional approaches which may be insensitive to costs or sensitive but with a fixed ratio for misclassification costs, including classical decis ion trees, ANN, and SVM. It is found that the proposed approach provides better results in detecting fraud and avoiding loss than the other approaches tested. One of the trees that are developed by using the combination of features is depicted in Figure below. It is clearly evident from the figure how the decision-making process has been made, and what are the significance levels of different features used.

For instance, the first feature in terms of significance level is "Median of sentiment value with threshold 0". Moreover, "third person plural pronoun" is another significant feature that represents deception and highlights the customers' efforts to talk about the third person while discussing their personal financial account. It can be seen from the figure that qualified assertion, negative emotions, causations, and nominalized verbs are among other significant features.

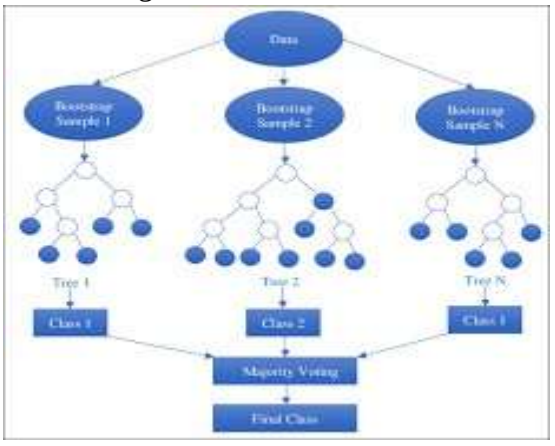
One of the most surprising features is "standard deviation (SD)" of sentiment values of responses, as it shows excessive changes in the customer's language.



Random Forest:

An ensemble of decision trees to enhance accuracy in classification using average prediction from different branches of the tree Random forest is a supervised machine learning technique which incorporates a number of decision tree algorithms into classifying and predicting an outcome. Decision trees are considered weak learners

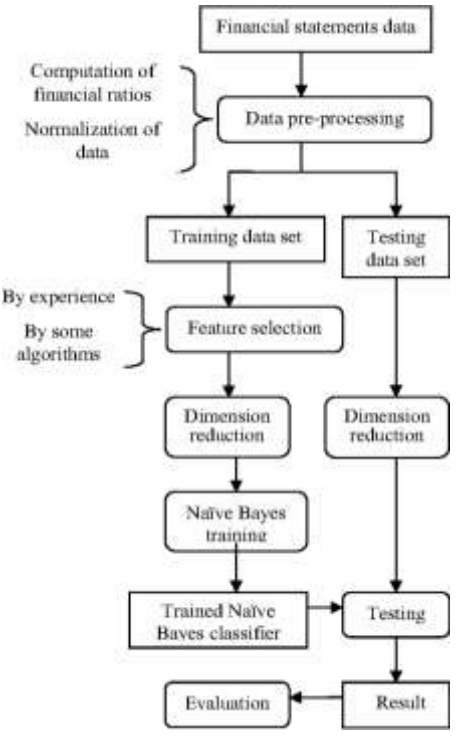
as they have very poor predictability. It operates under the theory of ensemble learning, where decision trees are used in classifying and solving problem. The architecture of random forest is shows in figure 3.



Naive Bayes:

One of the popular algorithms that are used in the field of fraud detection is Naive Bayes, because of its high effectiveness, it become prominent as a powerful algorithm and at the same time retains simplicity.In case of fraud detection, the Naive Bayes algorithm performs analysis of massive volumes of historical data to detect patterns and characteristics related to fraud. The principle of fraud detection using the algorithm is based on the probabilistic transaction nature of fraud, depending on the presence or absence of certain attributes, including the amount, time and behavior of consumers. Nowadays, in this age, where plastic money is widely used all around the globe, every new technology always comes with some vulnerabilities too. In such a situation, there may arise various anomalies that can cause monetary loss to users. The anomalies referred to here are considered financial frauds committed by certain parties in the financial world. Various methods have been proposed for the detection of the same in literature. However, in this research paper, the research aims to develop an automated technique to detect such frauds, in particular the ones linked to credit card transactions The first major benefit of this algorithm is its capacity to process very high volumes of data and come up with the results much faster. This plays a critical role in detecting fraud, since the algorithm is designed for the use in the modern digital financial payments environment.

Another important characteristic of any efficient fraud detection algorithm is the ability to rapidly process huge amounts of data either in real-time mode or in near-real- time mode.



Generative Adversarial Networks (GANs) : GANs are great for detecting fraud because they can create fake data that looks just like real fraud, helping train machines better. These networks are key parts of generative AI, alongside things like VAEs. In GANs, you've got a generator and a discriminator battling it out – one makes stuff, the other judges it. It's all about creating and rating until they get really good. For VAEs, it's more about using encoding and decoding to make new examples from what they learn.So, while both aim to generate new data, GANs do it through competition, and VAEs through compression and then reconstruction.

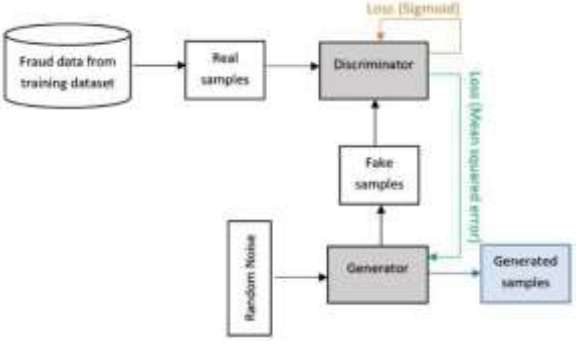


Figure 5: GAN architecture employed in this study consisting of a 5-layer FNN generator and discriminator, leading to the

generation of the final minority samples depicted by the blue square

FUTURE SCOPE

The ever-evolving digital payment environment has proved to be very threatening when it comes to fraudulent activities. But with equally disruptive technology used in conjunction with Artificial Intelligence, there is a lot of promise for the future.

Some of the areas of development and advancement include:

Advanced Fraud Anomaly Detection:

As algorithms continue to advance in detecting fraudulent behavior, the area of anomaly detection is set to see vast improvements where they can detect anomalies in large complex data sets.

Real-time Detection: This area, in particular, has been very effective because it uses an Artificial Intelligence algorithm which responds and escalates a potential fraudulent transaction as soon as it is detected.

Behavioral Biometrics: One such technology which is gaining popularity due to the fact that it uses a unique approach to detect fraud is the behavioral biometric approach. Here applications will monitor typing behavior, mouse activity, and touchscreen actions in order to detect anomalies which can result in fraudulent.

Behavior.Explainable AI (XAI): Regulatory policies are necessary to ensure transparency, and to avoid abuse/exploitation of artificial intelligence. Regulatory policies would require the use of explainable AI, meaning that the technology is able to detect and give reasons for such detections. The capability of the applications to detect and reason will become very important in the future.

VI] CONCLUSION

Artificial intelligence was initially known for its immense potential and possibilities within the mainstream ecosystem. In the modern world, it is one of the most important technologies that help develop solutions and improve application development. Due to the rapid change that is currently occurring, artificial intelligence is expected to become an irreplaceable tool when fighting fraudulent behavior in the context of digital payments. There are various kinds of advanced algorithms that may be used by enterprises in order to analyze huge amounts of transaction data and detect patterns that may suggest a potential fraudulent transaction. The list includes logistic regressions, decision trees, Naive Bayes and the newest GAN technology that can help detect abnormalities and suspicious activity that might be associated with fraud. All of these algorithms aim at finding the best possible way to minimize losses and regain the trust of digital transaction users. As the digital payment ecosystem becomes increasingly popular in the world of finance, artificial intelligence plays a significant role.

VII] References

[1] A. A. Adewumi and C. K. Ayo, "A survey of machine learning and nature inspired based credit card fraud detection techniques," International Journal of System Assurance Engineering and Management, vol. 8, no. 2, pp. 937-953, 2017.

[2] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," Statistical Science, vol. 17,no.3,pp.235-255,2002.

[3] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys,vol.41,no.3,pp.1-58,2009.

[4] IEEE-CIS Fraud Detection Dataset, Kaggle, 2019. [Online]. Available: https://www.kaggle.com/c/ieee-fraud-detection/data

[5] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436 - 444,2015.

[6] T. Fawcett, "An introduction to ROC analysis," Pattern Recognition Letters, vol. 27, no. 8, pp.861-874,2006.

[7] D. J. Hand and W. E. Henley, "Statistical classification methods in consumer credit scoring: A review," Journal of the Royal Statistical Society: Series A, vol. 160, no. 3, pp. 523 -541, 1997.

[8] J. Han, M. Kamber, and J. Pei, Data Mining:

Concepts and Techniques, 3rd ed. Amsterdam:Elsevier,2012.

[9] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Computation, vol. 9,no.8,pp.1735-1780,1997.

[10] A. K. Jain, M. N. Murty, and P. J. Flynn, "Data clustering: A review," ACM Computing Surveys,vol.31,no.3,pp.264-323,1999.

[11] Y. Kim, "Convolutional neural networks for sentence classification," in Proc. EMNLP, Doha,Qatar,2014,pp.1746-1751.

[12] A. Liaw and M. Wiener, "Classification and regression by randomForest," R News, vol. 2, no.3,pp.18-22,2002.

[13] Dal Pozzolo et al., "Learned lessons in credit card fraud detection from a practitioner perspective," Expert Systems with Applications, vol. 41, no. 10, pp. 4915-4928, 2014.

[14] Nilson Report, "The Nilson Report: Issue 1170," 2020. [Online]. Available: https://nilsonreport.com

[15] Cybersecurity Ventures, "Cybercrime Report 2023, " 2023. [Online]. Available: https://cybersecurityventures.com/cybercrime-report

[16] F. Pedregosa et al., "Scikit-learn: Machine learning in Python, " Journal of Machine Learning Research, vol. 12, pp. 2825-2830, 2011.

[17] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by backpropagating errors, " Nature, vol. 323, no. 6088, pp. 533-536, 1986.

[18] B. Scholkopf et al., "Estimating the support of a high-dimensional distribution, " Neural Computation, vol. 13, no. 7, pp. 1443-1471, 2001.

[19] K. P. Singh and M. C. Pandey, "Fraud detection in credit card transactions using machine learning, " in Proc. Int. Conf. Comput. Intell. Data Sci., Gurugram, India, 2018, pp. 1 - 6. 20.

[20] J. Tang, A. Alelyani, and H. Liu, "Graph mining: A survey of graph mining techniques, " in Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., Paris, France, 2009, pp. 1055 - 1064.

[21] Visa Inc., "Visa Data and Analytics, " 2023. [Online]. Available: https://www.visa.com/dataanalytics

[22] S. Wang, "Adaptive credit scoring with kernel learning methods, " in Proc. IEEE Int. Conf. Data Min., Omaha, NE, USA, 2005, pp. 987-990.

[23] Z. Zheng, "A survey on anomaly detection techniques for financial data, " Journal of Financial Data Science, vol. 1, no. 1, pp. 45-58, 2019.

[24] I. Goodfellow et al., "Generative adversarial nets, " in Proc. Adv. Neural Inf. Process. Syst., Montreal, Canada, 2014, pp. 2672-2680.

[25] European Commission, "General Data Protection Regulation (GDPR), " 2018. [Online]. Available: https://gdpr-info.eu

[26] California Consumer Privacy Act (CCPA), "California Legislative Information, " 2018. [Online]. Available: https://leginfo.legislature.ca.gov