International Journal of Management, IT & Engineering
Vol. 14 Issue 8, August 2024
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Fraud Detection in Digital payments Using Artificial Intelligence

Naga Rishyendar Panguluri
Software Engineering Manager at Discover Financial Services, Researcher
Manohar Sai Jasti
Software Development Engineerat Workday, Researcher

Abstract: *With rapid evolution & transformation in the digital ecosystem the world is witnessing unprecedented rise of digital transactions. The exponential growth of Digital payment transactions is countered with numerous security threats which pose significant challenges to enterprises & consumers. The proliferation of digital payments have led to a massive surge in fraudulent activities leading to financial losses and dent in consumer trust. To counter the threat, businesses need to combine traditional application with integration of Artificial Intelligence (AI) techniques in proactively detecting fraud. The approach of integrating Artificial intelligence has shown promising results in combating fraudulent and illegitimate activities in digital payment ecosystems. This research paper presents a comprehensive view of the advancement of utilizing Artificial intelligence in fraud detection in the digital payment space. Further provides various methodologies employed in fraud detection using machine learning algorithms and models.*

Keywords*- Fraud detection, machine learning, data analytics, artificial intelligence, adaptive learning mechanisms, XGBoost, Logistics Regression,*

I. INTRODUCTION

Rapid transformation in the Digital payment space has brought enormous convenience to consumers & businesses. However, along with the growth comes the threat of fraudulent activities in the digital payment ecosystem. Illegitimate and fraudulent transactions not only leads to significant financial loss but also negatively impacts the trust on digital payments usage.

To counter the challenges, businesses are increasingly adding layers of security using various means which also includes integration of machine learning algorithms.

Businesses have started relying on sophisticated software to detect fraudulent transactions thereby acting as digital detectives in the digital payment space. Mostly applications come inbuilt with innate ability to consume vast amounts of historical transaction records, which would include fields such as transaction amount, frequency, location from which transaction was initiated & nowadays even typical behaviours and apply the patterns to flag suspicious activities as they happen.

As the digitization process of the financial industry accelerates, the means of financial transaction fraud are becoming increasingly complex and varied, bringing great risks to individuals, enterprises and even the entire financial system. In this context, traditional fraud detection methods are increasingly difficult to effectively respond to emerging frauds due to their inherent limitations. In contrast, machine learning, with its powerful data processing capability, complex pattern recognition ability, and self-learning and adaptation, is considered a powerful tool against financial transaction fraud.[1]

The COVID-19 outbreak has brought unprecedented shifts for the global financial system and has hastened the adoption of digital payments. More insidious fraud schemes have risen as a result of these shifts, creating fertile ground for all sorts of financial fraud.[2] Fraudsters are always looking for the next opportunity to find a hole in the process, and merchants will always have more work to do and new problems to face when it comes to preventing fraud. And, with consumer demands ever-changing at a rapid pace, managing e-commerce payments can also be challenging for

merchants. But the data and trends in this year's report provide good reason for optimism that they can continue to advance and achieve success in both of these challenging arenas[3]

The research paper is set to outline solely on the approach of fraud detection in the digital payments space. It further lists out different types of frauds and how they occur along with ways and means to detect fraud which can essentially narrow down the losses and enhance the trust in the digital payments

II. FINANCIAL FRAUD IN DIGITAL PAYMENTS

There are various types of payment methods in digital payment ecosystems. Each method has been targeted by digital thieves in various ways to carry out fraudulent activities. Few of the noteworthy modes of digital payments are mobile wallets & payments, Peer to peer transfers & transactions via online shopping platforms. For each of the different methods perpetrators keep improvising their approach to identify and exploit vulnerabilities in the system

Here are some of the financial fraud in digital payment space-

Fraud using Stolen card (Payment card Fraud): In this type of fraud unauthorized transactions are carried out by digital criminals using stolen or fake credit card or debit card information. Information of the credit card/ debit cards are typically cloned using sophisticated devices which carry out card skimming. One such example of skimming of card information is at point-of-sale terminals or consumers are tricked to provide their card details using various phishing emails or SMS, which leads consumers to fake phishing websites

The systematization of types and forms of fraudulent intervention, their consequences and ways of counteraction taking into account the interests of users is made. Aim and tasks. The causes of payment card fraud, the main forms and types of possible fraudulent transactions and areas of payment card fraud were further classified and investigated. Research results. The investigation revealed the most common cases, including lost and stolen payment cards, counterfeit cards and fraudulent transactions without a payment card, and identified measures to combat them. At the same time, the ways of using different methods for the implementation of fraudulent transactions were analyzed. In the context of the rapid growth of e-commerce during the global pandemic, widespread fraud and steps to be taken against them have been revealed. [4]

Account Takeover: Account takeover fraud occurs when criminals gain unauthorized access to consumers' digital payment/ banking account, which can include mobile wallet or even online / mobile banking. This fraud is carried out by stealing access credentials of users and in some cases exploiting security vulnerabilities of the system. Once the digital criminals gain access, they tend to carry out unauthorized transactions and in some cases update the account settings helping them to continue illicit activities.. Account takeover is a form of online identity theft where a fraudster gains unauthorized access to an individual's account in a given system. Depending on the system, this unauthorized access can lead to severe consequences of privacy breach and financial loss to the victims, to the companies that maintain the system and to other users. In this paper, we present the work done in order to prevent and detect account takeovers at mobile.de, an online vehicle marketplace.[5]

Mostly fraudster do not undertake unauthorized transactions by accessing account multiple times, rather carry our those illegitimate transactions in limited attempts

Identity Theft: Another form of digital fraud where fraudsters unauthorizedly try to use an individual's personal information such as their name, address, national identity to even banking account details. While using such information digital criminals try & apply various financial products like loans or even credit cards & goes further to carry out transactions with means using stolen identity

The Identity Theft Assumption and Deterrence Act (ITADA), passed in1998 in the USA, states that identity theft occurs when a person "know-ingly transfers, possesses or uses, without lawful

authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." The term "means of identification" is defined as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." Because identity theft involves two separate elements, the theft of information and the fraudulent use of that information, schemes range from the simple to the complex, may be committed by offenders working alone or in groups, and are committed by an array of offenders, including employees of legitimate businesses to common street offenders.Moreover, although identity fraud cannot occur without identity theft, identity theft is not always followed by identity fraud; the two compo-nents may be committed by separate offenders with different skills depending on the complexity of the crime [6]

Phishing and Spoofing: This is one of most used exploits by digital criminals, where users are tricked into providing financial information to the fraudsters. This type of attacks typically gets initiated where users land in similar looking fake websites which mimics legitimate business websites and prompts users to provide their information such as their name, email address to even financial information like credit card or debit card details. These websites are often given as links in promotional emails or SMS which entices users with special offers or awards or rewards.

Phishing is the most common type of cyber threat existing today. In this paper the aim is to do a quick survey about phishing. Phishing is an attack made to gain unauthorized access to the sensitive information about a person on the internet by impersonating the websites they use. This paper also talks about the several means and mechanisms that exist to combat phishing attacks. The intruders mostly use emails, messages, or websites that appear to be from a trusted source to trick the victims into divulging sensitive information. Phished links are to be detected and the users must be protected from it. To assist enterprises in identifying and mitigating phishing risks, a number of industry solutions and technologies are available for phishing link detection. Email security gateways, endpoint protection, URL filtering, cyber suites etc. Most common types of phishing include Email phishing, SMS phishing etc. As mentioned above there are quite a few solutions available but most of it is for the Email phishing, SMS phishing still needs some attention. With the emergence of mobile banking in the recent times, SMS phishing has seen a sudden rise.[7]

The digital payments space has enormous convenience & massive potential but at the same time the likelihood of consumers falling pray to fraudulent transactions is high. To counter such unauthorized transactions requires a combination of multiple approaches.

Detecting fraud in the digital payment ecosystems warrants multi-pronged strategy that combines the strength of traditional methods & integrate with latest sophisticated technologies. Few of the detect mechanisms include continuous real time monitoring, multiple layers of security to educating users which is essential. From businesses perspective its imperative that additional security measures are being deployed not limited to strong authentication mechanisms like MFA (Multi Factor Authentication), strong encryption methods & robust detection methods to safeguard against potential fraudsters transactions being carried out.

Fraudsters typically keep evolving against any new safeguard mechanism. Therefore in-order to have effective counters both consumers and businesses should work together & undertake proactive steps to create a safer and more secure digital payment environment for everyone.

III. WHAT IS ARTIFICIAL INTELLIGENCE

Artificial intelligence commonly referred as AI is a simulation of human intelligence process by machines, mainly computer systems & applications. The process could combine multiple approaches ranging from learning, meaning acquisition of information including rules, reasoning using learned rules which are near approximate or definite

conclusions, & self correction. Artificial Intelligence (AI) can be put in two main categories. One, which is narrow in approach & designed for specific tasks. Two, General AI which is now commonly used integrated with various applications and which has capability to consume information, learn, store & apply such knowledge as per the domains selected trying to be closely similar to human intelligence.
Nowadays, usage of Artificial Intelligence has come into mainstream applications and are heavily used in various industries including Healthcare, Finance, Transportation, Education, Government & more.

The first trend is the integration of artificial intelligence (AI) in payments. AI is being utilized for fraud detection and prevention, leveraging algorithms to analyze transactional data and identify patterns of fraudulent activity. Additionally, AI enables personalized customer experiences by analyzing customer data and behavior, offering tailored recommendations and promotions. Furthermore, AI automation streamlines payment processes, saving time and resources for businesses. Cross-border payments represent another significant trend. Emerging technologies, such as blockchain and stablecoins, simplify cross-border transactions by reducing complexities and inefficiencies. These technologies enable transparent and secure peer-to-peer transfers, while digital payment platforms integrate with local payment systems, facilitating seamless cross-border transactions. Reduced fees and transaction times further enhance the efficiency of cross-border payments. Peer-to-peer (P2P) payments have experienced remarkable growth, providing individuals with convenient and instant payment solutions. P2P payment platforms integrate social features, allowing users to connect with their contacts and make payments within messaging apps or social media platforms. This integration enhances the user experience and disrupts traditional banking services, as users gain more control over their finances. Data security and privacy are increasingly important considerations in digital payments. Stricter data protection regulations, such as GDPR, ensure the secure handling of personal and financial information. Encryption and tokenization techniques protect transaction data, enhancing confidentiality and integrity. Balancing security and convenience is crucial to maintain user trust and widespread adoption of digital payments. In conclusion, businesses and consumers must stay informed about emerging trends in digital payments to adapt and capitalize on the opportunities presented. AI-driven fraud detection, simplified cross-border transactions, the growth of P2P payments, and robust data security measures are reshaping the digital payments landscape. Understanding these trends and their implications empowers stakeholders to navigate the evolving landscape and leverage digital payment solutions effectively. [8]

Machine Learning, as one of the key technologies in the field of artificial intelligence, has made significant advancements in recent years. This study provides a relatively systematic introduction to machine learning. Firstly, it gives an overview of the historical development of machine learning, and then focuses on the analysis of classical algorithms in machine learning.[9]

Key concepts in artificial intelligence (AI) include:

1. **Machine Learning (ML):** ML concepts are key to AI and its set of algorithms that allow applications to sift & learn from data and improve their performance over time without being explicitly programmed. Multiple algorithms can be used to better the accuracy of the results.

2. **Deep Learning:** A subset of ML which consists of multiple layers (hence deep) of neural networks to learn representations of various data. With advancement of applications, Deep Learning has achieved phenomenal success in recent times. A few of the uses of Deep Learning include image recognition, natural language processing, and speech recognition.

3. **Neural Networks:** Inspired by the structure of the human brain, neural networks are a fundamental component of deep learning. They consist of interconnected nodes (neurons) organized in layers and are capable of learning complex patterns.

4. **Natural Language Processing (NLP)**: NLP focuses on the interaction between computers and human language. It enables machines to understand, interpret, and generate human language, facilitating tasks such as language translation, sentiment analysis, and chatbots.

5. **Computer Vision**: Computer vision enables computers to interpret and understand the visual world, including tasks such as object detection, image classification, and image segmentation. Deep learning has significantly advanced the field of computer vision.

IV. WHAT IS DATA MINING

Data mining is an extremely important aspect of Artificial Intelligence. The process involves discovering data patterns, looking up correlations & creating datasets for gaining insights.Some notable tasks in the process of data mining are data cleaning, preprocessing, pattern discovery & knowledge extraction, which leads to unveil information that are hidden within data and could be extremely valuable.

A revolutionary technique for managing massive amounts of data from databases is data mining. These days, information is more commonplace in all types of businesses and industries. For a range of business objectives, fields choose data mining approaches, and data mining is what makes it possible for fields to establish the ideal customer baseline and cultivate long-lasting relationships. Statistical analysis, machine learning, predictive modelling, and database approaches are all combined in knowledge discovery.[10]

To have effective fraud detection the process of data mining is extremely crucial. The process typically enables identification of patterns, anomalies & suspicious traditional activities. Sifting through historical transactions records can bring out patterns which are hidden that can be used to distinguish legitimate transactions with illegitimate transactions. Therefore, the insights bought out becomes extremely valuable and help detecting fraudulent behaviours effectively in real-time.

The insights generated by the process of data mining is effectively used by organizations in business intelligence (BI) & advanced data analytics applications. In recent times many organizations have started harnessing historical data with deep analysis & combine it with real-time analytics that examine data stream as its created/collected

Effective data mining aids in various aspects of planning business strategies and managing operations. That includes customer-facing functions such as marketing, advertising, sales and customer support, plus manufacturing, supply chain management, finance and HR. Data mining supports fraud detection, risk management, cyber security planning and many other critical business use cases. It also plays an important role in healthcare, government, scientific research, mathematics, sports and more[11]

Key techniques used in data mining include:

Association Rule Learning: Identifying relationships and associations between variables in a dataset. In finance & digital payments, data mining can reveal associations between transactions Association rules are if/then statements that help to uncover relationships between unrelated data in a database, relational database or other information repository. Association rules are used to find the relationships between the objects which are frequently used together. Applications of association rules are basket data analysis, classification, cross-marketing, clustering, catalog design, and loss-leader analysis etc [12]

Clustering: is an approach where similar data points are grouped together based on their innate characteristics. The approach of Clustering helps data mining in identifying natural groupings within a dataset. The approach of Clustering and classification are key to fundamental tasks in Data Mining. Classification is used mostly as a supervised learning method, clustering for unsupervised learning (some clustering models are for both). The goal of clustering is descriptive, that

of classification is predictive (Veyssieres and Plant, 1998). Since the goal of clustering is to discover a new set of categories, the new groups are of interest in themselves, and their assessment is intrinsic. [13]

Classification: Is another approach in data mining which assigns predefined labels to data based on certain characteristics. This process of data mining helps the process of inferring knowledge from such huge data. Data Mining has three major components: Clustering or Classification, Association Rules and Sequence Analysis. By simple definition, in classification/clustering analyze a set of data and generate a set of grouping rules which can be used to classify future data. Data mining is the process is to extract information from a data set and transform it into an understandable structure. It is the computational process of discovering patterns in large data sets involving methods at the intersection of artificial intelligence, machine learning, statistics, and database systems. [14]

Regression: The approach is to predict the numerical values based on input variables. Regression analysis is widely used to understand the relationship between independent and dependent variables.
Due to the increasing number of customers as well as the increasing number of companies that use credit cards for ending financial transactions, the number of fraud cases has increased dramatically. Dealing with noisy and imbalanced data, as well as with outliers, has accentuated this problem. In this work, fraud detection using artificial intelligence is proposed. The proposed system uses logistic regression to build the classifier to prevent frauds in credit card transactions. To handle dirty data and to ensure a high degree of detection accuracy, a pre-processing step is used. The pre-processing step uses two novel main methods to clean the data: the mean-based method and the clustering-based method. Compared to two well-known classifiers, the support vector machine classifier and voting classifier, the proposed classifier shows better results in terms of accuracy, sensitivity, and error rate. [15]

V. TYPES OF ARTIFICIAL INTELLIGENCE ALGORITHMS USED FRAUD DETECTION

In order to detect fraud in digital payment ecosystems more than one approach needs to be deployed. Combinations of AI algorithms are used to have better accuracy for fraud detection. The concept of Machine learning is widely used in fraud detection which analyses vast amounts of data to pinpoint suspicious patterns and anomalies indicative of fraudulent activities.

Here are the few Algorithms which are used for Fraud Detection in Digital Payment -

Logistics Regression: is part of a statistical classification algorithm, used to predict binary values in a given set of independent variables (1 / 0, Yes / No, True / False) method used for binary classification tasks. [16] In the context of detecting fraud in digital payment ecosystem, this method can be deployed to classify a transaction are legitimate or illegitimate

Logistic regression is opted widely due to its nature of simplicity & effectiveness, especially when relation between input & log-odds of target variable is linear or can be transformed to be linear. However, the flip side being logistics regressions cannot capture complex non-linear relationship compared to other sophisticated algorithms such as decision tree & neural networks

Results show that the logistic regression model can achieve an accuracy of 94% in detecting fraudulent transactions. Additionally, we perform feature importance analysis to identify the most significant variables that contribute to fraud detection. Our findings suggest that variables such as transaction amount, country of origin, and time of day can be strong predictors of fraudulent transactions. our study highlights the potential of logistic regression for credit card fraud detection, even with an imbalanced dataset [17]

As per the image below, the fraud class takes the value "1", while the non-fraud class takes the value

International Journal of Management, IT & Engineering
Vol. 14 Issue 8, August 2024
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

"0". A threshold of 0.5 is used to differentiate between the two classes, as shown in figure 1. [18]

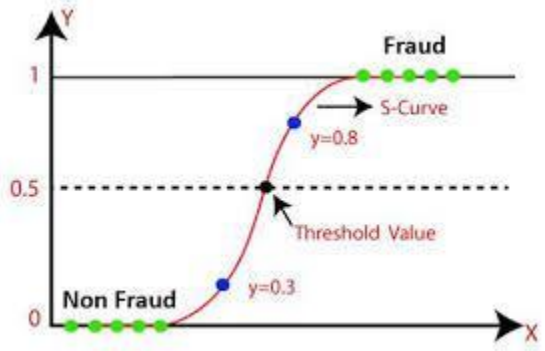
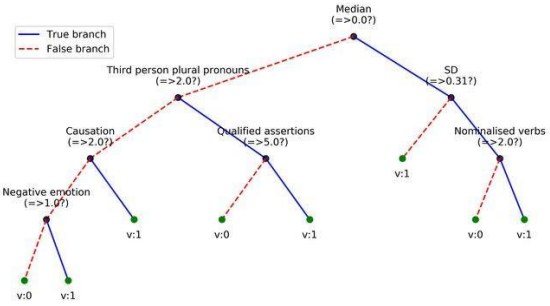


Figure 1:https://thesai.org/Downloads/Volume11No12/Paper_65-Fraud_Detection_in_Credit_Cards.pdf

Decision Trees: One of the widely used AI algorithms and is quite effective in identifying decision boundaries with vectors such as transaction amount, location, date & time.

A new cost-sensitive decision tree induction algorithm that minimizes the sum of misclassification costs while selecting the splitting attribute at each non-terminal node of the tree is developed and the classification performance is compared with those of the traditional classification methods, both cost-insensitive and cost-sensitive with fixed misclassification cost ratios, such as traditional decision tree algorithms, ANN and SVM. The results show that this cost-sensitive decision tree algorithm outperforms the existing well-known methods on our real-world data set in terms of the fraudulent transactions identified and the amount of possible losses prevented.[19]



One of the decision trees built with combined features is shown in Figure 2. The decision process is very visible from the tree and shows the importance of the features. For example, the most important feature is - Median of sentiment value with threshold 0. Another important feature is 'third person plural pronoun', which is an indication of deception, reflecting a customer's attempt to discuss third person, while the call is about his/her own financial account. It can also be noticed that qualified assertion, negative emotion, causation, and nominalized verb are also important linguistic features. Interestingly, a variation in sentiment values (SD) of responses, is also an important feature, indicating the too much change in the language of customer [20]

Random Forest: Ensemble of decision trees that improves accuracy of classification by averaging predictions from multiple tree branches

Random Forest is a supervised machine learning algorithm that uses a group of decision tree models for classification and making predictions [21]. Each decision tree is a weak learner because they have a low predictive power. It is based on ensemble learning, which uses many decision tree classifiers to classify a problem and improve the accuracy of the model [22].

Random forest is a combination of each good transaction fraud tree which is then combined into one model. Random Forest relies on a random vector value with the same distribution on all trees, each decision tree in e-commerce fraud detection which has a maximum depth. [23]

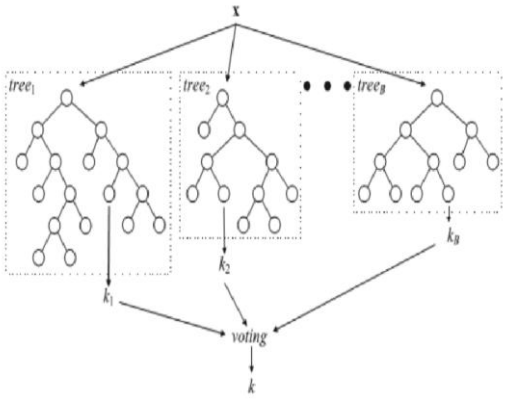


Figure 3: Architecture of Random Forest

International Journal of Management, IT & Engineering
Vol. 14 Issue 8, August 2024
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Naive Bayes: Is one of the widely used algorithm in fraud detection and by its effectiveness of the algorithm it gains prominence as a powerful algorithm yet maintaining its simplicity

In the context of fraud detection Naive Bayes works by analysing vast amounts of historical data in order to identify patterns & characteristics linked to fraudulent activities. The way algorithm detects fraud is by the means of probability of transaction being fraudulent depending on presence or absence of certain features like amount of transaction, time of the day & consumer behaviour

This is the era, where the plastic money concept is widely adapted all over the world, but every new technology has its own loopholes also. In this scenario many types of anomalies can happen which can harm the user economically. These anomalies can be defined as frauds in financial sector. To detect these types of frauds, many techniques and models are proposed by the researchers. In this study the proposed work tries to implement an automated model using different machine learning techniques for the detection of these kinds of frauds, especially related to credit cards transactions[24]

One of the primary advantages of this algorithm is its ability to handle very large data sets efficiently and outline predictions quite faster, which is key in fraud detection in the digital payments ecosystem.

The ability to churn vast amounts of data in real time or near real time is key to fraud detection systems, where timely identification of fraudulent transactions is crucial to minimize financial losses and also prevent multiple attempts by fraudsters.

Furthermore, Naive Bayes algorithm is quite apt to irrelevant features and works well even with limited training dataset, and which comes very useful for situations where procuring labeled training data for fraud detection could be a challenge.

While Naive Bayes is an extremely valuable algorithm in the area of fraud detection, its more often used in combination with other algorithms and methods to improve fraud detection accuracy and reliability.

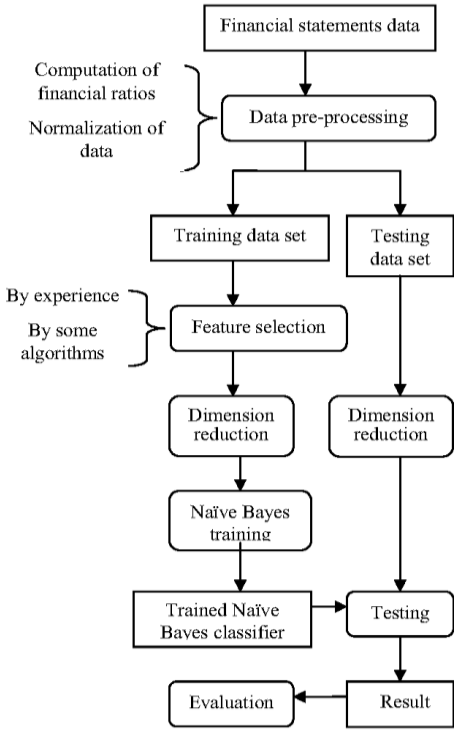


Figure 4:: Detection of fraudulent financial statements based on Naïve Bayes classifier [26]

Generative Adversarial Networks (GANs) :

Generative Adversarial Networks (GANs) can be effectively deployed for fraud detection by use of generating synthetic data samples that mimic fraudulent transactions, and augmenting the limited amount of real fraudulent data available for training machine learning models.

Generative models, such as generative adversarial networks (GANs) and variational autoencoders (VAEs), form the foundation of generative AI. GANs consist of two components: a generator network and a discriminator network, engaged in a competitive process of generating and evaluating content. VAEs, on the other hand, employ an encoder-decoder architecture to learn and generate new samples.[26]

International Journal of Management, IT & Engineering
Vol. 14 Issue 8, August 2024
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

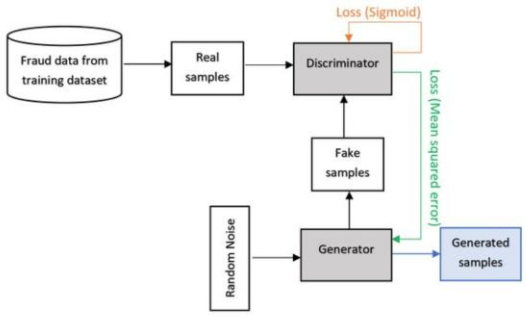


Figure 5: GAN architecture employed in this study consisting of a 5-layer FNN generator and discriminator, leading to the generation of the final minority samples depicted by the blue square [27]

FUTURE SCOPE

The rapidly evolving digital payment ecosystem has posed a significant threat in terms of fraudulent activities. However, with equally transformative applications in integration with Artificial Intelligence has enormous scope in the future.

Here are some potential areas of development and advancement:

Advanced Anomaly Detection: With algorithms becoming more and more sophisticated at detecting fraudulent activities the area of fraud detection will vastly improve. The algorithms would be able to identify hidden patterns while handling vast and complex datasets to indicate potential fraudulent transactions.

Real-time Detection: one of the key area which is highly effective is real- time detection. The application is powered by an Artificial Intelligence algorithm able to quickly identify, respond &escalate potential fraudulent transactions as it unfolds.

Behavioural Biometrics: An area which is fast up & coming that uses a unique approach of & enhances fraud detection would be behavioural biometric technique. Applications would start recording & looking at looking at typing patterns, mouse movements, and touchscreen interactions that can signify any anomalies leading to potential fraudulent transaction

Explainable AI (XAI): Regulator policies and compliance are required in order to maintain transparency and also to ensure no one abuses/ exploits the usage of Artificial Intelligence. The policies will mandate for explainable AI methods which not only detects but also provides with explanation of such decisions, typically reasoning. the ability of applications to detect and also reasons will gain prominence in future.

VI. CONCLUSION

Concluding, Artificial intelligence from having potential to be part of mainstream ecosystem have become integral part of application development and industrie's solution ecosystem. The speed at which the transformation is being witnessed in the last few years will ensure Artificial Intelligence powered applications will emerge as indispensable tools to combat fraudulent activities in the digital payments space.

Enterprise can leverage on advance algorithms with the likes of Logistics Regressions, Decision trees, Naive Bayes to the latest entrant of GAN (Generative Adversarial Networks), which can analyze vast amounts of transaction data to store patterns and identify anomalies and suspicious behaviour which indicate the possibility of potential fraudulent transactions. Most of these algorithms enable different approaches in fighting fraud which are focused on minimizing potential loss and restoring trust and faith in digital transactions..

As digital payment ecosystems continue to emerge as front runners in financial transactions, the role of Artificial intelligence will become more and more crucial underscoring the importance of investment in such methods & techniques in fraud detection technologies.

References

[1] Pan, Eryu. (2024). Machine Learning in Financial Transaction Fraud Detection and Prevention. Transactions on Economics, Business and Management Research. 5. 243-249. 10.62051/16r3aa10 .

[2]Gupta, Ruchika & Srivastava, Priyank & Taluja, Harish & Sharma, Sanjeev & Samant, Shyamal & Ratna, Sanatan & Sharma, Aparna. (2023). Leveraging Machine Learning Algorithms for Fraud Detection and Prevention in Digital Payments: A Cross Country Comparison. 10.1007/978-981-99-5994-5_33.

[3]Amin, Irtiqa. (2023). 2023 Global eCommerce Payments and Fraud Report.

[4]Taghiyev, Khayaladdin & Rustamov, Tamerlan & hasanzade, araz. (2021). Analysis of payment cards fraud transactions and measures to prevent them. Economic innovations. 23. 172-184. 10.31520/ei.2021.23.2(79).172-184.

[5]Kawase, Ricardo & Diana, Francesca & Czeladka, Mateusz & Schüler, Markus & Faust, Manuela. (2019). Internet Fraud: The Case of Account Takeover in Online Marketplace. 181-190. 10.1145/3342220.3343651.

[6]Vieraitis, Lynne & Copes, Heith & Powell, Zachary & Pike, Ashley. (2015). A little information goes a long way: Expertise and identity theft. Aggression and Violent Behavior. 20. 10-18. 10.1016/j.avb.2014.12.008.

[7] V, Mrs & Shirahatti, Simran & T, Soniya & Umair, Syed & Ahmed, Syed. (2024). Phishing - A Common Cyber Menace to Combat. International Journal for Research in Applied Science and Engineering Technology. 12. 2307-2310. 10.22214/ijraset.2024.60283.

[8]Potter, Kaledio & Klaus, Hubert. (2024). Emerging Trends in Digital Payments: The landscape of digital payments is constantly evolving.

[9] Research on Machine Learning with Algorithms and Development Authors Liqiang Yu Computational Social Sciences, The University of Chicago,Irvine CA, USA,Xinyu Zhao Information Studies,Trine University,Phoenix, USA, Jiaxin Huang Information Studies, Hao Hu Software Engineering,Zhejiang University,Hangzhou ,China,Bo Liu Software Engineering,Zhejiang University,Hangzhou,China DOI: https://doi.org/10.53469/jtpes.2023.03(12).02

[10] Kaderye, Golam & Arif, Ahsan & Kundu, Ronjon. (2024). Data Mining in Different Fields: A Study. International Journal of Innovative Science and Research Technology (IJISRT). 1828-1838. 10.38124/ijisrt/IJISRT24MAR1384.

[11]Ramakrishnan, Sreejit. (2023). The Importance of Data Mining & Predictive Analysis. international journal of engineering technology and management sciences. 7. 593-598. 10.46647/ijetms.2023.v07i04.081.

[12]Kumbhare, T. A., & Chobe, S. V. (2014). An overview of association rule mining algorithms. International Journal of Computer Science and Information Technologies, 5(1), 927-930.

[13]Rokach, L., & Maimon, O. (2005). Clustering methods. Data mining and knowledge discovery handbook, 321-352.

[14]Kesavaraj, G., & Sukumaran, S. (2013, July). A study on classification techniques in data mining. In 2013 fourth international conference on computing, communications and networking technologies (ICCCNT) (pp. 1-7). IEEE.

[15]Alenzi, H.Z., & Aljehane, N.O. (2020). Fraud Detection in Credit Cards using Logistic Regression. International Journal of Advanced Computer Science and Applications.

[16] Machine Learning For Credit Card Fraud Detection System Lakshmi S V S S1 ,Selvani Deepthi Kavila2 1,2Department of CSE, Anil Neerukonda Institute Of Technology And Sciences(A), Visakhapatnam-531162,India

[17]A. Mahajan, V. S. Baghel and R. Jayaraman, "Credit Card Fraud Detection using Logistic Regression with Imbalanced Dataset," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 339-342.

[18] javatpoint , website (2020). Available : https://www.javatpoint.com/logistic-regression-in-machine-learning (access 22 July 2020).

[19]Yusuf Sahin, Serol Bulkan, Ekrem Duman,A cost-sensitive decision tree approach for fraud detection, Expert Systems with Applications, Volume 40, Issue 15, 2013, Pages 5916-5923, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2013.05.021.

[20]Bajaj, Nikesh & Goodluck Constance, Tracy & Rajwadi, Marvin & Wall, Julie & Moniri, Mansour & Glackin, Cornelius & Cannings, Nigel & Woodruff, Chris & Laird, James. (2019). Fraud detection in telephone conversations for financial services using linguistic features.

[21] Prajwala, T. R. (2015). A comparative study on decision tree and random forest using R tool. International journal of advanced research in computer and communication engineering, 4(1), 196-199.

[22]Kabir, E., Guikema, S., & Kane, B. (2018). Statistical modeling of tree failures during storms. Reliability Engineering & System Safety, 177, 68-79.

[23]Saputra, Adi & Suharjito, Suharjito. (2019). Fraud Detection using Machine Learning in e-Commerce. 10.14569/IJACSA.2019.0100943.

[24]Gupta, Amit & Lohani, M. & Manchanda, Mahesh. (2021). Financial fraud detection using naive bayes algorithm in highly imbalance data set. Journal of Discrete Mathematical Sciences and Cryptography. 24. 1559-1572. 10.1080/09720529.2021.1969733.

[25]Deng, Q. (2010). Detection of fraudulent financial statements based on Naïve Bayes classifier. *2010 5th International Conference on Computer Science & Education*, 1032-1035.

[26]Ramdurai, Balagopal & Adhithya, Prasanna. (2023). The Impact, Advancements and Applications of Generative AI. 10. 1-8.

[27]Cheah, Patience & Yang, Yue & Lee, Boon Giin. (2023). Enhancing Financial Fraud Detection through Addressing Class Imbalance Using Hybrid SMOTE-GAN Techniques. International Journal of Financial Studies. 11. 110. 10.3390/ijfs11030110.