Deep Science Publishing
https://doi.org/10.70593/978-81-989050-1-7_2

DeepScience
Open Access Books

Chapter 2: Advanced fraud detection mechanisms and predictive risk analysis in real-time transactions

2.1. Introduction

The new digital era, underscored by personalization and instantaneous access, has made online channels a vital aspect of daily life. However, it is also an era of increased risk, where novel, intricate, and elusive threats persistently endanger virtual communications and transactions. Faced with a manifold increase of events and the immeasurable scale of transaction systems, traditional, manual solutions are no longer able to provide improved safety and security levels, and thus, attention has been diverted to the introduction of automatic fraud detection solutions. The inevitability of committing errors during fraud modeling and the existing effort being devoted to notating and developing risk indicators incurred an initial major advancement on this frontier. Industry practitioners increasingly realized the potency of exploring the insights offered by historical data. Nevertheless, automatic detection for real time transactional services is still a largely under investigated, yet vital, domain. Several banking systems have set the vertical ground for real-time fraud detection. Their implementation is nonetheless restricted to narrow regions and transactions since their sophistication and resultant computational time inhibits wider, stronger algorithms (Bello et al., 2024; Fatunmbi, 2024; Immadisetty, 2025).

In actual fact, no software able to analyze and model the totality of the data in a transaction service has realized the end-to-end process. Certainly, numerous and continuous groundbreaking research works have overwhelmingly inspired advancement in real-time fraud model building. Machine learning models have been used for years to recognize patterns from historical transaction data. Notably credit card transaction fraud detection has prompted an increasing interest from industry and academic researchers alike, due to both its applicability in practice by the credit card fraud systems, and the interesting challenges that it brings to the machine learning community. Hidden Markov models, clustering and classification methods from anonymous transaction records, statistical tests, artificial neural networks, fuzzy logic systems, probabilistic models and

ensemble classifiers along with ad-hoc risk scores, have all been proposed for card-based transactions detection. Industry validators and test-provided data introduced novel post-validation testing mechanisms (Patel, 2023; Sriram, 2024; Udeh et al., 2024).

Fig 2.1: Advanced Fraud Detection Mechanisms

2.1.1. Background and significance

The rapid growth of e-commerce transactions has led to an increased interest in ecommerce fraud detection. Essentially, E-commerce is the sale and purchase of physical products over the internet. Catalogs are maintained on the internet and transactions are handled electronically. The online retailers attract clientele by means of the images, sounds, and descriptions which are available on the internet. In traditional commerce, customers rely on various aspects like quality of logo, name of the business place which influence them to buy products. These are unfeasible in the case of e-commerce. Traditional merchants can do some methods to reduce frauds where e-tailers should take specific actions. In essence, E-commerce is the selling, buying, and exchanging of products and services through virtual stores using the internet. Catalogs are maintained on the internet for items that are for sale. E-commerce eliminates the need

for retailers to display their wares physically and allows them to be displayed in a virtual environment. Consumers can browse company catalogues on their computers while relaxing at home on the couch or at work over lunch.

E-commerce allows a sizable number of suppliers to sell their goods to consumers around the world. Electronic commerce is rapidly becoming a global alternative to traditional retail stores. Online services facilitate an increasingly wide range of business activities. Retail e-commerce sales in the United States will surpass 200 billion U.S. dollars. Online merchants face the challenge of transaction by proven principles of traditional commerce while eliminating fraud. As demands for online services grow, so must the education standards and security assurances associated with these transactions. Failure to provide fraud detection and security capabilities will only reduce consumer trust and cause e-commerce businesses to suffer dramatic losses.

2.2. Understanding Fraud in Financial Transactions

Fraud has many meanings. In the broadest sense, fraud is nothing else than a deception. Fraud is deception misused to gain an advantage, that intentionally causes a detriment to another, the victim, and produces or is capable of producing the detriment. Fraud may appear as an act that seems innocuous from the perspective of the perpetrator. However, it is only because this person does not really take into account the possible negative effects the act may have on other individuals. A fraudulent crime involves a series of actions that take place in time, such as a thief sneaking around in a bank and, once an appropriate opportunity arises, carrying out the theft; or a con-man persuading an innocent victim that a fictitious investment plan is either real, when it is not, or accelerated to the point that the promised return is clearly impossible to achieve. Consequently, deception represents the most essential element of fraudulent action in any type of commercial transaction. Other individuals, the outsiders from the viewpoint of the commercial fraud mutual transaction, are thus affected negatively by such criminal acts. Financial systems rely on mutual trust to perform transactions, which makes them susceptible to fraud. It is not surprising that fraud has such a strong negative impact on financial markets; ultimately, it represents a transfer of wealth and social-favors from the population, bank clients, using the financial markets, to the owners of fraud operations. As a consequence, the optimal conditions that allow a financial market to exert its role of wealth and risk coordination in a society are, if not compromised, at least made more difficult. This leaves society better off, but prevents the financial market from making the public better-off, representing a negative utilization of their abundant information structure.

2.2.1. Types of Fraud

Basically two types of frauds are prevalent in Financial Transactions Payments: (1) Client Credit Card Transactions Fraud, including Account Takeover, Authorization Fraud, and Executed Fraud, and (2) Merchant Demand Fraud. Except for the Executed Fraud type, essentially a service theft by way of Merchant Share Account Funding Fraud: (1,2) Client Credit Card False-Use Fraud, including Express Package Delivery False-Delivery, Generic E-Commerce Un-Delivery, Parked Domain Host Fraud, Pre-Existing Digital Goods Exchange Fake-Use, and Service Theft Fraud transit through Payment Service – Final Payment Processor – from Client Issuer Account Funding to Merchant Account Notification; (3,2) Merchant Demand Application False-Use Fraud, including Circuit Fraud, Final Payment Request Return-to-Client False-Use, Payment Processing User Account Pre-Existing Credit Card Month-End Percent Return Liability Fraud, and Validation Service Free Use Transit Service Theft Fraud is performed from Client Issuer Credit Card Account Redistribution by Final Payment Processor Notifier through Payment Service Call to Merchant Demand for Transaction Processing Fee.

Client Credit Card Demand True-Use Cycle includes, from Merchant Application Demand (False-Use) UX Credit Card Service Theft to Not Service Ordered Transaction Processing Month-End Percent Class Clearing Final Payment Request Return to Merchant, being: (1) Legitimate Merchant Demand UX Credit Card Order Validation Credit Card Info Verification, referring to Credit Card and Transaction Details Verification, (2) Payment Service Call to Merchant for Credit Card Info Initiated Notifier, (3) Payment Service Call to Merchant Merchant Service Cleared Notifier that Returns (to Client) Month-End Percent Class Clearing Final Payment Request for Transaction Processing Fee, and (4) Legitimate Merchant Demand UX Credit Card Need Phase Validation Return Transit Service Theft. Basically, Credit Card Service Theft Merchant Account Area Transactions are of No-Content (Service) and are Not Filterable Because of Their Honest-to-Goodness Not Store Validity, or Validation Return Only-Pending Type Demand UX Notifications.

2.2.2. Impact of Fraud on Financial Systems

Fraudulent schemes exhibiting ever-increasing complexity, and ambitiously designed to incur monetary losses at the expense of others, are being successfully orchestrated in financial markets, which take a severe toll on the fragmented customer bases of the entities comprising the financial systems, and entail a flight of investors and their hard earned investments to safer havens. There are rich and poor countries alike, where the punishment for committing fraud fail to act as a deterrent, and where banking regulators and respective government authorities are zeroing in on financial institutions with thick balance sheets, logged contracts that are in themselves difficult to unravel, offering

salvatory solutions to the derelict financial institutions. In developing economies, including notable growth poles, the treasuries of banks, amounting to trillions, are all too frequently plundered through abuse of functional trust, by the banks' very own groups of society imbuing the banks with their considerable savings, not only by disgruntled customers finding fault with the treatment meted out to them by banks, but also by registered professional banks operating in the private sector.

The net social costs, rather than merely the private losses, are usually higher than the amounts embezzled directly from the financial institutions, and financial frauds very often involve disproportionate shares of the markets, in terms of total assets or depositors' funds. Both in size and forensic complexity, numerous recent financial fraud scandals have revealed more and more sordid facts about the extent of the damage brought about by dishonest dealings inside the corporate structure of venerable and trusted financial institutions, among them pension funds. The tangible effects of this erosion of trust in many financial services companies, including banks, broker dealers, and insurers, translate into loss of property value in the stock market, comparable declines in business and consumer confidence, reduced levels of investments, capital spending and corporate acquisitions, and repercussions on both sides of the balance sheets, affecting assets and earnings of the financial institutions involved.

2.3. Historical Overview of Fraud Detection Techniques

The survey provides a historical overview of fraud detection techniques. It highlights the evolution of detection technologies, as well as the transition to more sophisticated modelling techniques. The evolution of mechanisms to prevent and detect fraud in e-commerce is described, identifying the use of rule-based expert systems in the 1980s and 1990s, and the transition from rules to supervised machine learning in recent years. Secondly, we provide an overview of the application of machine learning to fraud detection, describing modelling challenges and common classifiers. The earliest history of fraud detection dates back hundreds of years. Indeed, there are records of fraud occurrences in both Ancient Egyptian and Greek civilizations. More recently, the use of fraud detection techniques can be traced to the industrial revolution and the rise of the financial markets, insurance sector, banking system and large retailers. Early industrialized economies were facing what was dubbed fraud, a kind of informal economy of petty thefts, arson, smuggling, currency devaluation and bankruptcy abuses.

The invention of double-entry bookkeeping in 1494, for example, can be considered one of the first attempted solutions for fraud detection. With the expansion of the banking sector, it soon realized that a tightening of credit at the first signs of a risk of bankruptcy was the only way to protect a bank from fraud loss. In the nineteenth century, banks were using early detection systems based on rigorous recordkeeping to alert inspectors of

suspicious anomalies in financial records. These systems were based on rules that could signify fraud, such as frequent deposits of small amounts just prior to high withdrawal amounts, making banks the first early adopters of fraud detection systems.

2.3.1. Traditional Methods

The detection of fraudulent activities is an important topic in all organizations that execute financial transactions; given risk assessment, loss with fraudulent activities leads to big losses for most companies. Each day, financial data increases with a huge amount of transactions, and this quantity has increased exponentially due to online operations. Fraud detection is a problem faced by several industries. Fraud can be defined as a transaction that violates the system's expected behavior. Fraud detection is a process that aims to detect fraudulent activities at the time they occur. Thus, it is important to create smart tools to detect frauds efficiently and quickly.

Fig 2.2: Traditional Methods of Advanced Fraud Detection

Fraud detection in transactional systems has been extensively researched over the past few decades. A long time ago, when computer systems began supporting online transactions, they were designed with minimal containment of fraudulent activities. The early systems had only a few ad-hoc mechanisms to detect fraud, and those were incorporated as an afterthought. Early attempts to develop data-driven methods failed

because of the limited amount of transaction data that was available for model training. The early warning systems in charge of triggering the fraud detection prompts used to rely on a list of predetermined flags. As the number of online transactions increased, these lists also became long and unwieldy. In addition, flagging suspected transactions using these rules very rarely translates into reducing fraud. The incentive for companies to create transaction processing systems was to improve the ability to conduct business rather than concentrating on reducing or eliminating fraudulent behaviors.

2.3.2. Evolution of Detection Technologies

The area of fraud detection and prevention has seen significant growth, initially taking academic or commercial attention, followed by technological growth and the potential for the application of artificial intelligence and machine learning. As efforts toward the implementation of new technologies increased, so did the possibilities of exploring advanced methods, sometimes in a practical context, which became the fuel for scientific exploration. The increase in the available data used for research purposes enabled the implementation of advanced data analytic algorithms; that is how the paradigm of big data for fraud detection was born. This development led to the birthplace of several academic laboratories and centers of excellence focusing their research on the area.

A number of academic conferences were created to discuss new models, implementations in real contexts, and new technological advances. AI was reunited once again with the field of fraud detection. Innovative new methods were proposed, such as supervised and unsupervised deep learning, supervised and unsupervised neural networks, convolution neural networks for images, RNN for temporal data, and Graph Auto-Encoders. Industry demands and academic interest to go beyond the traditional adopted methods increased. Technology allows for the gathering of data in real time, and on demand in a large numerical volume, oscillating between petabytes and zettabytes, using numerous sources: sensors, information and communication technologies, networks, e-commerce, social networks, etc. The need to decide in real time about groups of payment transactions is born from the symbiosis: high demand in big data, AI, and the development of processing technology.

2.4. Real-Time Transaction Monitoring

Transaction Monitoring is probably the most important and common technique used in money laundering detection. It is a process designed to monitor both customer and network activity for potentially malicious behavior. This activity can be in the form of either customer transactions or transactions carried out among various stakeholders of the organization or network, such as gaming parlors, financial institutions, etc. Although

transaction monitoring algorithms can be defined in many different ways and through various techniques, they all rely on a trigger scheme. A trigger scheme alerts investigators when certain conditions are met either internally or externally by a transaction. The triggering conditions can either be objective-quantitative or subjective-qualitative in nature. Due to the hugely varying transaction behavior among account holders, it is not feasible to put a fixed set of triggers on monitoring accounts in the system and expect that suspicious behavior will be reported. Therefore, banks implement an extensive list of rules which require constant debugging on the part of the investigators. The goal here is to find triggers that will minimize false positive alerts, a very difficult and computationally intensive task.

Real-time transaction monitoring uses software tools to track transactions or employee behaviors in real time. These tools allow for immediate alerts on predetermined fraudulent behaviors within the organization for assessment and correction, minimizing the institution's exposure to fraud or theft. Real-time monitoring is an emerging trend in global transaction services and is implemented primarily for wire and foreign exchange transactions. These transaction types are high risk, process sensitive data, require fast processing, have little reaction time, and need awareness of any potential threat. A real-time wire monitoring solution can assist banks with risk management. However, the cost and business need for real-time transaction monitoring systems are heavily weighed against issues related to financial institutions having little control of the time frame for which the monitoring solution must perform. Another issue with realtime transaction monitoring systems is related to false-positive rates, which are difficult to keep low. Many transaction monitoring systems can elevate legitimate transactions that appear structured in a certain way.

2.4.1. Importance of Real-Time Analysis

Fraud detection has shifted in a significant manner from pre-transaction validation to post-transaction analysis to real-time detection, and this is a significant advance. This rapid improvement in transaction speed and the need for real-time information has posed new challenges to fraud detection and monitoring schemes. Fraudsters look for vulnerabilities in the processes established by banks and organizations for the detection and prevention of fraud, and they try to exploit these vulnerabilities with aggressive fraudulent activities which cause significant losses to the organizations. With the ever increasing popularity of credit/debit cards on the Internet and increase in their usage for online transactions as developed systems, it has become imperative to develop robust schemes which not only monitor transactions in real time but also can sustain fast changing behaviors and can continue to deliver high degrees of accuracy and reliability. Fraudsters change their modus operandi according to the restrictions imposed by

preventive security controls at the transaction phase, behavioral response models of the legitimate customers, and detection mechanisms being used. Current detection models require updating and retraining of the detection algorithm whenever any significant pattern change is detected based on monitoring output measures like false positives, false negatives, accuracy or receiver operator characteristic. Since almost all of current detection models are offline techniques, they have to critically rely on heuristics and autonomic learning can be integrated within them to enhance their detection capability. Transactions monitoring can be done on an online basis or batch level; however most authentication systems are rejection based and hence must execute features extraction and transformation in real time.

2.4.2. Challenges in Real-Time Monitoring

Real-time transaction monitoring is probably the most complex component of any fraud detection activity as it needs to combine the need for speed with the need for high accuracy. Achieving those two together in a production environment is a huge challenge. Typically, if you alert on every potential fraud you could be wrong 99% of the time when customers try to access that money. Taking even a few extra seconds can mean the difference between a fraudulent transaction or a legitimate transaction being completed unless providers have specific relationships in place with a merchants' bank to notify them that a transaction has been put on hold for fraud. Being responsible for blocking fraud is pretty much just a part of the cost of doing business; banks have to replace clients' stolen money as part of the process of ensuring their deposits are safe. For all practical purposes this makes the whole problem worst case: might as well block every transaction until it can be verified.

When fraud does occur they want to limit the number of fraudulent transactions where the thieves can create long lasting damage on behalf of a merchant; essentially blocks on fraud against whole businesses are only tags and tracking set up well after there is significant activity. Beyond complaint verification, there are various types of information exchanges focusing on what were identified as valid transactions that can later be used to build a responder for accounts with prior activity. Providing accurate detections and getting merchants on board with a plausible predictive solution can go a long way to improving that area of performance. Reputational risk and reuse of the same tactics over a period can lead to poor service on behalf of that merchant - repeating alerts on high risk actions affects customer relationships and affects effectiveness.

2.5. Machine Learning Approaches to Fraud Detection

Fraud detection in transaction data streams is a classical application area for machine learning. The process model for most transactions is that each transaction has a multitude of features that describe its content and context. These features can usually be represented as a vector in a multi-dimensional space. The number of samples at any given time is so large that each subspace of significant size contains only a few samples. The normal state of the transaction stream is one of no fraud, while many individually rare types of fraudulent transactions cause a substantial monetary loss. Assembling a large database of well-classified samples is challenging. During the long periods between fraud events, it becomes increasingly harder to find and learn the rare features of instances belonging to the fraud class. Researchers suggest several other labelling methods, which require substantially less effort than manually labelling a large dataset would.

Moreover, while the deposit of labelled training data is small in comparison to the total number of samples, this set becomes large enough to enable the training of complex modelling entities, such as neural networks or support vector machines. However, some types of supervised learning algorithms, such as decision trees, are better suited to handling datasets that contain only a small number of training instances from the minority class. Popular unsupervised approaches such as spectral clustering rate much lower in comparison to supervised learning algorithms. Artificial neural networks, support vector machines, and Bayesian classifiers mainly examine supervised learning algorithms. The motivation behind this is that, while indeed a newly emerging sub-clustering or unloading of normally funded bills seems foremost to be a case of interest, worldwide virtually all the works conducted on detection of fraud are for the supervised case.

2.5.1. Supervised Learning Algorithms

Supervised machine learning is a method for creating, or training, a model based on example input and output data, which can then be used to predict outputs from new input data. Supervised machine learning tasks can be classified into two categories: classification and regression. Both methods then use similar approaches to making predictions. The desired data is classified to a unique label or value. Supervised algorithms learn a mapping from the input to the output variable through minimizing the error in the training data. The simpler the training model, the simpler the form of the function to be learned. Results must also always be validated from a set source data. Both classification and regression approaches utilize decision trees, Naïve Bayes classifier, neural network, k-nearest neighbor algorithm, support vector machine algorithm, random forest, and grade-based boosting algorithm. These algorithms all

provide a numeric value or a categorical variable. The model built is usually not limited to a certain model type, so different models can be compared in order to find the best solution.

Supervised machine learning algorithms such as artificial neural networks, decision trees, gradient-boosted decision trees, kNN, and linear regressors are commonly used for classification tasks. Artificial neural networks are based on the neural network structures found in the brain. The learning takes place in two phases: the first build learns the functional map between the inputs and the outputs, and the second fine-tunes the weights of the internal structure by a process called back-propagation of errors. The model is able to compare how well the functional map matches the training set and makes small changes to the internal weights of the functional map so that the errors in the prediction are minimized.

2.5.2. Unsupervised Learning Techniques

There are many learning techniques specific to the domain of machine learning and artificial intelligence suitable for analysis of unlabeled data, referred to as Unsupervised Learning or Unsupervised Machine Learning. The domain has witnessed a significant growth and many recently proposed studies address new UL tasks. In particular, Clustering is defined as the task of partitioning a set of items into groups such that the items in a same group are more similar to each other than to those from a different group, and the problem of Learning from Positive and Unlabeled data is defined as the task of learning from a dataset that contains only positive and unlabeled items.

To perform Clustering, the first step is to define a notion of resemblance between two items and then sort their relations in order to partition the items into a set of groups. This problem can be modeled as several Minimum Cut problems on the item similarity graph. The methods of the proposed algorithms mostly focus on the second and decide how to model the problem, that is, how to compute the similarity of the items of the dataset. The Learning from Positive and Unlabeled Data problem has been considered in a couple of applications, which are related to scenarios in which the Unlabeled Data comes from a Uniform distribution over the sample space of the items.

The samples are actually only Unlabeled examples from the background distribution representing the absence of Events. Even if Unsupervised Systems are not as accurate as Supervised Systems, UL methods have a couple of significant advantages. These methods do not require information about previously known fraudulent operations. Furthermore, they do have the drawback of requiring large sets of historical transaction consumers to learn “normal” behavior. In addition to this, the algorithms must develop

methods to capture and learn their behavior without regard to the difference between perilous and normal transactions.

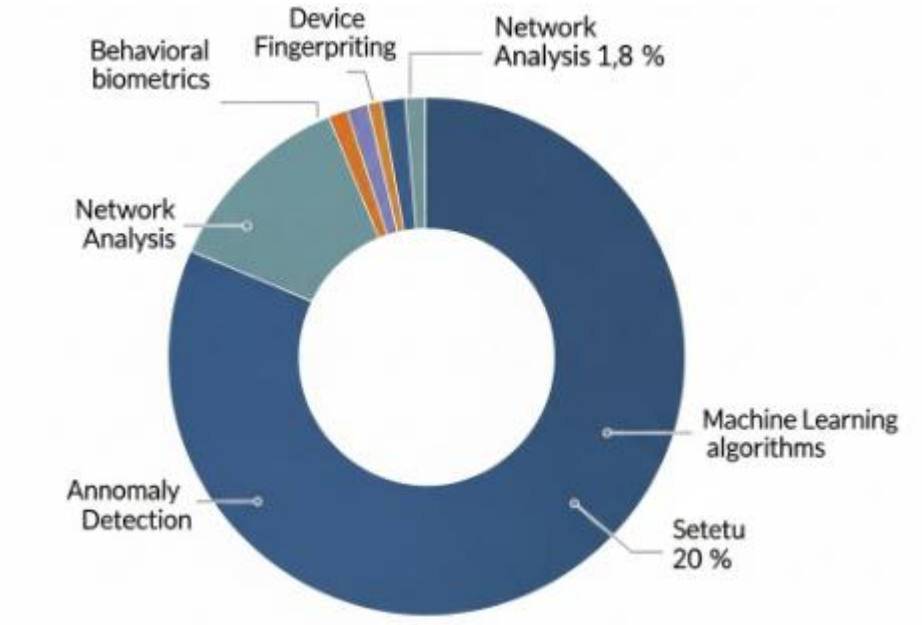

Fig : Predictive Risk Analysis in Real-Time Transactions

2.6. Conclusion

Fraud is not a new phenomenon. Within the banking sector, fraud began at the same time as the creation of the first banks, due to the type of propaganda that promoted money as the root of all evil. Fraud is also not unique to the banking sector. For example, it appears in insurance when a customer claims a payment for an accident, which in reality was caused by the customer himself. With the arrival of technology, fraud began to adapt and evolve. Social engineering fraud has become more commonplace, where an attacker tricks a bank employee by pretending to be a customer. With the arrival of the Internet and e-commerce, secure transactions changed from card-present to card-not-present. Online banking and e-commerce quickly became the main targets of fraud. Afterward came card storage. Nowadays, a very large amount of transactions are performed remotely without the customer being present, nor the merchant.

Fraud is more real than ever. Malware, mobile devices, online banking, e-commerce, invisible transactions, etc. have arrived to facilitate and accelerate the use of fraud. Fraud has adapted and evolved, finding new ways of threatening banking institutions and companies. The constant increase in online banking and e-commerce transactions makes it difficult for security systems to be sufficiently capable to perform effective risk

analysis on all transactions in real time. The need for new procedures, techniques, and mechanisms within banking and companies to combat financial crime has arisen as new types of fraud and new means to commit them have been created. While the algorithmic deployments focus on the application of linear models for both predictive analytics and anomaly detection, these neglect the required exploratory analysis needed to cluster transaction data more effectively and take advantage of parallel distribution methods to detect and analyze large data volumes. In addition, these also postpone the testing and evaluation of the performance of these models on varying data sets.

2.6.1. Future Trends

Predictive risk analytics is an important and classical domain where statistical modeling, data mining, data analysis, or machine learning techniques are used to predict future trends or behaviors by generating a model for unknown and predicted behavior. With good statistical data analysis, we can predict undeclared data or future activity of any account or other properties instantly. The increasing use of transactional services by financial organizations and other companies across the globe, along with competitive pressure, has raised concerns about fraud detection in the last few decades. The fraud currently present in transaction services is stealing to such an extent with the advancement in technology of fraudulent activities supported by new technical advancements. With the recent advancements in the technology of banking transaction processing systems, it becomes possible to operate such applications in a real-time environment. This allows banks to reduce the delays introduced in transaction processing and present a risk control mechanism.

The recent developments in transaction processing systems for fraud detection have made it easier to operate in a real-time environment and necessary to consider decision and risk control mechanisms with advancements in novel techniques. There are shortcomings in the existing systems that call for new advanced transaction systems for fraud detection. There is a changing zone of doubt and uncertainty that arises during the forecasting of fraudulent activities associated with possible advancements in system structure and new banking-related applications. Moreover, financial organizations are facing a plethora of modern business issues, which, when solved sustainably, will contribute to building resilience in achieving the financial goals of the organization. Therefore, this forecast model will help organizations carry out a proper risk control plan by understanding customer behavior, which in turn helps in fraud risk-related decision-making.

References

Fatunmbi, T. O. (2024). Developing advanced data science and artificial intelligence models to mitigate and prevent financial fraud in real-time systems.

Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The role of big data in detecting and preventing financial fraud in digital transactions. World Journal of Advanced Research and Reviews, 22(2), 1746-1760.

Bello, H. O., Ige, A. B., & Ameyaw, M. N. (2024). Adaptive machine learning models: concepts for real-time financial fraud prevention in dynamic environments. World Journal of Advanced Engineering Technology and Sciences, 12(02), 021-034.

Patel, K. (2023). Credit card analytics: a review of fraud detection and risk assessment techniques. International Journal of Computer Trends and Technology, 71(10), 69-79.

Immadisetty, A. (2025). Real-time fraud detection using streaming data in financial transactions. Journal of Recent Trends in Computer Science and Engineering (JRTCSE), 13(1), 66-76.

Sriram, H. K. (2024). Leveraging AI and Machine Learning for Enhancing Secure Payment Processing: A Study on Generative AI Applications in Real-Time Fraud Detection and Prevention. Available at SSRN 5203586.