American Journal of Financial Technology and Innovation (AJFTI)

ISSN: 2996-0975 (ONLINE)

VOLUME 3 ISSUE 1 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Financial Technology and Innovation (AJFTI)

Volume 3 Issue 1, Year 2025
ISSN: 2996-0975 (Online)
DOI: https://doi.org/10.54536/ajfti.v3i1.5168
https://journals.e-palli.com/home/index.php/ajfti

AI-Driven Fraud Detection in Digital Banking: Ml Approach for Secure and Transparent Financial Transactions

Oreoluwa Abimbola Serifat[1*], Roseline C. Igah[2], Kehinde M Balogun[3], Gershom Randy Mensah[4], Emmanuel Niiboye Odai[4]

Article Information

Received: August 25, 2025

Accepted: September 23, 2025

Published: October 25, 2025

Keywords

Artificial Intelligence (AI), Digital Banking, Fraud Detection, Machine Learning (ML)

ABSTRACT

The convenience of digital banking services has transformed the global financial industry and is now available to consumers all over the world. As with any advancement, there's an increase in associated risk. In this case, we have an upsurge in fraudulent activity, the mobility of cybercriminals, and their more advanced technologies to breach vulnerabilities within digital infrastructures. Indeed, financial crimes are constantly evolving like the rest of technology and society. Those who monitor and manually analyse systems are no match for the speed at which criminals can devise new rule-of-thumb schemes. This article examines how artificial intelligence and machine learning can reform the detection of fraud within digital banking systems. The research analyses different techniques of AI and ML, supervised learning, unsupervised learning, ensemble, and deep learning approaches, while also observing their uses in practical fraud detection systems. The paper also analyses the ethical and legal concerns involving the use of AI within banking, considering data issues, algorithmic discrimination, and other contentious aspects of legal compliance, including quasi-legal frameworks like GDPR and PCI-DSS. It also explores some of the newer directions in AI, like quantum computing, explainable AI (XAI), and federated learning, and their potential implications to improving fraud detection systems performance. Finally, the focus of this paper has been on a continuing effort and partnership across sectors in building resilient, secure, transparent financial systems. AI, ML, and blockchain technologies enhance the capability to prevent fraud in digital banking, while ensuring and maintaining customer trust and security in financial transactions.

INTRODUCTION

Digital banking represents a fundamental change in the finance by transforming the ways that people access and handle their money, for example (Mohmmed *et al.,* 2024). Digital banking, through online and mobile banking, or use of digital or e- wallets, has increased access to financial services by making them more accessible, convenient, and efficient (Barroso & Laborda, 2022; Oduro *et al.,* 2025). Consumers can now execute various banking transactions from any location at any moment which leads to enhanced financial inclusion and equal access to banking services. Digital banking solutions enable businesses to enhance operational processes while cutting operational expenses and offering customized services to their clients (Bueno *et al.,* 2024).

The expansion of the digital landscape creates greater opportunities for financial fraud to occur. Online transaction growth leads to a highly susceptible financial environment for numerous criminal activities (Kipngetich, 2025). Fraudsters exploit digital platforms to target financial system vulnerabilities using advanced techniques to overcome conventional security barriers. As digital platforms become essential for daily banking operations, there has been a substantial rise in fraudulent activities including identity theft, card-not-present fraud, account takeovers and money laundering (Adeyeri *et al.,* 2023). Traditional fraud detection methods that depend on rule-based algorithms and human supervision fail to match the speed and complexity of current fraudulent activities (Ismaeil, 2024).

As the fraud increases, the need for automated, innovative and real-time detection solutions is evident. Banking is realizing that traditional fraud detection has its weaknesses; high rates of false positives, expensive manual review process, and lack of ability to expose new, emerging fraud patterns. This realization has given rise to a more nuanced application of techniques, especially utilizing Artificial Intelligence and Machine Learning (AI/ML) (Olowu *et al.,* 2024). The need to adapt to new schemes and the capability of AI technologies in large data analysis, pattern recognition, and adaptation to new threats make it an increasingly important resource for improving the fraud detection systems in use. By leveraging these technologies, banks can prevent and minimize fraud before it occurs, enabling secure, efficient and transparent financial transactions (Ismaeil, 2024). This evolution towards fraud detection via AI, addresses the need for better intelligence, scalability, and real time capabilities in a more digital and online oriented industry. What is certain is that as the digital banking system has brought much benefit, it needs to be secured against new digital fraud threats, and thus protected just as much.

[1] Department of Data Analytics, Nexford University, USA
[2] Department of Management Science And Information Systems, Oklahoma State University, USA
[3] Department of Mathematics, Austin Peay State University, Tennessee
[4] Northeastern University, Massachusetts, USA
[*] Corresponding author's e-mail: oreoluwaabimbolaserifat@gmail.com

Hence the objective of this paper is to discuss how AI and ML could be fruitfully employed to improve the detection of fraud in digital banking as a novel and dynamic way to maintain security, efficiency, and transparency in a world where fraud in digital banking is becoming increasingly prevalent. The types of fraud in digital banking, AI and ML solutions to detect and deter fraud, practical examples of successful implementations that enhance the security and robustness of digital banking against ever-changing fraud techniques, and bolstering consumer confidence in banking transactions.

LITERATURE REVIEW

Digital banking has been a disruptive innovative force in financial services, changing how people and businesses interact with their finances in a big way (Bueno *et al.,* 2024). It is technology, internet access, and demand for reduced and efficient banking services that have motivated the transformation from physical to digital banking (Iwedi, 2024). For instance, with digital banking customers can check their account balances, transfer money, request loans, and pay bills online in their houses or anywhere by using their mobile phones (Javaid *et al.,* 2022). Also, financial institutions have strategically leveraged this technology to provide a spectrum of e-payment opportunities and services to their clientele (Igah & Luse, 2024).

Among the essential services of digital banking are online payments, which are transactions that help the transfer of money between individuals and businesses through the internet (Abdelrhman, 2025; Windasari *et al.,* 2022). The result has been that e-commerce has exploded as consumers now can purchase goods and services easily. Mobile banking applications take this convenience a step further, allowing individuals to view their accounts and execute transactions from their mobile phones and thus transforming banking into an even more accessible medium than before (Ezie *et al.,* 2023; Rahman *et al.,* 2024). Wallet applications like Apple Pay and Google Pay or apps from individual banks help consumers save and manage their payments information digitally, enabling fast and secure transactions without requiring physical cards (Khando *et al.,* 2022).

While digital banking has offered many advantages including financial inclusion for the unbanked, user-friendliness, cost- efficiency, etc, it has also increased the attack surface available to cybercriminals. In other words, the advantages of digital banking have also been problematic, as cybercriminals have taken advantage of online platform weaknesses to obtain personal information and carry out unauthorized illegal transactions, and therefore online banking has become subject to fraud and cybercrime activities (Aziz & Andriansyah, 2023; Mallesha & Hymavathi, 2024; Roszkowska, 2021).As a result, the financial sector faces increasing pressure to implement robust security measures to protect customers from the growing risk of fraud.

Fraud in Digital Banking

Digital banking fraud is the unauthorized and illegal utilization of digital banking systems to steal, manipulate and compromise financial data for an individual's own benefit. As a result, more and more fraudsters are taking advantage of online banking, utilizing multiple methods of exploiting weaknesses inherent in digital banking systems. These include, among the more common, identity theft (Venigandla & Vemuri, 2022), where fraudsters obtain personal data to pose as clients and gain access to their accounts.

Phishing is another form of scam in which customers are tricked into revealing sensitive information such as passwords and account numbers (Adaji *et al.,* 2024). The second most frequent form of fraud is transaction manipulation, where the fraudster is actually the one who initiates the transaction exploiting a loophole in the payment mechanisms (Adeyeri, 2024; Oduro *et al.*, 2025). Another related issue of grave concern is also money laundering, where criminals can disguise the source of illegal funds through sophisticated transactions on digital banking platforms that seem authentic (Bello & Olufemi, 2024; Olowu *et al.,* 2024; Khodabandehlou *et al.,* 2024). Also, without adequate security measures, funds can be moved illegally across borders using digital payment systems, making it even more difficult to get any form of control or trace these funds.

Consumer trust in the banking system is thus diminished as these scams are expensive for banks and other financial institutions to deal with (Adeyeri, 2024). The increased use of digital banking has made the implementation of advanced fraud detection systems capable of addressing and recognizing such fraudulent behaviours a necessity.

Traditional Fraud Detection Methods

Most banks use rule-based systems and human monitoring to catch fraud when it happens. In rule-based systems a predefined set of rules is utilized to identify potentially suspicious behaviour, for example, these sorts of rules could indicate abnormally large transactions or simultaneous multiple withdrawals from various locations. Goyal *et al.,* 2025; Metha, 2025). These systems have the ability to detect patterns of fraud that have been established, but they are limited in that they cannot evolve to detect emerging patterns of fraud. Traditional rule systems tend to be rigid; they can only catch fraud patterns that are in line with existing parameters and are unsuccessful at recognizing new fraud strategies that might be unpredicted patterns of fraud identified by existing parameters and would be ineffective in recognizing new fraud strategies that might not have been predictive of fraud patterns by existing parameters and would be ineffective at recognizing new fraud strategies that might not have been anticipated (Bello *et al.,* 2023; Ikemefuna *et al.,* 2024).

Fraud monitoring is also completed by humans, who review flagged transactions that were detected by rules or other non-automatic fingerprints of alleged fraudulent

activity (Hilal *et al.,* 2021). But human oversight adds an even more rigid layer of control, as it is highly laborious and also subject to mistakes given the enormous number of daily transactions. Plus, humans reviewing cases can be overwhelmed by the volume and complexity of rampant fraudulent activity, causing delays in the detection and subsequent action (Bello *et al.,* 2022).

Combined, these traditional techniques can produce high false positive rates which burden banking staff and lead to unneeded investigations. Just as fraudsters have continued to enhance their techniques, the conventional systems have become less effective to deal with the increasing complexity of this digital fraud and this has opened the door to more sophisticated, AI-based solutions for fraud detection.

Machine Learning in Fraud Detection

Fraud detection has changed with AI and ML as they help financial institutions, "analyse huge data sets in real-time and recognize intricate patterns that signal the possibility of fraudulent behaviour" (Adhikari *et al.,* 2024; Odufisan *et al.,* 2025). Unlike traditional rule-based systems, ML algorithms are trained on historical data and thus are adaptive in detecting patterns of both historical and emerging fraud. Supervised learning, unsupervised learning, and reinforcement learning are now commonly used in fraud detection systems by machine learning techniques (Sarker, 2021; Hernandez Aros *et al.,* 2024).

Supervised learning involves training a model using a labelled dataset with transactions already labelled as fraudulent or legitimate (Afriyie *et al.,* 2023). The model will then learn the patterns that distinguish these two in order to predict the probability of fraud in future transactions. Unlike, unsupervised learning is used for finding anomalies in unlabelled data (Venigandla & Vemuri, 2022). This is particularly advantageous in identifying novel or unknown patterns of fraud that are actually not found in the historical data. Also, reinforcement learning, where the model learns by interacting with the environment, becomes an effective fraud detection tool as it constantly improves the predictions of fraudulent actions (Sharma, 2024).

AI and ML applications to fraud detection writ large has been the subject of study in a couple of papers. In 2020 Li *et al.* concluded that individual algorithms performed worse than random forests and gradient boosting in the detection of credit card fraud, supporting the results of this study. Another example of research emphasizing the use of RPA and AI in online banking fraud detection is by Wang *et al.* (2019), who recommended hybrid RPA and AI predictive analytics system to be used as a cutting-edge approach for online banking fraud detection. Also, Oduro et, al. (2025) pointed out the potential of machine learning models to improve accuracy in fraud detection and decrease the false positive rate in digital banking systems.

MATERIALS AND METHODS

The study is based on secondary data concerning the use of Artificial Intelligence and Machine Learning in Fraud Detection in Digital Banking from among a general pool of published research articles. The required data was obtained by systematically identifying peer reviewed journal articles, conference proceedings, and industry reports retrieved through Google Scholar, IEEE Xplore, Elsevier, and other reputable journals. Selected articles were those that addressed digital fraud detection systems that implemented the use of AI and ML, specifically in regards to the categories of fraud detection systems of supervised learning, unsupervised learning, reinforcement learning, and ensemble methods. A method and finding section were extracted from each study of interest that focused on fraud detection in banking. A focus was on these techniques as employed in actual banking scenarios, specifically data preprocessing, model selection, and algorithm performance.

RESULTS & DISCUSSION

AI And ML Techniques for Fraud Detection

AI and ML thus represent an integral part of fraud detection systems, particularly in the context of online banking. These technologies allow banks to sift through

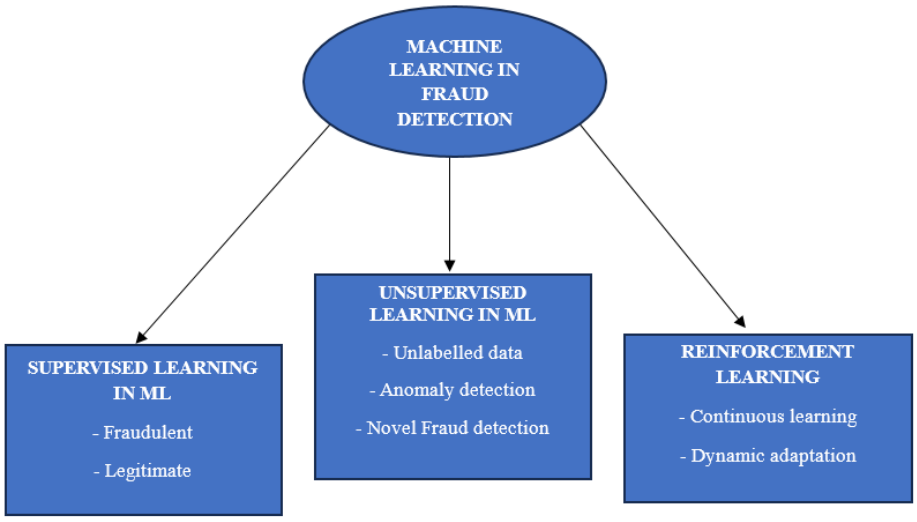

Figure 1: Machine Learning (ML) in Fraud Detection

massive volumes of transaction data and detect minute patterns in transactions that may be suggestive of fraud. While legacy fraud detection is primarily rule-based and human supervised, AI and ML algorithms apply knowledge to new data in real-time to adapt to shifting patterns of fraud.

AI and ML's main advantage in fraud detection is its capacity to handle, or "scale up", large datasets and find patterns within them (Adeyeri, 2024). By detecting both established as well as new patterns of fraud, these algorithms can aid in the prevention of fraud before it occurs. AI technologies can identify patterns of anomalies that would be hard to catch by human analysts or static rules-based systems. Rather, through their ability to use historical data and becoming better at predicting fraud over time, AI and ML "empower banks to detect new forms of fraud even before they happen" (Odufisan, 2025).

As the advancement of fraud schemes have also advanced detection methods are becoming obsolete. This ability to scale and adapt fraud is an important characteristic of AI and ML models. Overall, these technologies help banks not only to identify fraud as it is happening but also to anticipate and stop fraud before it occurs, increasing the security of the digital banking experience.

Common ML Techniques

Supervised Learning

Afriyie *et al.,* 2023 highlights that supervised learning is one of the most commonly employed methods in machine learning to detect fraud. This includes training a model on a labelled dataset in which there is knowledge of the outcome of each transaction whether it was fraudulent or legitimate. The model then "learns" to correlate patterns or groupings of input features, transaction amount, time, location, etc. with the target outcome fraud versus non-fraud.

Fraud detection often employs "Decision Trees" and "Random Forests" which are common fraud detection supervised learning algorithms (Salunke *et al.,* 2025). It forms a model shaped like a tree by repeatedly partitioning the data based on values of the features. The nodes are points at which a decision is made on a given feature and the leaves are the predicted classification as either fraud or non-fraud (Adeyeri, 2024; Afriyie *et al.,* 2023; Johora, 2024). Random forests are collections of decision trees. They aggregate multiple decision trees to increase accuracy and overfitting, which is a flaw of decision trees. Since it combines predictions from multiple trees, random forests are efficient tools, especially when dealing with large and feature-rich data (Ismaeil, 2024). Li *et al.* (2020) On top of that offered, as an example, logistic regression, decision trees and neural networks; who studied the efficiency of different machine learning methodologies, including logistic regression, decision trees and neural networks, in detecting credit card fraud. With regard to accuracy and detection rate, the research found that ensemble methods, such as random forests and gradient boosting, outperformed single algorithms.

Logistic Regression is a well-known algorithm that applies to supervised learning approaches for the detection of fraud (Adeyeri, 2024). Specifically, "it is a statistical method that "models the probability of a binary dependent variable, for example, presence versus absence or fraud versus no fraud, as a function of one or more independent variables". Logistic regression can also be an efficient and interpretable approach when there is a linear relationship between the features and the outcome. It is also useful in interpreting the importance of various features in the prediction of fraudulent transactions (Venigandla & Vemuri, 2022).

Unsupervised Learning

This is particularly relevant in the context of fraud detection in which obtaining label data is often hard but worse still it is impossible to obtain. On the other hand, supervised learning does not require labelled data to train the model. Instead, it seeks patterns and outliers in the data that do not adhere to normality (Khodabandehlou *et al.,* 2023).

K-means and more generally "Clustering methods" are frequently included among the techniques used for unsupervised learning within the specific domain of fraud detection (Huang *et al.,* 2024). Clustering categorizes similar data points based on characteristics. For example, K-means partitions the data into K clusters of like transactions. Most of which are "anomalous" or "fraudulent" transactions. This would assist in detecting outliers in the data points which are often indications of a possibility of fraud (Ali *et al.,* 2021).

Another common approach used for fraud detection is the 'Anomaly detection' algorithms, Unsupervised (Venigandla & Vemuri, 2022; Rojan, 2024). These are algorithms based on rare or anomalous patterns within the data which are unlike normal behaviour. Anomaly detection has been done by means of "Isolation Forests" and "One-Class SVM" (Support Vector Machines) amongst other methods. (Wei *et al.*, 2023). These models learn what the normal behaviour of the dataset is and treat anything that deviates from it as suspicious. In particular, anomaly detection could be very useful to detect a novel pattern for fraud that has never been previously experienced, and thus becomes an important technique to deploy against new fraud tactics.

Deep Learning

"Deep learning" is, in contrast to other traditional ML models, a more powerful approach to searching on massive datasets for more complex patterns of fraud, as it uses artificial neural networks containing multiple layers to model very complex relations in the data instead of traditional ML models (Xuan *et al.,* 2021; Bello & Olufemi, 2024). On top of that, large amounts of unstructured data like images, or transaction texts/narratives, which are harder to deal with by classical models, are also easily accommodated by these models.

Two examples of deep learning models that are used effectively for fraud detection are Convolutional Neural

Networks (CNNs) and Recurrent Neural Networks (CNNs) (Adeyeri, 2024). Convolutional neural networks, typically employed for image recognition, have the potential to be utilized for fraud detection as they excel at detecting patterns in an input of sequences or time series data, such as sequences of transactions (Bello *et al.* 2022; Bello & Olufemi 2024; Chowdhury 2024). RNN's, and specifically "Long Short-Term Memory (LSTM)" networks, are focused on spotting temporal dependencies within the data and therefore have good potential to be utilized for fraud detection in cases where the sequence of the events in relevant (Bhuiyan *et al.,* 2025; Mienye *et al.,* 2024; Muthunambu *et al.,* 2024). An example could be that an RNN can recognize fraud by the transactional pattern, or by the attempted login pattern recognition.

Deep learning methods have the advantage of being able to detect more complex patterns of fraud than what simpler machine learning methods would be able to detect. These types of models are bolstered when exposed to more data and so are particularly suited to be used in environments such as digital banking where also the fraudsters are constantly evolving their methods.

Ensemble Methods

The "Ensemble methods" combines the predictions of multiple models to improve accuracy and robustness (Olowu *et al.,* 2024). The theory behind ensemble methods is that by ensembling many models that each have some strengths and weaknesses we can form a stronger, more accurate model. "Boosting", which focuses on those training instances that are harder to classify by changing their weights iteratively, is one of the most popular ensemble methods. "Gradient Boosting" and "XGBoost" are widely used boosting techniques which have proven effective when used for fraud detection tasks (Ganaie *et al.,* 2022; Khan *et al.,* 2023).

"Bagging" or Bootstrap Aggregating is another form of ensemble method as described by Hernandez t al., 2022; Vens, 2013. Bagging takes multiple models (usually decision trees) trained on multiples subsets of data and averages they predictions. It is also a mechanism to reduce variance and avoid overfitting, especially for decision trees. An example of bagging is the "Random Forest" algorithm, which aggregates many decision trees for better predictions. Detecting fraud using integrated systems based on NLP, anomaly detection, and supervised learning offers 15-25% higher detection levels than using any of the three types of models individually, as shown in a sample study of 25 large financial institutions (Olowu *et al.,* 2024).

Ensemble methods have special applicability for fraud detection, since the trade-off between false positives and false negatives in that context is very important.

Data Preprocessing

High quality data is a requisite condition for effective performance of machine learning models. The first and most important step when creating any fraud detection model, is data preprocessing; this step ensures that the data is cleaner and structured for ease of use.

Data cleaning typically deals with issues of missing, duplicate, or inconsistent data. Records may be incomplete for technological reasons, such as system errors, or human reasons, such as input error. Such gaps must be filled because they are sources of bias or inaccuracy in predictions. Common methods include imputation by filling values with mean, median, or mode, or excluding records with missing values (Alam *et al.,* 2023).

This is often called "feature extraction" the process of determining which variables (or features) found in the data are useful in order to improve the accuracy of the model. For instance, the features of interest in the case of fraud might be the transaction amount, time, location and number of transactions. Identifying these characteristics in the input data is useful to provide lower dimensionality to the dataset and to allow the model focus on the important variables to make the prediction (Cherif *et al.,* 2022; Islam *et al.,* 2025).

These are known as "feature transformation" techniques that can also be used to normalize or standardize the features so that all variables are treated equally in the model. For example, the learning from data which contains large numerical values might be biased if they are not normalized. Two common ways of transforming data are known as "z-score normalization" and "min-max scaling", which normalize the data to a common range or distribution (Bello *et al.,* 2024).

Effective preprocessing is important for the training of accurate fraud detection models. Every properly cleaned and well-engineered data can significantly improve the performance of machine learning algorithms, which can in turn lead to more reliable fraud detection.

Model Evaluation and Metrics

Model evaluation is a crucial step in fraud detection modelling to ascertain that the models used are performing effectively and can be relied on. Several performance metrics are analysed in order to assess the model's capability of being not only effective at detecting fraud, but also being able to minimize false positives, as well as minimizing frauds that are missed.

A common metric to apply is "accuracy", which may not be a sufficient measure in the case of fraud detection as there is an imbalanced class problem in which the fraudulent transactions are a very small count as compared to the legitimate ones (Tejesh *et al.,* 2025). Instead "precision" and "recall" are usually more useful. Precision is the percentage of actual positive cases of fraud that were predicted to be fraud out of all cases that were predicted as fraud, and recall means the percentage of actual positive cases of fraud that were correctly predicted by the model (Dangsawang & Nuchitprasitchai, 2024).

The "F1- score", being the harmonic mean of precision and recall provides a single measure that is used to balance both and is particularly useful in cases of class imbalance. Receiver Operating Characteristic - Area Under the Curve

(ROC-AUC) analysis is another commonly used metric, which examines the true-positive versus false-positive ratio across various thresholds (Trucco *et al.,* 2019).

These measures help account for the fact that there is a trade-off between detecting fraud and annoying a non-fraudulent customer. These metrics are hence optimized since, in order to provide useful and accurate outputs, AI-based fraud detection tools need to be able to detect fraud in real time, while not impinging unduly on legitimate users.

Applications of Ai-Driven Fraud Detection In Digital Banking

In the last few years, a number of banks and financial institutions have adopted AI- ML systems successfully into their fraud detection processes and have seen major benefits in their fight against fraud. This is especially clear in the case of "AI-based credit card fraud detection systems". For example, big banking companies like American Express and Citibank already implement real-time AI solutions that mine massive datasets of transactions by identifying patterns within this data (Mejia, 2019; Owen, 2021). The systems flag these unusual behaviours, such as when international transactions of high dollar amount suddenly increase or spending habits shift rapidly, as potentially fraudulent. These AI models keep learning from every new transaction they analyse, thus getting better over time in identifying new types of fraudulent schemes and minimizing false positives.

The other is "anti-money laundering (AML) systems", which also have been successful in deploying AI to detect fraud. These days, banks and financial institutions apply AI to detect suspicious transactions connected with money laundering processes (Oyedokun *et al.*, 2024). For instance, systems can identify transaction networks in patterns typical of money laundering, such as layering and integration stages. These examples capture the use of AI for the augmentation of fraud detection systems, demonstrating its capability as a solution to combat more complicated forms of financial crime that cannot be addressed through conventional methods.

AI-Powered Fraud Prevention Systems

AI-driven fraud prevention technology is now embedded in the core of banking technology infrastructure and offers automated, real-time fraud prevention solutions. Rather, banks want to deploy machine learning models for security by means of analyzing transactions on the fly. These can automatically identify cases where the behaviour of a specific user deviates from what is considered normal – for instance, either an unusual transaction or a connection from an unusual place – and notify the authorities to investigate.

Working in real time is one of the major benefits of AI for fraud prevention. While rule based systems are checked and worked on in batches or through review by a human, an AI system has the capacity of running continuously and being reactive in real-time to flags of suspicious behaviour. Should the AI then determine a transaction to be suspicious, it may automatically block it from going through or request additional verification from the customer, preventing possibilities for a fraudulent transaction, while still allowing for a frictionless experience for valid customers.

Plus, AI models are very effective in minimizing false positives, or transactions wrongly identified as fraudulent. The high number of false alerts in conventional fraud detection systems can inundate bank employees and result in customer dissatisfaction. On the contrary, machine learning algorithms can train based on historical data so to increase time by time their accuracy in classifying legitimate versus fraudulent transactions.

Also, AI fraud prevention systems are continuously updated to be ahead of new fraud strategies. They also improve detection as the fraudsters get better by adapting to new schemes, all without the need for humans to intervene.

Integration with Existing Systems

Another important move towards securing transactions is the deploying of AI fraud detection systems integrated with banks' current infrastructures. Most banks already have their established processes handled through legacy systems and any AI implementation needs to blend into existing systems without hindering active operations. Therefore, the secret to achieving and maintaining this integration is to use APIs (Application Programming Interfaces) and data pipelines between the old and the new technology (Adeleke *et al.*, 2024).

An example of this type of system are transaction monitoring systems, in which data from several banking services, like mobile banking, online payments, and ATMs, are collected in real time and introduced into machine learning models for fraud detection purposes. Banks are able to forward transactions data to AI, that in turn detects fraud patterns. It enables an easy flow of information between platforms so that suspicious activities can be acted upon right away.

Also, AI systems can more readily and easily be connected to cloud computing platforms that provide the processing power to leverage use scale data analyses. Cloud computing offers the possibility of storing big data sets and training and deploying machine learning models without the need for expensive local infrastructure. This is helpful for smaller financial institutions that may not have the means to develop and maintain such difficult fraud detection systems.

In addition, when AI is merged with other methods, it gives room for banks to enlarge their capabilities to prevent fraud. In line with digital banking, the number of transactions is increasing, and these transactions can all be handled in real time through AI systems that are capable of learning patterns of fraud as the volume of such data increases, thereby, providing a strong level of security as banks go digital.

Challenges and Limitations

Using AI for detecting fraud in the banking sector include

several benefits, although, it is not without challenges. Privacy is one, as AI often needs access to highly-sensitive data on customers in order to operate, increasing the chance of breaches. Likewise, the expensive financial cost of executing more complex AI innovation, like deep learning networks, may be an obstacle for some banks. Moreso, low prevalence of fraudulent transactions makes it difficult to obtain high-quality labelled data to train the models, resulting in imbalanced datasets. These challenges need to be overcome to use the potential of AI to help in fraud prevention.

Ethical and Regulatory Considerations

The employment of Artificial Intelligence and Machine Learning technologies specifically in fraud detection has brought about considerable ethical issues, specifically regarding "bias", "fairness", and "transparency" (Adhikari *et al.,* 2024). Among these is machine learning bias. These models are usually trained on past data that can include societal biases. If biases in the datasets used to train the AI models are not carefully filtered out, the AI systems can reproduce these biases with unsound and unmeritocratic results. An AI trained on biased historical data could, for example, identify some population group as more likely to commit fraud, despite being actually no more at risk than others.

AI fairness is yet another primary issue. Artificial Intelligence fraud detection must be fair in that there is no abusing of a human being; no one is discriminated against, all customers are treated equitably, regardless of race, gender, socio-economic status, etc. This is especially problematic within financial services, where discriminatory conduct can lead to financial harm, loss of banking access, or being wrongfully accused of fraud.

"Transparency" is also of great importance in the context of using AI for fraud detection. Banks should only use AI-based decision models that are transparent and the reasons for decisions can be explained. Particularly when the ramifications are significant, such as blocking a transaction or freezing an account, it is important for both customers and regulators to comprehend the reasoning behind the outcomes of AI models. The absence of transparency can promote "black boxes" in AI systems, raising issues of trust concerning fairness and accountability (Ismaeil, 2024).

Regulatory Compliance

AI technology fraud detection programs are covered by much of the same financial regulations, as any acceptable program must use in order to be legally practiced. This is particularly true for sectors that involve sensitive financial data like banking. Perhaps more importantly, the most pertinent of these frameworks is the "General Data Protection Regulation (GDPR)" which sets stringent protocols around personal data collection, processing, and storage (Adaji *et al.,* 2025). AI systems for fraud detection would also need to be regulated under GDPR to safeguard customer information, translating to anonymising data employed in training these AIs and customers would have to provide their consent.

Plus, independently of GDPR, "Payment Card Industry Data Security Standards (PCI-DSS)" is another relevant mandate that governs AI systems when payment data is involved. PCI-DSS mandates that all financial institutions and any third-party vendors engage in rigorous security practices to protect cardholder information. Specifically, regarding sensitive payment data, it is critical that AI systems designed to address fraudulent credit card transactions are constructed with a view not to violate these standards (Onyekwuluje *et al.*, 2025; Shaul & Ingram, 2007).

Also, "Anti-Money Laundering (AML)" laws also define the role of banks and financial institutions in detecting money laundering. It is, therefore, very important that banks adhere to regulations regarding money laundering and that AI systems are designed in such a way that they can effectively recognize patterns of money laundering in order to safeguard financial transactions and keep them secure and intact (Oztas *et al.,* 2024).

Data Privacy

Keeping user data private without compromising on effective fraud detection is among the biggest issues for AI systems in the digital bank arena. But, as financial institutions increasingly turn to AI models to sift through large pools of sensitive customer data to identify potential indicators of fraud, the response to this risk cannot compromise individuals' privacy to achieve security. Most machine learning and deep learning applications of AI must be fed large sets of data, often including past transactions, customer information, and even biometric data. These processes and storage also create privacy concerns about the data since if a breach occurred an individual's financial information could be made public.

To alleviate the aforementioned issues, banks should adopt international data protection measures. This includes practices like encrypting and anonymizing data, securely storing data to prevent unauthorized access, and other measures to avoid data leaks. Plus, also in line with data minimization principles, their collection and processing should not exceed what is necessary to detect fraud.

Also, AI systems should necessarily be developed in line with privacy laws like GDPR, which grants individuals access and control rights over their data, including the ability to consult, amend, or delete it. Financial institutions should also ensure explainability of the AI models that detect fraud so that customers are aware of and can question data-usage by AI systems that might negatively impact them. Finding the right equilibrium between effective fraud detection and data privacy requirements is crucial to ensure trust and legal compliance in the context of digital banking practices.

Future Directions And Innovations

Promising technologies such as federated learning, explainable AI (XAI) and quantum computing, are

poised to take the future of AI and ML in fraud detection to thrilling new levels (Odeyemi *et al.,* 2024). Because quantum computing can process large sets of data with far greater speeds than classical computers, this technology can revolutionize fraud detection. These systems could be orders of magnitude faster and efficient in the search for fraudulent patterns, patterns that could be analysed even in real time, patterns that previously could not be.

A rising second area of interest is Explainable Artificial Intelligence (XAI), which aims at increasing transparency and interpretability of AI models. Since AI is now moving into more critical domains such as fraud detection, we need to ensure that the decision-making process is interpretable to humans. Because XAI provides more transparency into how models come to conclusions, it can help foster trust amongst customers and regulators.

One new technique, called federated learning, is a new way of training machine learning models in which the modelling occurs on distributed devices or servers rather than a centralized server, helping financial institutions to cooperate in building a better fraud detection system without the need to share sensitive customer data. The benefits include improved privacy and security as well as, more effective training of models across institutions.

Collaboration and Cross-Industry Solutions

A rise in the complexity of fraud as well as reliance on digital banking explains the growing collaboration between industries to produce more efficient fraud detection systems. Collaborative effort between banks, tech companies and regulators is needed to combat the ongoing evolution of digital fraud. Partnerships between the banks and tech organizations could provide the opportunity to create the best and newest technologies based on current trends including artificial intelligence, machine learning and cyber security.

Regulators also have an important role in enforcing legal and ethical issues with regards to fraud detection through the use of AI. International cooperation is also necessary since fraudulent schemes are frequently international. Collaborating with foreign institutions can provide the ability to exchange information, deal with international fraud and consolidate financial security methods and protocols.

The Role of Blockchain

Another technology that could meaningfully complement AI- powered fraud detection is blockchain, which has been described as a way to increase transaction security and transparency. As a distributed and tamper-proof record of transactions, blockchain technology makes it possible for transactions to be public and permanent.

Concerning fraud detection, blockchain technology can minimize the ability to commit fraudulent transactions such as manipulating transaction information, stealing identities, and laundering money. One illustration of this is the transparency of blockchain where once a transaction is imprinted it cannot be changed creating a secure audit record. It becomes very difficult to alter transaction data or be fraudulent without detection.

In addition, AI systems for fraud detection can take advantage of the decentralized structure of blockchain to improve accuracy of fraud detection by comparing transaction data across different networks. AI and blockchain combined can contribute towards a more robust and trustworthy financial system.

CONCLUSION

This study looked at how Artificial Intelligence or, AI and Machine Learning or ML have transformed the detection and prevention of fraud in digital banking. Digital banking contributes to accessibility, efficiency, and financial inclusion. The downside to this is also a rise in more complex forms of fraud, requiring advanced technology to combat it . Existing traditional fraud detection practices which are mostly rule-based, can no longer meet the complexity and changing nature of the digital fraud. AI and ML provide a more flexible and anticipatory mode to the detection of fraud. These technologies are able to recognize intricate patterns as well as alerts to fraud instantaneously which hugely increase the capability of detecting fraud with minimal false positives. Several ML methods such as supervised learning, unsupervised learning, deep learning, and ensemble methods were reviewed and have each been successfully used to fight fraud. On top of that, AI systems make fraud prevention more efficient because they continuously learn and adapt as new threats arise. The ethics and regulation of deploying AI for fraud detection is extremely important, such as aspects of bias, transparency, and privacy of data. Financial institutions are obliged to abide by regulations like GDPR, PCI-DSS, and AML laws, while at the same time maintain effective fraud detection mechanisms and the need to protect customer data. As digital banking is new, so must the security mechanism. While the use of AI and ML in fraud detection is a game changer, the constant need for development and research is imperative to keep up with more complex and advanced forms of fraud. Only through the cooperation between banks, technology companies, and regulators can we come up with complete and effective fraud prevention solutions. In the future, AI, machine learning and blockchain technology integrated can have the potential to build a safe, secure, transparent and resilient digital banking environment that will build trust and protect customer assets in digital economy and digital banking.

REFERENCES

Abdelrhman, A. B. (2025). Popularity of mobile transaction services in the banking sector. *American Journal of Financial Technology and Innovation, 3*(1), 23–31. https://doi.org/10.54536/ajfti.v3i1.3807

Adaji, C. C., Bello, A. A., Ukatu, C. E., Okika, N., Agboola, O. K., & Amomo, C. G. (2025). AI-powered cybersecurity governance: The role of business analysts in ethical AI deployment. *International Journal of Innovative Science and Research Technology, 10*(3), 1384-

1396. https://doi.org/10.38124/ijisrt/25mar924

Adeleke, A. G., Sanyaolu, T. O., Efunniyi, C. P., Akwawa, L. A., & Azubuko, C. F. (2024). API integration in FinTech: Challenges and best practices. *Finance & Accounting Research Journal, 6*(8), 1531-1554. https://doi.org/10.51594/farj.v6i8.1506

Adeyeri, T. B. (2024). AI-based fraud detection in banking and financial services. *International Journal of Enhanced Research in Science, Technology & Engineering, 13*(7).

Adhikari, P., Hamal, P., & Baidoo, F. J. (2024). Artificial intelligence in fraud detection: Revolutionizing financial security. *International Journal of Science and Research Archive, 13*(01), 1457–1472. https://doi.org/10.30574/ijsra.2024.13.1.1860

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal, 6*, 100163. https://doi.org/10.1016/j.dajour.2023.100163

Alam, S., Ayub, M. S., Arora, S., & Khan, M. A. (2023). An investigation of the imputation techniques for missing values in ordinal data enhancing clustering and classification analysis validity. *Decision Analytics Journal, 9*, 100341. https://doi.org/10.1016/j.dajour.2023.100341

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2021). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences, 12*(19), 9637. https://doi.org/10.3390/app12199637

Aziz, L. A. R., & Andriansyah, Y. (2023). The role of artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics, 6*(1), 110-132.

Barroso, M., & Laborda, J. (2022). Digital transformation and the emergence of the Fintech sector: Systematic literature review. *Digital Business, 2*(2), 100028. https://doi.org/10.1016/j.digbus.2022.100028

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. https://doi.org/10.30574/wjaets.2024.12.2.0266

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications, challenges, and opportunities. *Computer Science & IT Research Journal, 5*(6), 1505–1520.

Bello, O. A., Folorunso, A., Ejiofor, O. E., Budale, F. Z., Adebayo, K., & Babatunde, O. A. (2023). Machine learning approaches for enhancing fraud prevention in financial transactions. *International Journal of Management Technology, 10*(1), 85-109.

Bello, O. A., Folorunso, A., Ogundipe, A., Ajani, O. K., Budale, F. Z., & Ejiofor, O. E. (2022). Enhancing cyber financial fraud detection using deep learning techniques: A study on neural networks and anomaly detection. *International Journal of Network and Communication Research, 7*(1), 90-113.

Bhuiyan, M. S. M., Rafi, M. A., Rodrigues, G. N., Mir, M. N. H., Ishraq, A., Mridha, M., & Shin, J. (2025). Deep learning for algorithmic trading: A systematic review of predictive models and optimization strategies. *Array, 100390*. https://doi.org/10.1016/j.array.2025.100390

Bueno, L. A., Sigahi, T. F., Rampasso, I. S., Filho, W. L., & Anholon, R. (2024). Impacts of digitization on operational efficiency in the banking sector: Thematic analysis and research agenda proposal. *International Journal of Information Management Data Insights, 4*(1), 100230. https://doi.org/10.1016/j.jjimei.2024.100230

Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2022). Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University - Computer and Information Sciences, 35*(1), 145-174. https://doi.org/10.1016/j.jksuci.2022.11.008

Chowdhury, R. H. (2024). Advancing fraud detection through deep learning: A comprehensive review. *World Journal of Advanced Engineering Technology and Sciences, 12*(02), 606–613. https://doi.org/10.30574/wjaets.2024.12.2.0332

Dangsawang, B., & Nuchitprasitchai, S. (2024). A machine learning approach for detecting customs fraud through unstructured data analysis in social media. Decision Analytics Journal, 10, 100408. https://doi.org/10.1016/j.dajour.2024.100408

Ezie, O., Oniore, J., & Ajaegbu, P. C. (2023). Financial technology and economic growth in Nigeria: 2012Q1-2022Q4. *American Journal of Financial Technology and Innovation, 1*(1), 35–45. https://doi.org/10.54536/ajfti.v1i1.2325

Ganaie, M., Hu, M., Malik, A., Tanveer, M., & Suganthan, P. (2022). Ensemble deep learning: A review. *Engineering Applications of Artificial Intelligence, 115*, 105151. https://doi.org/10.1016/j.engappai.2022.105151

Goyal, K., Garg, M., & Malik, S. (2025). Adoption of artificial intelligence-based credit risk assessment and fraud detection in banking services: A hybrid approach (SEM-ANN). *Future Business Journal, 11*(1). https://doi.org/10.1186/s43093-025-00464-3

Hernandez Aros, L., Bustamante Molano, L. X., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications, 11*(1), 1-22. https://doi.org/10.1057/s41599-024-03606-0

Hernandez, M., Epelde, G., Alberdi, A., Cilla, R., & Rankin, D. (2022). Synthetic data generation for tabular health records: A systematic review. *Neurocomputing, 493*, 28–45. https://doi.org/10.1016/j.neucom.2022.04.053

Hilal, W., Gadsden, S. A., & Yawney, J. (2021). Financial

fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications, 193*, 116429. https://doi.org/10.1016/j.eswa.2021.116429

Huang, Z., Zheng, H., Li, C., & Che, C. (2024). Application of machine learning-based K-means clustering for financial fraud detection. *Academic Journal of Science and Technology, 10*(1), 33-39. https://doi.org/10.54097/74414c90

Igah, R., & Luse, A. (2024). Unravelling Biased Blocking in The Adoption of Payattitude NFC Electronic Payment in Nigeria: An Exploratory Analysis. *MWAIS 2024 Proceedings. 7*. https://aisel.aisnet.org/mwais2024/7

Ikemefuna, C. D., Okusi, O., Iwuh, A. C., & Yusuf, S. (2024). Adaptive fraud detection systems: Using ML to identify and respond to evolving financial threats. *International Research Journal of Modernization in Engineering Technology and Science, 6*(9). https://doi.org/10.56726/IRJMETS61738

Islam, S., Gupta, G. R., Chakraborty, A., Singh, S., Soni, A., & Patle, C. (2025). Detecting fraudulent transactions for different patterns in financial networks using layer weighted GCN. *Human-Centric Intelligent Systems*. https://doi.org/10.1007/s44230-025-00097-3

Ismaeil, M. K. A. (2024). Harnessing AI for next-generation financial fraud detection: A data-driven revolution. *Journal of Ecohumanism, 3*(7), 811–821. https://doi.org/10.62754/joe.v3i7.4248

Iwedi, M. (2024). Digital finance infrastructure and growth of commercial banking firms in Nigeria. *Discover Analytics, 2*(1). https://doi.org/10.1007/s44257-024-00022-1

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of blockchain technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2*(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073

Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Mahmud, M. A. A. (2024). AI-powered fraud detection in banking: Safeguarding financial transactions. *The American Journal of Management and Economics Innovations, 6*(06), 8-22.

Khan, A. A., Chaudhari, O., & Chandra, R. (2023). A review of ensemble learning and data augmentation models for class imbalanced problems: Combination, implementation and evaluation. *Expert Systems with Applications, 244*, 122778. https://doi.org/10.1016/j.eswa.2023.122778

Khando, K., Islam, M. S., & Gao, S. (2022). The emerging technologies of digital payments and associated challenges: A systematic literature review. *Future Internet, 15*(1), 21. https://doi.org/10.3390/fi15010021

Khodabandehlou, S., Golpayegani, A. H., & FiFrau, D. (2024). Unsupervised financial fraud detection in dynamic graph streams. *ACM Transactions on Knowledge Discovery from Data, 27*(5), 1-29.

Kipngetich, A. (2025). A review of online scams and financial frauds in the digital age. *GSC Advanced Research and Reviews, 22*(01), 302-329.

Li, X., Huang, J., Chen, C., & Zhang, Y. (2020). Credit card fraud detection using machine learning: A systematic literature review. *Expert Systems with Applications, 164*, 113909.

Mallesha, C., & Hymavathi, M. (2024). A review on AI and fraud detection in accounting: Reducing risks and enhancing financial security. *Academy of Accounting and Financial Studies Journal, 28*(2), 1-18.

Mejia, N. (2019). Artificial intelligence at Citibank - Current initiatives. *EmerJ Artificial Intelligence Research*. https://emerj.com/ai-at-citi/

Metha, S. (2025). AI-driven fraud detection: A risk scoring model for enhanced security in banking. *Journal of Engineering Research and Reports, 27*(3), 23–34. https://doi.org/10.9734/jerr/2025/v27i31415

Mienye, I. D., Swart, T. G., & Obaido, G. (2024). Recurrent neural networks: A comprehensive review of architectures, variants, and applications. *Information, 15*(9), 517. https://doi.org/10.3390/info15090517

Mohmmed, A. A., Rahma, A. M. S., & AbdulWahab, H. B. (2024). Digital wallets evolution: Navigating challenges, innovation and the future landscape. *Al-Qadisiyah Journal of Pure Science, 29*(1), Article 4. https://doi.org/10.29350/2411-3514.1248

Muthunambu, N. K., Prabakaran, S., Kavin, B. P., Siruvangur, K. S., Chinnadurai, K., & Ali, J. (2024). A novel eccentric intrusion detection model based on recurrent neural networks with leveraging LSTM. Computers, Materials & Continua/Computers, Materials & Continua (Print), 78(3), 3089–3127. https://doi.org/10.32604/cmc.2023.043172

Odeyemi, O., Mhlongo, N. Z. M., Nwankwo, E. E., & Soyombo, O. T. (2024). Reviewing the role of AI in fraud detection and prevention in financial services. *International Journal of Science and Research Archive, 11*(01), 2101–2110. https://doi.org/10.30574/ijsra.2024.11.1.0279

Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. O. (2025). Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria. *Journal of Economic Criminology, 100127*. https://doi.org/10.1016/j.jeconc.2025.100127

Oduro, N. D. A., Okolo, N. J. N., Bello, N. A. D., Ajibade, N. A. T., Fatomi, N. A. M., Oyekola, N. T. S., & Owoo-Adebayo, N. S. F. (2025). AI-powered fraud detection in digital banking: Enhancing security through machine learning. *International Journal of Science and Research Archive, 14*(3), 1412–1420. https://doi.org/10.30574/ijsra.2025.14.3.0854

Olowu, N. O., Adeleye, N. A. O., Omokanye, N. A. O., Ajayi, N. A. M., Adepoju, N. A. O., Omole, N. O. M., & Chianumba, N. E. C. (2024). AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. *GSC Advanced Research and Reviews, 21*(2), 227–237. https://doi.org/10.30574/gscarr.2024.21.2.0418

Onyekwuluje, T. P., Kpakpa, C. T., Panful, B., Apaflo, B. N., & Donkor, A. A. (2025). The role of IT compliance in enhancing cybersecurity measures for U.S. financial institutions. *International Journal of Research Publication and Reviews, 6*(1), 2600-2606.

Owen, R. (2021). Artificial intelligence at American Express - Two current use cases. *EmerJ Artificial Intelligence Research*. https://emerj.com/artificial-intelligence-at-american-express/

Oyedokun, O., Ewim, S. E., & Oyeyemi, O. P. (2024). A comprehensive review of machine learning applications in AML transaction monitoring. *International Journal of Engineering Research and Development, 20*(11), 730-743. https://www.ijerd.com

Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G., & Dogan, H. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. *Future Generation Computer Systems, 159*, 161–171. https://doi.org/10.1016/j.future.2024.05.027

Rahman, M., Yee, H. P., Masud, M. A. K., & Uzir, M. U. H. (2024). Examining the dynamics of mobile banking app adoption during the COVID-19 pandemic: A digital shift in the crisis. *Digital Business, 4*(2), 100088. https://doi.org/10.1016/j.digbus.2024.100088

Rojan, Z. (2024). Financial fraud detection based on machine and deep learning: A review. The Indonesian *Journal of Computer Science, 13*(3).

Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change, 17*(2), 164-196.

Salunke, Y., Phalke, S., Madavi, M., Kumre, P., Bobhate, G. (2025). Fraud detection: A hybrid approach with logistic regression, decision tree, and random forest. *Cureus Journal of Computational Science, 2*, es44389-024-02350-5. https://doi.org/10.7759/s44389-024-02350-5

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science, 2*(3). https://doi.org/10.1007/s42979-021-00592-x

Sharma, P. (2024). How reinforcement learning keeps fraud detection smart and quick: Adapting to new fraud tricks. *International Journal for Multidisciplinary Research (IJFMR), 6*(2). https://www.ijfmr.com

Shaul, J., & Ingram, A. (2007). Database activity monitoring. In *Elsevier eBooks* (pp. 201–224). https://doi.org/10.1016/b978-159749198-3.50010-x

Tejesh, P., Sai, G. P., Naveen, D., Khaleel, V. S., & Rao, V. H. (2025). Detection of fraud in banking transactions by machine learning algorithm. *International Journal of Research Publication and Reviews, 6*(4), 1775–1778.

Trucco, E., McNeil, A., McGrory, S., Ballerini, L., Mookiah, M. R. K., Hogg, S., Doney, A., & MacGillivray, T. (2019). Validation. In *Elsevier eBooks* (pp. 157–170). https://doi.org/10.1016/b978-0-08-102816-2.00009-5

Venigandla, K., & Vemuri, N. (2022). RPA and AI-driven predictive analytics in banking for fraud detection. *Tuijin Jishu/Journal of Propulsion Technology, 43*(4).

Vens, C. (2013). Bagging. In *Springer eBooks* (pp. 68–69). https://doi.org/10.1007/978-1-4419-9863-7_602

Wang, X., Liu, H., & Yu, Z. (2019). A hybrid approach for fraud detection in online banking transactions. *IEEE Access, 7*, 64101-64113.

Wei, C., Xie, G., & Diao, Z. (2023). A lightweight deep learning framework for botnet detecting at the IoT edge. *Computers & Security, 129*, 103195. https://doi.org/10.1016/j.cose.2023.103195

Windasari, N. A., Kusumawati, N., Larasati, N., & Amelia, R. P. (2022). Digital-only banking experience: Insights from Gen Y and Gen Z. *Journal of Innovation & Knowledge, 7*(2), 100170. https://doi.org/10.1016/j.jik.2022.100170

Xuan, C. D., Duong, D., & Dau, H. X. (2021). A multi-layer approach for advanced persistent threat detection using machine learning based on network traffic. *Journal of Intelligent & Fuzzy Systems, 40*(6), 11311-11329.