Magna Scientia Advanced Research and Reviews
eISSN: 2582-9394
Cross Ref DOI: 10.30574/msarr
Journal homepage: https://magnascientiapub.com/journals/msarr/

(Research Article)

AI-driven fraud detection systems: A comprehensive review of emerging techniques in U.S. financial crime prevention

Sophia Aryeetey [1,*] and Mary Magdalene Yeboah [2]

[1] *New Jersey, USA.*
[2] *Texas, USA.*

Magna Scientia Advanced Research and Reviews, 2026, 17(01), 368-380

Publication history: Received on 15 May 2026; revised on 25 June 2026; accepted on 27 June 2026

Article DOI: https://doi.org/10.30574/msarr.2026.17.1.0111

Abstract

Financial fraud remains an enormous threat to the health of the contemporary financial system, especially with the fast growth of digital banking, internet-based payment systems, and fintech applications. The existing rule-based and statistical-based fraud detection systems have not been efficient in detecting sophisticated and dynamic fraud schemes in extremely interconnected financial ecosystems. In response, artificial intelligence (AI) has become a strong technology that can enhance the ability to detect fraud cases in financial intermediaries. This study gives a critical overview of the new AI-based methods in detecting financial fraud and their application in preventing financial crimes in the U.S. The study synthesizes current applications of AI across banking operations, anti-money laundering (AML) frameworks, and fintech payment ecosystems while evaluating commonly used datasets and performance metrics for fraud detection research. The analysis further reveals the main issues that can impact AI-based systems of detecting fraud, such as an imbalance between classes in the fraud data, attacker (or adversarial) attacks, insufficient data, interpretability of models, and privacy concerns. In addition, the latest research topics like explainable artificial intelligence, graph neural networks, federated learning, and real-time fraud detection systems are reported as potential ways to enhance the effectiveness of fraud detection. As a review of recent findings in AI-based fraud detection studies, this article offers important information to researchers, financial institutions, and policymakers in the field by ensuring the enhancement of financial crime prevention strategies and the resilience of digital financial systems.

Keywords: Artificial Intelligence; Financial Fraud Detection; Machine Learning; Financial Crime Prevention; Digital Banking Security

1. Introduction

Financial fraud is a long-standing and sustained risk to the financial systems of the world in a digitized financial space, cutting across institutions, businesses, and customers. Payment fraud, identity theft, and financial manipulation are a few examples of fraudulent practices that damage the stability of the banking system, decrease consumer confidence, and cause significant economic losses to financial institutions and national economies (Afjal et al., 2023; Karpoff, 2021). Based on global assessments, fraud has moved into cyberspace as a result of the growing amount and complexity of fraud related to various financial transactions, creating the need for stronger protection from technological threats (Chukwu 2024). The growing sophistication of financial ecosystems brought about by online banking, mobile payments, and digital financial services has considerably increased the prospect of cyber-enabled financial crime (Chukwu, 2024; Sarna et al., 2025).

The United States has been especially salient in the growth of financial crime, which has been especially heightened with the proliferation of electronic transaction systems and digital financial services. According to reports on occupational

* Corresponding author: Sophia Aryeetey.

and financial fraud, billions of dollars are wasted due to fraudulent schemes every year, making it essential to implement measures to monitor and detect fraudulent activities in financial institutions (Afjal et al., 2023). With the increased automated and networked nature of financial transactions, fraudsters have developed more advanced methods that take advantage of vulnerabilities in digital payment systems and regulations (Karpoff, 2021; Chukwu, 2024). In contrast to falling victim to the usual types of fraud, financial institutions should implement specific policies to protect themselves from unidentified types of fraud. Fraud investigation systems that use rules and manual investigations cannot differentiate between complex and new types of fraud, resulting in a higher number of cases where fraud detection has been delayed by falsely identified cases of fraud, and also in less time spent investigating cases of fraud. Thus, using machine learning algorithms provides financial institutions with a more adaptable method to detect anomalies in order to strengthen their risk management practices (Sarna et al 2025; Amoako et al 2025).

Artificial intelligence (AI) and machine learning technologies have arisen to overcome these shortcomings to become potent tools in the detection and prevention of financial fraud in contemporary financial systems. The AI-based fraud detection systems draw on big sets of transaction data, behavioral analytics, and improved predictive algorithms to detect suspicious financial transactions in situ (Sarna et al., 2025; Chukwu, 2024).

When comparing technologies to traditional systems, financial institutions can utilize the technology to identify hidden transaction patterns; identify fraudulent entities that coordinate fraud across an entire company; and respond quickly to new emerging threats in the financial system (Afjal et al.,2023; Sarna et al.,2025). The current study describes what the newly created types of AI fraud detection techniques have done to assist in the fight against financial crime in the United States and discusses the current challenges, advancements in technology, and future directions of research in this area (Karpoff, 2021; Chukwu, 2024).

2. Comprehensive Review Methodology

In conducting this study, a comprehensive review methodology will be utilized to analyze and evaluate new artificial intelligence (AI) methods employed for detecting and preventing financial fraud in the United States. The review aims to provide an overview of contemporary literature across different disciplines, such as fintech, cybersecurity, machine learning, banking systems, and financial fraud prevention, to provide a broad understanding of current developments, implementation strategies, challenges, and future research directions.

A range of articles published in peer-reviewed journals, conference proceedings, industry reports, and regulatory publications, dated from 2020 to 2026, were used for analyzing relevant sources. The databases include Scopus, Google Scholar, IEEE Xplore, ScienceDirect, and SpringerLink. Search terms included “AI fraud detection,” “financial crime prevention,” “machine learning fraud detection,” “deep learning in banking security,” “graph neural networks fraud detection,” “anti-money laundering AI,” and “fintech fraud analytics.”

This review emphasized works that concentrate on AI-based fraud detection models, anomaly detection approaches, graph learning, explainable AI, federated learning, and real-time fraud monitoring. Selected studies were subjected to critical analysis and then classified based on thematic clusters such as evolution of fraud detection systems, methods of AI applications, data sets, measures, implementations, technologies, and challenges.

Such an extensive methodology allows the incorporation of multiple scholarly points of view along with new technological advancements, as well as the identification of existing gaps, methodological limitations, and future opportunities for improving AI-enabled financial crime prevention systems in the field.

3. Financial Fraud in the U.S. Financial Ecosystem

Financial fraud is an act of misrepresentation or manipulation used to gain financial benefit by using financial resources in financial systems without legal authority and/or misrepresentation. Financial fraud in the United States has been getting more complicated with the booming growth of digital banking and electronic payment systems, as well as interconnected financial systems that provide new possibilities to be exploited by cybercriminals (Nwinyi & Oman-Amoako, 2026; Akartuna et al., 2024). The widespread use of online financial services has increased the range of attacks due to fraud schemes, allowing criminals to use online payment systems, financial databases, and identity checks to commit unauthorized financial transactions (Roseline et al., 2022; Akartuna et al., 2024). Financial fraud poses an important issue to regulators and financial institutions because such fraudulent activities can damage the stability of the financial system, deter consumer trust, and cause individual and institutional losses to the tune of many financial resources (Sathya & Balakumar, 2022; Gaviyau & Sibindi, 2023).

With the ongoing evolution of financial systems to digital and network-based infrastructure, more sophisticated monitoring mechanisms and stringent regulatory frameworks are needed to reduce financial crime, as several key types of financial frauds are ongoing within the financial sectors of the U.S. financial ecosystem (Irvin-Erickson, 2024; Nazzari & Reuter, 2025). It is common to see credit card fraud take place when people use stolen credit card information for transactions during online shopping (for example, using your credit card at a store without physically having it in your possession). Identity theft is an example of another type of fraud where fraudsters use stolen personal information to access a person's financial accounts, conduct unauthorized transactions, and establish synthetic identities that can be manipulated to commit fraud (Irvin-Erickson, 2024; Ahmed, 2018).

According to Akartuna et al. (2024) and Nazzari & Reuter (2025), money laundering refers to a type of monetary crime in which illegal funds are hidden from view by means of complex transaction structures that have been creatively designed to hide where illegal money came from so that this illegal money can ultimately be put back into the economy. The examples of types of fraud that can be committed include, loan fraud (when someone falsifies their financial records to get a loan), and insurance or healthcare fraud (when people file false insurance claims or inflate the cost of their medical bills or create a way to get reimbursed for fraudulent actions) as described by Sathya & Balakumar (2022) and Gaviyau & Sibindi (2023). Another feature of modern financial fraud is adaptive fraud schemes that keep being developed to avoid detection system, cross-border cybercrime networks that leverage international financial systems, data-driven cybercrime schemes based on stolen financial and personal information, and well-organized cybercrime networks which coordinate multijurisdictional and multi-platform fraudulent schemes (Gaviyau & Sibindi, 2023; Nazzari & Reuter, 2025).

Table 1 Major Types of Financial Fraud

Fraud Type	Description	Key Characteristics	Key Studies
Credit card fraud	Unauthorized card transactions	Card-not-present fraud, phishing attacks	Roseline et al. (2022)
Identity theft	Misuse of personal identity data	Synthetic identities, account takeover	Irvin-Erickson (2024)
Money laundering	Concealing illicit financial proceeds	Placement–layering–integration stages	Akartuna et al. (2024)
Loan fraud	Manipulated loan applications	Income misrepresentation, falsified records	Xiong et al. (2022)
Insurance fraud	False or exaggerated claims	Medical billing manipulation	Sathya & Balakumar (2022)

4. Evolution of Fraud Detection Systems

The development of fraud detection systems has been on an upward trend because of the increased digitization and network of financial transactions in contemporary financial systems. Rule-based mechanisms of early fraud detection were mostly based on pre-defined rules and transaction limits and attempted to provide warning signs of suspicious behaviour like abnormally large withdrawals or unusual transaction patterns (Sarker et al., 2020). These systems were quite easy to install, and they acted as the first line of defence in the financial institutions against fraudulence transactions. Yet, the methods of detection, which relied on rules, were very reliant on delivered and structured rules and knowledge on fraud, a factor that curtailed flexibility to a changing fraud strategy and intricate financial transaction scheme (Chowdhury, 2024). With the growth of financial systems provided by online payment systems and digital banking platforms, criminals started to find more ways to compromise the limitations of the existing frameworks of rules-based fraud detection, which led to the necessity to develop more adaptive means of analysis (Sarker et al., 2020; Chowdhury, 2024).

To overcome these shortcomings, financial institutions started to apply statistical and data-driven model of fraud detection that could be able to analyse financial transactions data systematically. The logistic regression and the probabilistic analysis were among the statistical methods that allowed the analyst to detect any kind of abnormal financial behaviour and any outliers in the transaction data. In spite of the fact that these models were able to improve the analytical capacity of rule-based systems, they nevertheless were not able to identify complex and nonlinear patterns of fraud that are inherent in the contemporary financial landscape (Sarker et al., 2020; Chowdhury, 2024). The subsequent growth of the digital financial services further fueled the move toward the machine learning and artificial intelligence-based fraud detectors, which can better process mass data that includes transactions and detect fraud patterns (Yeboah et al., 2026). The predictive accuracy of machine learning algorithms, like the Random Forest and Support Vector Machines, is more accurate in predicting fraudulent behavior, whereas deep learning models, like the convolutional neural network and recurrent neural network, can identify more sophisticated behavioral patterns and organized fraud within financial networks (Sarker et al., 2020; Chowdhury, 2024).

Table 2 Evolution of Fraud Detection Approaches

Approach	Key Techniques	Advantages	Drawbacks
Rule-based systems	predetermined thresholds	Simple implementation	unable to identify novel fraud trends
Models of statistics	Logistic regression	Interpretable models	Limited complexity handling (Sarker et al., 2020)
Machine learning	Random Forest, SVM	High accuracy of prediction	Large datasets are necessary (Chowdhury, 2024)
Deep learning	CNN, RNN	Identify intricate fraud trends	Black-box interpretability problem (Chowdhury, 2024)

5. AI Techniques for Financial Fraud Detection

Artificial intelligence has become one of the most important components of the modern fraud detection systems as it has allowed maintaining the record of a prospective fraudulent act and finding the trends within the large amounts of financial transactions data. In comparison to the traditional methods which rely on rules, AI methods can be trained on the past financial data and be continuously more accurate at detection as the new patterns of transactions occur (Chowdhury, 2024; Uddin, 2025). Machine learning and deep learning algorithms have been actively utilized in financial systems to find unfavorable transactions, detect abnormal behavior of transactions and find organized networks of potential fraud operating through more than a single account or a number of institutions (Emmanuel, 2025). These artificial intelligence applications enable financial institutions to make sure that financial operations are made in real-time, identify the trends of suspicious activities, and reduce financial losses that might take place as a result of the fraud scheme.

5.1. Machine Learning Approaches

One of the most prevalent methods of identifying financial frauds are machine learning methods since they can learn more advanced effects based on the past transaction logistics. Random Forest, Support Vector Machines, and ensemble machine learning algorithms have been used to show a high predictive capacity to detect and report fraud in a financial transaction as well as improve the risk management process in a financial institution (Amoako et al., 2025). The machine learning algorithms, such as Random Forest, Logistic Regression, Support Vector Machines, Decision Trees and Naive Bayes, have been effectively deployed in the fraud classification domain, wherein they classify genuine and fraudulent payments based on the learnt features (Trivedi et al., 2020; Itoo et al., 2021). Such algorithms study the features of transactions such as size of transaction, location of transactions, time as well as behaviour of the transacting individual to identify abnormal behaviour which is linked to fraud. In fact, a Support Vector Machines, like the Random Forest models, can be trained to classify data as a fraud or legitimate transaction with the help of a large number of decision trees to attain high accuracy, whereas Support Vector machines could be trained to apply the optimal decision boundaries to classify fraudulent and legitimate transactions (Trivedi et al., 2020). When logistic regression model is used, it is considered a standard practice because it is not only simple to interpret but also to determine the probability of a transaction being fraudulent (Itoo et al., 2021).

5.2. Deep Learning Techniques

Deep learning methods are extensions of the principles of conventional machine learning methods and enable models to automatically acquire intricate features on the basis of high-sized information sets. The fraud detection system uses neural networks because they can maintain nonlinear relationships between variables of transaction and identify subtle behavior patterns that are related to fraud (Chowdhury, 2024; Uddin, 2025). CNNs can also be convenient in terms of detecting patterns that can be organized in the transaction data, and Recurrent Neural Networks (RNNs) and Long Short-term memory (LSTM) networks can be useful when it comes to analyzing sequential transactions of financial models over time (Uddin, 2025; Emmanuel, 2025). These deep learning models allow the fraud detection models to examine the behaviour of users with a series of transactions and identify the suspicious series of transactions that may be an indicator of a fraudulent behaviour.

In anomaly detection applications, autoencoders are also used in fraud detection systems. These deep learning models have been developed to mimic typical transaction patterns, while being also able to flag anomalies when the reconstruction error rates of the transaction patterns are very high (Emmanuel, 2025; Chowdhury, 2024). Because fraudulent transactions do not necessarily follow the pattern of normal transactions, autoencoders do not require the huge volumes of labelled fraud data to identify suspicious transactions. With the continued growth of the volume of financial transactions, deep learning algorithms have re-emerged as a valuable resource in managing large amounts of data and identifying complex fraudulent patterns in the digital financial system (Uddin, 2025; Emmanuel, 2025).

5.3. Graph-Based Fraud Detection

The use of graph-based fraud detection techniques has acquired considerable interest in the recent past due to the fact that most schemes in financial frauds are based on networks of related accounts and concurring transactions. Graph neural networks (GNNs) are financial networks, in which accounts are represented as nodes, and transactions are represented as a network between nodes (Cheng et al., 2025; Li et al., 2025). Through this representation, the fraud detection systems are able to examine the relationships between entities as well as detecting suspicious clusters of accounts that could be engaged in forming organized fraud. Graph-based techniques are especially useful in the detection of fraud rings, networks of money laundering, as well as collusive patterns of transactions that cannot be easily detected with the help of traditional transaction-level analysis (Rasul et al., 2024; Cheng et al., 2025).

Graph-based fraud detection systems often have links analysis techniques and network analysis, in order to recognize unusual associations involving accounts and detect the suspicious transactions of financial networks. Graph based model is able to discover unknown connections between the fraudsters as well as identify organized groups of fraudsters who span across the accounts or institutions with the help of a network structure and accountability of the financial transactions (Li et al., 2025; Rasul et al., 2024). As the interdependence between the financial systems is increasing, it is probable that graph-based learning algorithms will become significant in order to identify the structure of current-day complex fraud and improve financial crime detecting capacity.

5.4. Anomaly Detection Methods

Anomaly detection techniques are based on detecting transactions that are outlier in financial conduct. The methods work especially well in fraud detection since fraudulent transactions are typically occasional occurrences in large financial data (Maddila et al., 2020; Chowdhury, 2024). Clustering methods are used to group up the similar transactions by their attributes and mark the ones that do not fall within any cluster as possible anomalies. Some of the algorithms, including DBSCAN (Density-Based Spatial Clustering of Applications with Noise), are commonly employed to detect unusual transaction patterns in clusters of dense financial data (Ahmad et al., 2023). The use of Isolation Forest models is also very extensive since there they isolate anomalies by subdividing data points that do not resemble typical transaction patterns (Sarna et al., 2025).

5.5. Hybrid and Ensemble Fraud Detection Models

Ensemble and hybrid model of fraud detection involves the integration of more than one machine learning method in order to enhance the accuracy and strength of detection. The ensemble approaches combine the predictions of multiple algorithms to create more credible classification outputs; they usually perform better than single-model predictors in fraud detection tasks (Kumar et al., 2022; Bakhtiari et al., 2023; Baisholan et al., 2025). These models can also be supervised learning algorithms with unsupervised anomaly detectors to identify the familiar and unfamiliar fraud patterns (Chowdhury, 2024; Hafez et al., 2025; Soyombo, 2024). The hybrid frameworks combine data provided by more than one source, such as transaction, behavioral data, and network relationship to offer a more in-depth perspective of a fraudulent activity (Rasul et al., 2024; Uddin, 2025; Xiong et al., 2022).

Table 3 AI Techniques Used in Fraud Detection

Technique	Algorithms	Application
Supervised learning	Random Forest (RF), Support Vector Machines (SVM), Logistic Regression (LR)	Credit card fraud detection
Unsupervised learning	K-means, DBSCAN	Anomaly detection in transaction data
Deep learning	CNN, RNN	Behavioral fraud detection
Graph learning	Graph Neural Networks (GNN)	Detection of fraud networks
Hybrid models	Ensemble machine learning models	Multi-source fraud detection

6. Datasets and Evaluation Metrics in Fraud Detection Research

Research on fraud detection often uses historical transaction data to train predictive models, although real financial data is not readily available since it is regulated and private (Amoako et al., 2025). The success of artificial intelligence models in the context of fraud detection is directly related to the quality of data provided, as well as reasonable performance measurement parameters. Deep learning algorithms, as well as machine learning, need vast amounts of financial transaction data to acquire an idea of legitimate and fraudulent transactions (Compagnino et al., 2025; Sarna et al., 2025). Nonetheless, obtaining actual financial data is usually a constrained experience because of privacy and confidentiality laws, as well as regulatory compliance requests of the financial institution (Btoush et al., 2023; Baisholan et al., 2025; Soyombo, 2024). Therefore, most of the research utilizes publicly accessible or simulated data to enable researcher to train and test fraud detectors without revealing confidential financial data (Bakhtiari et al., 2023). The datasets are also helpful in assessing the fraud detection models and comparing the results of various artificial intelligence methods applied to financial crime detection (Baisholan et al., 2025; Btoush et al., 2023; Hafez et al., 2025).

6.1. Fraud Detection Datasets

Investigation into fraud detection often uses publicly accessible transaction data collections which model actual financial systems whilst maintaining the privacy of sensitive customer data (Btoush et al., 2023; Baisholan et al., 2025). The European Credit Card Fraud dataset is one of the most popular datasets and it has over 280,000 financial transactions, of which a small percentage are identified as fraudulent, which is representative of the imbalance in legitimate and fraudulent operations in the real world (Baisholan et al., 2025; Hafez et al., 2025). The other popular one is the IEEE-CIS Fraud Detection dataset that contains high volumes of e-commerce transactions and identity characteristics that would be used to develop the fraud detection models (Bakhtiari et al., 2023). Moreover, there are simulated datasets like PaySim, BankSim, and Sparkov, which are also using controlled experimental environments to test the algorithms of fraud detection. These datasets simulate the real-life behaviors of transactions and enable researchers to test the model of fraud detectors in various financial settings, such as in mobile payments, online transactions, and banking systems (Btoush et al., 2023; Baisholan et al., 2025; Bakhtiari et al., 2023).

6.2. Data Challenges in Fraud Detection

Regardless of the presence of a number of public datasets, the study of fraud detection is impacted by a series of data-related challenges that interfere with the performance and reliability of machine learning models (Baisholan et al., 2025; Hafez et al., 2025). Class imbalance is one of the greatest problems where fraudulent transactions usually constitute a very small fraction of the overall transaction data (Baisholan et al., 2025; Hafez et al., 2025). Such an imbalance renders machine learning models to learn meaningful fraud patterns as the models might turn biased towards prediction of legitimate transactions (Isangediok & Gajamannage, 2022). The second problem is that few fraud data are labelled because a significant number of frauds are not detected or reported in actual financial systems (Btoush et al., 2023). Moreover, real-world financial transaction data is often inaccessible due to privacy laws and stringent data protection policies, so much of the research has to do with using anonymized or synthetic data that might not fully represent the complexity of the fraud behavior in the real world (Baisholan et al., 2025; Btoush et al., 2023; Soyombo, 2024).

6.3. Evaluation Metrics for Fraud Detection Models

Performance metrics used to evaluate fraud detection models are specific since financial fraud data sets are extremely unbalanced (Emmanuel, 2025). The conventional accuracy scores used alone cannot be considered adequate to measure fraud detection systems since a model can be highly accurate by just relying on the principle of classifying most transactions as legitimate (Btoush et al., 2023; Hafez et al., 2025). Consequently, it is generally agreed by researchers that metrics like precision, recall, F1-score and Area Under the Receiver Operating Characteristic Curve (ROC-AUC) are used to evaluate the performance of a model (Emmanuel, 2025). Precision is used to measure the percentage of the falsely predicted fraudulent transactions that are falsely predicted, and recall is used to assess the capacity of the model to detect the falsely predicted cases of fraud correctly (Baisholan et al., 2025; Isangediok & Gajamannage, 2022). Particularly when imbalanced datasets are involved, the F1-score aids in preserving the accuracy and recall of the performance in a more efficient manner while identifying fraud. These metrics of evaluation will play a vital role in evaluating the effectiveness of machine learning models and making sure that the fraud detection systems can make correct identifications in suspicious transactions and reduce the instances of false alarms (Btoush et al., 2023; Baisholan et al., 2025).

7. Implementation of AI Fraud Detection in U.S. Financial Institutions

As online platforms in the provision of financial services grow, artificial intelligence has emerged as a critical technology in identifying and deterring financial fraud in the U.S. financial institutions. Electronic banking, mobile payment, and electronic commerce have been instrumental in raising the volume and sophistication of financial transactions that are carried out by the financial institution on a daily basis. This is why banks and other financial service providers depend more on AI-based fraud detection tools that can process large amounts of transaction data and detect suspicious financial behavior related to frauds and enhance money laundering monitoring in real time (Alex-Omiogbemi et al., 2024; Sarna et al., 2025; Boateng et al., 2025). Fraudulent transactions or unauthorised user activity can be detected by examining prior patterns of identical transaction types, how frequently they've occurred, their overall volume, and whether there are patterns that suggest unusual behaviour (Soyombo, 2024; Sarna et al., 2025). Smart systems using historical transactional data will identify ways to adapt to new patterns of fraud and enhance the ability of financial institutions to detect and respond to fraudulent activity in real-time, thereby reducing the risks of financial losses arising from cyber-enabled financial crime (Chukwu, 2024; Alex-Omiogbemi et al., 2024).

The operation of AI-based fraud detection systems in the United States is also well coordinated with the regulatory frameworks that are aimed at fighting financial crime and guaranteeing adherence to the financial sector. The financial institutions must have monitoring mechanisms that can detect suspicious financial transactions and report any possible fraud or illegal transactions (Gaviyau & Sibindi, 2023). The AI-based monitoring tools can assist these regulatory requirements by processing large volumes of financial data and automatically detecting any suspicious trends that could be indicative of a fraudulent organization or money laundering operations (Sarna et al., 2025; Soyombo, 2024). Enabled by these sophisticated machine learning models, we can analyse the complex relationship of transactions, while developing an understanding of unknown connections between accounts that may indicate a series of financial crimes (Kumar et al., 2022; Sarna et al., 2025). Automation of the transaction monitoring/risk assessment processes by Artificial Intelligence (AI) technologies will support regulatory compliance and create greater productivity in the detection of financial crime by financial institutions (Soyombo, 2024; Chukwu, 2024).

Along with regulations, AI technologies have been widely implemented for banking activities (i.e., fraud prevention), anti-money laundering, as well as in fintech payment platforms to help develop new methods of preventing fraudulent activity. Machine learning algorithms are used in banking systems to analyse the behaviour of customers in terms of transactions and account activities to detect anomalies that could indicate fraudulent transactions or misuse of identity (Alex-Omiogbemi et al., 2024; Soyombo, 2024). AI-based systems are used in anti-money laundering activities to analyze compound network structures of financial transactions to identify abnormal financial flows and retrieve patterns related to money laundering schemes or organized fraud networks (Nartey et al., 2026; Kumar et al., 2022). Fintech payment systems are also among the most common applications of AI technologies, where predictive models evaluate the risk of fraud in real time and prevent suspicious transactions before they can be processed (Ravi et al., 2025; Sarna et al., 2025). In the context of such applications, AI-based fraud detection systems essentially increase the capacity of financial institutions to protect the financial transactions, minimize the risk of frauds, and sustain the stability of the financial ecosystem in the United States (Chukwu, 2024; Soyombo, 2024).

Table 4 Applications of Artificial Intelligence in Financial Services

Use case	AI Techniques	Functions	Benefits	References
Fraud Detection through Banking	Anomaly detection, machine learning	Monitoring transactions and assessing fraud risk	Detect fraud in real time with greater accuracy	Alex-Omiogbemi et al. (2024); Soyombo (2024); Sarna et al. (2025)
Anti-Money Laundering (AML)	Network Analysis, machine learning	Detecting suspicious activity and monitoring transactions	Automated compliance, improved detection of financial crime networks	Nartey et al. (2026); Kumar et al. (2022)
Fintech Payment	Machine Learning, Predictive Modelling	Transaction monitoring and assessing fraud risk	Faster fraud prevention in digital payment systems	Ravi et al. (2025); Soyombo (2024)
Digital Banking Platforms (Identity Theft Prevention and Takeover)	Anomaly Detection, Behavioral Analytics	Identity Theft or Account Takeover	Reduced Cost and Improved Risk Management for Customers	Alex-Omiogbemi et al. (2024); Chukwu (2024)

8. Challenges and Limitations of AI Fraud Detection Systems

Although there has been an immense development of artificial intelligence in the detection of financial fraud, there are still a number of technical and operational factors that restrict the performance of such systems in the actual financial setting. Class imbalance is one of the greatest problems in the fraud data set because fraudulent transactions usually constitute a very negligible percentage of the entire transactions transacted by financial institutions. Since fraudulent transactions are significantly less common than regular transactions, machine learning models are usually biased to the majority class and achieve good overall accuracy at the cost of poor fraud detection (Baisholan et al., 2025; Btoush et al., 2023). Such lack of balance lowers the capabilities of a fraud detection model to accurately detect a fraudulent transaction, especially in highly skewed financial data. Different solutions to this problem have been suggested like oversampling, undersampling and cost-sensitive learning yet applying the methods successfully is still a concern in the research of fraud detection (Emmanuel, 2025; Hafez et al., 2025).

The other crucial weakness is the susceptibility of AI-based system of detecting fraud to adversarial attacks and manipulation of the model. Swindlers constantly change their tactics and alter attributes of transactions or behavioral patterns that can be interpreted like a legal financial operation and thus it is hard to differentiate between normal and fraudulent transactions using AI models (Chowdhury, 2024; Sarna et al., 2025). These antagonistic approaches have the potential to decrease the validity of algorithms that detect fraud and enable fraudulent transactions to avoid automated checks. Moreover, most of the modern machine learning and deep learning-based models in fraud detection are complex black-box systems, thereby making it challenging to understand how the models make predictions (Ribeiro et al., 2016). The lack of visibility into or ability to explain how an Artificial Intelligence (AI) model draws conclusions from data makes it difficult for auditors and compliance professionals (who work in industries that are heavily regulated by financial regulators) to justify their decision to use an automated method to detect fraud, or to ensure that automated fraud detection AI systems are equitable (Shpachuk et al., 2026; Oyeyemi et al., 2025).

Fraud detection systems based on AI also pose a high level of data privacy and data availability, especially because the information related to financial transactions is sensitive (Amoako et al., 2025). The privacy and data protection regulations that financial institutions are bound to follow frequently restrict the possibilities of sharing actual financial data to conduct a research and train a model (Shpachuk et al., 2026; Soyombo, 2024). As a result, most research on detecting fraud has used either anonymized or synthetic datasets, and this type of dataset likely does not provide enough accurate information to determine fraud's ever-evolving nature in the finance industry. A further problem in developing machine-learning algorithms is the lack of labeled fraud cases, as many fraudulent acts occur undetected or are only discovered after they occurred (Baisholan et al., 2025; Btoush et al., 2023). These issues raise the question of making AI models more transparent, better-structured data-sharing models, and privacy-sensitive machine learning technologies that can make fraud detection systems in the contemporary financial ecosystem more effective and reliable (Sarna et al., 2025; Chowdhury, 2024).

Table 5 Challenges of AI Fraud Detection Systems

Challenge	Description	Impact on Fraud Detection	Key References
imbalance in fraud datasets	imbalance Fraudulent transactions constitute an extremely small fraction of financial datasets	Models become biased toward legitimate transactions, resulting in low fraud detection recall	Baisholan et al. (2025); Btoush et al. (2023); Emmanuel (2025)
Attack on AI systems adversarial	Fraudsters can manipulate the characteristics of transactions to avoid detection models	Fraudulent transactions may bypass automated monitoring systems	Chowdhury (2024); Sarna et al. (2025)
Lack of explainability and black-box models	Black-box models yield a limited amount of transparency in making decisions	Regulators and auditors face challenges in interpreting model outputs	Ribeiro et al. (2016); Shpachuk et al. (2026); Oyeyemi et al. (2025)
Data protection and privacy problems	Real financial data requirements stricter privacy policies have to be observed	Limited use of real financial data to train a model	Shpachuk et al. (2026); Soyombo (2024)
Low access to labeled fraud information	A significant portion of frauds is not detected or mislabeled	Reduced predictive accuracy and poor generalization ability of a model	Baisholan et al. (2025); Btoush et al. (2023)

9. Emerging Trends in AI-Driven Fraud Detection

The high rate of development of digital financial systems, and the development of sophistication of financial crime, which demands computer systems has escalated the rate of development of new artificial intelligence methods of fraud detection. Despite the fact that the old machine learning models have contributed significantly to the improvement of capacity to detect fraud, the present technology is being used to improve transparency, scale, and inter-institutional collaboration within the systems of detecting frauds (Amoakoh et al., 2026; Sarna et al., 2025). Recent articles highlight the growing importance of explainable artificial intelligence, graph neural networks, federated learning systems and real-time AI detection piping in solving the shortcoming of existing models of fraud detection (Uddin, 2025; Nartey et al., 2026). It is believed that the new technologies will enhance the explanatory quality of models, detect intricate financial crime networks, promote cooperation between financial institutions in terms of fraud detection and detection of suspicious financial transactions in a digital financial environment (Soyombo, 2024; Oyeyemi et al., 2025).

9.1. Explainable Artificial Intelligence (XAI)

Explainable artificial intelligence is one of the key research directions in fraud detection because of the growing problem of questions about the clarity and responsibility of machine learning models deployed in financial systems. Most modern fraud detection models are based on sophisticated machine learning and deep learning models which have processes of decision-making that can be hard to interpret (Chowdhury, 2024; Uddin, 2025). Such a lack of transparency may make the regulators and financial institutions face difficulties and explain artificial decision-making of AI systems. Explainable AI methods can solve this problem by showing interpretations to predictions of models and determining which features affect the decisions taken during the fraud detection (Oyeyemi et al., 2025). XAI frameworks may lead to a more positive attitude towards automated fraud-identifying systems by promoting transparency and accountability, as well as ensure that the financial institution fulfills the regulatory standards that oversee algorithmic decision-making (Nartey et al., 2026; Soyombo, 2024).

9.2. Graph Neural Networks

Graph neural networks are one of the most promising advancements in financial fraud detection since most fraud programs have a structure of connected accounts and coordinated transactions acted upon. Conventional fraud detection models usually consider transactions on a case-by-case basis and restrict their capacity to identify sophisticated regulatory frameworks of financial crime prone to involve numerous individuals (Cheng et al., 2025; Li et al., 2025). Graph-based models of learning overcome this shortcoming by modelling financial systems as networks with entities (accounts, customers, or devices) being represented as nodes and transactions as edges between these nodes. The representation based on the network helps the AI models to study the connections among financial entities and discover suspicious clusters of transactions that can be a sign of organized fraud schemes (Rasul et al., 2024; Zhou et al., 2023).

Graph based methods of detecting fraud are especially useful in detecting multifaceted monetary criminal acts, including rings of fraud, collusive fraud, and network of money laundering that engage several financial accounts and transaction routes. Graph neural networks will be able to discover latent relationships among entities and identify abnormal flows of transactions, which would have been challenging to pick up with transaction-level models (Cheng et al., 2025). Graph-based learning methods are likely to be instrumental in enhancing the quality of fraud detection and allowing financial institutions to detect organized cybercrime networks, which are functioning across various platforms and jurisdictions because financial systems become more interconnected (Li et al., 2025; Sarna et al., 2025).

9.3. Federated Learning

Federated learning has become an alternative that holds potential in solving privacy issues in fraud detection systems. The financial institutions may also have huge amounts of transaction data that may enhance the fraud detection model greatly when pooled across the organizations. Nonetheless, most privacy laws and information security policies do not allow institutions to disclose confidential financial information to third parties (Soyombo, 2024; Sarna et al., 2025). Federated learning allows learning to be shared between two or more institutions without sharing raw data. Rather, the model is trained on a local level in each institution using its own data and exchanged with a centralized aggregation system with only model parameters or updates (Nartey et al., 2026). This collaborative learning model enables financial institutions to gain access to common wisdom without violating data privacy and regulation. Since the network of financial crimes may often cut across different institutions and geographical boundaries, federated learning could greatly improve the ability to detect cross-institutional fraud (Oyeyemi et al., 2025; Sarna et al., 2025).

9.4. Real-Time Fraud Detection

The growth of online banking services and digital payment systems has led to the escalation of the need of real-time detecting fraud systems that can detect suspicious financial activity in real-time. Conventional fraud detection systems tend to be based on batch processing methods that process transactions once they are completed and thus can slow down the process of detecting the fraud and incurring more financial losses (Ravi et al., 2025; Sarna et al., 2025). New AI-based real-time detection systems are based on streaming data analytics and machine learning algorithms that assess transaction risk when new transactions are executed. These systems assess the foundations of transaction, conduct trends, gadget data, and situational information in real time to decide whether a transaction is likely to be fraudulent or not (Chowdhury, 2024; Ravi et al., 2025). Companies can reduce their risk from fraud associated with financial transactions by enabling them to detect potential fraud before the transaction has completed in an Internet based financial transaction (Soyombo, 2024, Sarna, 2025). AI systems that are able to detect fraudulent transactions in real time and enable companies to detect and stop potentially fraudulent transactions before they are finalized, helps to increase the level of security associated with financial transactions making it harder for fraud to take place.

10. Research Gaps and Future Research Directions

Although the current advances in artificial intelligence have been used in detecting financial fraud, there are still a number of research gaps that make current detection systems ineffective and limited in scale. The primary weakness is that access to actual financial data is limited since in many cases, the financial institutions cannot distribute confidential data on certain transactions because of strict privacy policies and privacy-related reasons. Consequently, most research uses anonymized or artificial data which might not be reflective of the reality of real-world fraud operations or financial system dynamics. This is a constraint that limits the creation of very generalized fraud detection models that can be deemed to fit in varying financial environments. Moreover, unexplored machine learning models may struggle to identify meaningful trends of fraud because of the absence of large-scale labeled fraud, thus decreasing the model accuracy and detection reliability.

The other research gap is that the cross-institutional fraud detection systems have not been extensively developed, and thus they have not been able to detect the fraud schemes which may span across various financial institutions and jurisdictions. Most fraud detection models are built to work on single institutional datasets, limiting them to the detection of coordinated networks of frauds across multiple accounts or organizations. Also, there are no adequate solutions yet to the problem of model interpretability and explainability, especially in the case of complex deep learning models that act like black box. The absence of clear AI models may lead to the inability to comply with regulations and trust in automated fraud detection decisions. The study ought to be conducted in future to create explainable AI systems, privacy-sensitive data sharing systems and federated fraud detection system that enables financial institutions to effectively identify fraud without sharing sensitive financial information.

11. Conclusion

This review examined the evolution of financial fraud detection systems and the growing role of artificial intelligence in combating financial crime within modern financial ecosystems. The study has provided an emphasis on the way fraud detection evolved to go beyond the conventional rule-based and statistical methods to more sophisticated AI-based ones such as machine learning, deep learning, graph-based, and hybrid detection systems. These technologies allow the financial institutions to process the massive amount of transaction data, identify intricate fraud trends, and react to potential financial misconduct more effectively. The use of AI systems in the banking process, anti-money laundering and payment systems fintech were also the items of discussion in the review, and they showed how AI technologies contribute to the increased detection of fraud in real time and the monitoring of financial crime. Nevertheless, there are still a number of issues, such as imbalance in the classes of the fraud data, the use of AI systems in the adversarial attacks, the issues of privacy and data protection, and the lack of accessibility to the high-quality fraud data. To solve these problems, it is necessary to conduct additional research on explainable AI models, interactive fraud detection systems, and more sophisticated data-sharing models that will enhance the efficacy and transparency of AI based fraud detection in the future.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Afjal, M., Salamzadeh, A. and Dana, L.P., 2023. Financial Fraud and Credit Risk: Illicit Practices and Their Impact on Banking Stability. Journal of Risk and Financial Management, 16(9), p.386.

[2] Ahmad, H., Kasasbeh, B., Aldabaybah, B., & Rawashdeh, E. (2023). Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS). *International Journal of Information Technology*, *15*(1), 325-333.

[3] Ahmed, R. (2018). *Data mining techniques in financial fraud detection*. GRIN Verlag.

[4] Akartuna, E. A., Johnson, S. D., & Thornton, A. (2024). Motivating a standardised approach to financial intelligence: a typological scoping review of money laundering methods and trends. *Journal of Experimental Criminology*, 1-47.

[5] Alex-Omiogbemi, A. A., Sule, A. K., Omowole, B. M., & Owoade, S. J. (2024). Advances in cybersecurity strategies for financial institutions: A focus on combating E-Channel fraud in the Digital era. *Journal of cybersecurity and financial innovation*, *12*(3), 35-48.

[6] Amoako, E. K., Okeke, P. T., Boateng, V., Bonsu, M. A., & Oman-Amoako, M. (2025). Enhancing risk management and fraud detection in the U.S. financial industry through machine learning algorithms: Applications, challenges, and future directions. *World Journal of Advanced Research and Reviews, 28*(3), 134–144.

[7] Amoakoh, C. K., Nwinyi, I. P., & Ampofo, I. (2026). *AI-enabled assurance frameworks: A review of intelligent systems enhancing accuracy and independence in U.S. financial auditing*. *EPRA International Journal of Economics, Business and Management Studies (EBMS), 13*(2). **https://doi.org/10.36713/epra26251**

[8] Baisholan, N., Dietz, J. E., Gnatyuk, S., Turdalyuly, M., Matson, E. T., & Baisholanova, K. (2025). A Systematic review of machine learning in credit card fraud detection under original class imbalance. *Computers*, *14*(10), 437.

[9] Bakhtiari, S., Nasiri, Z., & Vahidi, J. (2023). Credit card fraud detection using ensemble data mining methods. *Multimedia Tools and Applications*, *82*(19), 29057-29075.

[10] Boateng, N. V., Amoako, N. E. K., Ajay, N. O., & Adukpo, N. T. K. (2025). Harnessing Artificial Intelligence for combating money laundering and fraud in the US financial industry: A comprehensive analysis. *Finance & Accounting Research Journal*, *7*(1), 37-49.

[11] Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. *PeerJ Computer Science*, *9*, e1278.

[12] Cheng, D., Zou, Y., Xiang, S., & Jiang, C. (2025). Graph neural networks for financial fraud detection: a review. *Frontiers of Computer Science*, *19*(9), 199609.

[13] Chowdhury, R. H. (2024). Advancing fraud detection through deep learning: A comprehensive review. *World Journal of Advanced Engineering Technology and Sciences*, *12*(2), 606-613.

[14] Chukwu, B. (2024). A Critical Intersection of cybersecurity, AI and fraud detection in the United States financial market. *International Journal of Science and Research Archive*, *17*, 289-297.

[15] Emmanuel, M. (2025). Deep Learning Architectures for Real-Time Anomaly Detection in Financial Transactions. *ResearchGate Publication, June*.

[16] Gaviyau, W., & Sibindi, A. B. (2023). Global anti-money laundering and combating terrorism financing regulatory framework: A critique. *Journal of Risk and Financial Management*, *16*(7), 313.

[17] Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, *12*(1), 6.

[18] Irvin-Erickson, Y. (2024). Identity fraud victimization: A critical review of the literature of the past two decades. *Crime Science*, *13*(1), 3.

[19] Isangediok, M., & Gajamannage, K. (2022, December). Fraud detection using optimized machine learning tools under imbalance classes. In *2022 IEEE International Conference on Big Data (Big Data)* (pp. 4275-4284). IEEE.

[20] Itoo, F., Meenakshi, & Singh, S. (2021). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *International Journal of Information Technology*, *13*(4), 1503-1511.

[21] Karpoff, J. M. (2021). The future of financial fraud. *Journal of Corporate Finance*, *66*, 101694.

[22] Kumar, S., Ahmed, R., Bharany, S., Shuaib, M., Ahmad, T., Tag Eldin, E., ... & Shafiq, M. (2022). Exploitation of machine learning algorithms for detecting financial crimes based on customers' behavior. *Sustainability*, *14*(21), 13875.

[23] Li, E., Chen, M., Xiang, S., & Chen, L. (2025). Graph Learning-Empowered Financial Fraud Detection: Progress and Future Directions. *Intelligent Computing*, *4*, 0146.

[24] Maddila, S., Ramasubbareddy, S., & Govinda, K. (2020). Crime and fraud detection using clustering techniques. In *Innovations in Computer Science and Engineering: Proceedings of 7th ICICSE* (pp. 135-143). Singapore: Springer Singapore.

[25] Nartey, O., Agyei, E., Anim, B., & Yeboah, M. M (2026). AI and blockchain in forensic auditing: A review of tools for investigating financial crimes in the U.S. *International Journal for Multidisciplinary Research, 8*(1).

[26] Nartey, O. L., Aryeetey, S., Apaflo, D. A., & Yeboah, M. M. (2026). *AI and blockchain in financial auditing: A systematic review of fraud detection techniques and their impact on investor confidence in U.S. market*. *EPRA International Journal of Research and Development (IJRD), 11*(3). https://doi.org/10.36713/epra2016

[27] Nazzari, M., & Reuter, P. (2025). How Well Does the Money Laundering Control System Work?. *Crime and Justice*, *54*(1), 000-000.

[28] Nwinyi, I. P., & Oman-Amoako, M. (2026). *AI-driven business analytics frameworks for government financial management: Advancing accountability and transparency in U.S. federal programs*. *EPRA International Journal of Economics, Business and Management Studies (EBMS), 13*(2). Journal DOI: 10.36713/epra1013|SJIF Impact Factor (2026): 8.748

[29] Oyeyemi, D. O., Okosieme, O. O., Idowu-Kunlere, O., Julius, E. A., & Nwinyi, I. P. (2025): Explainable AI For Credit Risk Assessment: Integrating Machine Learning With Business Analytics.

[30] Rasul, I., Shaboj, S. I., Rafi, M. A., Miah, M. K., Islam, M. R., & Ahmed, A. (2024). Detecting financial fraud in real-time transactions using graph neural networks and anomaly detection. *Journal of Economics, Finance and Accounting Studies*, *6*(1), 131-142.

[31] Ravi, V., Srivastava, V. K., Singh, M. P., Burila, R. K., Chippagiri, S., Pasam, V. R., ... & Prova, N. N. I. (2025, February). AI-powered fraud detection in real-time financial transactions. In *International Conference on Web 6.0 and Industry 6.0* (pp. 431-447). Singapore: Springer Nature Singapore.

[32] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining

[33] Roseline, J. F., Naidu, G. B. S. R., Pandi, V. S., alias Rajasree, S. A., & Mageswari, N. (2022). Autonomous credit card fraud detection using machine learning approach☆. *Computers and Electrical Engineering*, *102*, 108132.

[34] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, *7*(1), 41.

[35] Sarna, N. J., Rithen, F. A., Jui, U. S., Belal, S., Amin, A., Oishee, T. K., & Islam, A. M. (2025). AI Driven Fraud Detection Models in Financial Networks: A Review. *Ieee Access*.

[36] Sathya, M., & Balakumar, B. (2022). Insurance fraud detection using novel machine learning technique. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(3), 374-381.

[37] Shpachuk, V., Markova, O., & Adamyk, B. (2026). AI-driven financial fraud: key risks and legal protections for financial institutions. *Journal of Banking Regulation*, *27*(1), 6.

[38] 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*(1), 2101-2110.

[39] Trivedi, N. K., Simaiya, S., Lilhore, U. K., & Sharma, S. K. (2020). An efficient credit card fraud detection model based on machine learning methods. *International Journal of Advanced Science and Technology*, *29*(5), 3414-3424.

[40] Uddin, N. (2025). Role of AI in Preventing Financial Crime: A Comprehensive Analytical Review. *Journal of Economic Criminology*, 100200.

[41] Xiong, T., Ma, Z., Li, Z., & Dai, J. (2022). The analysis of influence mechanism for internet financial fraud identification and user behavior based on machine learning approaches. *International Journal of System Assurance Engineering and Management*, *13*(Suppl 3), 996-1007.

[42] Yeboah, M. M., Agyei, E., Anim, B., Nwinyi, P., & Nartey, O. L. (2026). AI in financial auditing: Addressing U.S. audit failures and strengthening PCAOB/SEC compliance. Sarcouncil Journal of Economics and Business Management, 5(1). DOI:10.5281/zenodo.18188728

[43] Zhou, Y., Sun, M., & Zhang, F. (2023). Graph Neural Network-Based Anomaly Detection in Financial Transaction Networks. *Journal of Computing Innovations and Applications*, *1*(2), 87-101.