IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 June 2025, accepted 28 July 2025, date of publication 5 August 2025, date of current version 15 August 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3596060

SURVEY

AI Driven Fraud Detection Models in Financial Networks: A Comprehensive Systematic Review

NUSRAT JAHAN SARNA, FARZANA AHMED RITHEN, UMME SALMA JUI, SAYMA BELAL, AL AMIN, TASNIM KABIR OISHEE, AND A. K. M. MUZAHIDUL ISLAM, (Senior Member, IEEE)

Department of Computer Science and Engineering, United International University, Dhaka 1212, Bangladesh

Corresponding authors: A. K. M. Muzahidul Islam (muzahid@cse.uiu.ac.bd) and Farzana Ahmed Rithen (frithen2410051@mscse.uiu.ac.bd)

This work was supported by the Institute for Advanced Research Publication Grant of United International University under Grant IAR-2025-Pub-051.

ABSTRACT Rapid advancements in digital innovation and globalization has significantly increased the complexity of financial networks, making them more vulnerable to fraud. Traditional fraud detection methods struggle to keep pace with evolving fraudulent strategies, contributing to an estimated global financial loss of $ 5 trillion. In response, this review paper explores the role of artificial intelligence (AI) in financial fraud detection, highlighting machine learning (ML), deep learning (DL), and hybrid models as transformative solutions. By analyzing vast datasets, AI can uncover hidden fraud patterns and dynamically adapt to emerging threats. Techniques such as supervised and unsupervised learning, along with advanced approaches like Graph Neural Networks (GNNs), have proven particularly effective in detecting various types of financial fraud, including payment fraud, identity theft, and money laundering. This paper presents a comprehensive taxonomy of AI-driven fraud detection methodologies, synthesizing insights from a substantial number of research papers. It systematically categorizes fraud detection techniques based on their application in different types of fraud, providing a structured framework to understand their effectiveness. In addition, it examines the role of cloud computing, edge AI, and distributed systems in enabling real-time transaction monitoring and fraud detection. Although AI significantly improves detection accuracy, reduces operational costs, and strengthens regulatory compliance, challenges such as model explainability, data privacy concerns, algorithmic bias, and the dynamic nature of fraud remain critical barriers to widespread adoption. Our review highlights the need for collaborative efforts among financial institutions, regulators, and technology providers to address these challenges. Future research should focus on improving the transparency of the AI model, integrating AI with blockchain for secure data sharing, and leveraging federated learning to enhance fraud detection capabilities. By addressing these challenges, AI can play a pivotal role in securing financial systems, minimizing fraud risks, and fostering cross-industry collaboration for more resilient fraud detection frameworks.

INDEX TERMS Fraud detection, AI models, financial networks, anomaly detection, financial fraud.

I. INTRODUCTION

Financial networks are complex and interconnected systems that enable the exchange of monetary value, financial instruments, and data among global institutions. These networks include banks, payment gateways, stock exchanges, and decentralized finance systems, forming the backbone of the global economy by enabling transactions, trade, and investments [1]. With the rapid rise of digital payments and blockchain technologies, the scope of financial networks has expanded, driving innovation and increasing transaction efficiency. However, this evolution has also made these networks

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Wei.

vulnerable to fraudulent activities, which require advanced mechanisms of protection and trust [2]. Fraud in financial networks encompasses a wide range of deceptive practices such as identity theft, money laundering, and payment fraud, exploiting vulnerabilities for monetary gain [3]. The global impact of such fraud is staggering, with an estimated $5 trillion lost annually [116]. Traditional fraud detection methods, like rule-based systems, often fail to keep pace with the growing sophistication of fraudulent schemes, leading to challenges such as false positives, inefficiency, and difficulty in real-time detection [4]. Artificial Intelligence (AI) offers transformative capabilities to address these issues, leveraging its ability to analyze massive datasets, detect hidden patterns, and adapt to emerging fraud tactics [5].

Techniques such as supervised learning for fraud classification and unsupervised learning for anomaly detection have proven to be particularly effective in combating financial fraud, offering the ability to detect both known and novel fraudulent patterns. While unsupervised techniques are excellent at identifying anomalies in unlabeled datasets—often uncovering previously unknown fraudulent behaviors—supervised models, trained on historical labeled data, can reliably distinguish between authentic and fraudulent transactions. Additionally, the area has undergone significant evolution thanks to advances such as graph neural networks (GNNs), which enable the analysis of large, interrelated transactional data and reveal hidden relationships and cooperative fraud schemes that older models might overlook. In addition to being extremely accurate and scalable, these AI-powered systems can handle enormous amounts of financial transactions in real-time, which is essential for early detection and prevention. As a result, operating expenses and false positives are significantly decreased, improving user experience and efficiency. AI is still a crucial technology for enhancing fraud detection capabilities and preserving the integrity of financial systems, despite several obstacles, such as poor data quality, difficult-to-understand sophisticated models, and ethical issues, including bias and transparency [5]. The increasing interest in using AI for fraud detection is driven by the urgent need to ensure the dependability and credibility of financial networks, particularly in light of the swift digital transition. The threat to people, companies, and entire economies is serious, as global financial fraud losses are projected to be in the trillions of dollars each year [4]. Adopting cutting-edge AI-driven solutions are crucial to staying ahead of these risks, as traditional methods like rule-based systems and manual audits have proven inadequate against today's constantly changing, technologically complex fraud techniques [3]. The dynamic nature of financial transactions driven by decentralized finance, mobile payments, and Internet banking requires real-time, flexible solutions. AI's capacity to evaluate enormous amounts of data, spot minute trends, and quickly and accurately forecast fraud is making it a game-changer. The objectives of this effort are to improve fraud detection, lower financial losses, improve regulatory compliance, and restore consumer confidence in digital financial services. In the end, it tackles the increasing demand for intelligent, scalable, and dependable technologies to protect the global financial system. Although the focus of this study is on AI methods for financial fraud detection, new issues, including model security, ownership verification, and intellectual property protection, particularly in federated learning and edge AI contexts, have also drawn attention recently [117], [118], [119], [120], [121], [122]. Figure 1 shows an overview of the AI-driven fraud detection system.

The purpose of this paper is to provide a comprehensive analysis of the current state of Artificial Intelligence (AI) in fraud detection within financial networks, highlighting its transformative impact, challenges, and future potential. By synthesizing existing research and practical applications, the review aims to explore how AI techniques, such as machine learning, deep learning, and natural language processing, are being leveraged to detect and prevent fraudulent activities in real-time. The main contributions of this paper are summarized in the following.

- We have proposed a comprehensive framework that organizes and synthesizes various techniques and approaches employed in fraud detection within financial networks.
- We have provided an in-depth analysis of AI models and algorithms, including machine learning and deep learning, that are widely used in fraud detection systems to effectively identify and mitigate fraudulent activities.
- We have systematically categorized fraud detection methodologies based on their application to different types of financial fraud, such as credit card fraud, money laundering, and insider trading, providing insight into their specific use cases and effectiveness.
- In addition, we have examined strategies for managing large volumes of financial transactions, highlighting the role of cloud computing, edge AI, and distributed systems in enabling real-time data processing and detection.
- We have studied a total of 121 research papers and summarized them. As a result, from a single paper, you can gain the collective knowledge of these 121 papers.
- Finally, we have identified critical research challenges, including the need to improve model accuracy, maintain data privacy, and address the constantly evolving nature of fraud, which needs to be resolved to achieve widespread adoption and scalability of AI-driven fraud detection systems.

The structure of the paper, shown in Figure 2, methodically introduces the investigation of AI for the detection of financial network fraud. Section II (Related Works) reviews the existing literature, summarizing significant developments and highlighting gaps in the application of AI techniques for fraud detection. Section III (Methodology) outlines the framework and methods used in this study, including the criteria for choosing and evaluating 121 research articles, as well as the classification of AI techniques. Section IV

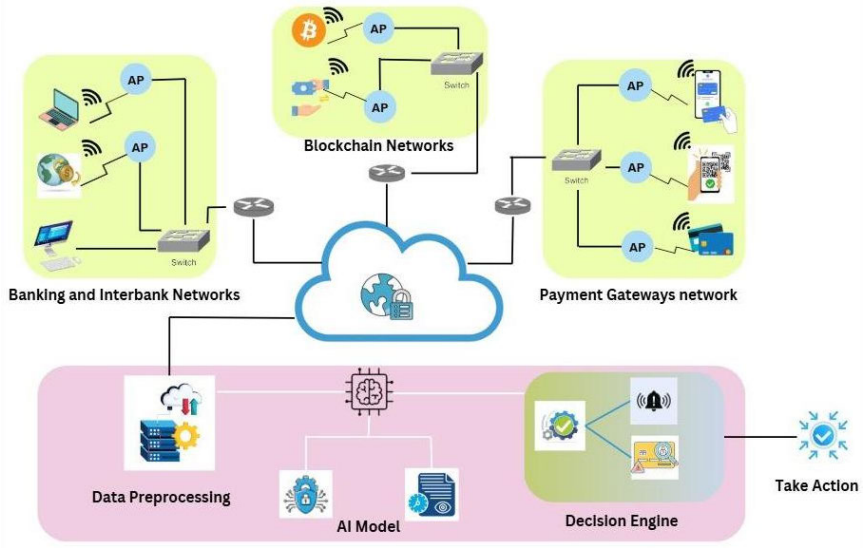

FIGURE 1. System Overview of AI-Driven Fraud Detection.

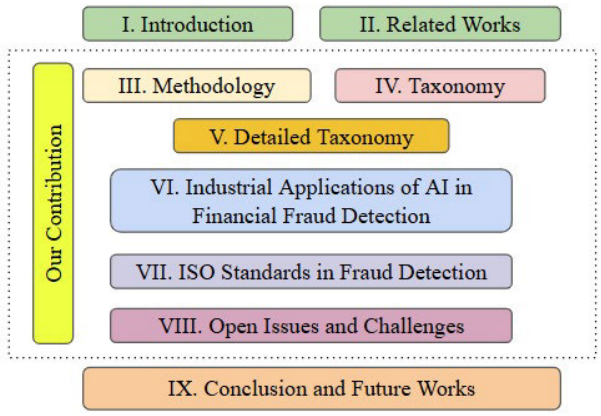

FIGURE 2. Organization of our review.

(Taxonomy) outlines the various steps and sub-steps involved in the work. In Section V (Detailed Taxonomy), we extract the components and provide their results, along with the related papers. In Section VI (Industrial Applications of AI in Financial Fraud Detection), we mention some research articles and articles based on this. In Section VII (ISO Standards in Fraud Detection), we mention some ISO standards for financial fraud detection that can help us detect fraud ethically. Section VIII (Open Issues and Challenges) offers insights into areas requiring further investigation, highlighting unresolved issues. The main contributions of the study are summarized in Section IX (Conclusion and Future Work), which also proposes avenues for enhancing AI-driven fraud detection systems.

II. RELATED WORKS

Fraud detection is an important problem in financial networks, especially as they become more complex and difficult to protect against. Artificial Intelligence (AI) has become one of the most effective means in the fight against financial fraud. This section aims to discuss the shift from earlier conventional methods to new-age AI methods including big data, blockchain, Machine learning, and Deep learning techniques. First, we compared our review paper with existing review papers. For this comparison, we mainly considered the Q1 and Q2 journal papers.

Compared to the existing literature, our suggested review takes a more comprehensive and integrated approach to the use of AI technology in financial fraud detection. In Table 1, a comparison table is presented that identifies gaps and limitations in recent research ([11], [25], [26], [28], [29], [63], [67], [69], [72], [73], [78], [82], [114], [115]), particularly in their failure to simultaneously focus on essential areas such as anomaly identification, fraud

TABLE 1. Comparison among review papers.

Paper	Year	AI	ML	Other (DL, BD, DM)	Fraud Detection	Anomaly Detection	Real Time Analysis
[114]	2025	✓	✓	✓	✓	×	✓
[115]	2025	✓	×	✓	✓	×	✓
[69]	2024	✓	✓	×	×	×	✓
[73]	2024	✓	×	×	×	×	✓
[67]	2023	✓	✓	✓	×	×	✓
[78]	2023	×	×	✓	✓	×	✓
[82]	2023	×	✓	✓	✓	×	✓
[63]	2022	×	×	✓	✓	×	✓
[72]	2022	✓	×	×	×	×	✓
[25]	2021	×	✓	✓	×	✓	✓
[26]	2021	×	×	✓	×	×	✓
[11]	2021	✓	✓	✓	×	×	✓
[28]	2021	×	×	✓	✓	✓	✓
[29]	2020	×	×	✓	✓	✓	✓
	Our Work	✓	✓	✓	✓	✓	✓

detection, and real-time analysis. For example, while most of the evaluated publications use Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), Big Data (BD), and Data Mining (DM) approaches, many do not address the real-time analysis required for successful fraud detection in dynamic financial networks.

In article [114], the authors described different AI models starting with Random Forests along with Convolutional Neural Networks and LSTM networks with evaluations of their detection capabilities of fraudulent transactions.

Traditional and innovative credit card fraud prevention techniques are analyzed in [115], where it is found that the equation-based and rule-based models struggled with dynamic fraud patterns, while the agent-based models effectively adapted to evolving fraud.

Common machine learning algorithms in banking include random forests, decision trees, and support vector machines. The study also highlighted banking applications and ethical challenges such as data privacy concerns and AI biases in financial decisions [69].

In [73], researchers investigated the ways artificial intelligence (AI) improves cybersecurity in financial transactions. The paper examined the role of artificial intelligence through automated techniques that protect against cyber threats and fraudulent activities, as well as automate security measures.

In [67], the study addressed data gathering issues and the importance of effective data preprocessing for improved detection performance.

Article [78] explores machine learning approaches, class imbalance issues, and feature engineering in fraud detection. It categorizes fraud detection constraints into data-related, security-related, and implementation issues, highlighting challenges like class imbalance, data scarcity, data drift, and overlapping data.

The findings in [82] provide a detailed review of the performance indicators and effectiveness of several algorithms in identifying credit card fraud. Many examined studies identified the lack of different datasets as a significant restriction that affects the quality and effectiveness of research output.

Better strategic decisions are made possible by the study's suggested service architecture, which links industry and research. The results indicate that AI increases marketing segmentation and customer service for basic tasks [63].

According to the study, credit card fraud is the most investigated kind, with the most recent research peaking in 2016. The two ML algorithms that are used most frequently are SVM and ANN [72].

In [25], researchers highlight SNA and graph-based techniques for improved fraud identification and propose the use of deep learning with preprocessing and contextual data to improve financial cybercrime detection.

The authors in [26] discuss numerous big data applications for financial risk management, such as credit risk assessment, liquidity risk assessment, and fraud detection. However, relying on complex algorithms may require large computational resources and experience, which might be prohibitive for some financial organizations.

According to the review, DL techniques, in particular graph models, CNNs, and autoencoders, are quite successful in detecting fraud. However, one of the biggest problems with AI-based anti-money laundering systems is still their lack of interpretability and transparency [11].

The most popular method, according to the analysis, was SVM (23%), followed by Random Forest and Naïve Bayes (15%). Credit card and insurance fraud are the main objectives of data mining for the detection of financial fraud (81.33%). Although hybrid models increase accuracy and decrease false positives, inconsistent datasets and assessment criteria continue to be a problem [28].

This study examines graph-based anomaly detection (GBAD) for fraud detection, emphasizing how well it models intricate relationships in networks such as insurance and banking. It offers a framework for comprehending GBAD applications and examines trends, problems, and solutions [29].

In this paper, we offer a detailed understanding of cutting-edge technology by combining fraud detection, anomaly detection, and real-time analysis in a novel way. It emphasizes real-time fraud prevention and anomaly detection while focusing on real-world applications, recent research from 2020 to 2025, and developing trends.

In addition to the high-quality Q1 and Q2 publications, we analyzed other studies that, although not of the same quality, still provide useful insights. For example, According to one of the studies published, it is possible to significantly improve fraud detection systems by using AI, data mining, and geolocation as complementary factors [110]. Another analysis found that supervised learning approaches, such as Random Forest and neural networks, are especially good at detecting fraudulent credit card transactions [27]. A thorough review found that supervised learning models are dominant in AI-driven fraud detection in the banking industry. Of the 112 publications analyzed, 45 focused on approaches such as decision trees, support vector machines, and neural networks [54].

III. METHODOLOGY

A. SEARCH STRATEGY

(a) Utilized Databases: To ensure a thorough coverage of related research, the literature for this study was compiled methodically from reliable academic databases. An important resource for researching developments in machine learning, artificial intelligence, and their uses in financial systems, particularly AI-driven fraud detection, is IEEE Xplore, which is well known for its large collection of academic publications. In the same way, Springer made excellent peer-reviewed articles and conference proceedings accessible, providing important information on AI-based fraud detection techniques. The retrieval of publications on machine learning, deep learning, and hybrid models, all

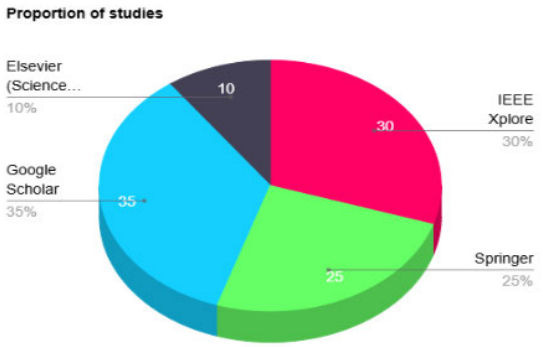

FIGURE 3. Proportion of Studies.

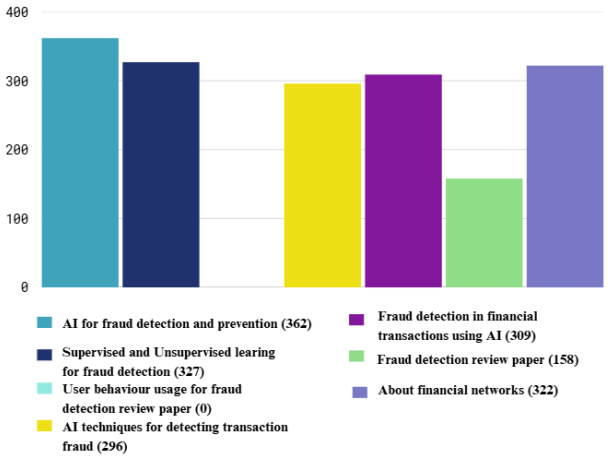

FIGURE 4. Proportions of Keywords.

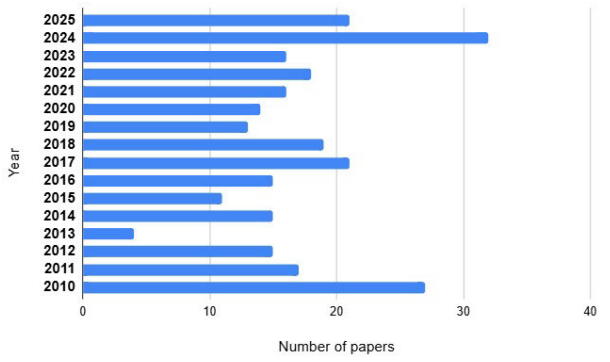

FIGURE 5. Time frame of related works.

crucial for comprehending complex fraud detection methods, was made possible using Elsevier's ScienceDirect platform. Furthermore, Google Scholar was used to find papers from a variety of publications and conferences outside the control of certain publishers, thereby expanding the scope of the literature study. We reviewed research papers from major publishers such as IEEE, Elsevier, Springer, MDPI, Taylor and Francis, ACM, Wiley/Sage, and various other local and emerging journals. Here, we present a pie chart in Figure 3 showing the proportion of studies.

(b) Keywords: The search strings are designed to capture various methodologies, types of fraud, and applications of AI in fraud detection. Keywords and phrases included:

- "AI for fraud detection and prevention"
- "Fraud detection in financial transactions using AI"
- "Supervised and Unsupervised learning for fraud detection"
- "Fraud detection review paper"
- "User behavior usages for fraud detection review paper"
- "About financial networks"
- "AI techniques for detecting transaction fraud"

In Figure 4, we present a graphical view of the proportions of keywords.

(c) Additional Considerations: Studies with experimental validation and real-world applications in financial fraud detection were included in the search to increase relevance. The search results are refined using boolean operators such as AND, OR, and NOT. For example: (("artificial intelligence" OR "AI") AND ("financial transactions" OR "fraud detection") ("deep learning" OR "machine learning") AND ("payment fraud" OR "insurance fraud").

(d) Including the Time Range: Figure 5's horizontal bar chart illustrates a consistent increase in research on AI-driven financial network fraud detection between 2010 and 2025. Although there were few publications between 2010 and 2015, suggesting that the topic was still in its infancy, interest began to rise rapidly in 2016 and peaked in 2024. This pattern illustrates how sophisticated fraud prevention is becoming more and more necessary as financial risks change. Future efforts will probably concentrate on AI-powered fraud detection for safer transactions, as the growth underscores AI's critical role in boosting security, trust, and resilience in contemporary financial systems.

B. DISTRIBUTION OF EXAMINED PAPERS BY RESEARCH METHOD

We have collected some related articles to better analyze the concept, and by doing this we found different types of articles. The pie chart in Figure 6 shows the number of research methods found in this work. The fundamental importance of summarizing and synthesizing previous work to identify gaps and suggest future directions in fraud detection research is demonstrated by the fact that 35.8% of the assessed studies used a literature review strategy. These designed experiments made up 24.5% of the total effort, which shows practical confirmation in the modeling of AI for the detection of fraud activity across financial networks. Much attention has already been paid to the use of quantitative analysis approaches, which are 15.1% as shown in the publications used in the research study to support the research findings. On the other hand, theoretical or conceptual approaches, which concentrated on creating frameworks or algorithms without many real-world applications, made up 13.2%Àlthough qualitative research represented 3. 8%, and often analyzed cases or

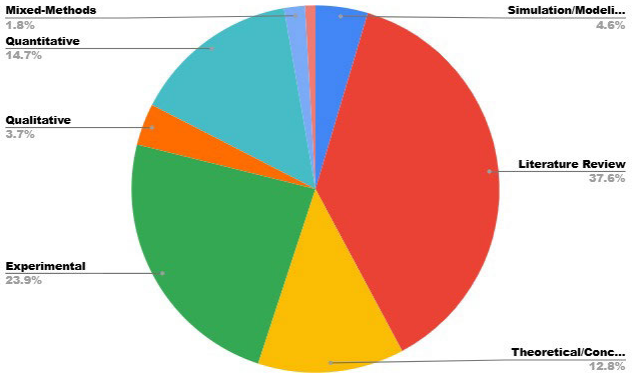

FIGURE 6. Distribution (%) of Research Methods.

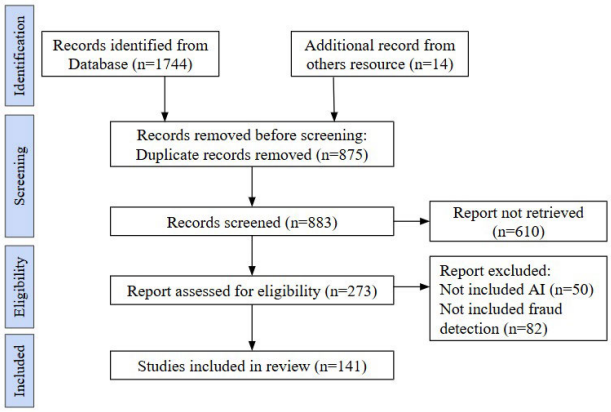

FIGURE 7. PRISMA Flow Diagram.

interviews to study anti-fraud implementations, simulation / modeling (4. 7%) reconstructed the financial network for fraud prediction, although less often than other approaches. A mixed methods technique, which combines qualitative and quantitative studies to generate more comprehensive insights, was used in just 1.9% of the articles.

This distribution shows that most of the research in this field is concerned with evaluating existing knowledge and validating AI models by means of experimental frameworks. Despite this, there is a considerable deficiency in the application of mixed-methods research that might aid in offering important insights into technical and operational aspects of AI-based fraud detection. In addition, even though theoretical work is valuable, focusing more on simulation and real-world case studies might serve well to enhance the use of the field. Finally, this conclusion states that the transformation of AI research in fraud detection depends on enhanced collaboration among the different disciplines to effectively transpose theory into practice in financial networks.

C. QUALITY ASSESSMENT

(a) Relevance to the Topic: Each study is assessed for its direct relevance to AI-based financial fraud detection, ensuring that it addressed at least one fraud type (e.g., payment fraud, identity fraud) and employed AI techniques like ML, DL, or Hybrid Models. Priority is given to studies focusing on financial transactions, fraud detection systems, or technologies with practical applications.

(b) Novelty of AI Techniques: Higher ratings are given to studies that suggested innovative approaches, such as hybrid models, graph neural networks, or reinforcement learning strategies. Papers that demonstrated the model's flexibility in responding to changing fraud trends or new threats were given precedence. In addition, companies that used Explainable AI (XAI) methods to improve transparency and guarantee regulatory compliance were given preference.

(c) Practical Applicability: The scalability of the studies in managing massive amounts of real-time financial transaction data was evaluated. Models that are evaluated in real-world situations or address real-world issues, such as computational cost and system integration are preferred.

D. SCREENING PROCESS

The systematic review procedure of the paper is depicted in the PRISMA [108] flow diagram of Figure 7. Finding 1,744 records from databases and an additional 14 records from other sources is the first step. A total of 883 records were reviewed after 875 duplicates were eliminated. Of these, 610 reports were not retrieved. In total, 273 reports are evaluated for eligibility; those that did not use AI (50) or fraud detection (82) were excluded. Ultimately, the review comprised 141 studies.

This is the PRISMA flow diagram, which outlines each step of the paper filtering process.

E. SELECTION CRITERIA

Criteria for Inclusion

Studies are chosen for review based on the following criteria:

- Concentrate on AI/ML Methods: Research that detects fraud in financial networks using artificial intelligence (AI) or machine learning (ML) techniques, such as supervised learning, unsupervised learning, deep learning, hybrid models, and reinforcement learning.
- Pertinence to the Identification of Financial Fraud: Articles that discuss particular forms of financial fraud, such as securities and trading fraud, insurance and claims fraud, transaction fraud, identity fraud, and payment fraud, among others.
- Type of Publication: Articles with confirmed scientific contributions that have been published in peer-reviewed journals, high-impact conference proceedings, or reliable internet sources.
- Validation through experimentation: Research demonstrating experimentally how well AI/ML methods identify fraud using performance indicators (e.g., accuracy, precision, recall, F1-score).

- Timeframe: To ensure that the latest developments in AI-based fraud detection are included, studies published between 2019 and 2024 are included.
- Language: English-language papers are designed for readability and analytical consistency.

Exclusion Criteria

To remove studies from the review, the following standards are used:

- Topics Unrelated to Financial Fraud: Research on fraud in unrelated fields (such as academic plagiarism or healthcare) unless it includes transferable AI techniques that may be used to combat financial fraud.
- Absence of AI Integration: Articles focusing on fraud detection or prevention techniques that do not integrate AI or ML.
- Absence of Experimental Support: Studies that only use theoretical models with no real-world applications or that do not offer enough experimental validation.

F. CATEGORIZATION FRAMEWORK

(a) Fraud Types: The reviewed studies encompass various types of financial fraud, categorized based on their focus areas. Payment fraud is a prominent concern, involving fraudulent activities such as credit or debit card misuse, online payment scams, and QR code fraud. Identity fraud, another critical area, deals with the unauthorized use of personal information to carry out transactions or identity theft. Transaction fraud highlights anomalies in financial activities, including unauthorized withdrawals or fund transfers. Cryptocurrency fraud, emerging as a modern challenge, involves deceptive schemes on blockchain platforms, such as Ponzi schemes and fraudulent initial coin offerings (ICOs). In addition, money laundering, which focuses on disguising the origins of illegally obtained funds by passing them through legitimate channels, represents a significant threat within the financial ecosystem.

(b) Methods (AI Methodologies): The reviewed studies are classified according to the AI methodologies they utilized, revealing a range of innovative techniques for the detection of financial fraud. Machine Learning (ML) approaches included supervised learning methods such as Logistic Regression, Decision Trees, Random Forests, and Support Vector Machines (SVM), alongside unsupervised learning techniques like K-Means clustering and anomaly detection methods such as Isolation Forest and DBSCAN. Deep Learning (DL) methodologies demonstrated significant promise, with Convolutional Neural Networks (CNNs) employed for detecting fraud patterns in image or spatial data, such as QR code authentication, and Recurrent Neural Networks (RNNs) or Long Short-Term Memory (LSTM) applied to sequential transaction analysis. Graph Neural Networks (GNNs) are specifically used for exploring relationships in networked data, including fraud rings and transaction graphs. Hybrid models, such as stacking approaches that combine ML and DL algorithms, and ensemble methods like bagging (e.g., Random Forest) and boosting (e.g., Gradient Boosting Machines), aimed at improving prediction accuracy. In addition, Reinforcement Learning (RL) facilitated adaptive fraud detection systems that dynamically learn optimal strategies to uncover fraudulent activities.

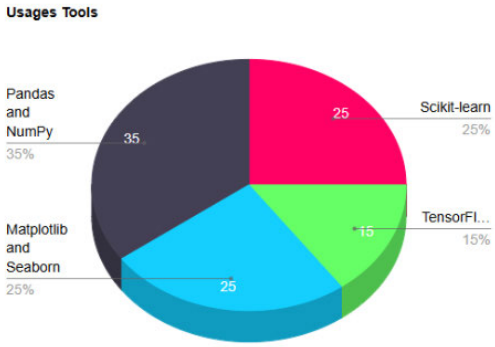

FIGURE 8. Usages tools.

G. TOOLS AND SOFTWARE

Python is used in the fraud detection system due to its robust libraries and frameworks. Pandas and NumPy are used for data analysis and manipulation, while Scikit-learn, TensorFlow, and PyTorch manage machine learning and deep learning tasks. Patterns are shown using programs like Matplotlib and Seaborn and anomaly identification is carried out with the use of autoencoders and isolation forests. When combined, these tools guarantee the effectiveness, scalability, and efficiency of the system in identifying fraud. Figure 8 shows the ratio of tools used.

Diverse tools are used for different tasks. Both LaTeX and Microsoft Word are frequently used to create documents. Languages such as Python and R are used for data analysis, while reference management programs such as Mendeley and Zotero aid in citation organization.

H. DATA EXTRACTION

Several fraud detection techniques, such as supervised learning, unsupervised learning, and hybrid approaches are the focus of the data extraction from the chosen research. Random Forests, Gradient Boosting, Autoencoders, Neural Networks, and anomaly detection techniques such as Isolation Forests were among the AI techniques frequently employed. The efficiency of the model is assessed using performance metrics such as accuracy, precision, recall, and F1-score, with a focus on reducing false positives and false negatives.

IV. TAXONOMY

In Figure 9, the taxonomy of AI for fraud detection in financial networks provides a comprehensive overview of how AI techniques are employed in financial fraud detection by categorizing the various components involved in the process. At the core of the taxonomy are the types of financial fraud, which include payment fraud, identity fraud, transaction fraud, insurance and claims fraud, securities

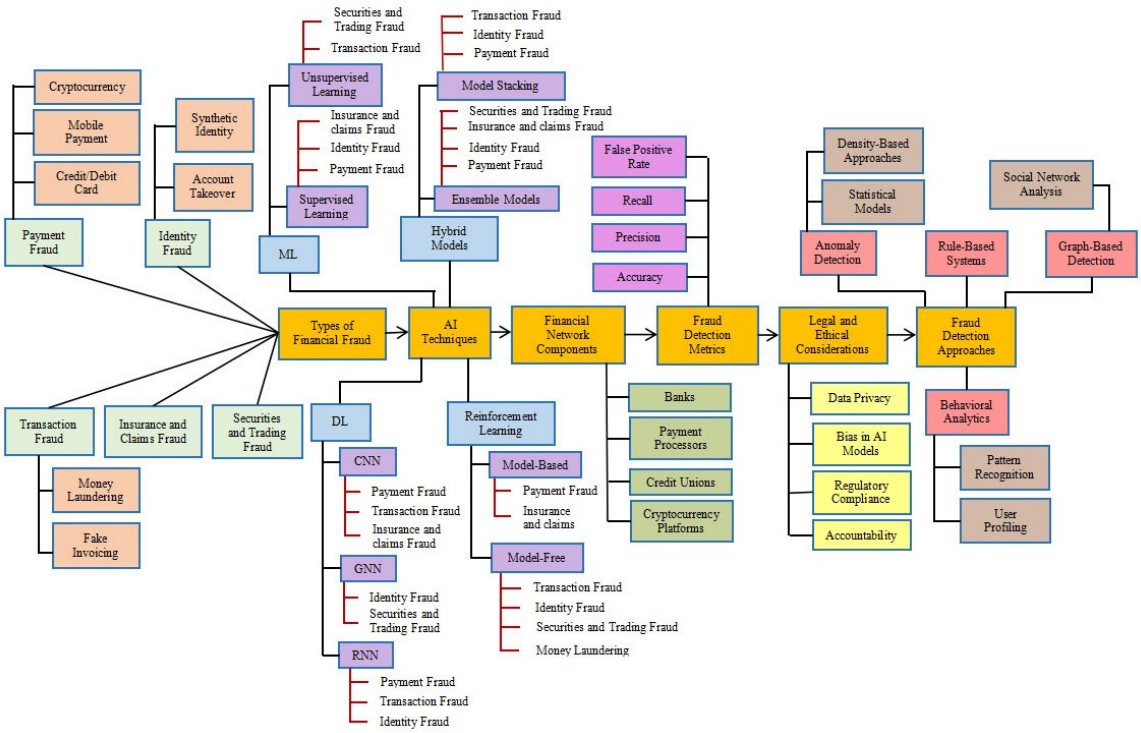

FIGURE 9. Taxonomy of AI for fraud detection in financial networks.

and trading fraud, money laundering, and fake invoicing. These types of fraud are associated with specific methods, such as cryptocurrency scams, credit or debit card fraud, synthetic identity creation, and account takeovers, which are common challenges in modern financial systems. Each type of fraud exposes unique vulnerabilities that require specialized approaches for effective detection.

The AI techniques used for fraud detection are divided into Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL). ML encompasses supervised learning, where labeled data is used to differentiate fraudulent and legitimate transactions, and unsupervised learning, which identifies anomalies without predefined labels, making it suitable for detecting novel fraud patterns. DL techniques such as Convolutional Neural Networks (CNN), Graph Neural Networks (GNN), and Recurrent Neural Networks (RNN) are applied to process complex data structures, recognize relationships, and analyze sequential patterns in transactional data. Reinforcement Learning further extends fraud detection through model-based approaches that simulate scenarios, such as claims in insurance fraud, and model-free techniques suitable for real-time applications like online payment monitoring.

The taxonomy also incorporates Financial Network Components, such as banks, payment processors, credit unions, and cryptocurrency platforms, which are key stakeholders in the fraud detection ecosystem. These components underline the importance of customized solutions for specific entities within the financial network. To assess the effectiveness of these AI systems, Fraud Detection Metrics such as precision, recall, accuracy, and false positive rates are used. These metrics ensure the robustness of fraud detection models by evaluating their ability to accurately and efficiently identify fraudulent activities while minimizing errors.

The framework also outlines various fraud detection approaches, including anomaly detection, rule-based systems, social network analysis, and graph-based techniques. These approaches leverage statistical models, density-based methods, and network analytics to identify fraud patterns and connections within financial transactions. In addition, the taxonomy addresses Legal and Ethical Considerations, highlighting critical issues such as data privacy, bias in AI models, regulatory compliance, and accountability. These considerations emphasize the need for an ethical and transparent implementation of fraud detection systems to maintain trust and fairness in the financial industry. This structured framework provides a holistic understanding of the integration of AI in financial fraud detection, balancing technological innovation with practical and ethical responsibilities.

V. DETAILED TAXONOMY

In this section, we elaborate the components of taxonomy.

A. TYPES OF FINANCIAL FRAUD

This section describes the first key element of the taxonomy, which is the types of financial fraud. There exist several types

of financial fraud that AI-based methods seek to identify and are categorized in this area of taxonomy.

1) PAYMENT FRAUD

Payment fraud includes schemes that involve credit or debit cards, online payments, and QR codes, and is one of the main categories. People use fraudulent payment methods to steal money and access personal information through credit cards, debit cards, and e-payment systems. Payment fraud operates in different ways and disrupts the lives of private citizens, their work activities, and bank partners. Several articles related to this type of fraud are observed that are listed in Table 2.

Article [109] has considered the use of supervised and unsupervised learning systems for fraud detection in eCommerce payment systems with AI central to data control, customers' identification, and adaptation to new threats. Therefore, in this research, an effort is made to find out how accurately predictive AI is advancing the state of eCommerce payments in cybersecurity. The study introduced a prototype application, AML2ink, which visualizes complex financial transaction patterns to identify suspicious activities such as high transaction volumes, U-turn transactions, transfers to high-risk countries, and irregular loan repayments [111]. This paper examined how AI and Big Data work together to strengthen biometric authentication processes to protect digital payment security. The model united machine learning algorithms and advanced analytics to deliver real-time protection against fraud and transaction security, as well as user identity verification [24]. This paper introduced a reliable profiling system to detect fraudulent payment behavior in online transactions. The implementation method of the credible individual behavior profiling framework spans two crucial phases [94].

a: CRYPTOCURRENCY

Frauds and crimes committed against digital cryptocurrencies, including Bitcoin, Ethereum, etc. make up cryptocurrency fraud. People lose money because cybercriminals take advantage of the distributed and private characteristics of digital currencies. Here in Table 3, we mention those types of papers where we have found cryptocurrency-related information:

The research presents an extensive evaluation of the data mining methods employed for the analysis of financial fraud from 2009 through 2019. A classification structure groups financial fraud incidents into credit card fraud, insurance fraud, financial statement fraud, and cryptocurrency fraud while examining performance metrics of 34 data mining techniques. Utility-based methods such as Support Vector Machines (SVM), Random Forest (RF), and Neural Networks dominate the field of fraud detection, yet SVM maintains its position as the top selection. This research review provides an accessible resource platform for researchers and practitioners through its compilation of current techniques and associated strengths and drawbacks [28]. The paper shows how fraud has become more common in cryptocurrency deals while stressing the need to prevent these types of scams [44].

b: MOBILE PAYMENT

People who commit mobile payment fraud use mobile wallets, QR codes, and contactless payment methods to illegally take money from users. Mobile payments face increasing security threats as many users adopt this convenient payment method.

c: CREDIT / DEBIT CARD

Credit/Debit Card Fraud exists when fraudsters improperly use another person's credit or debit card details to make purchases or steal funds from their account. When people or organizations perpetrate this fraud, it creates monetary losses plus puts victims at risk of having their identities stolen and their systems compromised. In the following papers in Table 4, we can see the existing work based on credit/debit card fraud:

The research outlines a framework to improve the detection of bank credit card fraud through artificial intelligence and combines it with data mining and geolocation analysis [110]. This paper investigates how machine learning technology can find credit card fraud and assesses its performance and difficulties [27]. The research analyzes how credit card fraud allows criminals to cover up money laundering. The large number of daily financial transactions creates obstacles in finding fraud [46]. The investigation explored the Machine Learning (ML) and Data Mining (DM) algorithm based approaches that detect Credit Card Fraud Detection (CCFD). The project highlighted the need to develop effective prediction algorithms that aim to detect fraudulent activity because fraudsters continue to try new tactics [83]. The proposed model provided superior performance to both traditional Naive Bayes and Support Vector Machine (SVM) methodologies through higher accuracy scores and enhanced Area Under the ROC Curve (AUC) results. Real-time analysis and powerful processing of large transaction datasets emerged from the improved capability of the model to detect fraud features [93]. The research presented a performance comparison between a simulation Annealing Technique-trained Artificial Neural Network (SA-ANN) and a proposed Hierarchical Temporal Memory model built using Cortical Learning Algorithms (HTM-CLA) which represents a new methodology for online anomaly detection systems [103].

2) IDENTITY FRAUD

When personal information is exploited for illegal access or transactions, identity fraud occurs. People who commit identity fraud use stolen personal information to pretend to be you to achieve financial or criminal goals. When someone loses their identity through fraud they suffer immediate damage to their money, credit history, and public standing.

TABLE 2. Comparison of Payment Fraud-related works.

Ref and Year	Main Idea	Used Method	Findings	Limitations
[94] 2021	• Provides a viable method in which to build and implement this profiling framework to carry out a valid individual behavior profiling that could be used in the detection of online payment fraud. • Establish a reliable profiling method for every user to detect anomalies in online payment behavior.	• Frequent Pattern Tree (FP-Tree) to build user-specific profiles mining on transaction history. • Logistic Regression, SVM, DNN, and Random Forest across various performance metrics, demonstrating superior precision, recall, specificity, accuracy, and F1-score in detecting fraudulent transactions.	• FP-Tree based profiling adapts well to involving user behaviors. • Achieves higher precision, recall, specificity, accuracy, and F1 score. • Outperforms Logistic Regression, SVM, DNN, and Random Forest.	• N/A
[109] 2020	• Explores the use of predictive AI enhances real-time fraud detection in e-commerce transaction. • Ensure secure transactions and manage risk dynamically through pattern recognition and anomaly detection system.	• Supervised learning. • Unsupervised learning (anomaly detection). • Reinforcement learning.	• AI methods outperform rule-based systems in accuracy and adaptability. • Reduce False Positives. • Real-time predictive analysis helps reduce detection latency and minimizes customer friction.	• Requires high-quality label data. • Limited focus on real-time fraud detection. • High computational requirements. • Missing to handle real-world deployment and scalability issues.
[111] 2019	• Propose data visualization framework to help analysts detect suspicious. • Enhances the identification of unusual transactions. • Use graphical visualization.	• Prototype system(AML²ink). • Suspicious clustering. • Visual link analysis. • U-Turn transactions for hidden pattern.	• Low cost visual tool AML to monitor suspicious and anomalies. • Enhanced detection of pecuniary transactions.	• Challenges in embedding the program. • Problems with number density.

a: SYNTHETIC IDENTITY

Fraudsters construct synthetic identities using legitimate SSN or taxpayer IDs together with fake personal information such as name and home address. Synthetic identities help criminals commit financial fraud and create major problems for banks, creditors, and law enforcement agencies.

b: ACCOUNT TAKEOVER

Once accounts are taken over, the attacker might carry out financial theft or launch new fraud attempts while spreading computer threats to other users.

3) TRANSACTION FRAUD

Anomalies in financial transactions, such as unapproved withdrawals or transfers, are the main focus of transaction fraud. In Table 5, we mention articles related to transaction fraud.

This paper aimed to investigate the application of developing an integrated system that combines both hybrid deep learning models and the Random Forest algorithm to identify financial fraud. From the experimental analysis, false positive rates are reduced to 15% and overall detection accuracy has improved to 20% [6]. The system provided a mechanized analysis approach that united machine learning protocols with data preprocessing functions and time-sensitive analytics to detect fraudulent arrangements effectively and precisely [12]. This research evaluated how machine learning (ML)–powered AI systems function to detect financial fraud inside Internet of Things (IoT) networks. Common advanced Machine Learning models, including Random Forests, Support Vector Machines (SVMs), and Neural Networks, serve to evaluate extensive and complex data collections from IoT devices [20]. This paper suggested using user behavior patterns from online transactions to detect fraud using a new fraud detection method. The system examines

TABLE 3. Comparison of Cryptocurrency-related works.

Ref and Year	Main Idea	Used Method	Findings	Limitations
[44] 2022	• To investigate the effectiveness of AI techniques in detecting and preventing fraudulent activities in cryptocurrency transactions. • Focus on dynamic, real-time, and intelligent fraud detection systems tailored to the complexities of decentralized finance.	• Supervised Learning (e.g., Decision Trees, SVM, Neural Networks). • Unsupervised Learning (e.g., Clustering, Anomaly Detection). • Deep Learning (e.g., CNN, RNN, LSTM, Transformers). • Graph-Based Techniques (e.g., Graph Neural Networks). • Behavioral and Sequence Analysis, Wallet Clustering.	• AI can identify complex fraud schemes, such as money laundering, phishing, and Ponzi schemes. • Supervised learning works well with labeled fraud datasets; unsupervised learning is effective for new, unknown fraud patterns. • GNNs help detect collaborative fraud across networks. • RNNs/LSTMs are useful in identifying temporal patterns in transactions.	• Lack of high-quality labeled datasets in the crypto domain. • High false positives can disrupt legitimate users. • Explainability and regulatory transparency are still challenging. • High computational cost for deep and graph-based models. • Limited access to off-chain or private transaction data.
[28] 2021	• Comprehensive review of data mining techniques used in financial fraud detection from 2009 to 2019. • Categorizes literature by fraud types and applied methods.	• Support Vector Machine (SVM) – most frequently used (23%). • Naïve Bayes, Random Forest – each 15%. • Other methods: Decision Trees, K-Nearest Neighbors (KNN), Logistic Regression, Neural Networks, Clustering, Outlier Detection. • Total of 34 data mining techniques were identified.	• Banking and insurance fraud accounted for 81% of studies. • SVM, Naïve Bayes, and Random Forest were the most commonly used. • Growing interest in cryptocurrency fraud detection. • Most research is concentrated in developed countries.	• Does not include studies beyond 2019 (misses newer techniques like deep learning, GNNs). • Limited focus on real-time fraud detection. • Few studies from developing economies. • Emphasis on classification; less attention to hybrid or ensemble approaches.

previous purchase data from time, IP, total amounts, and usage patterns to create a multipoint hyper-sphere layout [91].

a: MONEY LAUNDERING

Money laundering hides how crooks get illegal cash by making it seem like the money is legal. In Table 6, we have shown a comparison of some work related to money laundering.

The research analyzes the use of link analysis to reveal money laundering behavior in financial transaction data through visual representations [111]. The research examined financial crime detection alongside fraud prevention through graph computing methodologies and machine learning frameworks that utilize graph neural networks (GNNs) [9]. This paper evaluates how deep learning and explainable artificial intelligence work together to detect money laundering. The analysis shows that DL tools, including convolutional neural networks and autoencoders, excel at finding complex data patterns in financial transactions [11]. This document offered an extensive description of Anti-Money Laundering (AML) activities in Bangladesh covering historical development alongside legal authorities and state participation, as well as money laundering hazard zones. The paper examined the potential and success rate of Artificial Intelligence (AI) applications to detect money laundering operations and their proactive prevention abilities [74].

b: FAKE INVOICING

When people commit fraud, they use fake bills to make their illegal actions look legitimate and hide where they put their stolen money. People use fake invoicing methods mainly for TBML but also commit tax evasion, fraud, and financial crimes.

4) INSURANCE AND CLAIMS FRAUD

People commit insurance and claims fraud by lying to insurance companies to get money they do not qualify for. Users can commit fraudulent activities targeting multiple insurances from medical coverage to auto coverage, property insurance, life insurance, and disability insurance.

The research introduced SISBAR as an automated insurance system architecture built on AI capabilities that

TABLE 4. Comparison of Credit/Debit Card related works.

Ref and Year	Main Idea	Used Method	Findings	Limitations
[114] 2025	A systematic review of recent advances in credit card fraud detection using AI techniques, including machine learning, deep learning, and meta-heuristic optimization.	• Machine Learning (ML) • Deep Learning (DL) • Meta-Heuristic Optimization (MHO) • Hybrid AI Models	• AI models like ensembles, neural nets, and DL-MHO hybrids showed over 99% fraud detection accuracy.	• The imbalance of the data is threatening the training of models. • Current ML models have the problem of data imbalance and scalability.
[115] 2025	• A systematic review of current and emerging intelligent systems for credit card fraud detection (CCFD). • Integrates supervised and unsupervised learning with real-time analytics for fraud detection.	• Data Preprocessing Methods • Feature Selection (FS) Methods • Classification Models (Supervised Learning - SL) • Emerging Techniques	• Combined resampling methods, such as SMOTEENN and SMOTETomek. • Using traditional oversampling (SMOTE) or undersampling (Tomek links, ENN) alone.	• Change in fraudulent behavior may not be reflected in the existing models. • Dynamic fraud detection cannot be detected using static models.
[42] 2024	Emphasizes AI's role in detecting fraudulent banking transactions using various classification algorithms to enhance accuracy.	• ML algorithms applied: Logistic Regression, Decision Trees, KNN, Naïve Bayes, Random Forest, Isolation Forest. • Metrics: Accuracy, Precision, Recall, F1-Score	• Logistic Regression showed the highest performance with the best AUC. • Hyperparameter tuning and preprocessing enhance model performance.	• Limited data used; findings may not generalize across all financial institutions or fraud types. • Real-time detection in high-volume conditions is an obstacle to adopting models.
[61] 2024	• Reviews the impact of AI, ML, DL, and blockchain on finance and banking. • Highlights AI integration with blockchain and emerging tech like quantum computing.	• Neural Networks and SVM used for scoring, fraud detection, and predictive modeling. • Deep Learning (CNN, LSTM) used for complex data analysis and behavior prediction.	• Uses CNN and LSTM for advanced data analysis. • Quantum computing tackles complex computational problems in finance.	• Certain ML algorithms, such as logistic, are sensitive to noise in the data. • Tree-based models are time-consuming.
[69] 2024	• Systematic review of AI/ML in banking: applications, benefits, limitations, and key algorithms. • Credit risk analysis and fraud detection are key AI/ML applications using RF, DT, SVM, and LR.	• adhered to the 2020 PRISMA guidelines as one of the systematic reviews. • Common algorithms: Random Forest, Decision Tree, SVM, Logistic Regression.	• AI/ML enhance customer segmentation and credit risk assessment in banking. • One important use of AI and ML is related to fraud detection.	• Narrow data sources, relying on only three databases (Dimensions, Scopus, EBSCOhost) and excluding others with relevant research.
[53] 2023	• AI-based fraud detection, using neural networks and deep learning, improves accuracy and speed in banking.	• NN, MLP, and CNN • Their accuracy: NN: 67.58%, MPL: 87.88%, CNN: 82.86%	• AI helped JP Morgan detect fraud, saving $120 million. • 96% accuracy in fraud detection.	• Data privacy and sensitive data handling.
[83] 2023	Proposes ML and data mining models for detecting online credit card fraud by analyzing data trends across digital platforms.	• logistic regression, random forest, and naive bayes. • precision, and recall.	• Achieves high accuracy with logistic regression and random forest. • Stresses ongoing research as fraud tactics evolve.	• Limited comparison of algorithms. • Real-life data are usually of a low quality.

TABLE 5. Comparison of Transaction Fraud-related works.

Ref and Year	Main Idea	Used Method	Findings	Limitations
[139] 2025	Explores Blockchain and AI in digital banking, highlighting fraud reduction and improved financial inclusion.	• Conceptual synthesis • Comparative analysis • Thematic analysis	Uses qualitative literature review to overview blockchain and AI in digital banking.	• Does not have quantitative data verification. • The secondary information can be bias or missing
[141] 2025	Examines fraud behavior using big data in credit card sales, noting rising scams in online and offline purchases.	• ML and DL Techniques. • supervised learning algorithms	Introduces ML methods to reduce false alerts and improve fraud detection in financial industries.	• Fraud detectors may have 50/50 false acceptance rates. • Traditional systems use 400 validation techniques.
[37] 2024	Addresses fraud detection processes in financial institutions using federated learning.	• Federated Learning (FL) model • Explainable AI (XAI) enhanced transparency	• Achieves 93% accuracy, showing strong training convergence. • FL boosts accuracy while preserving data privacy.	Problems with class distribution and comprehen sibility of results.
[85] 2022	• Highlights AI/ML approaches in cybersecurity for detecting financial fraud. • AI/ML applications in financial fraud detection.	• Supervised ML • DL structures	• Random Forest achieved 42.65 in detection and 82.94 in accuracy. • Major improvement in fraud detection.	• N/A
[19] 2021	Examines advanced AI methods for anomaly detection, trends, and risk reduction in financial fraud.	• Machine learning, deep learning, and unsupervised learning for financial fraud.	• Supervised and unsupervised methods effectively detect fraud. • Real-time scoring improved customer experience and efficiency.	• Deep learning models require intensive computation. • Supervised methods rely on high-quality labeled data.
[6] 2020	Proposes combining hybrid deep learning with Random Forest to enhance fraud detection, leveraging DL's data handling and RF's interpretability.	• Hybrid deep learning and Random Forest for financial fraud detection.	• Fraud detection accuracy increased by 20%. • False positives decreased by 15%. • Reduced false positives.	• Complexity in real-time. • High computational demand.
[9] 2020	Evaluates graph computing and ML methods (GNNs) for financial fraud detection.	• Graph computing for financial crime detection.	• Uncover hidden patterns and anomalies. • Provide flexibility, scalability, and relational reasoning.	• Lack of robust interpretability methods
[20] 2020	• Using ML-based AI systems for financial fraud detection in IoT environments. • Emphasizes advanced ML models (RF, SVM, NN).	• Using AI for IoT fraud detection using ML algorithms.	• SVM and Random Forest achieved over 90% accuracy in fraud detection. • Uncovered new fraud schemes. • Identifying complex fraud patterns.	• N/A
[21] 2020	Proposes a user-centered XAI approach using scenarios to improve trust and effectiveness in fraud detection systems.	• AI • ML	• Boosts detection system awareness and credibility.	• Needs further testing.

TABLE 6. Comparison of Money Laundering related works.

Ref and Year	Main Idea	Used Method	Findings	Limitations
[74] 2024	• To systematically review the integration of AI techniques into Anti-Money Laundering (AML) systems, focusing especially on Bangladesh's context and its goal of becoming a smart nation by 2041. • To critically assess the current state, risks, legal frameworks, and future directions of AI-driven AML.	• Various AI/ML techniques: supervised learning, unsupervised learning, clustering, classification. • Integration of graph analytics, neural networks, and other advanced AI approaches in AML workflows. • Comparative analysis across AI modalities applied to AML.	• Growing use of AI in transaction monitoring, customer due diligence, network analysis, and risk-scoring phases of AML. • AI enhances detection rates and reduces false positives compared to traditional rule-based systems. • Identified gaps in regulatory alignment, data privacy, and context-specific implementations (e.g., Bangladesh).	• The geographic focus is heavily on Bangladesh, limiting global generalizability. • Review extends only up to 2024; excludes very recent innovations (e.g., advanced deep learning architectures). • Reliance on published academic sources may omit proprietary systems used in industry. • Ethical, legal, and privacy issues are noted but not deeply explored.
[11] 2021	• To critically review how deep learning (DL) and explainable AI (XAI) are applied to detect money laundering. • Assess the current landscape, focusing on model types, interpretability, data usage, and future research directions.	• DL Architectures: Convolutional Neural Networks (CNNs), Autoencoders. • Graph Deep Learning (GNNs) is emerging, often combined with Natural Language Processing (NLP). • Traditional ML includes statistical methods, SVM, decision trees, and clustering.	• CNNs and Autoencoders are the most commonly used DL models. • Graph DL with NLP is gaining attention. • 51% of reviewed ML methods are non-interpretable, and none used advanced XAI. • 58% of studies rely on outdated real data. • Key challenges: lack of labeled data, highly imbalanced datasets, limited recent real-world data.	• Very limited application of XAI, leaving interpretability insufficient. • Heavy reliance on old or synthetic datasets. • Few industry-deployed systems. • Research focuses on classification performance, with less attention to real-time detection or operational deployment.
[9] 2020	• Investigate the application of graph computing and graph neural networks (GNNs) in detecting financial crime and fraud. • Provide a practical lens on challenges and considerations when integrating graph-based methods into real-time transaction systems.	• Graph Neural Networks (GNNs), including graph attention networks and temporal GNNs. • Techniques for handling dynamic graphs, memory-efficient graph representations, and graph compression.	• Graph methods outperform traditional rule-based systems in uncovering complex fraud through network and subgraph analysis. • GNNs can capture relational patterns effectively and support dynamic/flexible modeling.	• Performance and latency constraints due to real-time response requirements in financial systems. • Data quality issues, noise, adversarial manipulation, labeled data scarcity, and model robustness challenges.

combines blockchain applications along with machine learning capabilities to identify fraudulent insurance claims and track risks. The framework utilized a permissioned blockchain to ensure secure data sharing among participants [8]. The system implemented device-sharing transaction and buyer-seller graph structures to identify sophisticated patterns that lead to the discovery of fraudulent activities [10]. According to this study, both supervised and unsupervised learning algorithms provided different strengths for fraud detection, with Gradient Boosting Machines performing excellently in recognizing established patterns and K-Means Clustering and Isolation Forests detecting unknown schemes [15]. This research paper studied the application of GBAD methods across fraud detection literature. GBAD helps detect relationships between data points and spot patterns within linked datasets including social networks, banking systems, and insurance fraud cases [29]. This study developed an approach to detect auto insurance fraud through predictive models by analyzing a public car insurance database using the Boruta algorithm [40]. This study revealed multiple drawbacks of AI-based fraud detection methods due to integrity concerns about biased algorithms and

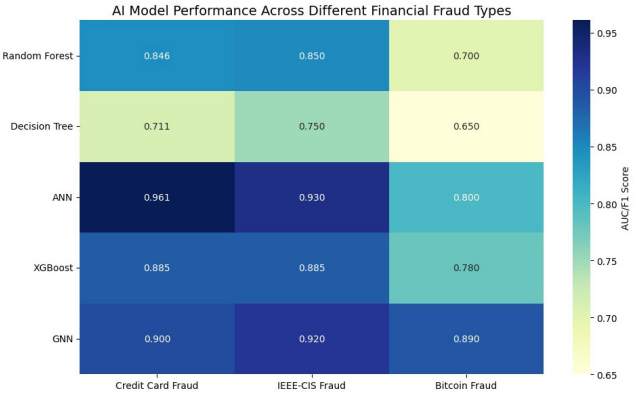

FIGURE 10. Performance Heatmap for Financial Fraud Detection.

system transparency problems that result in suspension of public trust and discrimination against specific population segments [58].

5) SECURITIES AND TRADING FRAUD

In securities fraud, people violate legal rules in financial markets to gain benefits by sharing wrong or misleading market details. Malign practices in securities trading harm investor earnings and threaten the market's honest operations. Several research articles demonstrate information on securities and trading fraud in Table 7.

6) COMPARISON OF MODEL EFFECTIVENESS

The performance of five AI models, Decision Tree, Random Forest, ANN, XGBoost, and GNN across three categories of financial fraud, credit card fraud, IEEE-CIS fraud, and bitcoin fraud is summarized in a heatmap shown in Figure 10. The findings are derived from three popular datasets: the Credit Card Fraud Detection Dataset (Kaggle; 284,807 transactions; creditcard.csv) [128], the IEEE-CIS Fraud Detection Dataset (Kaggle Competition; 590,000 transactions; train_transaction.csv, train_identity.csv) [129], and the Elliptic Bitcoin Transaction Dataset (Kaggle; 203,769 nodes; elliptic_txs_features.csv) [130].

Using a gradient color scheme, the heatmap shows lower performance with brighter yellow shades and higher AUC/F1 scores with darker blue shades. While GNN consistently performed well across all datasets, particularly in bitcoin fraud (0.890), ANN earned the highest score (0.961) in credit card fraud detection. This is probably because GNN can represent graph-based transaction data. The effectiveness of the decision tree was significantly lower, particularly when applied to the Bitcoin dataset (0.650). These results underscore the importance of selecting model architectures that align with the complexity and structure of the data. The heatmap also shows that performance differences are more noticeable in datasets with intricate network architectures, which are difficult for conventional models to handle.

B. AI TECHNIQUES

The taxonomy explores the AI methods used to solve financial fraud detection problems. The key to identifying fraudulent patterns is machine learning, which is divided into supervised and unsupervised learning. While recurrent neural networks (RNNs) and graph neural networks (GNNs) are used for sequential transactions and interconnected networks, respectively, deep learning techniques such as convolutional neural networks (CNNs) handle fraud detection in image-based or geographical data. Model-based and model-free techniques are part of reinforcement learning (RL), which adjusts to changing fraud trends. Stacking and ensemble approaches are examples of hybrid models that further improve detection capabilities by integrating numerous strategies for increased accuracy.

1) MACHINE LEARNING

Machine learning stands as the primary method of finding financial fraud patterns. Today, fraud detection systems use machine learning to work better by learning large datasets, detecting unusual activities, and doing this automatically. A significant number of research works have already been published based on machine learning models. We present some of them in Table 8.

This paper examined financial cybercrime through an investigation of criminal fraud tactics combined with a discussion on how machine learning (ML) and deep learning (DL) approaches protect against these offenses. The paper tracked the development of financial fraud from its inception to the effective measurement of anomaly detection strategies and current field obstacles [25]. In addition, further research revealed that machine learning approaches, including supervised and unsupervised methods, are widely utilized for anomaly discovery within procurement operations. Natural language processing proves to be successful when used for examining contractual text and uncovering problems. AI models provided better fraud activity detection capabilities through improved accuracy that reaches 25% higher than traditional methods. The results of the review showed how AI systems are linked with blockchain-based technology to build a strong institutional approach to prevent procurement fraud while maintaining data transparency and permanence [30]. The authors presented a distributed deep forest model built through the parameter server system. This system worked as a specific solution designed to handle extensive machine learning operations used in industrial applications, including fraud detection [101].

a: UNSUPERVISED LEARNING

Machine learning systems learn by studying unlabeled data, data without information showing which answers are correct. In Table 9, we compare some related works on unsupervised learning.

The research findings in [17] showed that random forests, together with support vector machines (SVM), along with

TABLE 7. Comparison of Securities and Trading fraud related works.

Ref and Year	Main Idea	Used Method	Findings	Limitations
[135] 2025	Proposes an Explainable Federated Learning (XFL) model to overcome the limits of rule-based and centralized AI in detecting evolving fraud patterns.	• Proposes an Explainable Federated Learning (XFL) model for financial fraud detection. • Combines privacy-focused Federated Learning (FL) with XAI methods like SHAP and LIME.	• XFL achieved 99.95% accuracy and 0.05% miss rate, outperforming AE (81.6%), VAE (93.8%), and FL+ID3 (89%).	• Data heterogeneity may reduce model generalization. • The current models are unexplainable and opaque.
[136] 2025	• Proposes a fraud detection system using Federated Learning (FL) and Explainable AI (XAI). • Highlights data sharing challenges due to strict data protection laws.	• Introduces a fraud detection approach combining Explainable AI (XAI) and Federated Learning (FL). • AI-based method for detecting unlabeled fraud in bank cybersecurity.	• FL-based fraud detection system performs well in most cases. • XAI (SHAP) ensures model decisions are transparent and interpretable.	• Traditional systems risk exposing confidential customer data. • Struggle to adapt to evolving fraud patterns in datasets.
[142] 2025	• Explores AI's rising role in combating fintech fraud amid growing digital threats like identity theft and payment fraud.	• Compares different AI-based fraud detection methods. • Examines supervised and unsupervised learning models.	• AI enhances accuracy and efficiency in fintech fraud detection. • Deep learning outperforms rule-based systems in detecting complex fraud schemes.	• AI systems may reflect dataset biases, causing demographic discrimination. • Neural networks require significant computational resources for training.
[60] 2024	• Showcases successful cases like reduced identity theft and insider trading using AI/ML. • Analyzed key AI and ML techniques used for fraud detection.	• Fraud detection uses various AI and ML methods. • Decision Trees are common supervised learning tools for fraud detection.	• Wells Fargo's AI system cut identity theft losses by 40%. • AI enhances security, reduces costs, and improves reliability in digital banking.	• Data quality issues. • Strong data governance is essential for clean, reliable training data.
[61] 2024	Reviews AI, ML, DL, and blockchain applications and their significant impact on innovation and efficiency in finance and banking.	• Analysis of AI, ML, deep learning, and blockchain in financial banking.	• AI enhances decision-making, innovation, and operational excellence, as highlighted in the paper.	• N/A
[49] 2023	• Highlights the increasing importance of AI in fraud detection. • AI improves fraud detection and customer trust, enhancing security.	• Analyzes supervised, unsupervised, and deep learning methods for fraud detection in financial products and services.	• GBM achieved the highest accuracy at 98.1%. • Random Forest followed with 97.4% accuracy. • LSTM reached 96.9% accuracy.	• LSTM models are very data-team sensitive. • LSTM models struggle with scarce or unstructured data.
[18] 2019	Expert-guided scenarios improve early fraud detection and explanation in banking systems.	AI uses behavior analysis, biometrics, anomaly detection, and ML to enhance fraud and money laundering detection.	• Explainable AI improves transparency in fraud detection tools.	• N/A

TABLE 8. Comparison of machine learning related works.

Ref and Year	Main Idea	Used Method	Findings	Limitations
[149] 2025	Proposes a scalable AI-microservices framework for real-time fraud detection and cybersecurity.	• conceptual review • Java Spring Boot	• AI enables real-time anomaly detection and fraud prediction.	• No empirical performance metrics. • Security and privacy implications
[133] 2025	Highlights how digitalization changes fraud patterns, making conventional detection systems ineffective.	• SHAP offers consistent model-specific explanations. • LIME creates simplified proxies for the complex behavior of models.	• AI improves fraud detection in international transactions. • Stakeholder collaboration boosts fraud detection success.	• False positives increase operational costs. • Delayed detection causes greater financial losses.
[145] 2025	Examines AI and ML trends in financial fraud detection, highlighting the need for advanced frameworks and real-time analytics.	• Uses bibliometric analysis with VOSviewer and Biblioshiny tools.	• Traces AI and ML trends in fraud detection. • Shows ML integration enhances fraud detection.	• ML-focused studies overlook emerging technologies like quantum computing.
[55] 2024	• Reviews recent ML and AI approaches outperforming rule-based fraud detection. • Discusses real-world impacts and future research for improving fraud detection systems.	• Reviews ML/AI advancements over rule-based fraud detection and future research directions.	• LR achieved 92% accuracy and 89% precision. • Decision Trees achieved 94% accuracy, 91% precision, and 0.96 AUC-ROC. • SVM achieved 93% accuracy and 90% precision.	• Data Quality issues.
[25] 2021	• Explores types of financial fraud and how ML/DL detect and prevent evolving cybercrimes.	• Using ML and DL for financial cybercrime detection.	• Compares deep learning anomaly detection methods and highlights rising demand for GAD in identifying malicious financial actors.	• Reliance on preprocessing techniques. • ML/DL models rely on preprocessing and contextual data, making practical use challenging.
[30] 2020	• Presents a systematic review on using AI to detect and prevent corruption in procurement. • AI analyzes procurement data to detect anomalies, manage risks, and enhance transparency.	• Anomaly detection in procurement is widely done using supervised and unsupervised ML methods.	• AI models show up to 25% higher accuracy in fraud detection than traditional methods. • AI and blockchain integration strengthens fraud prevention in procurement.	• N/A
[101] 2019	Proposes a distributed deep forest model implemented via a parameter server system.	Focuses on large-scale ML for fraud detection using MART as base learners with efficiency improvements.	• Outperformed current methods in fraud detection (AUC=0.9997). • The model outperformed existing methods in detecting cash-out fraud at Ant Financial, achieving higher AUC, F1-Score, and KS-Score.	Needs further study on regression and multi-class tasks.

unsupervised clustering and dimensionality reduction methods, succeed in detecting different fraud patterns. The hybrid machine learning approach provided vital improvements to the accuracy of fraud detection along with enhanced operational productivity over standard fraud-detecting systems [51].

b: SUPERVISED LEARNING

A machine learning approach called supervised learning trains the model to use data that is called labeled data. Data consists of input features along with their corresponding accurate output (label). In Table 10, we present a comparison of related works on supervised learning.

The paper investigates the application of AI-enhanced data engineering techniques for real-time fraud detection in digital transactions. The system integrates machine learning instruments with advanced data purification and streaming analysis tools to detect fraud patterns promptly with reliable precision [12]. The study showed that supervised learning models, such as Gradient Boosting Machines, could perform well in identifying established fraud patterns with high precision, while unsupervised learning models such as K-Means Clustering and Isolation Forest could have better results in detecting new frauds [15]. In particular, the study showed that supervised learning models such as Random Forest and SVM obtained the best accuracy rate on the fraud detection task, above 90% in most cases, and performed better in separating fraudulent and legitimate transactions [20].

2) HYBRID MODELS

Fraud detection models using hybrid approaches combine various machine learning and deep learning techniques to leverage the strengths of each and improve the overall performance and precision of fraud detection systems. In hybrid methods, the goal is to integrate different approaches, such as supervised, unsupervised, or ensemble techniques, to enhance the ability to detect complex patterns and fraud in transaction data. This research paper focuses on integrating hybrid deep learning models with the random forest algorithm for financial fraud detection. The proposed approach harnesses the strengths of deep learning models in processing high-dimensional data, while utilizing the interpretability and decision-making capabilities of random forests [6]. In particular, the review showed that the COVID-19 pandemic had fueled a huge upsurge in fraudulent activities, with a global financial loss for 2023 reaching $34 billion. The most effective hybrid models were found and scored the highest accuracy at 99.38% [75].

a: MODEL STACKING

Stacked generalization (model stacking) is an ensemble learning technique that combines several models in order to improve prediction accuracy. Basically, you train a bunch of base models with the same dataset and then use another (meta) model called a stacker (or a stacker) to combine the output of your models into a single output. This allows us to take advantage of the strengths of different models and also reduce over-fitting and improving generalization.

b: ENSEMBLE MODEL

Machine learning paradigm that combines several models, or ''learners,'' to improve the predictive performance of an overall 'system' The basic idea is that the ensemble of various models produces a better generalization (result) than any single model, this is specifically true for the complex problems with the assistance of data like fraud detection. Ensemble methods are very powerful in specific fields, such as financial fraud, where the pattern of fraud is often tricky, diverse in variety, and complicated.

3) DEEP LEARNING

While working with large data groups, deep learning finds simple connections using neural networks with multiple layers. Deep learning works well in finding fancy types of fraud by understanding how data is linked in complicated ways. In Table 11, we provide a comparative analysis of related studies on deep learning.

The research used deep learning methods to find financial statement fraud, combining financial statement ratios with textual analysis of Management Discussion and Analysis sections in annual reports using HAN [7]. The research demonstrated how AI-powered database management systems modify both FinTech transaction speeds and fraud detection capabilities. The main goal explored how machine learning together with deep learning alongside natural language processing enhances fraud detection while improving transactional processes [22].

a: CNN

CNNs work like a deep learning system that handles grid-like data, especially images, and can help spot financial fraud when looking at patterns in data and location information. One research showed that hybrid deep learning networks and Random Forest techniques improve the effectiveness of financial fraud detection. They combined deep learning models for handling big data with Random Forest to make better decisions about financial fraud detection and also created a dual-purpose model using CNN and LSTM networks to recognize transaction patterns across different time points and location types [6]. The proposed system mixed AI technologies such as CNNs for face and fingerprint verification along with unsupervised learning to spot irregular patterns of user activity [24].

b: GNN

GNNs work better than regular neural networks with square or line data by handling connections between objects in graphs, which helps spot fraud in the detailed web of money transfers. A paper studied how GNNs and graph machine

TABLE 9. Comparison of unsupervised learning related works.

Ref and Year	Main Idea	Used Method	Findings	Limitations
[138] 2025	• Identify anomalous patterns without labeled datasets. • AI-driven frameworks for unsupervised fraud detection in banking cybersecurity.	• Clustering(e.g., k-means), Graph-based analysis, autoencoder, NLP. • IoT security integration.	• Quantitative results show precision of 87%, recall of 82%, F1-score of 84%. • Frameworks enhance detection capabilities through NLP and graph theory integration.	• Lack of empirical validation using real-world banking data.
[147] 2025	• AI enhances fraud detection and cybersecurity.	• Deep Learning, ML. • Federated learning, • Explainable AI.	• Accuracy and adaptability. • Privacy and regulatory risks.	• Limitations of industrial deployment. • Lack of real-world regulatory.
[51] 2023	• Used Hybrid ML models for advanced fraud detection in digital banking. • Focus on combining real-time anomaly detection and customer behavior analysis.	• Supervised learning (e.g., Random Forest, SVM). • Unsupervised techniques (e.g., Isolation Forest, Autoencoders). • Synthetic data generation like SMOTE.	• Hybrid models improve accuracy and efficiency • Random Forest + Autoencoder, this combination showed strong detection rates. • Performance metrics accuracy, precision, recall, F1 score, and AUC-ROC were computed and showed robust performance	• Complex and resource-intensive banking infrastructure. • Face challenges in real-time deployment due to computational complexity.
[19] 2021	• Explore how AI can modernize financial fraud detection by overcoming the limitations of rule-based systems. • emphasizes anomaly detection, risk mitigation, and pattern recognition using AI.	• Supervised techniques (SVM, Random Forest, Gradient Boosting) for known-fraud classification. • Unsupervised approaches (K-Means, DBSCAN) for discovering outliers. • DL architectures (ANNs, CNNs, RNNs) for complex pattern recognition.	• Supervised and unsupervised approaches are feasible for fraud detection. • High accuracy and precision in identifying fraudulent transactions when labeled data was available by SVM, Random Forests, and Gradient Boosting. • K-Means, DBSCAN were effective in detecting anomalies in unlabeled data.	• Demand-driven by high-quality data. • Missing discussion on privacy, ethical governance, standards, and compliance. • Computational complexity of deep learning models, and the limited model transparency. • Smaller institutions may face resource constraints in adopting these advanced technologies.
[17] 2020	• Focuses on AI-based fraud detection in E-commerce. • Different techniques like anomaly detection, transaction monitoring, and risk mitigation are described	• ML models for anomaly detection. • Unsupervised algorithms scanning failed logins, unusual purchase behavior. • Behavioral analysis is used to detect user behavior anomalies during transactions.	• Hybrid use of Supervised and unsupervised learning are effective for fraud detection. • Real-time AI monitoring to improve detection of suspicious patterns like unusual purchase amounts, login abnormalities.	• Requires large amounts of high-quality labeled data. • Real-time adaptation challenges. • Limited public availability of the dataset.

learning methods can detect financial crime and fraud patterns in data. Graph-based analysis efficiently reveals the connections between transactions and helps us locate unusual patterns, track fraudulent groups, and identify money laundering schemes [9]. Another research examined how graph computing technology and machine learning with a special focus on GNNs helped detect financial crimes and fraud. Graph-based methods showed how different financial activities are connected to spot abnormal patterns and help stop criminal financial networks [9].

TABLE 10. Comparison of supervised learning related works.

Ref and Year	Main Idea	Used Method	Findings	Limitations
[140] 2025	• Big data in credit card transactions is used in online and offline purchases .	• Hybrid ML model (anomaly detection + DNN classification). • Stream processing, scalability via big data framework.	• 98% fraud detection, low 0.3 FP, real-time detection under 20ms.	• Traditional methods . • Data privacy concerns.
[143] 2025	• Discusses AI-driven models for detecting financial fraud effectively. • Enhances security and reduces financial losses with predictive analytics, ensuring adaptive defenses against evolving fraud tactics.	• AI with blockchain. • Convolutional Neural Networks (CNNs).	• Real-time fraud detection and reduce false positives. • Explainability tools like SHAP values. • CNNs identify fraudulent activities. • Integration of AI with blockchain enhances financial security.	• Data privacy concerns hinder effective AI deployment. • Adversarial threats pose risks to AI-driven systems. • Scalability issues complicate handling large transaction volumes
[146] 2025	• Integrate AI and Big data analytics Focus on two key functions risk assessment and fraud detection.	• ML model (predict risk analysis and anomaly detection). • DL architectures (complex fraud signals).	• Real-time transection monitoring. • Improves security and reduces losses.	• Integration with legacy systems is complex and costly.
[20] 2020	• Explore how machine learning–driven AI can detect financial fraud within IoT environments. • Highlight real-time monitoring and adaptive learning to handle the high-volume, heterogeneous data streams from IoT devices.	• Supervised learning: classification on labeled historical IoT transaction data. • Unsupervised learning: anomaly detection and clustering to uncover novel fraud patterns. • Clustering + classification pipeline, with adaptive learning and frequent retraining.	• ML-driven AI can distinguish legitimate vs fraudulent transactions in real time within IoT ecosystems. • Pipeline techniques like feature selection and adaptive retraining improve accuracy and adaptability.	• The paper is conceptual; it lacks empirical implementation results or live deployment metrics. • Datasets and evaluation metrics are described in the abstract only—no performance figures (e.g. precision, recall) are provided.
[15] 2019	• Investigate advanced AI methods for detecting fraud in travel insurance.	Systematic review of AI techniques applied to travel insurance fraud.	• Supervised models • Unsupervised techniques	• No empirical validation or performance metrics provided.

c: RNN

RNNs are an essential tool in three important areas - speech recognition, language modeling, and fraud detection, making it possible to understand transaction sequences and identify fraudulent patterns as they evolve. The paper studied how computer-based systems could help reduce fraudulent insurance claims in medical settings. The paper showed traditional rule-based systems weren't strong enough anymore and introduced different machine learning and deep learning methods, such as supervised learning and deep learning models, that could improve results [16].

4) REINFORCEMENT LEARNING

Unlike supervised or unsupervised learning, RL does not teach the model from the data instead it must learn through trial and error. Therefore, the agent explores actions and updates its strategy based on rewards received by it in such environments where the system needs to learn more over time from new environments.

Reinforcement learning has received interest in fraud detection because it is able to adapt its performance and continuously improve as new fraud patterns emerge. In environments where fraud detection systems need to respond in real-time to constantly changing fraudulent tactics and strategies, it serves its utility.

C. FINANCIAL NETWORK COMPONENTS

The taxonomy takes into account the organizations that detect fraud and emphasizes their functions within the larger financial system. As the backbone of financial systems, banks

TABLE 11. Comparison of deep learning related works.

Ref and Year	Main Idea	Used Method	Findings	Limitations
[131] 2025	Adopts AI with ML/DL to enhance real-time fraud detection using big data, predictive analytics, XAI, and bias mitigation.	• literature review	• Enhance predictive accuracy and throughput. • Effectively uncovers complex fraud transactions.	• Data privacy, regulatory compliance, and model interpretability.
[144] 2025	Proposes a hybrid MoE model using RNNs, Transformers, and Autoencoders for detecting anomalies in decentralized transactions.	• RNN • Transformer encoders • Autoencoders	• Achieved 98.7% accuracy, 94.3% precision, and 91.5% recall • Hybrid model outperformed standalone approaches.	• Explainability and model interpretability aspects remain underexplored. • Scalability and latency in production.
[132] 2025	Develops a GNN-based fraud detection system with XAI for transparency, addressing regulatory and compliance needs.	• GNN • XAI • Integration of risk mitigation strategies	• Improves trust and regulatory compliance. • Enhances detection accuracy and risk management.	• Compliance challenges. • Dependence on high-quality and comprehensive transaction data.
[134] 2025	Evaluates AI methods for banking fraud detection, proving superiority over rule-based systems.	• Descriptive and comparative analysis • ML, and DL	• Improved precision, speed, and adaptability. • Addressed transparency, fairness, and accountability.	• Lacks detailed empirical performance metrics.
[79] 2023	• Utilizes a graphical and qualitative review approach. • Review and analyze AI-based cyber threat intelligence (CTI) within the banking sector.	• Machine Learning(patten recognition,identify anomalies). • Internet of Things(Security purposes IoT devices). • Deep learning(NLP applied to threat intelligence, advanced intrusion detection process).	• Steady rise in AI applications for cyber threat intelligence Gence. • Effectiveness of various ML methods for fraud detection. • Actionable intelligence that informs decisions and responses to threats.	• Significant gap in AI usage in African banks. • Limited investigation into deep learning methods. • Class imbalance in fraud detection
[84] 2022	• Explore the rising problem of fraudulent credit card transactions. • Using Deep learning for credit card fraud detection. • Inherent challenges in accurately detecting these fraudulent activities.	• K-Nearest Neighbors, Naive Bayes, SVM, Binary Classifiers, deep Neural Network classifier. • Generate credit-card fraud dataset. • GAN-generated synthetic data	• Optimal performance is achieved. • Combined model trained with data from GANs. • Offered a more transparent assessment than traditional accuracy measures.	• Imbalance in datasets. • Complex structure of differentiate between fraudulent and genuine transactions.
[7] 2020	• Investigates financial statement fraud detection using deep learning. • Propose HAN model and integrate two types of features, financial ratios, and Textual features analysis of managerial language in annual reports.	• Preprocess structured data in financial ratios and unstructured data MD&A sections. • Implement HAN: LSTM encoder+attention at word and sentence levels to model text hierarchy. • FIN+TEXT features.	• Architecture gives strong classification performance when text features are included. • Provides interpretable "red-flag" sentences that provide actionable insights for auditors, enhancing the practical utility of fraud detection tools.	• N/A

are vulnerable to a variety of fraud risks, such as identity and transaction fraud. Payment processors deal with financial data in real time; therefore, they need strong AI solutions to identify anomalies. The different operating frameworks of the cryptocurrency platforms and credit unions complicate efforts to detect fraud. These elements work together to create the framework that AI-driven systems need to function well in order to prevent financial crime.

1) BANKS

The central institution in the financial network is the banks and they perform transactions, lending, depositing, and various other financial services. In particular, they are especially prone to a variety of forms of fraud, such as identity theft, transaction fraud, and account takeover, among other things. Sensitive financial data are being processed by both individual and corporate clients in the hands of banks, so they have to make sure that their systems are fit for detecting fraudulent actions. The paper proposed a conceptual model to enhance detection of credit card fraud by banks using artificial intelligence, data mining, and geolocation techniques. It discussed how AI leveraged real-time transactional data analysis, identified patterns, and learned to adapt to the emergence of fraud, thereby increasing accuracy in fraud detection and reducing the number of false positives [110]. Effect of the COVID-19 pandemic on the banking sector: Adoption of artificial intelligence and machine learning technologies is examined in the banking sector. A SWOT analysis is conducted to assess the strengths, weaknesses, opportunities, and threats of AIML implementation in banks [76].

2) PAYMENT PROCESSORS

Payment processing works as a middleman between a merchant, their customer, and financial institutions. In real time, they complete financial transactions so they have to be part of fraud detection. Due to the volume of transactions they process, they need robust fraud-checking systems to catch fraudulent payments and protect financial information.

3) CREDIT UNIONS

A credit union is a member-owned financial institution that provides value similar to that of a bank. Usually, they serve smaller communities or special groups, and offer more personalized services. Although they aren't as busy processing transactions as large banks, credit unions can fall victim to credit card fraud, account takeovers, and loan fraud.

4) CRYPTOCURRENCY PLATFORMS

Services that handle the storage and exchange of cryptocurrencies such as Bitcoin, Ethereum, and other digital currencies include both cryptocurrency platforms (exchanges, wallets, and trading platforms). Since the anonymity of cryptocurrency transactions and decentralized structure, these platforms are highly prone to fraud like money laundering, phishing, and fraudulent trades amongst others. The paper surveyed techniques of data mining applied to financial fraud detection from 2009 to 2019. It identified and categorized financial fraud, covering credit card fraud, cryptocurrency fraud, insurance, and financial statement fraud, and evaluated the performance of 34 data mining techniques [28].

D. FRAUD DETECTION METRICS

When assessing the effectiveness of AI models employed in fraud detection, metrics are essential. According to the taxonomy, accuracy, precision, and recall are crucial indicators of a model's capacity to distinguish between fraudulent and legitimate activity. Furthermore, a model's false positive rate is a crucial metric for assessing its dependability since it makes sure that legitimate transactions aren't inadvertently reported, which could cause disruptions and erode client confidence. In Table 13, we mention performance detection metrics used in the existing study.

1) FALSE POSITIVE RATE

A fraud detection model's error rate for normal transactions shows FPR by identifying genuine purchases as fraudulent. The reliability of a fraud detection system depends on FPR evaluation because excessive error rates disrupt customer service and compromise system trust. The research showed predictive AI improved fraud detection while lowering error rates and reacting faster to changing fraud techniques. The research highlighted how supervised and unsupervised models worked together with hybrid methods along with Apache Kafka and Spark Streaming for real-time analytics to reach optimal fraud detection results [109]. When false positive rates are high, they force legitimate customers to deal with frustration and can destroy their faith in the system. Keeping low false positive rates helps to ensure that our model remains reliable for users and works correctly.

2) RECALL

A fraud detection model identifies true fraud occurrences through its recall measurement. High specificity evaluation demonstrates that the model effectively identifies real fraudulent transactions which need urgent action. When a system finds most of the existing fraud events it helps companies stop financial losses and lower their exposure to risk. This measure is of special importance when fraudulent activities that are incorrectly disregarded would cause serious problems.

3) PRECISION

The PPV metric examines whether our fraud detection model correctly identifies fraudulent transactions from its total findings. Precision shows how well faulty purchases get detected from total flagged transactions by preventing incorrect warnings. When detection accuracy is high investigators receive fewer incorrect alerts to review and make fewer mistakes in their investigations. An effective fraud detection system needs to be built to achieve good accuracy without missing true cases.

TABLE 12. Performance detection metrics used in the existing study.

Metrics	Formula	References
False Positive Rate	$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}}$	[109], [6], [24], [54], [65], [66], [91]
Recall	$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$	[10], [12], [13], [32], [36]- [38], [41], [43], [45], [49], [51], [55], [88], [90], [94], [99], [105], [106], [137]
Precision	$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$	[10], [12], [13], [19], [24], [27], [32], [36]- [38], [41], [43], [45], [49], [51], [55], [56], [71], [88], [90], [91], [94], [96], [99], [105], [106], [137]
Accuracy	$\text{Accuracy} = \frac{\text{TN} + \text{TP}}{\text{TN} + \text{FN} + \text{FP} + \text{TP}}$	[6], [8], [12], [13], [20], [28]- [30], [32], [37], [38], [41], [45], [49], [51], [53]- [55], [65], [75], [82], [85]- [90], [96], [99], [104], [105], [106]

4) ACCURACY

The accuracy score assesses how well a fraud detection system works by showing what percentage of transactions it recognizes correctly. When accuracy evaluates models across large datasets it shows overall precision but fails to detect problems that appear when fraud instances are scarce. It shows how well the model functions overall. In large datasets that heavily favor real transactions this evaluation technique may not deliver reliable results.

E. LEGAL AND ETHICAL CONSIDERATIONS

It is critical to address ethical and legal issues as AI solutions are used more and more in financial fraud detection. Given the sensitive information involved in financial transactions, data privacy is a major concern. To guarantee impartial and equitable detection systems, bias in AI algorithms needs to be reduced. Adherence to legal norms requires regulatory compliance, and accountability mechanisms must be put in place to hold stakeholders accountable for the results of AI implementations.

1) DATA PRIVACY

Keeping customer personal data safe is very important when making financial fraud systems because they store and handle information like who they are and their purchases. Data privacy efforts must happen to protect personal info and meet rules like GDPR and CCPA, or customers won't trust you. To keep data safe, we use encoding to hide information, unlink data to people, and store everything correctly.

2) BIAS IN AI MODELS

Biased or insufficient data might occasionally make AI models used for fraud detection unfair. Historical injustices are frequently the source of these biases. We must employ representative, varied data and test the models frequently to ensure equity. Explainable AI contributes by encouraging openness and fairness for all.

3) REGULATORY COMPLIANCE

To work properly AI fraud detection systems must follow all necessary legal rules. Companies need to follow data privacy rules and sector rules plus separate rules for each location. When companies do not meet legal requirements, they may face monetary penalties plus damage to their reputation. Companies need to partner with lawyers to keep sound records while making sure their models provide clear explanations that external groups can accept.

4) ACCOUNTABILITY

Stakeholders must accept responsibility for AI system results including unexpected outcomes to make accountability work. Every part of this system needs clear job definitions to work properly.

F. FRAUD DETECTION APPROACHES

This section examines the methods for identifying fraudulent activity. While graph-based detection uses networked data to find fraud rings or related activity, anomaly detection finds departures from typical behavior. To find links between fraudulent entities, social network analysis is utilized. Density-based methods and rule-based systems offer organized frameworks for spotting trends that point to fraud. These methods serve as the cornerstone of all-inclusive fraud detection systems and are frequently enhanced by AI techniques.

1) ANOMALY DETECTION

Anomaly detection systems find transaction behaviors that differ markedly from normal patterns. It helps identify fraud methods beyond those with clear historical patterns. This system hunts for unusual transactions that might represent fraudulent actions because fraud patterns remain unknown. Detecting anomalies helps security teams find suspicious activities at the beginning and this process works well together with other methods for better fraud detection. The research presented an in-depth look at financial cybercrime while exploring both ML and DL technologies for recognizing and stopping criminal tactics. The research showed how financial fraud techniques have evolved over time along with how anomaly detection methods succeed and fail to fight cyber fraud in finance [25]. Also, another research analyzed how graph-based anomaly detection methods help detect fraud activities. GBAD better showed how to handle

complex links between items and spots hidden designs in grouped information from various domains [29].

a: DENSITY-BASED APPROACHES

Data density regions help density-based systems detect anomalies in their analysis. Fraud tracks clearly show up among scattered normal transactions because data points are far apart. These methods can locate natural groupings of acceptable conduct and easily identify suspicious behavior when used with large datasets.

b: STATISTICAL MODELS

Statistical models find unusual behaviors by mathematically studying data to see if results differ from standard patterns. These statistical tools establish certainty levels for what should be viewed as regular behavior. When data matches these limits system designers detect probable fraud. Statistical models offer basic fraud detection methods that run well but fail to adapt to sophisticated changing fraud schemes.

2) RULE-BASED SYSTEM

A rule-based system depends on set rules and limit values to spot fraudulent transactions. The system uses established rules from experts and recognizers of past fraud patterns to detect suspicious activity. The system marks transactions for review when they breach one or more established rules. The simple design and deployment of rule-based systems make them straightforward to use yet their set rules struggle to spot emerging fraud methods and need regular updates to help catch new fraud tactics. The research looked at how GNNs and graph machine learning helped detect financial crimes and fraudulent activities. Graph-based methods effectively recognize relationships and patterns in financial transactions, allowing them to identify unusual transactions and uncover money laundering schemes [9]. Another research analyzed how artificial intelligence algorithms help financial systems better find fraudulent activities. It integrated machine learning Gradient Boosting and Random Forest systems with special data preparation methods to create an automated fraud spotting platform. The AI-powered solution worked better with new fraud patterns and helped businesses reduce both false alarms and traditional fraudulent detection issues [13].

3) GRAPH-BASED DETECTION

Using graphs helps experts find secret links between bank accounts, users, and their transactions. When we understand how transactions connect different accounts we can spot organized criminal groups and coordinated attacks better. This method spots linked criminal activities better than basic detection approaches because its network analysis points out hard-to-find connections in financial crimes. The paper presented InfDetect which is a large-scale graph-based system that finds e-commerce insurance fraud. The system found fraudulent behavior by studying multiple graph types including traffic, connection sharing, and trading records [10]. The evaluation revealed that graph-based models combined with autoencoders and multi-channel CNN algorithms help detect suspicious commercial activities precisely. The study showed that graph convolutional networks captured transaction relationships well while autoencoders detected weak export pattern differences [11].

a: SOCIAL NETWORK ANALYSIS

By mapping the links between network members, Social Network Analysis (SNA) improves graph-based fraud detection by exposing hidden linkages that conventional transaction monitoring could miss. SNA can detect complex schemes like money laundering and organized financial crimes by examining relationships and identifying fraud clusters and linked fraudulent companies. SNA identifies patterns across several entities, revealing collusive behaviors and unusual connections, in contrast to rule-based systems that concentrate on individual transactions. By taking a comprehensive approach, financial institutions may better monitor illegal activity and reduce risks by proactively spotting and dismantling fraudulent networks before they do serious harm.

4) BEHAVIORAL ANALYTICS

Behavioral analytics studies what users normally do so it can detect changes that might mean someone is being dishonest. Our system records a user's typical actions and helps us find unusual events like transactions beyond the norm or unexpected device usage locations. The suggested model tracked customer spending anomalies by processing data with real-time analytics methods and non-linear regression stats. Also, the model helped customers identify their new spending patterns without depending fully on past records [110]. Another biometric authentication system combined AI technology to evaluate facial expressions and fingerprints with unsupervised algorithms that spot behavior changes [24].

a: PATTERN RECOGNITION

Behavioral analytics tools detect stable patterns in user activities as they happen over multiple days. The system detects normal user activities by studying their transaction orders and other behavior-tracking information. When normal behavioral patterns are known the system detects unusual activity. By recognizing unique user actions this technique finds uncommon changes like sharp spending increases or surprising transaction locations.

b: USER PROFILING

The system builds complete user profiles by combining past behavior and taste information. New data keeps updating this profile so that the system can respond better to user changes. The system uses user profiles to notice unexpected purchase actions that look like fraud. The method increases fraud detection performance by taking into account each user's specific details, which helps spot suspicious actions better.

TABLE 13. Overview of AI models and their applications in financial fraud detection.

Ref and Year	Proposed Model (s)	Implementation/Usage
[123] 2022	Logistic Regression, Decision Tree, Random Forest with PCA and Undersampling	Practical experimentation on payment datasets
[124] 2022	Autoencoders, One-Class SVM, Clustering, Isolation Forest	Theoretical analysis and literature survey
[125] 2024	Generative AI, Large Language Models (LLMs), FraudGPT	Conceptual discussion with emerging use cases

VI. INDUSTRIAL APPLICATIONS OF AI IN FINANCIAL FRAUD DETECTION

The use of artificial intelligence (AI) in identifying and stopping financial fraud has grown more crucial as a result of Industry 4.0's quick development and the broad acceptance of digital financial services. Several academic studies about financial fraud in industry and industry reports emphasize how AI is revolutionizing actual financial systems.

These advancements are supported by industry insights in addition to academic research. AI is currently a key component of banking companies' fraud detection methods, per a 2025 Forbes Tech Council article. Machine learning algorithms can identify unusual transaction patterns using behavioral analytics, allowing for early intervention and customer protection [126]. In a similar vein, IBM (2024) talks of integrating AI into end-to-end fraud management systems, emphasizing features like adaptive learning, real-time risk scoring, and document verification based on natural language processing [127].

VII. ISO STANDARDS IN FRAUD DETECTION

Financial institutions gain from quicker transactions, greater market access, and improved customer service as they become more integrated in the digital economy. But there are also significant drawbacks to this integration, with fraud being a big issue. Financial security is increasingly at risk from sophisticated threats such as identity theft, transaction fraud, money laundering, and cyberattacks.

To address these risks, international organizations have developed standardized frameworks like ISO standards. These give financial organizations instructions for implementing efficient fraud detection, guaranteeing regulatory compliance, fostering client trust, and minimizing financial losses.

In Table 14, every standard is described together with its particular uses, application range with role, and special function in identifying and stopping fraud. Our paper focuses exclusively on three ISO standards: ISO 8583 for card-based transactions, ISO/TR 22239 for financial crime risk management, and ISO/IEC 27001 for information security.

VIII. OPEN ISSUES AND CHALLENGES

In this section, we outline several open issues and challenges associated with AI-driven fraud detection models in Financial Networks. These challenges are summarized as follows.

- **Evolving Fraud Patterns:** With the use of cutting-edge technology, such as deep fakes, synthetic identities, and cross-platform tactics, financial fraud schemes have become more complex. Continuous model retraining and updates are necessary, as AI algorithms trained on historical data often find it difficult to adjust to these rapidly changing fraud tendencies.
- **Imbalanced Datasets:** A small percentage of financial data is made up of fraudulent transactions, which causes the datasets to be extremely unbalanced. AI algorithms are less able to identify infrequent but crucial fraudulent activity as a result of this imbalance, which favors non-fraudulent cases. It is still difficult to develop methods for dealing with unbalanced datasets.
- **Interpretability of AI Models:** Many advanced AI techniques, such as deep learning, operate as ''models with limited explainability,'' making it difficult to explain their decision-making processes. This lack of interpretability creates challenges in regulatory compliance, auditing, and gaining stakeholder trust. Developing interpretable models without compromising accuracy is a pressing concern.
- **Balancing Fraud Detection Metrics:** Many fraud detection systems suffer from high false positive rates, leading to operational inefficiencies and customer dissatisfaction, requiring better precision and recall balancing.
- **Regulatory Compliance and Ethical Concerns:** Ensuring regulatory compliance and maintain user privacy while using AI-based fraud detection remains a challenge, particularly with increasing concerns about AI bias and accountability.
- **Limitations of Current Fraud Detection Approaches:** The effectiveness of fraud detection approaches like anomaly detection, graph-based detection, and behavioral analytics is limited by evolving fraud techniques that can evade existing models, necessitating continuous updates and improvements.
- **Scalability of AI Models:** Massive amounts of real-time financial transactions across international networks must be handled by fraud detection systems. A recurring problem is making sure that AI models continue to be effective and scalable in such demanding circumstances without sacrificing latency or accuracy.
- **Bias and Fairness:** AI algorithms can unwittingly exhibit bias, resulting in discriminatory practices towards specific demographics or customer categories. For example, fraud detection systems may disproportionately highlight transactions from specific locations or client profiles. Ensuring fairness and bias reduction in AI models is a critical challenge for equitable fraud detection.

TABLE 14. The table below of ISO standards that are relevant to Financial systems [113].

Standard	ISO Name	Usage	Role in Fraud Detection
ISO 20022	Financial Services Messaging	Defines how financial institutions communicate transactions globally, including detailed originator and beneficiary information.	Provides enriched data that enables AI/ML models to detect anomalies, such as inconsistent sender/receiver behavior.
ISO 8583	Card-Based Transactions	Governs electronic transactions involving payment cards, formatting messages from ATMs or POS systems.	Helps AI detect irregularities in transaction amounts, locations, and merchant details, identifying suspicious patterns.
ISO/TR 22239	Financial Crime Risk Management	Provides guidelines to manage risks related to fraud, money laundering, and financial crimes.	Standardizes Suspicious Activity Reports (SARs), enabling effective processing and detection of suspicious activities.
ISO/IEC 27001	Information Security Standard	Secures data management, ensuring financial communications are encrypted and protected from unauthorized access.	Ensures message security and integrity, preventing interception or tampering in financial transactions.
ISO 4217	Currency Codes	Defines globally recognized currency codes, reducing confusion in international transactions.	Detects mismatches in currency codes and transaction amounts, flagging potential manipulations in cross-border fraud.
ISO 11568	Key Management	Provides encryption guidelines, ensuring only authorized parties can read or modify transaction messages.	Makes unauthorized alterations nearly impossible, enabling AI systems to trust data authenticity and spot fraud effectively.

- **Resource Constraints in Small Institutions:** Smaller financial institutions, such as credit unions, often lack the resources and expertise to implement advanced AI-based fraud detection systems. This creates a gap in fraud prevention capabilities between large and small institutions, which require cost-effective and accessible solutions.

IX. CONCLUSION AND FUTURE WORK

In this study, we had the specific objective of conducting a detailed analysis of how AI, ML, data mining, big data, and blockchain complement each other in strengthening financial fraud detection methods. In this regard, we went on a quest in the territory where mathematics and information dwell to look for the best strategies that can be embraced to curb what has become an increasing menace of fraud. This paper sought to demystify the connections that exist between AI, ML, data mining, big data, blockchain, and the financial security web as global society becomes saturated with cutting-edge technology solutions. Our purpose was to identify efficient strategies that could increase the robustness of the financial infrastructure, promote trust, and maintain the privacy and security of transactions in an environment increasingly exposed to cyber threats. Together, the results of this research demonstrate that AI and ML are capable of raising the bar on financial fraud prevention and provide a basis for subsequent developments that can help maintain the stability of the financial sphere against new types of threats.

Future works must focus on improving Interpretability, integrating AI and blockchain, and employing federated learning to reinforce user privacy protection. Moreover, developing more accurate and scalable real-time fraud detection systems that we could not previously afford will become essential to combating new threats. Getting better at transparency and coordination between involved players, industry and, in effect, financial regulation will greatly depend on the symbiotic relations between the financial institutions, the regulators, and the academics to ensure that these alarm systems powered by AI technology keep on improving and continue to ensure that the financial network boasts of strong security. Besides, we highlight the importance of explainable AI in fraud detection to maintain regulatory compliance and confidence. Complex AI decision-making has been successfully explained by methods like LIME and SHAP. LIME delivers human-readable explanations for each fraud prediction, but SHAP provides strong feature attribution both locally and globally. These technologies are crucial for practical implementation in financial institutions and greatly improve model transparency when joined with counterfactuals and rule-based anchor explanations. Notably, decentralized fraud analysis that protects privacy can be made possible using GNNs with Federated Learning. Combining RL with LLMs may make it easier to identify adaptive fraud strategies in both structured and unstructured data. Finally, QML combined with Deep Learning may enhance performance and scalability in complex fraud situations.

REFERENCES

[1] *Brandeis University*. Accessed: Dec. 10, 2024. [Online]. Available: https://people.brandeis.edu/~blebaron/classes/agentfin/GaiKapadia.html

[2] M. Martín and M. D. Valiña, "Heuristics, biases and the psychology of reasoning: State of the art," *Psychology*, vol. 14, no. 2, pp. 264–294, 2023.

[3] Y. Zhang, Y. Lu, and F. Liu, "A systematic survey for differential privacy techniques in federated learning," *J. Inf. Secur.*, vol. 14, no. 2, pp. 111–135, 2023.

[4] *PwC Global Annual Review 2021*. Accessed: Dec. 10, 2024. [Online]. Available: https://www.pwc.com/gx/en/about-pwc/global-annual-review-2021/downloads/pwc-global-annual-review-2021.pdf

[5] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decis. Support Syst.*, vol. 50, no. 3, pp. 559–569, Feb. 2011.

[6] A. K. Kalusivalingam, A. Sharma, N. Patel, and V. Singh, "Enhancing financial fraud detection with hybrid deep learning and random forest algorithms," *Int. J. AI ML*, vol. 1, no. 3, pp. 1–10, 2020.
[7] P. Craja, A. Kim, and S. Lessmann, "Deep learning for detecting financial statement fraud," *Decis. Support Syst.*, vol. 139, Dec. 2020, Art. no. 113421.
[8] N. Dhieb, H. Ghazzai, H. Besbes, and Y. Massoud, "A secure AI-driven architecture for automated insurance systems: Fraud detection and risk measurement," *IEEE Access*, vol. 8, pp. 58546–58558, 2020.
[9] E. Kurshan, H. Shen, and H. Yu, "Financial crime & fraud detection using graph computing: Application considerations & outlook," in *Proc. 2nd Int. Conf. Transdisciplinary AI (TransAI)*, Sep. 2020, pp. 125–130.
[10] C. Chen, C. Liang, J. Lin, L. Wang, Z. Liu, X. Yang, J. Zhou, Y. Shuang, and Y. Qi, "InfDetect: A large scale graph-based fraud detection system for e-commerce insurance," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2019, pp. 1765–1773.
[11] D. V. Kute, B. Pradhan, N. Shukla, and A. Alamri, "Deep learning and explainable artificial intelligence techniques applied for detecting money laundering—A critical review," *IEEE Access*, vol. 9, pp. 82300–82317, 2021.
[12] N. Devarasetty, "AI-enhanced data engineering for real-time fraud detection in digital transactions," *Revista de Inteligencia Artificial en Medicina*, vol. 10, no. 1, pp. 1–31, 2019.
[13] B. R. Chirra, "AI-driven fraud detection: Safeguarding financial data in real-time," *Revista de Inteligencia Artificial en Medicina*, vol. 11, no. 1, pp. 328–347, 2020.
[14] M. Celestin and N. Vanitha, "Artificial intelligence in fraud detection: Are traditional auditing methods outdated" in *Proc. Int. Conf. Recent Trends Arts, Sci., Eng. Technol.*, 2019, pp. 180—186.
[15] B. P. Kasaraneni, "Advanced ai techniques for fraud detection in travel insurance: Models, applications, and real-world case studies," *Distrib. Learn. Broad Appl. Sci. Res.*, vol. 5, pp. 455–513, Mar. 2019.
[16] B. B. P. Kasaraneni, "AI-driven approaches for fraud prevention in health insurance: Techniques, models, and case studies," *Afr. J. Artif. Intell. Sustain. Develop.*, vol. 1, no. 1, pp. 136–180, Mar. 2021.
[17] S. R. Gayam, "AI-driven fraud detection in e-commerce: Advanced techniques for anomaly detection, transaction monitoring, and risk mitigation," *Distrib. Learn. Broad Appl. Sci. Res.*, vol. 6, pp. 124–151, Nov. 2020.
[18] S. P. Pattyam, "AI in data science for financial services: Techniques for fraud detection, risk management, and investment strategies," *Distrib. Learn. Broad Appl. Sci. Res.*, vol. 5, pp. 385–416, Oct. 2019.
[19] S. R. Gayam, "Artificial intelligence for financial fraud detection: Advanced techniques for anomaly detection, pattern recognition, and risk mitigation," *Afr. J. Artif. Intell. Sustainable Develop.*, vol. 1, no. 2, pp. 377–412, Dec. 2021.
[20] D. E. Bowen, "An organizational behavior/human resource management perspective on the roles of people in a service organization context: Frameworks and themes," *Int. J. HRM Organizational Behav.*, vol. 8, no. 4, pp. 1–16, Oct. 2020.
[21] D. Cirqueira, D. Nedbal, M. Helfert, and M. Bezbradica, "Scenario-based requirements elicitation for user-centric explainable AI: A case in fraud detection," in *Machine Learning and Knowledge Extraction*, A. Holzinger, P. Kieseberg, A. M. Tjoa, and E. Weippl, Eds., Cham, Switzerland: Springer, 2020, pp. 321–341.
[22] D. Narsina, J. Gummadi, S. S. M. G. N. Venkata, A. Manikyala, S. Kothapalli, K. Devarapu, M. Rodriguez, and R. Talla, "AI-driven database systems in fintech: Enhancing fraud detection and transaction efficiency," *Asian Accounting Auditing Advancement*, vol. 10, pp. 81–92, Dec. 2019.
[23] P. Agarwal, "Redefining banking and financial industry through the application of computational intelligence," in *Proc. Adv. Sci. Eng. Technol. Int. Conf. (ASET)*, Mar. 2019, pp. 1–5.
[24] G. K. Patra, "AI and big data in digital payments: A comprehensive model for secure biometric authentication," *Educ. Admin., Theory Pract.*, vol. 2024, pp. 773–781, Aug. 2024.
[25] J. Nicholls, A. Kuppa, and N.-A. Le-Khac, "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape," *IEEE Access*, vol. 9, pp. 163965–163986, 2021.
[26] A. Dosovitskiy et al., "An image is worth 16×16 words: Transformers for image recognition at scale," in *Proc. Int. Conf. Learn. Represent.*, 2020, pp. 1–16.
[27] R. Ganjeshwar, P. Roy, and D. P. Mishra, "A review: Credit card fraud detection using machine learning," *IJSDR*, vol. 6, no. 7, pp. 101–107, Jul. 2021.
[28] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100402.
[29] T. Pourhabibi, K.-L. Ong, B. H. Kam, and Y. L. Boo, "Fraud detection: A systematic literature review of graph-based anomaly detection approaches," *Decis. Support Syst.*, vol. 133, Jun. 2020, Art. no. 113303.
[30] Y. T. Berru, V. F. L. Batista, P. Torres-Carrión, and M. G. Jimenez, "Artificial intelligence techniques to detect and prevent corruption in procurement: A systematic literature review," in *Proc. Int. Conf. Appl. Technol.* Cham, Switzerland: Springer, 2019, pp. 254–268.
[31] H. A. Javaid, "How artificial intelligence is revolutionizing fraud detection in financial services," *Innov. Eng. Sci. J.*, vol. 4, no. 1, pp. 1–7, 2024.
[32] R. Mohan, M. Boopathi, P. Ranjan, M. Najana, P. K. Chaudhary, and A. K. Chotrani, "AI in fraud detection: Evaluating the efficacy of artificial intelligence in preventing financial misconduct," *J. Electr. Syst.*, vol. 20, no. 3s, pp. 1332–1338, Apr. 2024.
[33] S. Singh, "Artificial intelligence and machine learning in financial services: Risk management and fraud detection," *J. Electr. Syst.*, vol. 20, no. 6s, pp. 1418–1424, Apr. 2024.
[34] Z. Wang, Q. Shen, S. Bi, and C. Fu, "AI empowers data mining models for financial fraud detection and prevention systems," *Proc. Comput. Sci.*, vol. 243, pp. 891–899, Jan. 2024.
[35] P. Raghuwanshi, "AI-driven identity and financial fraud detection for national security," *J. Artif. Intell. Gen. Sci.*, vol. 7, no. 1, pp. 38–51, Dec. 2024.
[36] D. Kuttiyappan and V. Rajasekar, "AI-enhanced fraud detection: Novel approaches and performance analysis," in *Proc. 1st Int. Conf. Artif. Intell., Commun., IoT, Data Eng. Secur.*, Pune, India, Nov. 2023, pp. 23–25.
[37] T. Awosika, R. M. Shukla, and B. Pranggono, "Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection," *IEEE Access*, vol. 12, pp. 64551–64560, 2024.
[38] A. K. Lin, "The AI revolution in financial services: Emerging methods for fraud detection and prevention," *Jurnal Galaksi*, vol. 1, no. 1, pp. 43–51, May 2024.
[39] A. C. Ozioko, "The use of artificial intelligence in detecting financial fraud: Legal and ethical considerations," *Multi-Disciplinary Res. Develop. J. Int.*, vol. 5, no. 1, pp. 66–85, Jan. 2024.
[40] F. Aslam, A. I. Hunjra, Z. Ftiti, W. Louhichi, and T. Shams, "Insurance fraud detection: Evidence from artificial intelligence and machine learning," *Res. Int. Bus. Finance*, vol. 62, Dec. 2022, Art. no. 101744.
[41] J. Sekar, "Real-time fraud prevention in digital banking a cloud and AI perspective," *J. Emerg. Technol. Innov. Res.*, vol. 10, pp. P562–P570, Jan. 2023.
[42] F. T. Johora, R. Hasan, S. F. Farabi, J. Akter, and M. A. A. Mahmud, "AI-powered fraud detection in banking: Safeguarding financial transactions," *Amer. J. Manage. Econ. Innov.*, vol. 6, no. 6, pp. 8–22, Jun. 2024.
[43] C. Yu, Y. Xu, J. Cao, Y. Zhang, Y. Jin, and M. Zhu, "Credit card fraud detection using advanced transformer model," in *Proc. IEEE Int. Conf. Metaverse Comput., Netw., Appl. (MetaCom)*, Aug. 2024, pp. 343–350.
[44] O. Patel, "AI-driven fraud detection in cryptocurrency transactions," *Int. J. Adv. Res. Eng. Technol.*, vol. 13, no. 2, pp. 80–99, Feb. 2022.
[45] S. Putha, "AI-powered fraud detection in retail transactions: Techniques, implementation, and performance evaluation," *J. Mach. Learn. Healthcare Decision Support*, vol. 2, no. 1, pp. 92–132, 2022.
[46] V. Shende, S. Nandgave, and M. Bhonsle, "Credit card fraud detection using AI," *Grenze Int. J. Eng. Technol.*, vol. 8, no. 2, pp. 1–4, 2022.
[47] H. J. Ritika et al., "Fraud detection and management for telecommunication systems using artificial intelligence (AI)," in *Proc. 3rd Int. Conf. Smart Electron. Commun. (ICOSEC)*, Oct. 2022, pp. 1016–1022.
[48] N. Al-Naseri, "The growing importance of AI in fraud detection," *J. Artif. Intell. Res. Appl.*, vol. 2, no. 1, pp. 464–488, 2022.
[49] M. Z. Islam, S. K. Shil, and M. R. Buiya, "AI-driven fraud detection in the us financial sector: Enhancing security and trust," *Int. J. Mach. Learn. Res. Cybersecurity Artif. Intell.*, vol. 14, no. 1, pp. 775–797, 2023.
[50] A. Gautam, "The evaluating—The impact of artificial intelligence on risk management and fraud detection in the banking sector," in *Proc. Int. Conf. Neural Inf. Process. Syst.*, 2019, pp. 1–16.
[51] S. S. Kuna, "AI-enhanced fraud detection systems in digital banking: Developing hybrid machine learning models for real-time anomaly detection and customer behavior analysis," *J. Artif. Intell. Res. Appl.*, vol. 3, no. 2, pp. 1086–1130, 2023.

[52] E. Wong, "Artificial intelligence in financial services: Risk management and fraud detection," *Innov. Comput. Sci. J.*, vol. 9, no. 1, pp. 1–9, 2023.

[53] G. Sabbani, "AI in credit card fraud detection: Innovations and future directions," *North Amer. J. Eng. Res.*, vol. 4, no. 1, pp. 1–4, 2023.

[54] N. A. Faisal, J. Nahar, N. Sultana, and A. A. Mintoo, "Fraud detection in banking leveraging ai to identify and prevent fraudulent activities in real-time," *Non Hum. J.*, vol. 1, no. 1, pp. 181–197, Oct. 2024.

[55] P. Kamuangu, "A review on financial fraud detection using AI and machine learning," *J. Econ., Finance Accounting Stud.*, vol. 6, no. 1, pp. 67–77, Feb. 2024.

[56] I. Yuhertiana and A. H. Amin, "Artificial intelligence driven approaches for financial fraud detection: A systematic literature review," *KnE Social Sci.*, vol. 2024, pp. 448–468, Jul. 2024.

[57] D. Kuizinienė, T. Krilavičius, R. Damaševičius, and R. Maskeliūnas, "Systematic review of financial distress identification using artificial intelligence methods," *Appl. Artif. Intell.*, vol. 36, no. 1, Dec. 2022, Art. no. 2138124.

[58] P. Adhikari, P. Hamal, and F. B. Jnr, "Artificial intelligence in fraud detection: Revolutionizing financial security," *Int. J. Sci. Res. Arch.*, vol. 13, no. 1, pp. 1457–1472, Sep. 2024.

[59] O. Olowu, A. O. Adeleye, A. O. Omokanye, A. M. Ajayi, A. O. Adepoju, O. M. Omole, and E. C. Chianumba, "AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity," *GSC Adv. Res. Rev.*, vol. 21, no. 2, pp. 227–237, Nov. 2024.

[60] M. Nweze, E. K. Avickson, and G. Ekechukwu, "The role of AI and machine learning in fraud detection: Enhancing risk management in corporate finance," *Int. J. Res. Publication Rev.*, vol. 5, no. 10, pp. 2812–2830, Oct. 2024.

[61] M. Paramesha, N. Rane, and J. Rane, "Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: A comprehensive review," *SSRN Electron. J.*, vol. 1, no. 2, pp. 51–67, 2024.

[62] E. Indriasari, H. Prabowo, F. L. Gaol, and B. Purwandari, "Intelligent digital banking technology and architecture: A systematic literature review," *Int. J. Interact. Mobile Technol.*, vol. 16, no. 19, pp. 98–117, Oct. 2022.

[63] O. H. Fares, I. Butt, and S. H. M. Lee, "Utilization of artificial intelligence in the banking sector: A systematic literature review," *J. Financial Services Marketing*, vol. 28, no. 4, pp. 835–852, Dec. 2023.

[64] H. Sadok, F. Sakka, and M. E. H. El Maknouzi, "Artificial intelligence and bank credit analysis: A review," *Cogent Econ. Finance*, vol. 10, no. 1, Dec. 2022, Art. no. 2023262.

[65] P. Zanke, "AI-driven fraud detection systems: A comparative study across banking, insurance, and healthcare," *Adv. Deep Learn. Techn.*, vol. 3, no. 2, pp. 1–22, 2023.

[66] S. Poudel and U. R. Dhungana, "Artificial intelligence for energy fraud detection: A review," *Int. J. Appl.*, vol. 11, no. 2, p. 116, 2022.

[67] E. Stracqualursi, A. Rosato, G. Di Lorenzo, M. Panella, and R. Araneo, "Systematic review of energy theft practices and autonomous detection through artificial intelligence methods," *Renew. Sustain. Energy Rev.*, vol. 184, Sep. 2023, Art. no. 113544.

[68] S. Kalyani and N. Gupta, "Is artificial intelligence and machine learning changing the ways of banking: A systematic literature review and meta analysis," *Discover Artif. Intell.*, vol. 3, no. 1, p. 41, Dec. 2023.

[69] R. Jáuregui-Velarde, L. Andrade-Arenas, P. Molina-Velarde, and C. Yactayo-Arias, "Financial revolution: A systemic analysis of artificial intelligence and machine learning in the banking sector," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 14, no. 1, p. 1079, Feb. 2024.

[70] R. Nai, E. Sulis, and R. Meo, "Public procurement fraud detection and artificial intelligence techniques: A literature review," in *Proc. 23rd Int. Conf. Knowl. Eng. Knowl. Manage.*, 2022, pp. 1–13.

[71] O. O. Oguntibeju, M. Adonis, and J. Alade, "Systematic review of real-time analytics and artificial intelligence frameworks for financial fraud detection," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 13, no. 9, pp. 1–4, Sep. 2024.

[72] A. Ali, S. A. Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, T. Elhassan, H. Elshafie, and A. Saif, "Financial fraud detection based on machine learning: A systematic literature review," *Appl. Sci.*, vol. 12, no. 19, p. 9637, Sep. 2022.

[73] M. R. Faraji, F. Shikder, M. H. Hasan, M. M. Islam, and U. K. Akter, "Examining the role of artificial intelligence in cyber security (CS): A systematic review for preventing prospective solutions in financial transactions," *Int. J. Religion*, vol. 5, no. 10, pp. 4766–4782, Jul. 2024.

[74] M. N. U. Milon, "Gravitating towards artificial intelligence on anti-money laundering a PRISMA based systematic review," *Int. J. Religion*, vol. 5, no. 7, pp. 303–315, May 2024.

[75] Y. Yanto, L. Lisah, and R. Tandra, "The best machine learning model for fraud detection in banking sector: A systematic literature review," *eCo-Buss*, vol. 7, no. 2, pp. 1361–1384, Dec. 2024.

[76] C. Antal-Vaida, "A review of artificial intelligence and machine learning adoption in banks, during the COVID-19 outbreak," in *Proc. Int. Conf. Bus. Excellence*, vol. 16, 2022, pp. 1316–1328.

[77] M. S. Iqbal, A. Abd-Alrazaq, and M. Househ, "Artificial intelligence solutions to detect fraud in healthcare settings: A scoping review," in *Studies in Health Technology and Informatics*, 2022.

[78] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 1, pp. 145–174, Jan. 2023.

[79] E. R. Ndukwe and B. Baridam, "A graphical and qualitative review of literature on AI-based cyber-threat intelligence (CTI) in banking sector," *Eur. J. Eng. Technol. Res.*, vol. 8, no. 5, pp. 59–69, Oct. 2023.

[80] S. Gaffaroglu and S. Alp, "Detecting frauds in financial statements: A comprehensive literature review between 2019 and 2023 (June)," *PressAcademia Proc.*, vol. 18, no. 1, pp. 47–51, 2024.

[81] V. Kanaparthi, "Transformational application of artificial intelligence and machine learning in financial technologies and financial services: A bibliometric review," 2024, *arXiv:2401.15710*.

[82] E. A. L. Marazqah Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, "A systematic review of literature on credit card cyber fraud detection using machine and deep learning," *PeerJ Comput. Sci.*, vol. 9, p. e1278, Apr. 2023.

[83] D. Rai, "Credit card fraud detection using machine learning and data mining techniques—A literature survey," *Int. J. Appl. Eng. Manage. Lett.*, vol. 23, pp. 16–35, Jul. 2023.

[84] F. Baratzadeh and S. M. H. Hasheminejad, "Customer behavior analysis to improve detection of fraudulent transactions using deep learning," *J. AI Data Mining*, vol. 10, no. 1, pp. 87–101, 2022.

[85] B. Narsimha, C. V. Raghavendran, P. Rajyalakshmi, G. K. Reddy, M. Bhargavi, and P. Naresh, "Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application," *Int. J. Electr. Electron. Res.*, vol. 10, no. 2, pp. 87–92, Jun. 2022.

[86] J. Li, "E-commerce fraud detection model by computer artificial intelligence data mining," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–9, May 2022.

[87] P. Gupta, "Leveraging machine learning and artificial intelligence for fraud prevention," *Int. J. Comput. Sci. Eng.*, vol. 10, no. 5, pp. 47–52, May 2023.

[88] A. Kotagiri, "Mastering fraudulent schemes: A unified framework for ai-driven us banking fraud detection and prevention," *Int. Trans. Artif. Intell.*, vol. 7, no. 7, pp. 1–19, 2023.

[89] V. Tamraparani, "Leveraging AI for fraud detection in identity and access management: A focus on large-scale customer data," *J. Comput. Anal. Appl.*, vol. 31, no. 4, pp. 1–9, 2023.

[90] P. Khare and S. Srivastava, "AI-powered fraud prevention: A comprehensive analysis of machine learning applications in online transactions," *J. Emerg. Technol. Innov. Res.*, vol. 10, no. 9, pp. f518–f525, 2023.

[91] L. Chen, Z. Zhang, Q. Liu, L. Yang, Y. Meng, and P. Wang, "A method for online transaction fraud detection based on individual behavior," in *Proc. ACM Turing Celebration Conf.*, May 2019, pp. 1–8.

[92] Y. Meng, Z. Zhang, W. Liu, L. Chen, Q. Liu, L. Yang, and P. Wang, "A novel method based on entity relationship for online transaction fraud detection," in *Proc. ACM Turing Celebration Conf.*, May 2019, pp. 1–10.

[93] X. Kewei, B. Peng, Y. Jiang, and T. Lu, "A hybrid deep learning model for online fraud detection," in *Proc. IEEE Int. Conf. Consum. Electron. Comput. Eng. (ICCECE)*, Jan. 2021, pp. 431–434.

[94] J. Cui, C. Yan, and C. Wang, "A credible individual behavior profiling method for online payment fraud detection," in *Proc. 4th Int. Conf. Data Storage Data Eng.*, New York, NY, USA, Feb. 2021, pp. 22–30.

[95] O. Adijat Bello and K. Olufemi, "Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities," *Comput. Sci. IT Res. J.*, vol. 5, no. 6, pp. 1505–1520, Jun. 2024.

[96] K. Kalluri, "AI-driven risk assessment model for financial fraud detection: A data science perspective," *Int. J. Sci. Res. Manage.*, vol. 12, no. 12, pp. 1764–1774, Dec. 2024.

[97] A. K. M. Emran and M. T. H. Rubel, "Big data analytics and AI-driven solutions for financial fraud detection: Techniques, applications, and challenges," *Innovatech Eng. J.*, vol. 1, no. 1, pp. 269–285, Nov. 2024.

[98] A. F. A. Mohammed and H. M. A. A. Rahman, "The role of artificial intelligence (AI) on the fraud detection in the private sector in Saudi Arabia," *J. Arts, Literature, Humanities Social Sci.*, vol. 100, pp. 472–506, Jan. 2024.
[99] T. A. Iqbal, E. Ahmed, A. Rahman, and M. R. H. Ontor, "Enhancing fraud detection and anomaly detection in retail banking using generative AI and machine learning models," *Amer. J. Eng. Technol.*, vol. 6, no. 11, pp. 78–91, Nov. 2024.
[100] A. Al-Fatlawi, A. A. T. Al-Khazaali, and S. H. Hasan, "AI- based model for fraud detection in bank systems," *Fusion, Pract. Appl.*, vol. 14, no. 1, pp. 1–9, 2024.
[101] Y.-L. Zhang, J. Zhou, W. Zheng, J. Feng, L. Li, Z. Liu, M. Li, Z. Zhang, C. Chen, X. Li, Y. Qi, and Z.-H. Zhou, "Distributed deep forest and its application to automatic detection of cash-out fraud," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 5, pp. 1–19, Sep. 2019.
[102] I. Sadgali, N. Sael, and F. Benabbou, "Performance of machine learning techniques in the detection of financial frauds," *Proc. Comput. Sci.*, vol. 148, pp. 45–54, Jan. 2019.
[103] E. N. Osegi and E. F. Jumbo, "Comparative analysis of credit card fraud detection in simulated annealing trained artificial neural network and hierarchical temporal memory," *Mach. Learn. with Appl.*, vol. 6, Dec. 2021, Art. no. 100080.
[104] A. Izotova and A. Valiullin, "Comparison of Poisson process and machine learning algorithms approach for credit card fraud detection," *Proc. Comput. Sci.*, vol. 186, pp. 721–726, Jan. 2021.
[105] R. B. Asha and K. R. S. Kumar, "Credit card fraud detection using artificial neural network," *Global Transitions Proc.*, vol. 2, no. 1, pp. 35–41, Jun. 2021.
[106] S. Bagga, A. Goyal, N. Gupta, and A. Goyal, "Credit card fraud detection using pipeling and ensemble learning," *Proc. Comput. Sci.*, vol. 173, pp. 104–112, Jan. 2020.
[107] K. Chen, A. Yadav, A. Khan, and K. Zhu, "Credit fraud detection based on hybrid credit scoring model," *Proc. Comput. Sci.*, vol. 167, pp. 2–8, Jan. 2020.
[108] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *Systematic Rev.*, vol. 10, no. 1, pp. 1–9, Dec. 2021.
[109] R. Khurana, G. Christopher, and E. Charles, "Fraud detection in ecommerce payment systems: The role of predictive AI in real-time transaction security and risk management," *Int. J. Appl. Mach. Learn. Comput. Intell.*, vol. 10, no. 6, pp. 1–32, 2020.
[110] B. K. Nkomo and T. Breetzke, "A conceptual model for the use of artificial intelligence for credit card fraud detection in banks," in *Proc. Conf. Inf. Commun. Technol. Soc. (ICTAS)*, Mar. 2020, pp. 1–6.
[111] K. Singh and P. Best, "Anti-money laundering: Using data visualization to identify suspicious activity," *Int. J. Accounting Inf. Syst.*, vol. 34, Sep. 2019, Art. no. 100418.
[112] J. M. Karpoff, "The future of financial fraud," *J. Corporate Finance*, vol. 66, Feb. 2021, Art. no. 101694.
[113] *Standard*. Accessed: Jun. 2, 2025. [Online]. Available: https://www.iso.org/standards.html
[114] I. Y. Hafez, A. Y. Hafez, A. Saleh, A. A. A. El-Mageed, and A. A. Abohany, "A systematic review of AI-enhanced techniques in credit card fraud detection," *J. Big Data*, vol. 12, no. 1, p. 6, Jan. 2025.
[115] E. Oztemel and M. Isik, "A systematic review of intelligent systems and analytic applications in credit card fraud detection," *Appl. Sci.*, vol. 15, no. 3, p. 1356, Jan. 2025.
[116] *Fraud Costs The Global Economy Over US$5 trillion*. Accessed: May 31, 2025. [Online]. Available: https://www.crowe.com/global/news/fraud-costs-the-global-economy-over-us%245-trillion
[117] H. Nie and S. Lu, "FedCRMW: Federated model ownership verification with compression-resistant model watermarking," *Expert Syst. Appl.*, vol. 249, Sep. 2024, Art. no. 123776.
[118] H. Nie, S. Lu, J. Wu, and J. Zhu, "Deep model intellectual property protection with compression-resistant model watermarking," *IEEE Trans. Artif. Intell.*, vol. 5, no. 7, pp. 3362–3373, Jul. 2024.
[119] H. Nie and S. Lu, "PersistVerify: Federated model ownership verification with spatial attention and boundary sampling," *Knowl.-Based Syst.*, vol. 293, Jun. 2024, Art. no. 111675.
[120] H. Nie and S. Lu, "Securing IP in edge AI: Neural network watermarking for multimodal models," *Int. J. Speech Technol.*, vol. 54, no. 21, pp. 10455–10472, Nov. 2024.
[121] H. Nie, S. Lu, M. Wang, J. Xiao, Z. Lu, and Z. Yi, "Verichroma: Ownership verification for federated models via RGB filters," in *Proc. Eur. Conf. Parallel Process.* Cham, Switzerland: Springer, 2024, pp. 332–345.
[122] X. Yuan and H. Nie, "Beyond protection: Unveiling neural network copyright trading," *Knowl.-Based Syst.*, vol. 320, Jun. 2025, Art. no. 113617.
[123] V. Chang, L. M. T. Doan, A. Di Stefano, Z. Sun, and G. Fortino, "Digital payment fraud detection methods in digital ages and industry 4.0," *Comput. Electr. Eng.*, vol. 100, May 2022, Art. no. 107734.
[124] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial fraud: A review of anomaly detection techniques and recent advances," *Expert Syst. Appl.*, vol. 193, May 2022, Art. no. 116429.
[125] A. Sina, "Open AI and its impact on fraud detection in financial industry," *J. Knowl. Learn. Sci. Technol.*, vol. 2, no. 3, pp. 263–281, Sep. 2024.
[126] Accessed: Jun. 2, 2025. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2025/04/30/ai-applications-in-fraud-detection-in-the-banking-industry/
[127] *IBM*. Accessed: Jun. 2, 2025. [Online]. Available: https://www.ibm.com/think/topics/ai-fraud-detection-in-banking
[128] *Kaggle*. Accessed: Jun. 2, 2025. [Online]. Available: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud
[129] *Kaggle*. Accessed: Jun. 2, 2025. [Online]. Available: https://www.kaggle.com/competitions/ieee-fraud-detection
[130] *Kaggle*. Accessed: Jun. 2, 2025. [Online]. Available: https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
[131] C. Oko-Odion, "AI-driven risk assessment models for financial markets: Enhancing predictive accuracy and fraud detection," *Int. J. Comput. Appl. Technol. Res.*, vol. 14, no. 4, pp. 80–96, 2025.
[132] D. Vallarino, "AI-powered fraud detection in financial services: GNN, compliance challenges, and risk mitigation," *Compliance Challenges, Risk Mitigation*, vol. 2025, pp. 1–34, Mar. 2025.
[133] A. Kumar Veldurthi, "The role of AI and machine learning in fraud detection for financial services," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 4, pp. 757–771, May 2025.
[134] M. S. Islam and N. Rahman, "AI-driven fraud detections in financial institutions: A comprehensive study," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 1, pp. 100–112, Jan. 2025.
[135] S. K. Aljunaid, S. J. Almheiri, H. Dawood, and M. A. Khan, "Secure and transparent banking: Explainable AI-driven federated learning model for financial fraud detection," *J. Risk Financial Manage.*, vol. 18, no. 4, p. 179, Mar. 2025.
[136] L. L. Scientific, "AI-driven fraud detection and security solutions: Enhancing accuracy in financial systems," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 8, pp. 1–9, 2025.
[137] S. Kandhikonda, "AI-enhanced fraud detection in financial services: A technical deep dive," *Int. J. Sci. Technol.*, vol. 16, no. 1, pp. 1–23, Mar. 2025.
[138] R. Kumar and S. Kiran, "AI-driven frameworks for unsupervised fraud detection in banking cybersecurity," *Int. J. Sci. Eng. Appl.*, vol. 14, no. 3, pp. 1–5, 2025.
[139] D. Pramudito, J. Na'am, and F. Ernawan, "Exploring blockchain and AI in digital banking: A literature review on transactions enhancement, fraud detection, and financial inclusion," *Sistemasi*, vol. 14, no. 3, p. 1448, May 2025.
[140] K. Challa, "AI driven fraud detection in digital payments using big data and machine learning," *Amer. J. Anal. Artif. Intell.*, vol. 3, no. 1, pp. 1–14, 2025.
[141] D. A. Oduro, J. N. Okolo, A. D. Bello, A. T. Ajibade, A. M. Fatomi, T. S. Oyekola, and S. F. Owoo-Adebayo, "AI-powered fraud detection in digital banking: Enhancing security through machine learning," *Int. J. Sci. Res. Arch.*, vol. 14, no. 3, pp. 1412–1420, Mar. 2025.
[142] K. Oyelade, "AI-driven fraud detection in fintech: Enhancing security and customer trust," ResearchGate, Tech. Rep., Feb. 2025.
[143] H. O. Bello, "Developing predictive financial fraud models using AI-driven analytics within cybercrime-resilient security ecosystems," IJRPR, ResearchGate, Georgia, USA, Tech. Rep., 2025.
[144] A. Soyele, "Cross platform anomaly detection using hybrid ai models for multi-layered financial fraud in decentralized systems," IRJMETS, ResearchGate, Illinois Univ., Illinois, USA, Tech. Rep., 2025.
[145] H. Thakkar, S. Datta, P. Bhadra, H. Barot, and J. Jadav, "Artificial intelligence and machine learning in fraud detection: A comprehensive bibliometric mapping of research trends and directions," *Ann. Library Inf. Stud.*, vol. 72, no. 2, pp. 138–150, 2025.
[146] S. Iseal, O. Joseph, and S. Joseph, "AI in financial services: Using big data for risk assessment and fraud detection," ResearchGate, Tech. Rep., Jan. 2025.

[147] K. A. W. Aslam, "AI-driven fraud detection: Strengthening cybersecurity in finance and ensuring ethical considerations," Tech. Rep., 2025.
[148] H. Dawood, "Strategic adoption of AI for fraud prevention in financial institutions: A systematic literature review," *Int. J. Risk Fraud Reliab.*, vol. 1, no. 1, p. 118, 2025.
[149] E. Kokogho, P. E. Odio, O. Y. Ogunsola, and M. O. Nwaozomudoh, "A cybersecurity framework for fraud detection in financial systems using AI and microservices," *Gulf J. Advance Bus. Res.*, vol. 3, no. 2, pp. 410–424, Feb. 2025.

NUSRAT JAHAN SARNA received the B.Sc. degree in computer science and engineering from United International University (UIU), Dhaka, Bangladesh, in 2023, where she is currently pursuing the M.Sc. degree in computer science and engineering. She was a Grader with the Department of Computer Science and Engineering, UIU, for the digital system design course, from August 2022 to January 2023. She has one international journal publication. Her research interests include software engineering, AI, machine learning, the IoT, project management, and networking.

FARZANA AHMED RITHEN received the B.Sc. and M.Sc. degrees in computer science and engineering from United International University (UIU), Dhaka, Bangladesh, in 2024 and 2025, respectively. Her research interests include software engineering, cloud computing, and machine learning. Additionally, she is also interested in network security and the Internet of Things (IoT). She has published one international journal article.

UMME SALMA JUI received the B.Sc. degree in computer science and engineering from the University of Asia Pacific, Dhaka, and the M.Sc. degree in computer science and engineering from United International University (UIU), Bangladesh, in 2025. She is currently a Web Developer in a software firm. Her research interests include software engineering, the IoT, and AI. She has also published a conference paper on the challenges of implementing project management frameworks in small and medium-sized software enterprises.

SAYMA BELAL received the B.Sc. degree in computer science and engineering from Independent University, Bangladesh, and the M.Sc. degree in computer science and engineering from United International University (UIU), Dhaka, Bangladesh, in 2025. Her research interests include software engineering, the IoT, and healthcare technologies.

AL AMIN received the B.Sc. degree in computer science and software engineering from American International University-Bangladesh (AIUB), Dhaka, Bangladesh. He is currently pursuing the M.Sc. degree in computer science and engineering with United International University (UIU), Dhaka. He is employed as a Software Engineer. His research interests include software engineering, machine learning, the Internet of Things (IoT), and networking.

TASNIM KABIR OISHEE received the B.Sc. and M.Sc. degrees in computer science and engineering from United International University, Dhaka, Bangladesh, in 2025. She is currently working as a Remote Software Quality Assurance Intern at a1qa, a software testing company based in Colorado, USA. Her research interests include blockchain, artificial intelligence, and machine learning.

A. K. M. MUZAHIDUL ISLAM (Senior Member, IEEE) received the M.Sc. degree in computer science and engineering from Kharkiv National University of Radio Electronics (NURE), Ukraine, in 1999, and the D.Eng. degree in computer science and engineering from Nagoya Institute of Technology (NiTech), Japan, in 2007.

From January 2011 to January 2017, he was a Senior Lecturer at Malaysia–Japan International Institute of Technology (MJIIT) of the Universiti Teknologi Malaysia (UTM), Malaysia, and an Adjunct Professor at the Military Institute of Science and Technology (MIST), Bangladesh. Thereafter, he was an Associate Professor and the Head of the Department of Computer Science and Engineering (CSE) at the University of Liberal Arts Bangladesh (ULAB), Bangladesh, until September 2018. He is currently a Professor with the Department of CSE, United International University (UIU), Bangladesh. He has published 113 international research publications (including one edited book, two book chapters, 38 peer-reviewed indexed journals, and 72 conference papers). He has secured several national and international research grants and supervised ten Ph.D., four M.Sc., and more than 25 B.Eng. students through their graduation. His research interests include network architecture, communication protocol, cognitive radio networks, wireless sensor networks, the IoT, cloud computing, healthcare, and smart farming. He was a member of the Sectoral Committee of BAETE, IEB, from September 2021 to August 2022, and an Expert on Outcome Based Accreditation. He has served at the IEEE Bangladesh Section, in 2022 and 2023. He is the Initiator and the General Chair of the International Conference on Bangabandhu and Digital Bangladesh (ICBBDB 2023 and ICBBDB 2021) and the Lead Editor of the book *Bangabandhu and Digital Bangladesh* (Springer CCIS, 2022). He is also an Initiator and the TPC Chair of ICAICT international conferences, e.g., ICAICT 2016 and ICAICT 2020. He has also served as the TPC Chair for ETCCE 2020 and 2021 international conferences. Earlier, he has served as the Secretariat for ICaTAS 2016 international conference, Malaysia, and the 7TH AUN/SEED-Net 2014 International Conference on EEE. He is a Chartered Engineer (C.Eng.) and a fellow of IEB.