DOI: http://dx.doi.org/10.26483/ijarcs.v17i3.7443

ISSN No. 0976-5697

Volume 17, No. 3, May-June 2026

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

AI-POWERED FRAUD DETECTION IN DIGITAL FINANCIAL PLATFORMS: A STATE-OF-THE-ART SURVEY

Bhalchandra Bapat
Independent Researcher
bhalchandra@ssbm.ch

Abstract: This rapid pace of digitization of financial services has greatly amplified the scale, complexity, and variety of financial transactions. Consequently, it has led to an increase in sophisticated fraudulent activities that challenge conventional detection methods. Manual and traditional solutions that are rule-based are unlikely to be effective in dealing with up-and-coming trends of fraud since they possess low levels of flexibility, high operation costs, and constrained capabilities of responding to fraud. As a result, AI has turned into a paradigm shift that can enhance the detection of fraud through automated learning and real-time analysis, and high-precision anomaly detection. The survey gives a detailed analysis of AI-based ML, deep learning (DL), unsupervised learning, and natural language processing (NLP) models applied to detect fraudulent behaviour in financial ecosystems. The paper has provided a detailed overview of what external and internal fraud is, examined traditional approaches and identified the downsides that can only be addressed with the help of AI. Besides that, it offers the most recent publications to analyze the progress of algorithms, performance metrics, the introduction of new tendencies, and the increased role of explainable and privacy-conscious AI. This work offers a comparative analysis of the latest models and points out how AI could make current fraud detection techniques more accurate, scalable, and flexible. The findings suggest that additional innovation needs to be maintained to address more intricate, data-driven financial fraud problems.

Keywords: Artificial Intelligence, Machine Learning, Deep Learning, Natural Language Processing, Fraud Analytics, Financial Fraud, Financial Cybersecurity

I. Introduction

The risks of financial fraud are serious, and they are caused by the rapid growth of digital transactions, which pose threats to the global financial ecosystem. Financial fraud, which has been defined as misleading methods of acquiring financial gain, has recently posed a big threat to businesses and organizations. Financial statement fraud can be described as a deliberate deception or misrepresentation by individuals employed by an organization. Financial fraud is a serious problem faced by companies in all corners of the world, including developing countries. The financial impact of financial fraud on the business is negative since it may destroy client confidence and the reputation of the company[1][2]. This can be detrimental to the reputation of the company and the customers, as well as its profitability. Throughout most countries, financial fraud offenses frequently encompass falsification of transactions, misappropriation of cash and alteration of financial data.

These fraudulent activities might include understating obligations, manipulating expenses, exaggerating assets, and misstating revenues. The end game of these fraud types too often is to appear more prosperous or financially sound than the company was initially[3]. To identify such frauds, the conventional means, such as human checks and verifications, are not accurate, costly and time-consuming[4]. Further, they tend to be inflexible and thus are unsuited to deal with the dynamism of Financial Fraud. The volume and complexity of transactions might make the human fraud detection procedure laborious and ineffective. Thus, fraud prevention is one of the aspects that requires the employment of advanced technology interventions.

In this context, AI has particularly become an agent of change and is able to transform fraud detection[5]. Applications of ML and DL, AI-based systems have gained popularity as a tool to identify abnormal trends in big data, detect fraudsters in real time, and reduce losses. The efficiency of such systems in different sectors, such as banking[6] Insurance and healthcare, has become topics of extensive research and discussion[7]. AI has many benefits for financial fraud detection systems. Potentially, AI-based systems may handle and analyze massive volumes of data significantly more effectively than traditional techniques, leading to faster and more accurate fraud detection. Additionally, AI systems may learn from previous fraud tendencies and gradually enhance their detection capabilities[8]. The increased attention to the use of AI in fraud detection can be attributed to the fact that the reliability and validity of financial networks have never been as crucial as they are now, given the rapid digitalization. The threats to individuals, businesses and even economies are serious, as global financial fraud is estimated at trillions of dollars annually.

A. Structure of the paper

This paper has the following structure: Section II explains the financial fraud environment and describes the various forms of fraud and standard methods for detecting them. Section III delves into the use of AI in fraud detection. Section IV addresses use of AI-based methods, such as ML, DL, unsupervised learning, and NLP models. Section V considers the current literature. Section VI concludes the study and discusses potential future research areas.

II. Financial Fraud Landscape and Detection

It is possible to classify the many forms of financial fraud into two main groups: internal and external fraud. Out-of-band attacks on institutions that operate online, as well as identity theft, include external fraud such as credit card, payment and loan fraud. Internal fraud, e.g., money laundering and tax evasion, involves insider access to conceal illegal financial transactions. Traditional detection methods, such as rule-based systems, statistical models, and human evaluations, have long been the foundation of fraud prevention. However, their incapacity to be more flexible, scalable, and responsive underscores the need for more intelligent, data-driven strategies.

A. Types of Financial Fraud

Financial Fraud is a wide-ranging term that entails the use of a wide range of deceptive practices that aim at attaining illegal financial benefit by a variety of means[9]. In order to create particular and efficient detection systems, one must be aware of many forms of fraud and their features. There are two major types of financial fraud, namely internal and external fraud.

1) External Fraud

External fraud is a form of fraud where stakeholders are not directly controlled by an organization.

- **Credit Card and Payment Fraud:** The largest form of external fraud has been found to be credit card fraud. This group comes to include unauthorized transactions that are made using the information of stolen cards, or with the assistance of advanced fraud means. The studies conducted in this field generally seek to investigate the trends of the transaction, the buying behaviour, time constraints of utilizing the card and geographical peculiarities to ascertain the signs of likely fraud. The advent of contactless payment methods, DigitalWallets, online payment systems, and point-of-sale fraud has broadened the scope of payment fraud as a result of the digital revolution. The rising complexity of payment fraud has spurred a plethora of research in response to the proliferation of digital payment mechanisms.
- **Loan Fraud:** A variety of fraudulent activities occur throughout the loan lifecycle, including but not limited to false loan applications, schemes including identity theft, income fraud, and inflated property values. To detect potential fraud, ML models used to detect loan fraud often examine applicant data patterns, inconsistencies in credit histories, application timing, and cross-references.

2) Internal Fraud

Fraudulent actions performed by individuals with authorized access to an organization are known as internal fraud. Approximately 46% of examined publications focus on various forms of internal fraud.

- **Money Laundering:** Money laundering fraud refers to complicated arrangements aimed at concealing the source of the illegally acquired funds by incorporating them into the stream of legitimate financial transactions. According to the UN, 25% to 5% of the world's GDP, or USD 800 billion to USD 2 trillion in current US currency, is expected to be laundered annually[10]. The money laundering detection ML models use suspicious transaction network patterns, customer behavioral anomalies, sequence of account activities, and cross-institutional transaction flows that are likely to identify their laundering operations.
- **Tax Fraud:** Tax fraud involves an intentional distortion of information to tax authorities with aim of minimizing tax liability under the guise of a number of schemes. ML algorithms that specialize in this field look for patterns of possible tax avoidance by comparing taxpayer networks, analyzing data inconsistencies, and analyzing patterns of business activity.

B. Traditional Fraud Detection Techniques

The foundation of financial organizations' security frameworks for decades has been traditional fraud detection techniques[11]. Such methods are based on a set of rules, statistical methods, and human experience to detect and thwart fraud.

1) Rule-Based Systems

The simplest method of detecting fraud in banking institutions is the rule-based systems. Such systems work based on a predefined set of conditions or, rather, rules that, when activated, indicate transactions as possible fraudulent ones. Fraud Detection system is a rule-based system that comprises a few elements:

- **Rule Engine:** The fundamental element that handles transactions in accordance with the specified ruleset.
- **Rule Repository:** A database of fraud detection rules kept up to date by the organization.
- **Alert Management System:** A method for managing and ranking notifications produced by rule infractions.
- **Case Management System:** Tools for looking into and fixing transactions that have been reported.

Financial institutions use a variety of strategies to implement rule-based systems:

Static rules recognize many transactions from the same account in a short period of time or indicate transactions above a certain value, among other predefined thresholds and circumstances[12]. Although these rules are simple to implement, they need regular human adjustment. For example, dynamic rules modify transaction amount thresholds based on a client's spending behaviors or customer characteristics. They are predicated on predetermined logic, albeit being more complicated than established rules. Figure 1 illustrates the conventional fraud detection process.

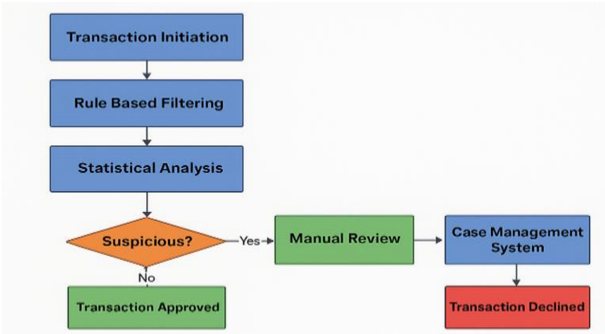

Fig. 1. Traditional Fraud Detection Workflow in a Financial Institution

2) Statistical Methods

Conventional fraud detection methods use various statistical tools to find abnormalities and patterns that might be signs of fraud in addition to rule-based approaches.

- Regression Analysis is used to analyze the relationships between variables to determine patterns that are related to fraudulent activities. Regression models in fraud detection learn baseline relations between transaction characteristics and detect changes in transaction patterns[13].
- Anomaly Detection detects outliers that do not follow normal patterns of behavior based on Z-score analysis methods, the Interquartile Range (IQR) method, and control charts.
- Pattern recognition methods, such as sequence analysis, association rules, and clustering, identify recurring sequences or combinations of events that may indicate fraud.

3) Manual Review Processes

In spite of the technology, human expertise is an important element in the conventional fraud detection systems. When it comes to detecting fraud, analysts rely on their intuition, experience, contextual knowledge, adaptability, and judgment. With the use of case management systems, teams of professional fraud analysts at financial institutions review transactions that have been reported, look into suspicious activities, and provide final decisions on fraud cases[14]. Conventional means of detecting fraud have their own unique merits but are severely constrained in the current fast-changing world of fraud.

4) Limitations

The conventional methods have some limitations as indicated below:

- **Poor adaptability to new forms of fraud:** The system cannot identify new or novel ways of fraud because rules are fixed, and thus, it would take longer to identify new threats unless these are updated manually by analysts.
- **Scalability issues with increasing data:** As transaction rates increase, the system might not have the ability to compute a high number of rules well and decrease speed and real-time detection.
- **Rule explosion over time:** Ongoing introduction of new rules promotes an even more complex structure that is hard to manage and can result in overlaps, contradictions, or lower performance.
- **Binary and rigid decision-making:** Most rule-based systems consider a transaction as a fraud or a non-fraud, with no attempt to score or rank it as a risk of fraud, with the more developed approaches.
- **Reactive and not proactive response:** These systems totally depend on prior fraud knowledge. New fraud behaviors are unpredictable and unanticipated, and thus, they are not effective in dynamic threat environments.
- **Data silos that impede cross-channel analysis:** With rule-based systems, many operate independently across departments or channels, which prevents the system from relating patterns across various sources of transactions.

III. Artificial Intelligence In Financial Fraud Detection

The rising amount of digital transactions renders traditional Fraud Detection systems incapable of dealing with the complexities of today's financial system. The present transaction environment renders conventional approaches for data management inefficient due to its high data pace and varied quantity. Fraud detection procedures have undergone a significant change thanks to artificial intelligence (AI). AI is distinct in that it can evaluate enormous volumes of data and identify patterns and anomalies in real time that are invisible to human analysts.

A. AI Capabilities in Fraud Analytics

The advent of automated fraud detection systems was a pivotal moment in the history of FraudDetection. However, they worked to some degree, although they were labor-intensive, time-consuming, and prone to human error. As the quantity and intricacy of financial transactions keep rising, a solution was urgently required that was capable of processing large datasets in a shorter time and detecting fraud in real time[15][16]. The fraud detection process became more efficient, faster and scalable because of automated systems. Specifically, AI was central to the automation of the transactional data analysis process, which allows financial institutions to identify the presence of anomalies and trends that may indicate fraud with greater precision than ever before[17]. The following are some of the AI methods provided that aid in fraud detection:

- Supervised learning, this is when an AI model is trained with Labeled Data, where the model is taught to identify patterns that are related to legitimate and fraudulent transactions. New and unseen data can then be predicted using this model.
- On the other hand, unsupervised learning does not have labeled datasets and determines patterns or anomalies in accordance with natural structures in the data. By identifying typical and questionable behavior, the two techniques may aid in the detection of fraud.
- Algorithms can now automatically construct hierarchical data representations thanks to deep learning methods, especially neural networks, which have completely transformed fraud detection. The ability of neural networks to handle very complicated, non-linear interactions makes them ideal for detecting intricate patterns that may indicate fraud [18]. The accuracy of fraud detection algorithms has also significantly increased due to their ability to independently extract data characteristics.
- Another branch of AI that has been used to fraud detection is NLP. NLP algorithms may be utilized to find language patterns that might indicate fraud in textual data, such as transaction descriptions or conversation logs. By offering language insights, NLP also helps make fraud detection more broad and sophisticated.

B. ML Advantages in Financial Systems

ML plays a key role in financial FraudDetection as it assists in identifying an unusual pattern, identifying abnormal fraud activities and improving predictive accuracy of risk assessment. The main advantages of fraud detection with it are discussed below:

- **Better Speed and Efficiency:** ML can assist financial institutions to operate with large volumes of transactional information at unbelievably high speeds. It takes less time to identify and address any fraudulent behavior since suspicious activity may be reported almost instantly because to this faster processing speed.
- **Constant Availability:** ML models operate 24/7, unlike human analysts or other manual systems. This is sustained surveillance so that any fraudulent activity is detected at any time, even outside business hours, on weekends, or on holidays, and it provides financial systems with protection.
- **Cost Savings:** ML can assist financial organizations to cut down the costs that are incurred during the manual investigations since it automates much of the fraud detection process[19]. Moreover, fraud detection at the early-stage results in avoiding major financial losses, and this contributes to cost-efficiency in the long-term perspective.
- **Increased Learning Capacity:** The models of ML make progress when they are subjected to new data and patterns. In the case of financial fraud, it means that the system becomes more effective in detecting new fraud mechanisms, adapting to new criminal behaviour and enhancing its predictive capabilities, which do not require rewriting.
- **Better Accuracy:** ML systems can recognize intricate and nuanced trends in information that could be missed by rule-based systems or human analysts[20]. Such capacity results in greater detection accuracy, less FP and FN, preventing the misidentification of legitimate transactions and the neglect of legitimate fraud instances.

- **Less Human Interaction:** ML avoids the use of humans to a large extent since it automates regular detection activities. This reduction allows human professionals to concentrate on high-risk or more complicated situations, improving the overall efficiency and effectiveness of fraud management teams[19].

The Figure 2 represents the advantages of ML in financial Fraud Detection.

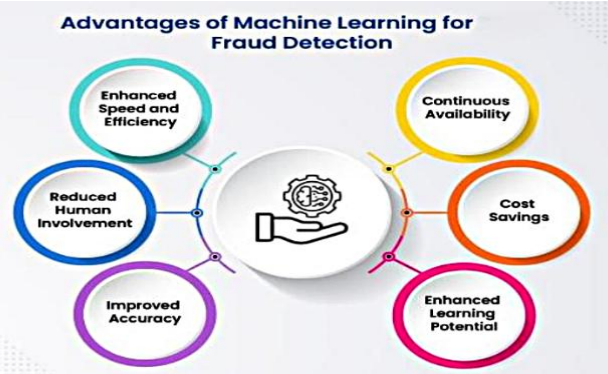

Fig. 2. Advantages of AI for Fraud detection

IV. Techniques for Financial Fraud Detection

The detection of financial fraud is based on sophisticated AI methods to detect suspicious operations with a high level of accuracy. Supervised Learning models are used to categorize transactions based on the presence of productive information, whereas DL is used to capture intricate patterns based on neural networks. Unsupervised approaches identify abnormalities without labels, and NLP models understand financial text. A combination of these methods can have a strong impact on fraud detection performance and reduce FP.

A. *Supervised Learning Model*

Supervised learning in financial fraud detection involves applying data-driven algorithms that learn patterns of legitimate and fraudulent behavior to recognize suspicious transactions in real time. In Ali Hagag study introduces a Supervised ML technique for fraud detection. These methods are used by the suggested ML system to identify fraudulent transactions[21]. The supervised learning part is trained using a labeled dataset that contains both legitimate and fraudulent transactions. The study's dataset included 284,807 credit card transactions. Four models based on Python were created once the data was prepared. The K-Nearest Neighbors (KNN) algorithm accurately identified whether 99.94% of credit card transactions were legitimate or fraudulent.

B. *Deep Learning Model*

DL in financial fraud detection involves applying multi-layered neural network models that automatically discover high-level patterns and representations from transaction data to detect fraud. Zorion recommends a CCFD solution based on DL. Pre-processing, normalization, and feature selection are necessary before the credit card transaction data is fed into the DL and LSTM Model[22]. The study shows the performance of the LST Mmodel, which achieved 99.92% accuracy. These results show that the DL approach has a low FP and high accuracy when it comes to identifying credit card fraud.

C. *Unsupervised Machine Learning Model*

Unsupervised ML in the financial sector detects fraud by identifying anomalies in transactions without labeled data, using algorithms. The research by Ismail and Haq employs Unsupervised Learning to enhance financial fraud detection in businesses. The proposed approach analyses data with the help of data analytics and an unsupervised ML algorithm to accurately identify trends, abnormalities, and signs of fraud[23]. To identify instances of Missing Values and data imbalance, exploratory data analysis techniques were used. A 99.7% accuracy was obtained using the isolation forest method.

D. *Natural Language Processing (NLP) model*

The application of computational methods to detect and understand textual financial data to determine the possibility of fraud is known as NLP in financial fraud detection. Yang explores the use of Antitechnology for precise financial fraud detection, especially with regard to the creation and maintenance of Fin Chain-BERT[24]. Experimental data proved effectiveness of Fin Chain-BERT model and its optimization methods. The Fin Chain-BERT model had the advantage of better loss functions and lightweight technologies. Using Loss Function, a model with an acc, rec, and prec of 0.97 was created. Figure 3 illustrates the comparison of the various techniques of AI in detecting financial fraud in terms of accuracy.

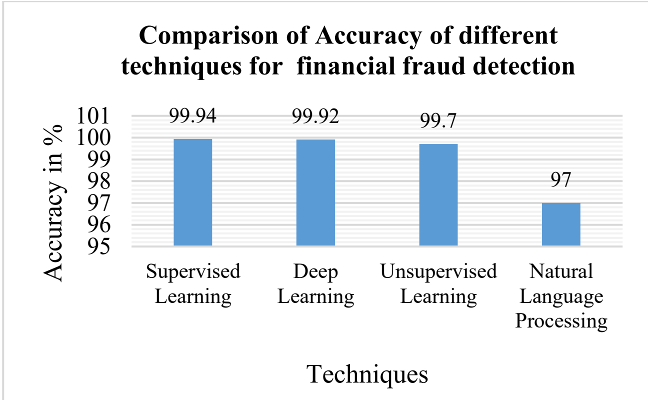

Fig. 3. Comparison of different techniques for financial fraud detection

V. Literature Review

The section discusses recent studies on ML models for Fraud Detection in financial system and how they have improved detection accuracy, scalability, and decision-making efficiency. The recent work is tabulated below:

Jahan Sarna et al. (2025) discusses how AI can be utilized to detect financial fraud, mentioning ML, DL, and hybrid models as ground-breaking solutions. Through large-scale data analysis, AI can discover new fraud trends and dynamically respond to new threats. GNNs and other methods have been very effective in identifying several types of financial crime, such as money laundering, identity theft, and payment fraud. This study compiles the findings of several trials and gives a thorough taxonomy of AI-based fraud detection methods. It offers a methodical grouping of fraud discovery techniques by their application in diverse types of fraud, providing a pathway to gauge their performance [25].

Boltaev and Rakhmatullaev (2025) introduce the latest developments in AI-driven financial fraud detection techniques, including three methodological pillars: ML, DL, and hybrid models. The fundamental algorithms, such as DT, RF, SVM, NN, and ensemble learning models, are presented, as well as the advantages of the methodology, realistic constraints, and performance considerations. The significance of data imbalance, interpretability of models, privacy protection, and the dynamism of fraudulent behavior are also mentioned in the study. The future of financial fraud detection systems is expected to be open, privacy-conscious, and globally scalable; hence, new directions are being particularly considered such as explainable AI, federated learning, and graph neural networks[26].

Kamuangu (2024) article offers the in-depth examination of the recent algorithms of overcoming financial fraud, specifically focusing on the role of ML and AI. The study examines the history of financial crime in more detail and highlights the inherent inefficiencies of conventional rule-based and manual Fraud Detection techniques. Subsequently, key studies and effective uses that have revolutionized fraud detection are pointed out and ML and AI are addressed. The evaluation measures (ROC-AUC, F1score, rec, acc, and prec) are being investigated. Next, various ML and AI algorithms are presented, such as the enigmatic RF, the trusted SVM, and the sophisticated neural networks. As comparative analysis develops, it possible to discover the advantages and limitations of particular ML and AI systems[27].

Olowu et al. (2024) describes how AI and data science methods are now being used in financial organizations' fraud detection systems, with a focus on improving cybersecurity systems. Examine the effectiveness of various ML algorithms, DLstructures, and real-time monitoring systems in detecting fraud by closely evaluating industry reports, peer-reviewed literature, and empirical research conducted within the last ten years. A meta-analysis of 47 studies found that, in comparison to older rule-based systems, modern AI-based fraud detection systems reduce FP by 40-60% and achieve Detection Rates of 87-94%. Additionally, integrated AI methods that combine supervised and unsupervised learning strategies constantly show better results in identifying new fraud trends and responding to new threats[28].

Sood et al. (2023) In order to identify new domains of AI-based fraud detection, research employs a methodical literature review technique. 241 research publications over the last 20 years have been examined by the writers. The papers in the literature review came from the Scopus database. The results of the meta-analysis and network analysis demonstrate this study domain's upward tendency. The VOSviewer program is used to examine author-coauthor network cooperation. Future study fields were also selected, and the critical research domain was determined using K-means clustering. Researchers in the future may refer to this work while examining the usage of AI methods for preventing and detecting financial fraud[29].

Ali et al. (2022) employed the Kitchenham method, which summarizes the findings after extracting and synthesizing the pertinent articles using well-established processes. Several research from reputable electronic database collections have been assembled using the specified search techniques. The inclusion/exclusion criteria were followed in the selection, compilation, and analysis of 93 articles. An outline of the most prevalent types of fraud, evaluation criteria, and well-known ML algorithms for detecting fraud is given in the article. Most research that looked at the application of ML techniques for fraud detection employed SVM and ANN, and the most prevalent kind of fraud addressed by ML approaches was credit card fraud[30].

Table I gives a comparative description of the latest AI-based ML models used in the financial fraud detection, their areas of interest, mode of operation, and performance

TABLE I. COMPARATIVE ANALYSIS OF EXISTING STUDIES ON AI-POWERED FRAUD DETECTION IN FINANCIAL SYSTEMS

Authors	Focus of Study	Key Contributions	Advantages	Limitations	Recommendations
Jahan Sarna et al. (2025)	Taxonomy of AI-driven fraud detection models	Developed structured categorization of ML, DL, and hybrid models; emphasized GNN effectiveness	Provides a comprehensive framework for understanding fraud detection techniques; highlights adaptability of AI to emerging fraud	No empirical comparison of models; lacks real-time deployment insights; limited discussion of cross-financial-system interoperability	Conduct benchmarking studies; evaluate real-time performance; explore cross-platform integration of fraud detection systems
Boltaev & Rakhmatullaev (2025)	Advances in ML, DL, hybrid models & emerging directions	Reviewed core algorithms; identified future trends including FL, GNNs, and XAI	Strong methodological overview; highlights modern privacy-preserving and explainability trends	No unified comparison of hybrid vs standalone models; limited focus on large-scale deployment challenges	Develop unified evaluation frameworks; include scalability and enterprise-level constraints in future analyses
Kamuangu (2024)	ML/AI approaches for addressing financial fraud	Explored history of fraud detection; discussed ML/AI algorithms and evaluation metrics	Offers strong performance analysis; provides insights into strengths/weaknesses of ML models	Does not map fraud types to suitable models; lacks emerging fraud types like crypto and synthetic identity fraud	Include fraud-type-to-model mapping; expand scope to modern fraud categories
Olowu et al. (2024)	AI and data science for detecting bank fraud	Meta-analysis showing 87–94% detection accuracy; highlighted real-time monitoring	Demonstrates clear superiority of AI models over rule-based methods; covers large dataset of studies	Limited focus on unsupervised methods; lacks discussion on scalability and integration challenges in banks	Evaluate anomaly detection models; explore enterprise scalability and system integration issues

Sood et al. (2023)	SLR of 241 AI-driven fraud detection publications	Network analysis, clustering of research themes, identification of emerging trends	Broad coverage of literature; strong visualization of research landscape	Does not deeply compare model performance; lacks integration of emerging models like GNNs and FL	Expand clustering categories to include modern architectures; provide performance-based comparisons
Ali et al. (2022)	ML-based fraud detection using Kitchenham SLR	Identified most common ML algorithms (SVM, ANN) and popular fraud domains	Provides foundational understanding of ML in fraud detection; strong systematic approach	Limited to ML; excludes DL, GNN, and hybrid models; lacks coverage of diverse fraud types	Include DL and GNN models; broaden fraud categories; integrate interpretability and hybrid approaches

VI. Conclusion and Future Work

ML is a key element in financial fraud detection, and this survey shows that contributions from ML, DL, supervised and unsupervised learning, and NLP methods collectively enable the detection of fraudulent activities in digital banking ecosystems. The use of supervised models can still be applied in the detection of familiar fraud patterns, and the unsupervised methods complement them by detecting abnormal or new activities that are not in line with the historical transactions. DL solutions go to the next level by automatically generating more complex features on big financial data, and NLP algorithms extend the fraud analysis to textual data, including customer messaging, dispute statements and transaction descriptions. In addition to the methodological comparisons, the survey also examines the bigger trends of fraud-detection research, such as scalability, the evolving nature of fraud tactics and the sheer size of the digital-payment market. The comparison of these techniques indicates that the supervise learning is more efficient and effective than other techniques of detecting financial fraud. Further studies can be conducted on the hybrid architecture to unify such practices so that systems can be able to identify both structured and unstructured indicators of fraud more effectively. Other recommendations are privacy-preserving collaboration between institutions, adaptive learning strategies that update models in response to changes in fraud behaviour, and increased transparency to enhance regulatory trust and explain ability in the operational banking environment.

References

[1] S. A. Pushkala, “Deep Learning Techniques for Real-Time Fraud Detection in Financial Transactions,” in *2025 International Conference on Computational Innovations and Sustainable Technologies (ICCIST)*, IEEE, Dec. 2025, pp. 1–7. doi: 10.1109/ICCIST67338.2025.11438826.

[2] A. A. Almazroi and N. Ayub, “Online Payment Fraud Detection Model Using Machine Learning Techniques,” *IEEE Access*, vol. 11, pp. 137188–137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[3] R. K. Rao and V. N. Mandhala, “Unveiling Financial Fraud: A Comprehensive Review of Machine Learning and Data Mining Techniques,” *Ingénierie des systèmes d Inf.*, vol. 29, no. 06, pp. 2309–2334, Dec. 2024, doi: 10.18280/isi.290620.

[4] A. K. Lin, “The AI Revolution in Financial Services: Emerging Methods for Fraud Detection and Prevention,” *J. Galaksi*, vol. 1, no. 1, pp. 43–51, 2024.

[5] J. W. Sajja, G. B. Komarina, and N. K. R. Choppa, “The Convergence of Financial Efficiency and Sustainability in Enterprise Cloud Management,” *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 4, May, pp. 964–992, 2025, doi: 10.32996/jcsts.2025.7.4.110.

[6] S. Singamsetty, “Efficacy of Data Governance a Cutting Edge Approach to Ensuring Data Quality in Machine Learning for Banking Industry,” in *2024 2nd International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, IEEE, Dec. 2024, pp. 1–7. doi: 10.1109/SCOPES64467.2024.10991944.

[7] V. Sikarwar, “AI-Powered Process Mining for Intelligent, Personalized Customer Experience in the Insurance Sector,” *Int. J. Res. Publ. Eng. Technol. Manag.*, vol. 8, no. 4, pp. 12418–12428, 2025, doi: 10.15662/IJRPETM.2025.0804007.

[8] P. Adhikari, P. Hamal, and F. B. Jnr, “Artificial Intelligence in fraud detection: Revolutionizing financial security,” *Int. J. Sci. Res. Arch.*, vol. 13, no. 01, pp. 1457–1472, 2024.

[9] A. A. Compagnino *et al.*, “An Introduction to Machine Learning Methods for Fraud Detection,” no. Ml, pp. 1–32, 2025.

[10] M. Narayan, P. Shukla, and R. Kanth, “AI-driven fraud detection and prevention in decentralized finance: A systematic review,” *AI-Driven Decentralized Financ. Futur. Financ.*, pp. 89–111, 2024.

[11] C. Bagwe, “Fraud Detection in Financial Institutions: AI VS. Traditional Methods,” *Int. J. Sci. Res. Eng. Trends*, vol. 10, no. 6, pp. 3274–3279, 2024, doi: 10.61137/ijsret.vol.10.issue6.654.

[12] M. Ahmed, A. N. Mahmood, and M. R. Islam, “A survey of anomaly detection techniques in financial domain,” *Futur. Gener. Comput. Syst.*, vol. 55, pp. 278–288, 2016.

[13] J. Perols, “Financial statement fraud detection: An analysis of statistical and machine learning algorithms,” *Audit. A J. Pract. \& Theory*, vol. 30, no. 2, pp. 19–50, 2011.

[14] S. Barman, U. Pal, M. A. Sarfaraj, B. Biswas, A. Mahata, and P. Mandal, “A complete literature review on financial fraud detection applying data mining techniques,” *Int. J. Trust Manag. Comput. Commun.*, vol. 3, no. 4, pp. 336–359, 2016.

[15] A. Chandrashekar, R. V. Prabhu, and D. Munivel, “Big Data Integration in the Insurance Industry: Enhancing Underwriting and Fraud Detection,” *J. Comput. Intell. Robot.*, vol. 3, no. 1, 2023.

[16] D. Patel, “Explainable Risk Decision Systems Using Artificial Intelligence Models for Payment Fraud Identification with Mitigation,” in *2026 14th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, Mar. 2026, pp. 01–06. doi: 10.1109/ISDFS69419.2026.11459006.

[17] N. Uddin, “Role of AI in Preventing Financial Crime: A Comprehensive Analytical Review,” *J. Econ. Criminol.*, p. 100200, Oct. 2025, doi: 10.1016/j.jeconc.2025.100200.

[18] O. Odeyemi, N. Z. Mhlongo, E. E. Nwankwo, and O. T. Soyombo, “Reviewing the role of AI in fraud detection and prevention in financial services,” *Int. J. Sci. Res. Arch.*, vol. 11, no. 1, pp. 2101–2110, 2024, doi:

10.30574/ijsra.2024.11.1.0279.

[19] H. Sugiarto, Masruchan, and I. W. Siwantara, "Artificial Intelligence in Financial Decision-Making: Opportunities and Challenges for Investment Strategies," *J. Inform. Ekon. Bisnis*, pp. 364–370, Jun. 2025, doi: 10.37034/infeb.v7i2.1140.

[20] N. Kandregula, "Leveraging Artificial Intelligence for Real-Time Fraud Detection in Financial Transactions: A Fintech Perspective," *World J. Adv. Res. Rev.*, vol. 3, no. 3, pp. 115–127, 2019.

[21] A. H. Ali and A. Ali Hagag, "An enhanced AI-based model for financial fraud detection," *Int. J. Adv. Appl. Sci.*, vol. 11, no. 10, pp. 114–121, 2024, doi: 10.21833/ijaas.2024.10.013.

[22] P. K. Zorion, L. Sachan, R. Chhabra, V. Pandey, and D. H. Fatima, "Credit Card Financial Fraud Detection Using Deep Learning," *SSRN Electron. J.*, 2023, doi: 10.2139/ssrn.4629093.

[23] M. M. Ismail and M. A. Haq, "Enhancing Enterprise Financial Fraud Detection using Machine Learning," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 4, pp. 14854–14861, 2024, doi: 10.48084/etasr.7437.

[24] X. Yang *et al.*, "FinChain-BERT: A High-Accuracy Automatic Fraud Detection Model Based on NLP Methods for Financial Scenarios," *Information*, vol. 14, no. 9, p. 499, Sep. 2023, doi: 10.3390/info14090499.

[25] N. Jahan Sarna *et al.*, "AI Driven Fraud Detection Models in Financial Networks: A Comprehensive Systematic Review," *IEEE Access*, vol. 13, pp. 141204–141233, 2025, doi: 10.1109/ACCESS.2025.3596060.

[26] F. H. Boltaev and N. G. Rakhmatullaev, "Artificial Intelligence Techniques For Financial Fraud Detection: A Comprehensive Review Of Machine Learning, Deep Learning, And Hybrid Models," *Econ. Innov. Technol.*, vol. 13, no. 2, pp. 160–174, 2025.

[27] P. Kamuangu, "A Review on Financial Fraud Detection using AI and Machine Learning," *J. Econ. Financ. Account. Stud.*, vol. 6, pp. 67–77, 2024, doi: 10.32996/jefas.6.1.7.

[28] O. Olowu *et al.*, "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, doi: 10.30574/gscarr.2024.21.2.0418.

[29] P. Sood, C. Sharma, S. Nijjer, and S. Sakhuja, "Review the role of artificial intelligence in detecting and preventing financial fraud using natural language processing," *Int. J. Syst. Assur. Eng. Manag.*, vol. 14, no. 6, pp. 2120–2135, 2023.

[30] A. Ali *et al.*, "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Appl. Sci.*, vol. 12, no. 19, Sep. 2022, doi: 10.3390/app12199637.

