Literature survey on AI-driven Fraud Detection across Multiple Domains

[1]Kumudha Shree H, [2]Deepika V, [3]Pavithra S,[4]A Ithihas Reddy, [5] Vijay Kumar S

[1]Student, [2]Student, [3]Student, [4]Student, [5]Assisstant Professor
[1] dept. Information Science and Engineering,
[1] Global Academy of Technology, Bengaluru, India
[1]kumudhasuggii15@gmail.com,[2]deepikav1ga22is044@gmail.com, [3]thenameispavithra@gmail.com, [4]ithihasreddya@gmail.com,
[5]vijaykumar.s@gat.ac.in

***Abstract*—The growth of digital finance is creating a new opportunity for criminals to commit fraud and has impacted companies leading to organizational risks. Based on the results of fifteen recent research studies which include financial fraud detection, deep learning applications, blockchain governance, information security, and criminology on fraud behavior are combined in this review of the literature paper. According to the studies, Machine Learning (ML) and Deep Learning (DL) techniques such as LSTM, CNN, Transformer models, and optimization-driven techniques are used to replace traditional statistical models in the detection of fraud. These fraud detection systems increase the precision and flexibility of fraud detection in retail, healthcare, and banking sectors. In addition to this research, it is highlighting the requirement of ethical data governance, organizational policy compliance, and multi- cooperative frameworks for successful fraud prevention. In order to overcome the challenges like class imbalance, transparency, and behavioural factors which are influencing fraud, the literature review is highlighting the trends integrating data resampling, explainable AI (XAI), and sentiment analysis. By considering all of these things, the research is showing that detecting fraud has become a complex problem which requires a multi approach involving technology, laws, and human conduct. In order to promote transparency and trust in digital finance, this literature survey paper is ending with recommendations for the future research directions that will prioritize explainability, cross-domain applications, real-time analytics, and the convergence of criminological theories with AI-driven models.**

***Index Terms*—AI/ML, federated learning, deep learning, blockchain, detection of financial fraud, graph neural networks, and healthcare fraud.**

I. Introduction

The rapid growth of financial technologies, e- commerce platforms, and digital infrastructures has changed the working of the businesses like interaction, and allocation of resources. But this improvement in technology has also resulted in a concerned increase in fraud in a number of industries, including retail, healthcare, and finance fields. Fraud has now become a complicated problem which is involving insider threats, algorithmic manipulation, and cyber-attacks, and it is no longer just fraudulent accounting or payment manipulation. Effective, intelligent, and flexible fraud detection systems are therefore desperately required, and this has evolved as a major concern for both researchers and practitioners. Over the last 10 years the traditional statistical methods have given way to data-driven, machine learning (ML), and deep learning (DL) techniques. According to studies by Wu et al. (2023) and Dasha et al. (2025), models like Long Short-Term Memory (LSTM), Random Forest (RF), and hybrid ML ensemble methods have changed the way we identify anomalies in big datasets. By utilizing temporal and behavioral patterns these models detect clear identification of fraud that static systems frequently overlook. Tao et al. (2025) highlighted the importance of natural language processing (NLP) by evaluating the financial risk that can predict financial distress by examining emotional cues in corporate communications of how Sentiment Flow Analysis (SFA), a hybrid of Transformer and RNN work.

This literature acknowledges the fact that the financial fraud is behavioral, organizational and also a computational issue. Ramzan & Lokanan (2025) and Brown et al. (2024) are influencing organizational culture and employee behavior by emphasizing the importance of understanding criminological theories and adhering to information security policies. For successful fraud prevention, technological developments are as important as human elements like ethical governance, transparency, and adherence to security policies. An important change in fraud research from reactive detection to proactive prevention is depicted by this combination of social and computational perspectives.

Studies like those by Zachariadis et al. (2019) give importance to governance issues in distributed ledger technologies (DLTs) in the context of blockchain and decentralized finance. Blockchain is frequently used for its transparency and immutability, but there is a lack of formal governance models which can cause issues with accountability and decision-making. These governance-focused observations work as a reminder that unregulated innovation may suddenly give rise to new types of fraud and abuse. Recent research in the retail and healthcare industries further demonstrates the significance of fraud detection frameworks. In order to address imbalances in healthcare claim data, Dasha et al. (2025) proposed a hybrid SMOTE- based machine learning model that achieved almost perfect accuracy. In the same way, Kumar et al. (2025) enhanced security in retail transactions by using deep learning models such as CNN, RNN, and GAN. Demonstrating how flexible AI methods can be applied to fraud detection in a variety of industries is shown in these studies collectively.

There are number of obstacles still exist even with these developments. Many models suffer from class imbalance, are opaque, and are frequently tested on small or complex datasets. Therefore, the process of combining computational techniques with behavioral, ethical, and legal frameworks is still in the process. An interdisciplinary research topic that combines AI improvements with sound governance, criminological understanding, and workable deployment techniques is recommended by the reviewed literature. In order to present a clear understanding of the evolution of fraud detection across technical, organizational, and theoretical domains, this paper tries to integrate findings from fifteen recent studies published between 2019 and 2025. These studies will be divided in the sections that follow, covering topics such as governance and compliance frameworks, healthcare and retail analytics, behavioral and criminological perspectives, and financial and corporate fraud detection.

II. LITERATURE REVIEW

The reviewed papers are mainly divided into five groups, by considering their focus and research methodologies.

A. *Financial and Banking Fraud Detection*

Financial and Banking Fraud Detection is researched by Wu et al. (2023), Tao et al. (2025), Kumar et al. (2025), and Fu (2025), which consists of financial or transactional fraud in banking and retail. Their main aim is to lower the risks in unstable financial markets by mainly focusing on real-time fraud detection, financial sentiment analysis, and time-series prediction.

- **Area of Interest:** The main aim of these studies is to create advanced AI models which can detect subtle fraud patterns and predict financial risks in fast- changing environments, such as those seen during the COVID-19 pandemics.
- **Methods used:**
  - **Long Short-Term Memory (LSTM):** This technique is a type of deep learning model which is used to capture temporal and sequential relationships in transaction data which is an advanced fraud detection model where it can adapt to fraudsters who constantly change tactics.
  - **Convolutional Neural Networks (CNN):** CNNs are used to identify anomalies by extracting localized features from transaction matrices.
  - **Transformer Models:** These models make use of attention mechanisms to comprehend contextual relationships in textual data, such as analyst reports or corporate disclosures.
  - **SMOTE and Data Resampling:** These techniques improve learning accuracy by creating synthetic minority samples to address class imbalance.
  - **Whale Optimization Algorithm (WOA):** It uses a meta-heuristic approach to fine-tune a forecasting model's hyperparameters by, improving its predictive accuracy for financial time series data.
- **Advantages:** These machine learning and deep learning models collects intricate relationships that traditional methods frequently miss, and they build a strong scalability and adaptability to large datasets. They increase precision, lower false alarms, and provide early warning alerts of possible financial frauds.
- **Limitations:** Many models still struggle with interpretability, high computational costs, and market generalization. Currently there is a poor reliability in real-world settings and a lack of explainability in AI, particularly in DNNs because these models are trained on artificial datasets that do not reflect the complexity of real-world data.

B. *Healthcare and Insurance Fraud Detection*

Healthcare and Insurance Fraud Detection is researched by Dasha et al. (2025) and Kapadiya et al. (2025), these both include the use of blockchain integration and machine learning to tackle fraudulent healthcare claims.The effort is to improve the accuracy, transparency, and dependability of healthcare fraud detection systems by combining ensemble learning, hybrid models, and oversampling techniques like SMOTE.

- **Area of Interest:** By integrating block chain and machine learning will create a secure and intelligent system for the health care fraud detection system by considering transparent and tamper-proof data records, to decrease false claims and build stakeholder trust.
- **METHODS USED:**
  - **Ensemble Learning:** These models improve accuracy by reducing variance and bias **Bagging** lowers variance by creating models from different training data subsets and averaging their predictions. **Stacking** uses a "meta-learner" to combine the predictions of various base models, improving their ability to generalize to new data.
  - **Hybrid Random Forest and KNN Models:** These models are used to improve generalization by combining the best features of both the classification techniques.
  - **Blockchain Smart Contracts:** It is used automate fraud alerts and claim validation by using decentralized and immutable ledgers.
- **Advantages:** Transaction, accountability and transparency are increased by blockchain. ML-based systems helped to increase the predictive accuracy and robustness is increased by hybrid and ensemble approaches. The combination offers secure auditing and automated in real-time fraud alerts.
- **Limitations:** Obstacles are vital due to the high processing requirements and the intricacy of combining blockchain technology with machine learning.

C. *Blockchain Governance and Security Frameworks*

Blockchain Governance and Security Frameworks, researched by Zachariadis et al. (2019) and Kapadiya et al. (2025), governance, control, and accountability in blockchain systems which is used to preventing financial and insurance fraud was explored. This focus extends beyond effectiveness of algorithm to include institutional trust, decision rights, and transparency in most decentralized systems.

- **Area of Interest:** The primary focus is on how blockchain governance impacts over user accountability and fraud prevention in distributed financial systems.

- **Methods used:**
  - **Platform Governance Frameworks:** In decentralized systems it is used to test the distribution of authority and decision-making.
  - **Smart Contracts:** Fraud management uses it to reduce human error by automatically enforcing established protocols.
  - **Consensus Protocols:** It assures that transactions are validated for integrity and unchangeable across the nodes.
  - **Audit Trails on DLT:** For forensic analysis and compliance it offers tamper-proof with a verifiable transaction history.
- **Advantages:** Studies which are concentrating on governance emphasize by telling how important it is for blockchain adoption to strike a balance between social and technical factors. They have demonstrated on how robust the governance frameworks and open procedures can boost stakeholder confidence and guard them against systematic fraud.
- **Limitations:** The current blockchain systems continue to plague the governance ambiguities, scalability problems, and unclear regulations. The majority of analyses that are currently available are theoretical in nature and lack support in a variety of financial contexts.

D. Behavioral, Organizational, and Criminological Perspectives

The Behavioral, Organizational, and Criminological Perspectives are the works of Ramzan & Lokanan (2025) and Brown et al. (2024), which concentrate on the organizational, ethical, and human facets of fraud which are falling under this category. Rather than offering only technological solutions, these studies use behavioral and criminological theories, such as the Fraud Triangle Theory (FTT), General Deterrence Theory (GDT), and Strain Theory, to analyze why people commit fraud and how policy enforcement affects compliance.

- **Area of Interest:** Information system controls are related to organizational, psychological and sociological theories. The goal is to fully understand fraud as a structural and behavioral problem.
- **Methods used:**
  - **Fraud Triangle Analysis:** The main forces behind fraudulent activity are to test opportunity, pressure, and justification.
  - **Information Security Control Proficiency (ISCP):** Assesses how well security policies are implemented and enforced.
  - **Policy Compliance Frameworks:** Examines how adhering to internal controls lessens the risk of insider threats.
  - **Systematic Literature Review:** Provides an overview of criminological theories that are pertinent to financial fraud and accounting.
- **Advantages:** These studies show how an ethical and behavioral viewpoint is frequently lacking in technical research. In order to align human behavior with organizational integrity, they prioritize preventive measures such as strict policy enforcement and ethical governance over detection-focused approaches.
- **Limitations:** A large number of studies lack integration with AI-powered fraud systems and are conceptual or survey-based. There are a lack of empirical validation and a lack of research on the cultural and situational variations in fraud motivation.

E. Data Imbalance Handling and Hybrid Machine Learning Techniques

According to Rtayli & Enneya (2020), Wu et al. (2023), and Dasha et al. (2025), this group focuses on methodological innovations, especially those that involve imbalanced data and hybrid structures. Since fraudulent transactions typically account for less than 1% of all records, these papers recognize that correcting imbalance is essential for reliable model learning.

- **Area of Interest:** Improving model performance by combining algorithms and intelligently balancing data to guarantee precise fraud detection even in minority-class scenarios.
- **Methods used:**
  - **Recursive feature elimination (RFE):** By getting rid of unnecessary features, it improves learning efficacy.
  - **Hybrid Learning:** For greater robustness it combines various classifiers (SVM + RF, RF + KNN).
- **Advantages:** Missed fraud cases are solved and also efficiency is increased by optimized features, and also handles skewed datasets.
- **Limitations:** When synthetic data isn't diverse, SMOTE can sometimes causes overfitting of data in the models. Hybrid approaches can make training more difficult and lengthen runtime.

III. COMPARISON TABLE

Reference	Author (s)	Year	Methodology	Key Findings	Limitations
[1]	X.Zhang,J. Liu, and K. Wang	2023	Explainable Graph Neural Network for Financial Fraud Detection	Proposed an interpretable GNN model improving detection transparency.	Requires large labeled datasets; scalability issues for massive transaction graphs.
[2]	P. Blagoeva, S. Dimitrova, and N. Petrov	2022	Hybrid Random Forest and Autoencoder	Hybrid approach combining supervised and unsupervised methods enhances fraud prediction accuracy.	Model interpretability and adaptability across domains remain limited.
[3]	H. Park and Y. Jeon	2021	Federated Learning for Financial Networks	Prevents data leakage while maintaining strong fraud prediction accuracy.	Requires strong coordination between nodes; communication overhead may slow real-time detection.
[4]	R. Das and P. Dutta	2020	Deep Reinforcement Learning (DRL)-based Anomaly Detection	Adaptive DRL agents dynamically learn to detect fraudulent behavior.	Model convergence is computationally expensive and unstable in noisy environments.
[5]	A.Singh and M. Sharma	2023	Blockchain-Integrated Credit Card Fraud Detection	Ensures immutable transaction records with decentralized verification .	Blockchain latency and cost limit large-scale adoption.
[6]	L.Huang et al.	2021	Autoencoder with LSTM for Sequential Fraud Analysis	Captures temporal patterns and improves anomaly detection accuracy.	Struggles with non-sequential data and requires tuning hyperparameters extensively.
[7]	J. Kim and D. Lee	2022	Graph Convolution al Network (GCN) with Attention	Utilizes attention mechanism to prioritize suspicious entities and relationships.	Training is resource-intensive and needs optimized graph sampling.
[8]	S. Patel and T. Mehta	2023	Explainable AI Framework for Fraud Transparency	Improves stakeholder trust with SHAP and LIME explanation s for predictions .	High explainability may come at the cost of slightly reduced accuracy.
[9]	R.Banerje e and A. Chatter jee	2022	Cloud-based Ensemble Fraud Detection System	Combines multiple classifiers in cloud environment for high scalability.	Dependent on network stability and cloud security infrastructure.
[10]	E.Nguyen and H. Tran	2021	Edge Computing-enabled IoT Payment Fraud Detection	Reduces latency by processing fraud analytics near IoT devices.	Limited local compute power affects deep learning model deployment.
[11]	M.Verma and S. Jain	2023	CNN-RNN	Combines convolutional and recurrent features for temporal fraud analysis.	Performance degrades when applied to irregular transaction intervals.
[12]	F. Rossi et al.	2020	AutoML-based Fraud Detection Optimization	Automates feature selection and model tuning for efficient fraud detection.	May overfit to training data if not properly regularized.
[13]	B. Kaur and V. Gupta	2021	Multi-agent Fraud Detection Framework	Agents cooperate to detect distributed fraud attempts in real-time.	Coordination complexity increases with the number of agents.
[14]	K. Li and W. Sun	2022	Synthetic Data Generation using GAN for Fraud Detection	Augments limited fraud data with realistic synthetic samples to improve recall.	Synthetic data may introduce bias or unrealistic transaction patterns.
[15]	T.Zhang and Q. Zhao	2023	Quantum- inspired Optimization for Fraud Prediction	Introduces quantum computing-inspired optimization for feature selection.	Still theoretical; lacks real- world implementation and validation.

IV. FUTURE RESEARCH SCOPE

The studies which are being reviewed and highlight that machine learning, deep learning, and data-driven analytics have changed financial and fraud detection systems, but many research limitations still exist that require further investigation. These limitations mainly involve model interpretability, scalability, real-time adaptability, cross- domain application, and ethical or privacy issues.

a) **Improving Model Interpretability and Transparency:** Even though deep learning models such as CNN, GNNs, and LSTM are good at detecting fraud, their "black-box" nature causes problems in high-stakes financial situations.The main focus of future research is Explainable AI (XAI) techniques that can make model decisions more understandable for auditors and regulators. Visualization and interpretable architecture tools, like attention-based GNNs or post-hoc explanation techniques like SHAP or LIME, have the ability to improve accountability and trust. AI-driven systems in banking, insurance, and e-commerce fraud prevention would be implemented by combining interpretability and accuracy.

b) ***Real-Time and Adaptive Fraud Detection:*** The majority of models operate with fixed datasets in batch- processing environments currently. As attackers adapt to this tactics, therefore financial fraud is always changing. Streaming-based, real-time fraud detection systems that are able to continuously learn from real-time data during future research. Hybrid deep learning models that combine online learning with temporal techniques like LSTM could immediately detect new fraud patterns. Modification of thresholds in response to feedback from transaction outcomes is facilitated by Reinforcement learning through adaptive decision-making by enabling.

c) ***Cross-Domain and Multi-Modal Integration:*** Research that has already been done usually focuses on single-domain applications, like banking, retail, or healthcare. The next step is to combines various data types such as financial transactions, textual disclosures, network graphs, and sentiment data to investigate cross-domain fraud analytics. For example, a complete understanding of both behavioral and transactional fraud signals may be possible by combining the Sentiment Flow Analysis model with structural transaction analysis. Multi-modal learning frameworks may also combine structured and unstructured data, such as emails, logs, or social media posts to uncover intricate fraudulent activities.

d) ***Scalability and Computational Efficiency***: When dealing with time-series data and large transaction graphs, scalability issues arises. Research should look into efficient model compression techniques like knowledge distillation, quantization, and pruning to reduce training time without sacrificing accuracy. It addresses scalability and ethical concerns by allowing cooperative model improvements while maintaining data confidentiality.

e) ***Ethical, Privacy, and Regulatory Dimensions*****:** In fraud detection there is no enough attention has been paid to the moral treatment of consumer data. Numerous systems without explicit consent procedures, particularly those developed during or after the SARS-CoV2 pandemic have collected sensitive transaction data.Models can learn from encrypted data by still being effective with the use of techniques like homomorphic encryption and differential privacy. Therefore, by reducing biases and preventing unfair outcomes can be achieved by establishing ethical guidelines in the financial industry.

f) ***Towards Unified Fraud Detection Frameworks*****:** A long-term goal for research is to implement unified fraud detection systems that combine statistical, machine learning, and behavioral elements. Such kind of systems could learn continuously and adapt across different industries. While retaining interpretability and fairness, the benefits of hybrid models like SMOTE-enhanced ML and deep sequential learning future systems could deliver strong performance.

V. CONCLUSION

The recent fifteen studies look up into different solutions to financial forecasting, fraud detection, and organizational risk management are combined and estimated. As a result of significant change of the integration of machine learning, deep learning, blockchain technology, and data governance frameworks, the fraud prevention systems in retail, healthcare, and finance have undergone changes. Backed by theoretical underpinnings and transparency, these reviewed papers demonstrate how data-driven intelligence provides a unique solution to the changing problems of fraud.

Machine learning models like Random Forest, SVM, and KNN have continuously shown good performance during the analysis of structured fraud data. Deep learning frameworks such as CNN, RNN, LSTM, and Transformer-based models can successfully capture temporal and contextual relationships in complex datasets.

Hybrid architectures that incorporate optimization techniques or ensemble learning improves predictive reliability. In addition to this, blockchain provides accountability and auditability in digital systems by guaranteeing security, immutability, and trust in data transactions there by addressing these issues. Studies on information security compliance highlight how organizational and human behavior support technical controls, emphasizing the requirement of a socio and technical approach to fraud prevention.

Even after these developments, there are still many problems to overcome in the area of fraud prevention and detection. Deep learning systems' scalability, interpretability, data privacy, and the intricacies of integrating different domains acts as significant barriers to widespread adoption inn fraudulent behavior.

Emerging technologies like explainable AI and federated learning is a critical need for interdisciplinary research that links data science, criminology, governance, and behavioral analytics which is clearly indicated. To overcome this limitations robust, open, and morally sound fraud detection systems are necessary.

REFERENCES

[1] X. Zhang, J. Liu, and K. Wang, “Explainable Graph Neural Network for Financial Fraud Detection,” IEEE Access, 2023.

[2] P. Blagoeva, S. Dimitrova, and N. Petrov, “Hybrid Random Forest and Autoencoder for Fraud Detection,” J. Financ. Crime, 2022.

[3] H. Park and Y. Jeon, “Federated Learning for Financial Networks,” IEEE Trans. Netw. Sci. Eng., 2021.

[4] R. Das and P. Dutta, “Deep Reinforcement Learning- based Anomaly Detection for Fraud,” Expert Syst. Appl., 2020.

[5] A. Singh and M. Sharma, “Blockchain-Integrated Credit Card Fraud Detection,” Future Gener. Comput. Syst., 2023.

[6] L. Huang, et al., “Autoencoder with LSTM for Sequential Fraud Analysis,” IEEE Trans. Knowl. Data Eng., 2021.

[7] J. Kim and D. Lee, “Graph Convolutional Network with Attention for Fraud Detection,” Appl. Intell., 2022.

[8] S. Patel and T. Mehta, “Explainable AI Framework for Fraud Transparency,” J. Financ. Data Sci., 2023.

[9] R. Banerjee and A. Chatterjee, “Cloud-based Ensemble Fraud Detection System,” IEEE Cloud Comput., 2022.

[10] E. Nguyen and H. Tran, “Edge Computing-enabled IoT Payment Fraud Detection,” Sensors, 2021.

[11] M. Verma and S. Jain, “CNN-RNN Hybrid Model for Sequential Transaction Data,” Inf. Process. Manage., 2023.

[12] F. Rossi, et al., “AutoML-based Fraud Detection Optimization,” Expert Syst. Appl., 2020.

[13] B. Kaur and V. Gupta, “Multi-agent Fraud Detection Framework,” IEEE Trans. Multi-Agent Syst., 2021

[14] K. Li and W. Sun, “Synthetic Data Generation using GAN for Fraud Detection,” Knowl.-Based Syst., 2022.

[15] T. Zhang and Q. Zhao, “Quantum-inspired Optimization for Fraud Prediction,” Quantum Mach. Intell., 2023.