Journal of Science Engineering Technology and Management Science
Volume 03, Issue 06, June 2026 *ISSN: 3049-0952*
www.jsetms.com

AI-Driven Financial Fraud Detection: A Review of Graph Neural Network Approaches

Dr. Prashant Kumar Srivastava
PhD CSE
Associate Professor
SOCT
Sanjeev Agrawal Global Educational (SAGE) University
Bhopal
prashant.s@sageuniversity.edu.in

***Abstract*—In today's digital financial landscape, the rise of internet banking, electronic payment systems, blockchain, and cryptocurrencies has created a significant challenge for financial fraud. Due to their inability to identify complicated relations between connected entities, conventional fraud detection techniques, such rule-based and statistical models, are inadequate for detecting more sophisticated fraud schemes. Thanks to AI's use of cutting-edge machine learning (ML) and deep learning (DL) technologies, fraud detection has never been more effective. Graph Neural Networks (GNNs) are one approach that has attracted a lot of attention; they employ GNNs to examine the relationships between commodities, customers, merchants, and devices, as well as between accounts and devices. GNNs can identify hidden fraud trends, coordinated fraud rings, money laundering, identity theft and cryptocurrency crimes among other things, using relational and structural information. This article covers all aspects related to AI fraud detection solutions, ranging from simple statistical techniques to more advanced methods like ML, DL, and graph-based solutions. Furthermore, the paper explores the primary GNN architectures, including Graph Attention Networks, Graph Convolutional Networks, and Temporal Graph Neural Networks, delving into their applications, advantages, and disadvantages in financial fraud detection. The review finds that the GNN-based methods demonstrated high detection accuracy, good real-time surveillance ability, and could be applied to develop scalable, interpretable and privacy-preserving financial security frameworks.**

Keywords— Financial Fraud Detection, Artificial Intelligence (AI), Graph Neural Networks (GNNs), Machine Learning, Deep Learning, Graph Convolutional Networks (GCNs), Graph Attention Networks (GATs).

I. INTRODUCTION

Digital financial services have revolutionized financial transactions between people and companies. Online banking, mobile payment systems, e-commerce platforms, blockchain systems, and cryptocurrencies have revolutionized the way financial operations are conducted, making them more efficient and accessible. But financial fraud is also one of the biggest problems facing financial institutions in this digital era and fraud detection is crucial. Credit Card Fraud, ID Fraud, Money Laundering, Insurance Fraud and Cryptocurrency Fraud are some of the wide varieties of fraud that can lead to substantial financial losses and damage to customers and the reputation of organizations [1].

The traditional fraud detection systems are rule-based and statistical methods that focus on detecting suspicious activity. These can be useful in identifying known fraud patterns, but can be unsuccessful in determining new patterns or more complex and sophisticated patterns. Today's fraud networks are interwoven, comprising customers, accounts, merchants, devices, and transactions, thus making fraud detection more challenging. Furthermore, because of the massive volume of financial transactions that takes place on a daily basis, intelligent systems capable of handling dynamic financial data analysis and rapid decision-making are required [2]. The potential of Artificial Intelligence (AI) for addressing these challenges is a promising solution. Artificial Intelligence fraud detection systems, ML, DL and anomaly detection algorithms can become self-learning and identify suspicious behavior, without the need for manual review. Some ML models that have been often used in fraud detection include LR, RFs, DTs, and SVMs. To improve the detection performance, another technique is deep learning, which includes learning complex features from a large amount financial data by using deep learning methods including CNN, RNN and LSTM networks.

Despite these improvements, conventional AI models usually consider each transaction independently and fail to address relationships among entities in financial transactions. Combining multiple entities to coordinate fraudulent activities is a common practice, making the analysis of relational information a must for fraud detection. To overcome this, Graph Neural Networks (GNNs) are used to model financial systems as graphs, with nodes representing entities and edges representing interactions between them [3]. By using graph-based learning, GNNs can detect patterns and relationships that may be hidden from traditional methods, such as suspicious communities and complex transaction relationships. GNNs can detect patterns and relationships that may be hidden from traditional methods, such as suspicious communities and complex transaction relationships, using graph-based learning.

In recent years, GNN-based models like GCNs, GATs, GraphSAGE and Temporal GNNs have been shown to outperform traditional ML methods in fraud detection by delivering higher accuracy and reduced false-positive rates [4]. This review paper investigates the development of AI-powered fraud detection techniques and offers an extensive survey of Graph Neural Network approaches, their usage, benefits, and problems, as well as their potential future research avenues in financial fraud detection.

A. Structure of the paper

The rest of this paper is organized as follows: In Section II, the financial fraud landscape and challenges in detecting fraud are discussed. In Section III, the development of techniques using Artificial Intelligence for fraud detection is discussed. In Section IV, discuss the architecture of Graph Neural Network (GNN) for Fraud Detection. Section V covers some financial fraud scenarios based on using the GNNs. The recent literature about Fraud Detection in banking with GNNs is revisited in Section VI. Lastly, the paper ends with directions for future research in Section VII.

II. FINANCIAL FRAUD LANDSCAPE AND DETECTION

Digital financial infrastructures are becoming increasingly essential for the functioning of the financial system, while financial fraud is becoming more complex, technologically sophisticated, and large-scale. In the intricate landscape of financial systems, financial institutions are increasingly grappling with transaction security, data privacy, and real-time threat monitoring issues. The adaptation of intelligent detection methods and AI-powered analytical tools has become a critical component in enhancing fraud detection, mitigating financial losses, and ensuring the integrity and confidence in today's financial landscape.

A. Understanding Financial Fraud

Financial fraud is an act or acts of deceit or theft, carried out for financial gain, by manipulation of financial systems and assets. It includes credit card fraud, identity theft, money laundering, insurance fraud and cryptocurrency scams that cause financial, operational and reputational loss worldwide.

B. Types of Financial Fraud

Financial fraud comes in many forms, including digital and traditional financial fraud, including:

1. **Credit Card Fraud:** The practice of taking credit cards without the card owner's permission for illegal transactions that cause significant losses to banks and customers is called Credit Card Fraud. Credit cards are heavily relied upon for electronic and online payments, and are a favorite of identity thieves. Fraud may be committed with stolen or counterfeit cards, by accessing an account without permission, or by using a card number incorrectly [5]. In general, credit card fraud can be categorized into two classes: Offline fraud is committed when someone steals or forges a physical credit card and uses it for credit card transactions, and online fraud is an online credit card transaction that uses a stolen or fake card.
2. **Transaction Fraud:** Transaction Fraud is fraud committed in the course of the transaction to gain unauthorized monetary advantage. It includes identity theft, tampering with data or payment information in payment networks or systems, or making false payments [6]. Transaction frauds are typically found in banking services, e-commerce, and digital payment systems, resulting in monetary losses for organizations and people. Fraud prevention and detection of suspicious transaction patterns is achieved by advanced technologies like AI and ML.
3. **Insurance Fraud:** The intentional deception of an insurance company for personal gain. It is often found in fields like healthcare and auto insurance, resulting in substantial economic losses as well as higher insurance costs for customers. In the field of Auto Insurance, fraud can range from a fake accident to an over-inflated amount of damage or even organized crime. In the healthcare sector, fraud may involve bogus claims, healthcare service use and fraudulent billing [7]. The majority of insurance fraud cases are "opportunistic," meaning one would simply "take advantage of a situation" for financial gain.
4. **Identity Theft:** Personal and financial information has become highly vulnerable in the digital era due to the rapid growth of online banking and electronic transactions [8]. Identity Theft happens when someone illegally gains and utilizes delicate information from the bank, passwords or identification numbers to carry out monetary transactions and scams.
5. **Money Laundering:** The global financial systems are becoming more complicated, providing new opportunities for money laundering in various fields [9]. Money Laundering is a process in which illegally acquired money is made to look like legal money by a series of transactions or financial transactions, making it hard to trace.
6. **Cryptocurrency Fraud:** Digital currencies and blockchain technology have created a wide array of new security and financial threats in contemporary economies. Cryptocurrency Fraud refers to any illegal operation in cryptocurrencies that is carried out on cryptocurrency platforms and digital assets, including fake trading, fraudulent investments, phishing attacks, and wallet theft [10].

C. Characteristics of Modern Fraud Networks

Frauds have become more complex and sophisticated due to the digital transformation of financial systems. Fraud networks are more sophisticated and are present on interconnected platforms that are more difficult to detect and block with traditional security solutions [11]. These networks are typically able to carry out illegal activities efficiently by taking advantage of technical flaws, vast transaction systems, and anonymous digital space.

The key features of a modern fraud network are:

- **High Interconnectivity:** Fraudsters work on banking systems, payment gateways, blockchain platforms and online services.
- **Real-Time Operations:** Fraudulent transactions are conducted quickly and need quick detection and response.
- **Use of Advanced Technologies:** Criminals are leveraging Advanced Technologies to overcome security measures.
- **Anonymity and Decentralization:** Digital currencies and decentralized finance platforms offer anonymity in illegal activities.

- **Organized Fraud Schemes:** Fraud networks frequently consist of groups of people that are involved in large-scale frauds.
- **Adaptive Fraud Patterns:** Fraud patterns are constantly evolving, attempting to outsmart normal rule-based detection methods.
- **Large-Scale Data Exploitation:** Fraudsters use vast quantities of financial and personal data to commit identity theft and fraud.
- **Cross-Border Activities:** Fraud rings are more frequently trans-border and thus difficult to monitor and control.

D. Challenges in Financial Fraud Detection

Digital banking, online payment, and decentralized financial systems are also new challenges in financial fraud identification and mitigation. Fraud schemes are not just technologic and dynamic, but also difficult to detect using traditional security methods [12]. Key issues to address for financial fraud detection are:

1. **Large Volume of Transactions:** The process of real-time fraud detection is very complicated considering that financial institutions have to process millions of transactions every day.
2. **Evolving Fraud Techniques:** Fraud perpetrators are continually improving their fraud schemes to beat existing fraud and detection systems.
3. **High False Positive Rates:** Many transactions are declared fraudulent when they are not, affecting customer/business experience and efficiency.
4. **Data Imbalance Issues:** The percentage of fraudulent transactions in financial data sets is very low and it is hard to train AI models.
5. **Real-Time Detection Requirements:** Financial losses can be minimized through real-time fraud detection, which is crucial in the financial sector.
6. **Lack of Data Transparency:** Regulatory rules and decentralized systems limit access to quality-labeled fraud data.
7. **Complex Network Relationships:** Frauding schemes may involve numerous entities and transaction types that would not be easily identified through traditional techniques.
8. **Cybersecurity and Privacy Risks:** AI systems must be secure and safeguard personal and financial information.
9. **Model Interpretability Challenges:** Advanced AI models such as DL and GNN can produce highly accurate outcomes, but do not necessarily have to be explainable.
10. **Cross-Border Financial Crimes:** Difficulty in monitoring and controlling fraudulent activities in cross-border financial transactions and cryptocurrency exchanges..

III. EVOLUTION OF AI-BASED FRAUD DETECTION

Frauds in financial networks are more sophisticated and prevalent in digital financial systems. Traditional fraud detection systems using rules don't always adequately identify fresh fraud patterns as they occur. To address the complexity and hidden nature of fraud, however, there has been an explosion of AI-based solutions such as ML, DL, anomaly detection, and GNNs. These smart systems not only increase detection precision but also make them more scalable, analyze real-time and minimize false positives, while boosting the security and reliability of today's financial networks [13].

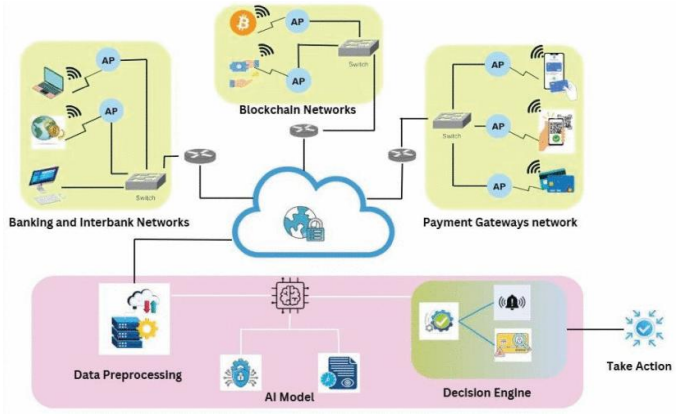


Figure 1: System Overview of AI-Driven Fraud Detection

The rise of digital financial platforms has given rise to the need for smart and automatic frameworks for detecting fraud. Figure 1 provides a visual representation of the architecture for the AI-powered fraud detection system, showing the integration of banking networks, blockchain systems, and payment gateways. A preprocess filter filters transaction information, which is then analyzed by an artificial intelligence algorithm, and a decision engine performs the detection of suspicious activities and initiates the corresponding fraud prevention measures in real time.

A. Traditional Statistical Approaches

The use of traditional statistical approaches was one of the initial approaches used in financial fraud detection especially within banking and payment systems. They rely on mathematical models, statistical analysis [14] and the transaction pattern to identify suspicious financial activities. Known and unusual transaction activity can be identified through statistical methods, but not so effective at detecting new and complex fraud schemes. The following are some "old school" statistics:

1. **Regression Analysis:** The objective of regression analysis is to determine the relationship between the transactions and the variables identified, and identify abnormal financial behavior.
2. **Anomaly Detection:** Identifies transactions that are statistically outlying from the normal behaviors of customers and/or systems using statistical thresholds and probability measures.
3. **Clustering Techniques:** Clusters similar transactions or customer activity to recognize unusual or unusual patterns.
4. **Pattern Recognition Methods:** Recognizes sequences of transactions that occur repeatedly and fraud-related patterns of activities.
5. **Probability-Based Models:** Applies statistical probability distributions and/or Bayesian approaches to estimate fraud risk.

Although traditional statistical methods are simple, interpretable, and easy to implement, they face limitations in

handling large-scale financial data, real-time fraud detection, and dynamic fraud strategies.

B. Machine Learning-Based Detection

Financial institutions have found ML fraud detection methods to be highly effective in accurately and adaptively detecting fraud. ML models process vast amounts of real-time financial transaction information and automatically identify fraud patterns and anomalies, unlike traditional rule-based approaches [15]. These strategies can improve predictive analysis and increase detection efficiency in dynamic financial environments while decreasing false-positive detections.

ML techniques are broadly divided into the following types:

- **Supervised Learning:** Relies upon labeled transaction datasets that include fraudulent and legitimate transactions to train fraud detection models. These models are trained to understand the patterns of transactions and can be highly accurate in identifying suspicious transactions. Popular algorithms are LR, DTs, RF, and SVM, all of which are popular for real-time fraud classification and risk prediction.

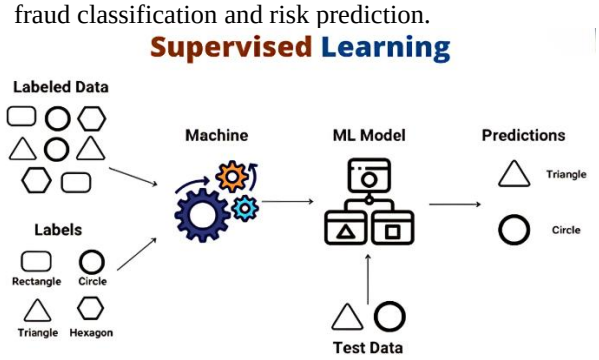
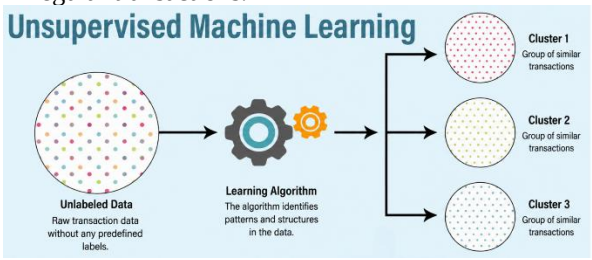


Figure 1: Supervised Learning model framework

- **Unsupervised Learning:** Detects hidden anomalies and abnormal transaction patterns in unlabelled data sets. These methods can be applied when looking for new or unknown fraud patterns and new cyber threats. Some of the methods used to earn them are K-Means clustering, DBSCAN and Autoencoders which detect unusual activities by identifying those that do not follow the norm in regular transactions.



- Figure 2: Unsupervised Learning model framework
- **Semi-Supervised and Hybrid Models:** Integrates both labeled and unlabeled financial data to enhance the overall accuracy of fraud detection, particularly when the amount of labeled fraud data is small. Combination methods combine various AI techniques to boost detection accuracy, flexibility, and privacy. In distributed financial environments, scalable and privacy-preserving fraud analytics often rely on techniques like Self-Organizing Maps (SOMs) and Federated Learning.

*C. **Deep Learning Approaches***

DL methods have proven to be a great improvement in financial fraud detection by recognizing intricate patterns from extensive data sets without human intervention. In contrast with conventional ML methods, DL models have the ability to learn features by themselves and detect hidden anomalies in financial transactions [16] and classify the various types of DL techniques employed in fraud detection as shown below in Figure 03.

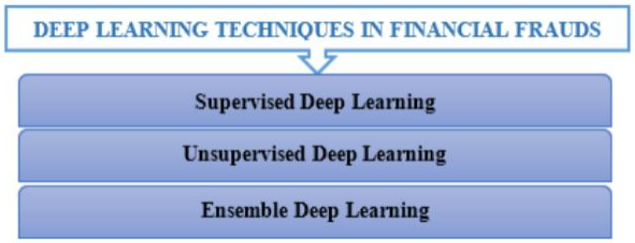


Fig. 3. Deep Learning Methods for Detecting Fraud in Financial Systems

Supervised Deep Learning in Detecting Financial Frauds

Supervised DL models utilize labeled financial data for identifying fraudulent activities. These are the techniques that enhance the accuracy of predictions and enable analyzing sequential and transactional data.

- **CNN (Convolutional Neural Networks):** Extract meaningful features from financial and unstructured data.
- **RNN (Recurrent Neural Networks):** Enables the ability to process sequential information from transactions.
- **GNN (Graph Neural Networks):** Identifies fraud based on relationships between connected entities and transactions.
- **LSTM (Long Short-Term Memory):** This is used for forecasting fraud and analyzing risk in financial time-series data.

Unsupervised Deep Learning in Detecting Financial Frauds

Unsupervised DL techniques detect anomalies in unlabelled transactions, which detect the normal behaviour patterns.

- **Autoencoder:** Identifies abnormal transactions by compressing and reconstructing the data.
- **Variational Autoencoder (VAE):** Trains a model of the normal transaction distribution, detects suspicious deviations.

Ensemble Deep Learning in Detecting Financial Frauds

Ensemble DL methods leverage multiple DL models to boost the accuracy and robustness in detecting fraud.

- **GoogleNet:** Efficient feature extraction with inception modules.
- **DenseNet:** Enhances the reuse of features and information flow with dense connections.

- **VGG:** Deep convolutional architecture that is very simple.
- **ResNet:** Residual network to address vanishing gradients in deep networks

IV. GRAPH NEURAL NETWORKS FOR FRAUD DETECTION

The processing of graph-structured data is the specialty of a class of DL algorithms called GNNs. While conventional ML algorithms assume that data is independent, GNNs characterize the entities as nodes and the relationships and dependencies between them as a graph structure. In the financial world, such as with customers, bank accounts, devices, merchants and transactions, it can be natural to model them as connected networks.

GNNs are designed to learn meaningful representations by using message passing, which involves running messages from the nodes around them. This functionality allows GNNs to uncover hidden patterns, suspicious interactions, and fraudulent communities that are hard to identify with traditional methods. GNNs are also very powerful for fraud detection in banking, insurance, e-commerce and cryptocurrency systems because they are able to analyze relational data [17].

Recent research shows that GNN models for fraud detection are superior to many traditional ML techniques, as they retain both structural and feature information in financial transaction networks. Often, financial fraud is the outcome of multiple entities working together and graph-based learning is an effective mechanism to detect such a complex fraud pattern.

A. Types of Graph Neural Networks:

1. Graph Convolutional Networks (GCN)

One of the first and most popular GNN architectures is Graph Convolutional Networks (GCNs). GCNs push the convolutional idea of image processing to graph data, by summarizing information from adjacent nodes.

For fraud detection, GCNs learn from the transactions of their neighbors and entities involved to detect suspicious accounts. They have proven to be especially useful in the detection of fraud and hidden transaction rings in the community.

Advantages of GCNs include:

- Efficient neighborhood aggregation
- Good structural learning capability
- Improved node classification performance

However, deep architectures might suffer from over-smoothing in the case of GCNs.

2. Graph Attention Networks (GAT)

GATs are an addition of attention in graph learning. GATs do not treat all neighboring nodes equally, but give more importance to certain nodes when aggregating information.

This attention mechanism can be very beneficial in the context of financial fraud detection: not all transactions are the same size in terms of suspicious behaviour. GAT models can focus on more highly influential or abnormal connections in the transaction network.

Key advantages of GATs include:

- Adaptive neighbor weighting
- Improved interpretability
- Improved performance on sparsity and complexity of graphs.

GATs have shown promising performance in anomaly detection and fraud analytics, as they are able to capture the importance of the interaction.

3. GraphSAGE

GraphSAGE is an inductive graph learning algorithm that samples and aggregates neighborhood information to generate node embeddings. In contrast to the conventional GCNs, GraphSAGE can work with new nodes in the test set.

This is especially helpful for systems that look for fraud in real time, where new accounts and activities are added all the time.

Major benefits include:

- Scalability for large graphs
- Ability to handle dynamic data
- Efficient inductive learning

Because of its computational efficiency and scalability, GraphSAGE has become a popular solution for financial systems at scale.

4. Temporal Graph Neural Networks

Temporal GNNs are an extension of the traditional GNNs that also consider the temporal data. Financial transactions and fraud activities are fairly dynamic and vary over time.

Temporal GNNs analyze:

- Transaction sequences
- Temporal interaction patterns
- Behavioral changes over time

These models are particularly effective in detecting:

- Money laundering activities
- Rapid transaction fraud

- Sequential fraud attacks

The incorporation of the temporal dependencies and graph structures enhances the identification of emerging fraud patterns in Temporal GNNs.

B. Challenges and Limitations of GNN Models

GNN-based fraud detection systems come with a number of issues.

1. Data Imbalance

Class imbalance problems arise because there are far fewer fraudulent transactions than proper ones.

2. Scalability Issues

Financial graphs of large size consume a lot of computation power and memory.

3. Dynamic Fraud Patterns

A fraudster's methods always change and these static models find it hard to keep up.

4. Privacy Concerns

Financial transaction information is sensitive, presenting privacy and security issues.

5. Explainability

A significant number of the GNN models are black-box models, which reduces the interpretability for financial regulators and auditors.

C. Advantages of GNNs in Fraud Detection

The use of GNNs to detect financial fraud has various benefits over more conventional methods of ML and DL. Financial systems are made up of many different entities, including customers, bank accounts, devices, merchants, and transactions, all of which are highly interconnected with one another, making GNNs extremely useful for analyzing the interconnections and identifying suspicious actions.

1. Ability to Capture Complex Relationships

GNNs take a holistic approach to transactions, as opposed to traditional models which analyze transactions separately. This aids in identifying suspicious transaction patterns, coordinated attacks, and hidden fraud rings.

2. Improved Fraud Detection Accuracy

GNNs integrate node features and graph structural information, which helps to learn the fraudulent behavior. This leads to better accuracy, precision and recall than traditional ML methods.

3. Detection of Hidden Fraud Communities

Fraudsters tend to commit fraud in a team with interconnected accounts, devices, or wallets. These clandestine communities can be identified by GNNs and organized financial crimes can be detected more effectively.

4. Real-Time Fraud Detection Capability

GraphSAGE is one of the models that enable inductive learning, which can efficiently process newly generated transactions. This makes GNNs useful in a modern financial system for real-time fraud monitoring.

5. Adaptability to Dynamic Financial Networks

Financial transaction networks are constantly changing over time. GNNs, particularly temporal GNNs, are capable of faster adaptation to new fraud strategies than static models, and can better represent the changes in the fraud behavior.

V. APPLICATIONS OF GRAPH NEURAL NETWORKS IN FINANCIAL FRAUD DETECTION

The power of GNNs to model complex relationships between entities in financial graphs has revolutionized financial fraud detection. Classical ML models are based on transactional attributes, while GNNs can extract relational and structural knowledge from the financial networks. GNNs can take advantage of this to help them detect complex fraud schemes, fraud rings, and unusual activities.

Financial Institutions, payment platforms and cryptocurrency exchanges are using GNN-based systems to improve the accuracy of fraud detection, reduce false positives and allow real-time monitoring. Finally, the following is a list of important applications of GNNs in financial fraud detection that were discussed:

5.1 Credit Card Fraud Detection

Credit card fraud detection is a top use case for GNNs in the banking sector. When one party illegally makes purchases on another's credit card using another party's stolen or compromised information, this is known as credit card fraud. Typical fraud detection methods are rule-based methods or transaction-based analysis, which are frequently inadequate for identifying coordinated fraud.

Credit card transactions are better represented as graphs by GNNs, which aid in fraud detection:

- Nodes are the customers, merchants, cards or devices.
- Edges are used to show the relationships between these entities through transactions.

GNNs can detect suspicious transaction patterns, atypical spending habits and secret fraud communities by analyzing these transaction networks. Oftentimes fraudulent accounts show patterns of interconnected transactions, devices or sequences of transactions. These relational dependencies can be effectively captured by GNNs.

GCNs and GATs are widely adopted for credit card fraud detection. The reason why GAT models are more effective is that they pay more attention to the suspicious neighboring transactions, which leads to the enhancement of the performance of anomaly detection.

Several studies have demonstrated that GNN-based fraud detection systems deliver better precision and lower false positive rates than traditional ML methods including LR, DT, and RF. Moreover, GraphSAGE models can detect in real time, as they are able to process newly generated transaction data efficiently.

GNNs play a crucial role in financial institutions' fraud detection systems by improving their capacity to detect advanced fraud attempts and reduce financial losses.

5.2 Banking and Online Payment Fraud

The banking & online payment landscape has undergone massive digitalization, resulting in heightened susceptibility to fraudulent transactions, phishing, fake online payments, and account takeover. Fraud detection is a complex and hard task in online environments due to the volume and complexity of transactions.

GNNs address these issues by modeling banking ecosystems as graphs and using graph processing to obtain information from the graph. In such systems:

- Nodes may represent users, bank accounts, mobile devices, IP addresses, or merchants.
- Edges indicate transaction relationships, login activities or shared credentials.

GNNs analyze interactions between these entities and look for suspicious behavior. For instance, if several transactions are entered with the same device or IP address, this can be a sign of coordinated fraud. In the same way, if the number of transactions changes drastically or there are unusual sequences of transactions, this may be a red flag for fraud.

Temporal GNNs are particularly useful in online payment fraud detection, as they take into account the temporal nature of transactions. They can identify fraudulent transfers that happen over short periods of time.

GNN-based systems are advantageous for banking institutions in a number of ways:

- An enhanced ability to accurately detect fraud.
- Installing a fire alarm in the home can lower the number of false alarms.
- Real-time monitoring capability
- Enhanced identification of fraud rings and organized cybercrime networks is made. Enhanced fraud ring and organized cybercrime identification is accomplished.

The application of graph-based learning models is increasingly gaining importance in contemporary digital payment systems, contributing to enhancing their security and trust.

5.3 Anti-Money Laundering (AML)

Money laundering is a significant financial crime in which illegally obtained money is hidden from the public in complicated processes. Traditional AML systems are based on predefined rules and monitoring techniques using thresholds. The methods of modern money laundering, however, are extremely complex networks of transactions and difficult to detect using traditional techniques.

GNNs offer a viable solution involving the representation of money transfer activities as transaction graphs. In AML systems:

- The nodes are people, organizations, accounts or financial institutions.
- Edges are transfers of funds or financial interactions.

The money laundering operations are usually conducted via chains of transactions, shell accounts, and cycles of money. GNNs can be used to find these hidden structures by learning relationships between the interconnected entities.

AML systems based on graphs can:

- Detecting suspicious transaction chains
- Finding implicit relationships between accounts
- Identifying laundering networks and their activities
- Monitoring abnormal transaction flows

Graph Attention Networks are particularly useful for AML applications since they emphasize informative suspicious transactions in their learning process. Furthermore, the heterogeneous GNNs can also handle multiple entity types simultaneously, improving their ability to detect entities in complex financial scenarios.

GNNs are revolutionizing the banking landscape worldwide, improving compliance and reducing financial crimes.

5.4 Cryptocurrency Fraud Detection

Blockchain technology and cryptocurrencies have grown at a fast pace, providing a new range of financial innovations, as well as new opportunities for fraud. There are several types of cryptocurrency fraud, such as phishing, Ponzi schemes,

hoax token projects, illegal money transfers, ransomware, and scams. Blockchain systems are decentralized and anonymous, making it difficult to track fraudulent activities.

The unique graph-based structure of blockchain transactions makes GNNs highly effective in identifying fraudulent cryptocurrency transactions. In a network of cryptocurrency transactions:

- The wallet addresses are displayed as nodes.
- The edges indicate the transactions conducted by the wallets.

GNNs are used to analyze the graph of blockchain transactions, identify abnormal transaction patterns, suspicious wallet behaviors and fraudulent communities of transactions. Transaction patterns of cryptocurrency fraud are often very interconnected and repetitive, and can be explored and identified through graph analysis.

Temporal GNNs further enhance cryptocurrency fraud detection by analyzing the temporal sequence of transactions. These models can detect anomalies in transactions and fraudulent transactions in blockchain networks.

Here are some potential uses of GNNs in cryptocurrency fraud detection:

- The ability to identify fraudulent wallet addresses.
- Identify Ponzi Schemes
- The monitoring of illegal money transfers
- Detection of ransomware payment networks
- Blockchain anomaly detection

This transparency of the blockchain information and the relational learning capability of GNNs offer significant potential for enhanced security in decentralized financial systems.

VI. LITERATURE REVIEW

The literature review highlights the growing role of AI, ML, and GNNs for detecting financial fraud, their impact on improving detection accuracy, real-time monitoring, explainability, scalability, privacy protection, and regulatory compliance, and the challenges they face including bias, interpretability, and the changing nature of fraudulent schemes:

S. Pochincharla *et al.*, (2026) A hybrid thematic analysis was performed on the extracted data to develop a Grounded Theory of AI Adoption Pathways. The analysis found that operational efficacy (RQ1) depends on the GNNs for the fight against complex fraud rings. In an architecturally oriented approach (RQ2), Distributed Intelligence is required, Federated Learning is shown to be a tool to enable collaboration within GDPR constraints and Edge-Cloud hybrids are shown to reach sub-100ms latency. However, for governance (RQ3), it is also required to be mandatory and conduct constant bias monitoring, and bias audits indicate that some cross-border transactions see a 22% increase in FP[18].

N. Albert and A. Finnegan (2025) suggested a dual-component architecture based on statistically sensitive outlier detection algorithms in combination with relational pattern analysis from GNNs. The framework builds flexible, non-static graphs of the transactions, which include complex relationships between customers, merchants, devices, and places, and builds adaptive anomaly-scoring systems to recognize new fraud patterns. The experimental results on the IEEE-CIS Fraud Detection dataset show a 15–30% higher accuracy in fraud detection compared to traditional machine learning techniques, with a reduction in false positives of around 33%. The system's inference latencies are less than 50 milliseconds, which is suitable for the requirements of real-time payment processing systems [4].

D. Vallarino (2025) presents a fraud detection system based on GNN, which fuses the concepts of network science, DL, and XAI to improve fraud prevention in financial systems while complying with AML and KYC regulations. Unlike traditional models, GNNs can more effectively uncover hidden dependencies, collusive fraud, and synthetic identity fraud by structuring financial transactions as graphs. It compares the performance of GNNs with the Random Forest and XGBoost methods, and shows that GNNs have a better recall and detection accuracy. Furthermore, think about the efficiency of calculation and real-time feasibility, pointing out the scalability difficulties of AI use for fraud prevention in high-volume monetary environments. The results indicate that incorporating GNNs into financial information systems and fintech platforms greatly improves the precision of fraud detection, risk evaluation, and regulatory clarity [19].

M. Alabi (2025) AI-driven fraud detection systems leverage ML and anomaly detection to identify suspicious transactions in real-time, significantly reducing financial losses and enhancing security. Algorithmic trading involves using AI models to process huge amounts of data, forecast market moves, and make highly accurate trades at a rapid pace, maximizing profits and reducing risk. Moreover, AI improves risk assessment through predictive analytics and DL to assess creditworthiness, identify market volatility, and ensure regulatory compliance. However, there are several limitations to this, including data privacy, understanding the models, and ethical issues [20].

Olawale Olowu *et al.*, (2024) indicate the current status of AI and data science techniques in banking fraud detection systems, focusing on enhancing cybersecurity measures. Review and analyze the effectiveness of different ML algorithms, DL architectures and real-time monitoring systems for fraud detection, systematically from peer-reviewed literature, industry reports and empirical studies from the last 10 years. Researchers have found that modern AI fraud prevention tools are able to detect fraud at 87-94% rates and lower false-positive rates by 40-60% compared to traditional rule-based systems (based on a review of 47 studies). Additionally, integrated AI techniques that fuse supervised and unsupervised learning methods have consistently proven to be the most effective for recognizing new types of fraud and detecting new threats[21].

Y. Zhou, M. Sun, and F. Zhang (2023) propose a holistic solution based on GNN to detect anomalies in financial transaction networks. The methodology builds mixed

graphical representations of financial transactions, taking into account temporal dynamics and multi-entity relationships. The proposed adaptive GNN structure can detect suspicious patterns and can be applied to dynamically-sized graphs by using the attention mechanism. The experimental results prove its effectiveness on the old-fashioned ML techniques, and it achieves a precision of 94.7% and a recall of 92.3% in fraud detection applications. The framework deals with the challenge of scalability and yet satisfies requirements for interpretability for regulatory purposes. The method is effective in identifying money laundering schemes and networks of fraud that undetected by the traditional methods [22].

Recent research on AI-based financial fraud detection using GNNs is summarized in Table I, which outlines the focus of the research, major contributions, advantages, limitations, and recommendations for future research on the aspects of scalability, explainability, privacy and real-time financial fraud-detection performance.

TABLE I: A SUMMERY OF THE STUDY ON AI-DRIVEN FINANCIAL FRAUD DETECTION USING GRAPH NEURAL NETWORK

Authors	Focus of Study	Key Contributions	Advantages	Limitations	Recommendations
S. Pochincharla et al. (2026)	AI adoption pathways in financial fraud detection	Developed a Grounded Theory framework integrating GNNs, Federated Learning, Distributed Intelligence, and XAI for fraud detection governance	Improved operational efficiency, low-latency processing, and regulatory compliance support	Bias issues in cross-border transactions and complexity in distributed architectures	Develop stronger bias mitigation frameworks and scalable governance models for real-time fraud systems
N. Albert and A. Finnegan (2025)	AI-driven financial fraud detection using GNNs and anomaly detection	Proposed a dual-component framework integrating Graph Neural Networks with anomaly detection for dynamic transaction graph analysis	Improved fraud detection accuracy, reduced false positives, and achieved low-latency real-time detection	Dependence on large-scale transaction graph construction and high computational complexity	Future work should focus on scalable architectures, lightweight models, and improved adaptability to evolving fraud patterns
D. Vallarino (2025)	GNN-based fraud detection with XAI integration	Proposed a GNN framework combining network science, deep learning, and XAI for AML and KYC compliance	Higher recall and detection accuracy than Random Forest and XGBoost with improved transparency	Scalability and computational complexity in high-frequency financial systems	Optimize scalable GNN architectures for large-scale real-time financial environments
M. Alabi (2025)	AI applications in fraud detection and financial risk assessment	Discussed AI-driven anomaly detection, algorithmic trading, predictive analytics, and risk assessment	Real-time fraud identification, optimized trading decisions, and improved risk management	Challenges related to data privacy, interpretability, and ethical concerns	Focus on ethical AI governance and interpretable predictive models in finance
Olawale Olowu et al. (2024)	AI and data science techniques in banking fraud detection	Meta-analysis of AI-powered fraud detection systems using ML, DL, and monitoring systems	High detection rates and reduced false positives compared to rule-based systems	Limited adaptability to rapidly evolving fraud behaviors and dependency on quality datasets	Develop adaptive hybrid AI systems capable of detecting emerging fraud patterns
Y. Zhou, M. Sun, and F. Zhang (2023)	GNN-based anomalous transaction detection	Proposed adaptive heterogeneous GNN architecture with attention mechanisms for transaction analysis	High precision and recall with effective identification of money laundering networks	Interpretability and scalability challenges in dynamic transaction graphs	Improve explainable and lightweight GNN frameworks for large-scale deployment

VII. CONCLUSION AND FUTURE WORK

Financial fraud is taking advantage of the digital revolution and the rapid growth of online payment platforms and decentralized financial networks, remaining a major risk to financial systems. Traditional fraud detection methods, based on rules or statistics, cannot detect fraud patterns or the subtle connections between related entities. In this review, the authors reviewed the evolution of fraud detection techniques with an emphasis on how the technique has evolved from traditional ML and DL techniques to GNN-based techniques. GNNs are proving to be more effective in financial information structured in a graph, such as identifying complex fraud patterns, organized fraud rings, money laundering and cryptocurrency-related offenses. Architectures such as Graph Convolutional Networks, Graph Attention Networks, GraphSAGE and Temporal GNNs have surpassed traditional methods in accuracy, scalability and real-time monitoring.

However, there are some drawbacks, such as data imbalance, computational complexity, model interpretability, privacy concerns, and the ever-changing nature of fraud tactics. In the future, the development of Explainable GNN models with privacy protection and secure distributed frameworks should be explored. Furthermore, there are lightweight and scalable architectures of GNNs needed to handle the dynamic financial networks of large size. Improvements in these areas will further boost the effectiveness, transparency, and reliability of AI financial fraud detection systems.

REFERENCES

[1] 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, pp. 227–237, 2024.

[2] O. Ogundimu, "Artificial Intelligence in Financial and Operational Risk Management: A Critical Analysis," *Cogniz. J. Multidiscip. Stud.*, vol. 5, no. 3, pp. 484–506, Mar. 2025.

[3] N. Kim, S. Patel, R. Mendoza, A. Martinez, I. Cruz, and P. Singh, "Graph Neural Networks for Anomaly Detection in Financial Transactions." 2025.

[4] N. Albert and A. Finnegan, "Combining Graph Neural Networks and Anomaly Detection for Low-Latency Credit Card Fraud Prevention." pp. 1–13, November, 2025.

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

[6] I. D. Mienye and N. Jere, "Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions," in *IEEE Access*, 2024, vol. 12, pp. 96893–96910, July.

[7] S. K. Joginipalli and V. Gummadi, "Advancing Insurance Fraud Detection: Leveraging Machine Learning and AI Techniques," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 13, no. 8, pp. 15344–15351, August, 2024.

[8] C. J. Zhang, A. Q. Gil, B. Liu, and M. Anwar, "AI-BASED IDENTITY FRAUD DETECTION: A SYSTEMATIC REVIEW." pp. 1–31, January, 2025.

[9] L. S. Goecks, A. L. Korzenowski, P. G. T. Neto, D. L. de Souza, and T. Mareth, "Anti-money laundering and financial fraud detection: A systematic literature review." pp. 1–15, April, 2022.

[10] A. A. AHMED and A. O. O. ALABI, "Secure and Scalable Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review," 2024, vol. 12, pp. 102219–102241, August.

[11] T. Pourhabibi, K.-L. Ong, B. H. Kam, and Y. L. Boo, *Fraud detection: A systematic literature review of graph-based anomaly detection approaches*, vol. 133. Elsevier B.V, 2020.

[12] G. Burlacu and I.-B. Robu, "Financial Fraud. Challenges and Solutions for Financial Auditing and Accounting Professionals – a Bibliometric Research," *Audit Financ.*, vol. 22, no. 175, pp. 532–546, July, 2024.

[13] A. Sarna, N. and A. Rithen, F. and S. Jui, U. Belal, S. and Amin, and A. K. M. Oishee, Al and Kabir Tasnim and Muzahidul Islam, "AI Driven Fraud Detection Models in Financial Networks: A Comprehensive Systematic Review," in *IEEE Access*, 2025, vol. 13, pp. 141204–141233, August.

[14] O. Martinez, "STATISTICAL TECHNIQUES FOR DETECTING FRAUD IN LARGE-SCALE FINANCIAL TRANSACTIONS ACROSS INDUSTRIES," *Brainae J. Business, Sci. Technol.*, vol. 4, no. 10, pp. 355–365, October, 2020.

[15] S. K. Vangibhurathachhi, "Machine Learning for Fraud Detection in Financial Transactions," *Int. J. Sci. Technol.*, vol. 16, no. 1, pp. 1–9, March, 2025.

[16] K. K. Ahir, "A Review of Emerging Deep Learning Approaches and Technologies for Fraud Detection in Financial Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 6, no. 8, p. 274, 2026.

[17] S. Motie and B. Raahemi, "Financial fraud detection using graph neural networks: A systematic review," *Expert Syst. Appl.*, vol. 240, p. 122156, 2024.

[18] S. Pochincharla, D. J. Lawson, F. Kabir, D. D. Wilson, and M. Sameer, "AI-Powered Fraud Detection in Financial Networks: A Systematic Literature Review." pp. 1–15, March, 2026.

[19] D. Vallarino, "AI-Powered Fraud Detection in Financial Services: GNN, Compliance Challenges, and Risk Mitigation." pp. 1–34, February, 2025.

[20] M. Alabi, "AI in Financial Services: Fraud Detection, Algorithmic Trading, and Risk Assessment." pp. 1–10, March, 2025.

[21] Olawale 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, November, Nov. 2024.

[22] Y. Zhou, M. Sun, and F. Zhang, "Graph Neural Network-Based Anomaly Detection in Financial Transaction Networks," *J. Comput. Innov. Appl.*, vol. 1, no. 2, pp. 87–101, July, 2023.