International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Financial Fraud Detection Using Graph Neural Networks (GNNs)

Mr. Pallyvela Satishbhasker, Assistant Professor, Department of Computer Science Engineering,
ACE Engineering College, Ankushapur, Hyderabad satish.pallyvela@aceec.ac.in (Corresponding Author)

Vangala Satwik
Department of Computer science
ACE Engineering College
Hyderabad, 501301, India
satwikvangala@pm.me

Indirala Chinna
Department of Computer science
ACE Engineering College
Hyderabad, 501301, India
chinnaindirala@gmail.com

Chintala Isaiah Raju
Department of Computer Science
ACE Engineering College
Hyderabad, 501301, India
isaiahraju2004@gmail.com

I. ABSTRACT

Financial fraud detection is a major challenge in modern digital financial systems due to the increasing volume and complexity of transactions. Traditional machine learning approaches treat transactions as independent entities, making them ineffective in identifying coordinated fraud patterns.

This research proposes a **Graph Neural Network (GNN)-based fraud detection system** that models financial transactions as a graph, where users, accounts, and merchants are represented as nodes and transactions as edges. The system utilizes advanced GNN architectures such as **GraphSAGE and Graph Attention Networks (GAT)** to capture both structural and feature-based relationships.

To improve detection performance, the system incorporates feature engineering and graph-based learning techniques. Experimental results demonstrate improved performance in terms of **accuracy, precision, recall, and F1-score**, along with better fraud detection capability compared to traditional methods.

The proposed system provides a scalable, efficient, and real-time solution for detecting financial fraud in large-scale transaction networks.

.

II. INTRODUCTION

The rapid growth of **online banking, digital payments, and e-commerce platforms** has significantly increased the number of financial transactions worldwide. While these advancements improve convenience, they also introduce new opportunities for fraudulent activities.

Traditional fraud detection systems rely on rule-based approaches or classical machine learning models, which often fail to detect complex fraud patterns. These systems treat transactions as isolated events and do not consider relationships between entities such as users, accounts, and merchants.

To address these limitations, this research introduces a **Graph Neural Network (GNN)-based approach** for fraud detection. By representing transactions as a graph structure, the system can analyze interconnected relationships and identify hidden fraud patterns.

The proposed system aims to improve detection accuracy, reduce false positives, and enable real-time fraud detection, making it suitable for modern financial systems.

accurately classified at an earlier stage. This dynamic control enables the model to skip unnecessary layers, reduce latency, and

III. LITERATURE REVIEW

[1] Bryan Perozzi, Rami Al-Rfou, and Steven Skiena (2014) introduced *DeepWalk*, a graph-based learning approach that generates latent representations of nodes in a network using random walks. This method captures structural relationships in graph data, making it highly relevant for financial fraud detection. However, it does not directly incorporate node features, limiting its effectiveness in complex financial systems.

[2] Thomas N. Kipf and Max Welling (2017) proposed Graph Convolutional Networks (GCNs), which apply convolution operations directly on graph structures. GCNs effectively capture both node features and relationships, making them suitable for fraud detection tasks. Despite their effectiveness, they struggle with scalability on large-scale financial transaction graphs.

[3] Petar Veličković et al. (2018) developed Graph Attention Networks (GATs), introducing attention mechanisms to assign different importance to neighboring nodes. This improves the model's ability to detect suspicious patterns in financial networks. However, GATs are computationally intensive and may not be optimal for real-time fraud detection systems.

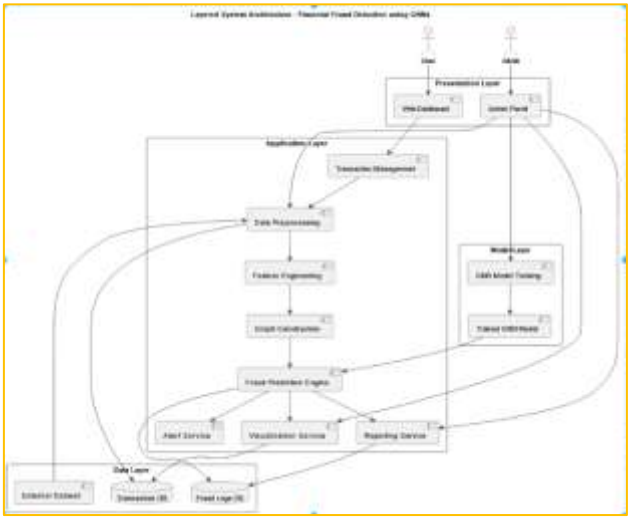
[4] European Central Bank (various reports) and prior studies on traditional machine learning techniques highlight the use of Logistic Regression, Decision Trees, and Random Forests for fraud detection. While these methods perform well on structured transaction data, they fail to capture relational dependencies between entities, limiting their effectiveness in detecting coordinated fraud.

[5] Yoshua Bengio et al. (2015) explored deep learning techniques such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) for financial data analysis. These models improve accuracy but require large labeled datasets and fail to model graph relationships explicitly. This makes them less suitable for fraud scenarios involving interconnected entities.

[6] Neo4j (2018) and related research on graph databases demonstrate the effectiveness of storing and querying financial transactions as graph structures. These systems enable real-time fraud detection by identifying suspicious relationships dynamically. However, they rely heavily on query design and may lack predictive learning capabilities compared to GNN-based approaches.

IV. METHODOLOGY

The proposed methodology models the financial transaction environment as a graph in order to detect fraudulent activities more effectively than traditional transaction-level methods.



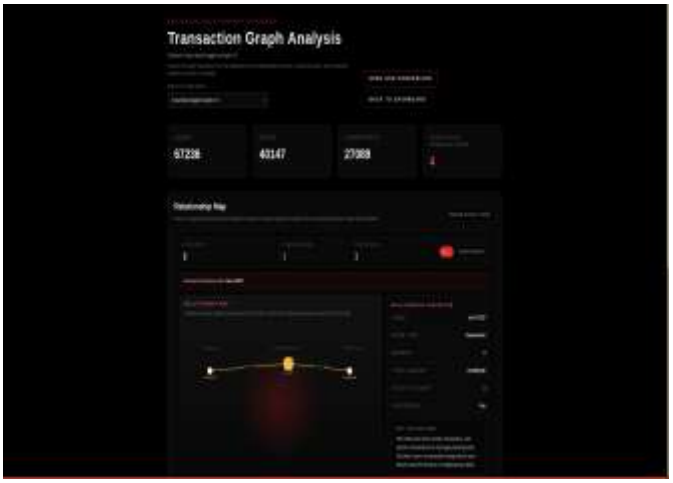
Initially, transaction data is collected from structured sources and preprocessed by removing duplicates, handling missing values, normalizing numerical attributes, and encoding categorical fields. Relevant transaction and entity-level features are then extracted to capture behavioral and relational fraud patterns.

Next, the processed data is transformed into a graph, where nodes represent entities such as users, accounts, and merchants, while edges represent transactions between them. This graph structure enables the system to preserve dependencies and interaction patterns that are essential for fraud analysis. A Graph Neural Network, such as GraphSAGE or GAT, is then trained on the graph to learn embeddings that combine node attributes with neighborhood context. The trained model classifies transactions as fraudulent or legitimate based on learned structural and behavioral representations.

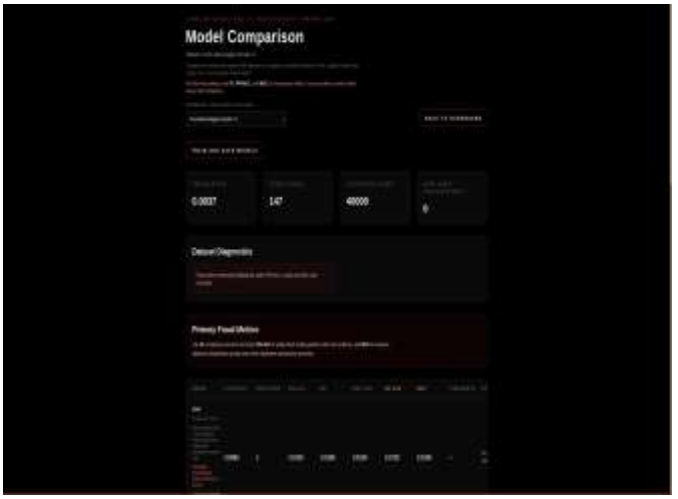
Finally, the prediction results are used to generate fraud scores, alerts, and analytical reports. Suspicious transactions are flagged for administrative review, while reports and visualization modules support interpretation of fraud patterns and monitoring of model performance. In this way, the methodology provides an end-to-end pipeline for accurate, scalable, and real-time financial fraud detection.

V. RESULTS

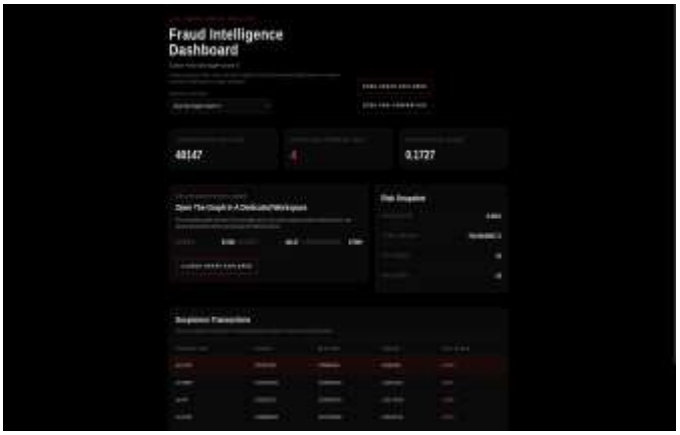
Fraud Detection



Fraud Detection Through Graph Nodes



Comparison with other ML models



The proposed system is evaluated using standard classification metrics:

- Accuracy
- Precision
- Recall
- F1-score
- ROC-AUC

Observations:

- Higher fraud detection accuracy compared to traditional models
- Improved recall, detecting more fraudulent cases
- Reduced false positives
- Efficient handling of large-scale transaction data

The results confirm that GNN-based models significantly enhance fraud detection performance.

VI. DISCUSSION

The proposed **Graph Neural Network (GNN)-based financial fraud detection system** demonstrates significant improvements over traditional fraud detection approaches. By modeling financial transactions as a graph, the system effectively captures both **transaction-level features** and **relational dependencies** among entities such as users, accounts, and merchants. This ability to incorporate structural information enables the detection of complex fraud patterns, including coordinated attacks, mule account networks, and cyclic transaction behaviors, which are typically difficult to identify using conventional machine learning models.

One of the key strengths of the proposed system is its capability to perform **representation learning on graph-structured data**. Through neighborhood aggregation and message passing mechanisms, the GNN learns embeddings that encode both local and global context. As a result, the system can identify anomalies not only based on individual transaction attributes but also based on how entities interact within the network. This leads to improved **fraud recall and detection sensitivity**, ensuring that more fraudulent activities are captured.

.

VII. FUTURE DIRECTIONS

The proposed system provides a strong foundation for graph-based financial fraud detection; however, several enhancements can be explored to further improve its performance, scalability, and real-world applicability.

One important direction for future work is the integration of **temporal graph neural networks (TGNNs)**. Financial transactions are inherently time-dependent, and incorporating temporal dynamics can help the system detect evolving fraud patterns, such as rapid transaction bursts, delayed fraud strategies, and time-based anomalies. By modeling time-aware relationships, the system can improve early fraud detection and provide more accurate predictions.

Another promising area is the adoption of **explainable AI (XAI) techniques** for GNN models. Enhancing interpretability will allow analysts to understand why a transaction was flagged as fraudulent, which is crucial for regulatory compliance and decision-making. Techniques such as attention visualization, subgraph extraction, and feature attribution can be integrated to provide meaningful explanations of fraud predictions.

VIII. CONCLUSION

This research presents a **Graph Neural Network-based financial fraud detection system** that effectively identifies fraudulent transactions by analyzing relationships between entities.

The system improves detection accuracy, reduces false positives, and supports real-time fraud detection. By leveraging graph-based learning, the proposed approach overcomes the limitations of traditional methods and provides a scalable solution for modern financial systems.

IX. REFERENCES

[1] Kipf TN, Welling M (2017) Semi-Supervised Classification with Graph Convolutional Networks. In: Proc. Int. Conf. Learn. Represent. (ICLR).

[2] Hamilton WL, Ying Z, Leskovec J (2017) Inductive Representation Learning on Large Graphs. In: Proc. Adv. Neural Inf. Process. Syst. (NeurIPS), pp 1024–1034.

[3] Veličković P, Cucurull G, Casanova A, Romero A, Liò P, Bengio Y (2018) Graph Attention Networks. In: Proc. Int. Conf. Learn. Represent. (ICLR).

[4] Akoglu L, Tong H, Koutra D (2015) Graph-Based Anomaly Detection and Description: A Survey. Data Min. Knowl. Discov., 29(3), pp 626–688.

[5] Weber M, Domeniconi G, Chen J, Weidele DK, Bellei C, Robinson T, Leiserson CE (2019) Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics. In: Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min. (KDD).

[6] Ngai EWT, Hu Y, Wong YH, Chen Y, Sun X (2011) The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature. Decis. Support Syst., 50(3), pp 559–569.

[7] Chalapathy R, Chawla S (2019) Deep Learning for Anomaly Detection: A Survey. ACM Comput. Surv., 52(4), pp 1–38.

[8] Pandey A, Sahu S (2020) Detecting Financial Fraud Using Machine Learning and Data Mining Techniques. Int. J. Adv. Comput. Sci. Appl., 11(6), pp 98–104.