International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

A Hybrid Graph Neural Network and Machine Learning Approach for Financial Fraud Detection

K Naresh[1], Pandi Sindhu Priya[2]

[1]Assistant Professor, Department of MCA, Annamacharya Institute of Technology and Sciences, Tirupati, Andhra Pradesh, India.

[2]Postgraduate, Department of MCA, Annamacharya Institute of Technology and Sciences, Tirupati, Andhra Pradesh, India.

How to Cite this Article:

Priya, P. S. (2026). A Hybrid Graph Neural Network and Machine Learning Approach for Financial Fraud Detection. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.066

https://doi.org/10.55041/ijcope.v2i4.066

Abstract

The swift expansion of digital transactions has made financial fraud detection more crucial. Due to their incapacity to capture links between transactions, traditional machine learning models frequently fail to identify intricate and dynamic fraud patterns. Graph Neural Networks (GNNs) and traditional machine learning methods like Random Forest, Logistic Regression, and XGBoost are used in this paper to create a hybrid fraud detection system. By modeling transaction data as a graph with nodes representing entities and edges representing links between them, the suggested method enables the system to identify structural patterns and hidden dependencies. To improve detection performance, sophisticated GNN architectures such as Graph Convolutional Networks, Graph Attention Networks, and GraphSAGE are employed. According to experimental findings, graph-based techniques greatly increase the accuracy of fraud detection when compared to conventional methods. To enable real-time prediction and analysis, a Flask-based web application is used to further deploy the system. This study shows how well relational learning and feature-based models work together to detect fraud.

Keywords

Fraud Detection, Graph Neural Networks, Machine Learning, GCN, GAT, GraphSAGE, XGBoost, Financial Transactions, Data Mining, Cybersecurity

I. Introduction

Fraud detection is a crucial field of study and application since the growing reliance on digital financial systems has resulted in a notable increase in fraudulent activity. Every year, financial institutions suffer significant losses as a result of sophisticated fraud schemes that constantly change to evade detection systems. The intricate linkages that exist between several transactions are frequently missed by conventional approaches, such as rule-based systems and simple machine learning models, which mainly concentrate on individual transaction attributes. Their efficacy in identifying coordinated or network-based fraud is diminished by this constraint.

Recent developments in graph-based learning have opened up new avenues for relational data modeling. It is possible to capture relationships and patterns of interaction by representing elements like users, accounts, and transactions as interconnected nodes in a transaction network. Graph Neural Networks are excellent for fraud detection jobs because they apply deep learning methods to graph topologies. In order to increase detection accuracy and robustness, this research suggests a hybrid framework that combines graph-based models with conventional machine learning algorithms. The system can detect both overt and covert fraud tendencies due to the mix of structural and feature-based learning, offering a more complete solution.

II. Methodology

Data preprocessing, graph construction, model development, and deployment are all included in the methodical approach of the suggested methodology. To guarantee data quality and consistency, the dataset first goes through preprocessing procedures such resolving missing values, normalizing numerical features, and encoding categorical variables. For the purpose of evaluating the model, the processed data is subsequently divided into training and testing sets.

Converting transaction data into a graph structure is a crucial part of the process. In this form, linkages like shared properties or interactions are represented by edges, while transactions or entities are represented by nodes. The system may identify hidden dependencies that are not apparent in conventional tabular data thanks to this graph-based representation.

Graph Neural Networks and conventional machine learning algorithms are both used in the model development stage. To set baseline performance, traditional models like Random Forest, Gradient Boosting, Logistic Regression, and XGBoost are used. Graph Convolutional Networks, Graph Attention Networks, and GraphSAGE are examples of sophisticated GNN models that are simultaneously trained to identify structural patterns in the graph. By combining data from nearby nodes, these algorithms are able to recognize intricate fraud patterns.

Standard measures, including accuracy, precision, recall, and F1-score, are used to assess each model's performance. Ultimately, real-time fraud prediction and visualization are made possible by integrating the top-performing model into a Flask-based web application. The system's usability and accessibility for actual use are guaranteed during the deployment phase.

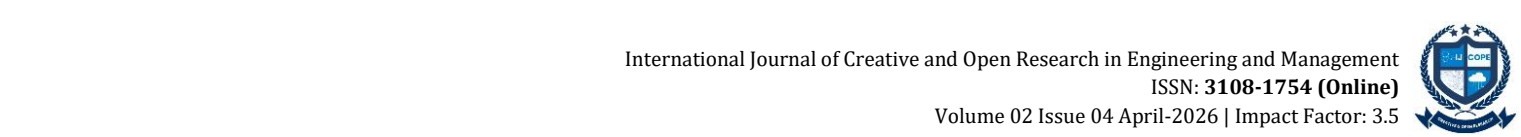
III. Dataset, Problem Statement, and Objective

The dataset utilized in this research is made up of structured transaction records with a variety of attributes, including transaction amount, user behavior, and labels that indicate whether a transaction is legitimate or fraudulent. To accommodate various modeling techniques, the data is preprocessed and converted into tabular and graph representations. Modeling interaction patterns is made possible by treating transactions or entities as nodes in the graph representation and the links between them as edges.

The inability of conventional fraud detection algorithms to recognize intricate and related fraud patterns is the main issue this work attempts to address. The majority of current methods overlook the interconnectedness of transactions, which is essential for identifying organized fraud. This project's goal is to create an intelligent fraud detection system that makes use of both graph-based and machine learning methods. Through an intuitive user interface, the system seeks to increase detection accuracy, decrease false positives, and offer real-time predictions. The study also aims to show the benefits of graph-based learning in fraud detection and compare the performance of various models.

IV. Result and Discussion

Users can interact with the fraud detection model through the developed system's web-based interface, which was created using Flask. Transaction input, fraud prediction, and analytical visualization are just a few of the features that the application offers. While the prediction site enables users to enter transaction details and receive immediate categorization results showing whether the transaction is authentic or fraudulent, the



home page provides an overview of the system. An analytics dashboard also shows data-derived insights, including model performance indicators and fraud distribution.

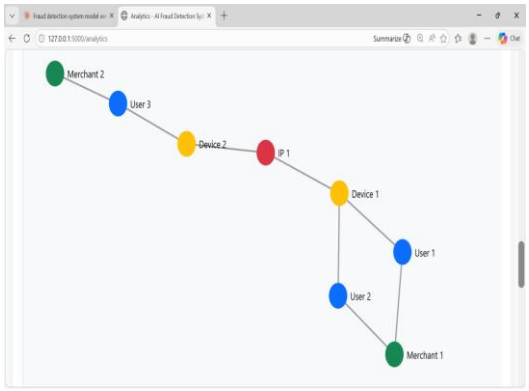


Fig: Diagram-1

The application's user interface, prediction outcomes, and graphical analysis are depicted in screenshots. These illustrations aid in showcasing the suggested system's usefulness in actual situations as well as its practical application. Each figure should have an appropriate caption explaining its function and significance inside the system.

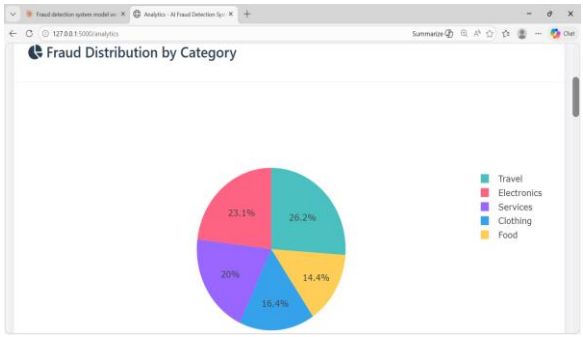


Fig: Category Chart

V. Objective

Graph Convolutional Networks, which are the basis for many contemporary graph-based applications, were first presented by Kipf and Welling as an efficient technique for semi-supervised learning on graph-structured data. Graph Attention Networks, developed by Velickovic and associates, enhance representation learning by giving nearby nodes varying degrees of attention. GraphSAGE, an inductive framework for learning node embeddings on huge graphs, was created by Hamilton et al. and is appropriate for dynamic datasets. XGBoost, a scalable and effective gradient boosting framework popular in machine learning applications, was introduced by Chen and Guestrin. The Random Forest algorithm was developed by Breiman and is still a reliable and popular ensemble learning technique. Furthermore, a number of research on bank fraud detection emphasize how crucial data mining and machine learning methods are becoming for spotting fraudulent activity in large-scale transaction systems.

VI. Conclusion

In order to overcome the shortcomings of current methods, this research develops a hybrid fraud detection system that integrates Graph Neural Networks with conventional machine learning models. The system can capture intricate interactions between transactions by utilizing graph-based representations, which improves detection robustness and accuracy. The comparison analysis shows that GNN models are more effective than traditional algorithms at spotting complex fraud patterns.

The model's practical applicability and real-time deployment potential are demonstrated by its integration into a Flask-based application. The suggested method offers a scalable and effective answer to contemporary fraud detection problems. Future research could concentrate on improving system scalability to manage massive transaction networks, investigating more sophisticated deep learning architectures, and integrating real-time streaming data.

References

[1] S. A. Pushkala, "Identification of Financial Fraud Using Graph Neural Network and LSTM with Autoencoder-Based Data Refinement," Journal of International Crisis and Risk Communication Research, vol. 9, no. 1, pp. 198–213, 2026.

[2] R. Huang, "FinGuard-GNN: Dynamic Graph Neural Network Framework for Financial Fraud Detection," Frontiers in Business, Economics, and Management, 2025.

[3] S. Lu, "Graph Neural Network Model in Financial Fraud Detection," IEEE International Conference on Intelligent Computing and Robotics (ICICR) Proceedings, 2025, pp. 998–1002.

[4] Y. Varma, "Graph Neural Networks for Real-Time Fraud Detection in Financial Services," Journal of Intelligent Systems and Pattern Recognition, 2024.

[5] CaT-GNN: Improving Credit Card Fraud Detection using Causal Temporal Graph Neural Networks, Y. Duan, G. Zhang, S. Wang, et al., arXiv preprint arXiv:2402.14708, 2024.