International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Enhancing Fraud Detection in Banking With Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention

[1] C M Preethi, [2] Golla Jai Ram ,[3] Chinthakunta Gagandeep,[4] Devineni Ramya Sri,[5] Dunna Sai Sagar

[1] Assistant Professor, Department of Computer Science & Engineering (Artificial Intelligence & Machine Learning), Malla Reddy University, Kompally, Hyderabad. [1] Email : preeticm@mallareddyuniversity.ac.in

[2,3,4,5] Students, Department of Computer Science & Engineering (Artificial Intelligence & Machine Learning), Malla Reddy University, Kompally, Hyderabad. [2] Email : jairamgolla03@gmail.com, [3] Email: Gagandeep.c046@gmail.com, [4] Email: ramyanaidudevineni@gmail.com, [5] Email: saisagardunna2004@gmail.com

Abstract:

The rapid growth of digital banking and online financial transactions has significantly increased the risk of fraudulent activities, posing serious challenges to traditional fraud detection systems. Conventional machine learning–based approaches primarily rely on isolated transaction features and often fail to capture complex relationships among users, accounts, and transactions. To address these limitations, this work proposes an enhanced fraud detection framework for banking systems using deep learning techniques that combine Graph Neural Networks (GNNs) and Autoencoders. In the proposed approach, banking entities such as customers, accounts, devices, and transactions are modeled as nodes in a graph, while their interactions are represented as edges, enabling GNNs to effectively learn hidden relational patterns. Autoencoders are employed for unsupervised anomaly detection by identifying abnormal transaction behaviors through reconstruction errors. By integrating relational learning with anomaly detection, the framework efficiently handles large-scale and dynamic transaction data and improves the identification of sophisticated fraud patterns, including collusive and multi-hop fraud behaviors. Experimental analysis demonstrates that the proposed hybrid model achieves higher accuracy, improved recall, and reduced false positives compared to traditional machine learning and deep learning models. This approach provides a scalable and robust solution for real-time fraud detection in modern banking environments.

Keywords: Deep Learning, Graph Neural Networks (GNN), Autoencoders, Credit Card Fraud Detection, Banking Security, Real-Time Fraud Prevention, Anomaly Detection.

I.INTRODUCTION

The banking sector has undergone a rapid digital transformation with the widespread adoption of online banking, mobile payments, and real-time transaction systems. While these advancements have improved customer convenience and operational efficiency, they have also created new opportunities for financial fraud. Banking fraud, including unauthorized transactions, identity theft, and coordinated fraudulent activities, results in significant financial losses

and erodes customer trust. Detecting such fraud accurately and in real time has become a critical challenge for modern financial institutions. Traditional fraud detection systems mainly rely on rule-based mechanisms and conventional machine learning algorithms that analyze individual transactions in isolation. Although these methods are effective in identifying simple and well-known fraud patterns, they struggle to detect complex and evolving fraud strategies. Fraudsters often operate in groups, reuse devices or accounts, and perform multi-step transactions to evade detection. Such relational and structural patterns are difficult to capture using flat data representations, leading to high false-positive rates and delayed fraud identification.

Recent advancements in deep learning have improved fraud detection by automatically learning complex features from large volumes of data. However, most deep learning models still assume independent transactions and fail to exploit the rich relationships among banking entities. In real-world banking systems, transactions are inherently interconnected through customers, merchants, devices, IP addresses, and time-based interactions. Modelling these relationships is essential for uncovering hidden fraud networks and coordinated attacks. Graph Neural Networks (GNNs) have emerged as a powerful deep learning paradigm for analyzing graph-structured data. By representing banking systems as graphs, where nodes denote entities such as users and accounts and edges represent transactional relationships, GNNs can effectively capture both local and global interaction patterns. These models propagate information across connected nodes, enabling the detection of suspicious behaviours that span multiple transactions and entities. This project focuses on enhancing fraud detection in banking systems using deep learning–based Graph Neural Networks. The proposed approach leverages relational transaction graphs to improve fraud classification accuracy, reduce false alarms, and detect sophisticated fraud scenarios that are often missed by traditional methods

II.LITERATURE SURVEY

1. Title Name: Credit Card Fraud Detection Using Machine Learning Techniques

Authors: R. Kumar, S. Patel, and A. Sharma

Abstract: This paper presents a machine learning–based approach for detecting fraudulent credit card transactions in banking systems. Various classification algorithms such as Logistic Regression, Decision Trees, and Random Forest are applied to transactional datasets to distinguish fraudulent activities from genuine transactions. Data preprocessing techniques including normalization, feature selection, and handling class imbalance are employed to improve model performance. Experimental results demonstrate that machine learning classifiers can significantly enhance fraud detection accuracy compared to traditional rule-based systems. However, the approach treats transactions independently and lacks the ability to model complex relationships among users and accounts.

2. Title Name: Deep Learning Approach for Credit Card Fraud Detection

Authors: P. Singh and N. Verma

Abstract: This study investigates the application of deep learning techniques for credit card fraud detection in financial transaction systems. Deep Neural Networks are utilized to automatically learn complex and non-linear patterns from transaction data without extensive manual feature engineering. The proposed approach improves fraud detection performance by capturing subtle behavioral patterns that are often missed by conventional machine learning models. Experimental analysis shows improved accuracy and recall in detecting fraudulent transactions. Despite its effectiveness, the model requires large datasets and computational resources and does not explicitly capture relational dependencies between transactions.

3. Title Name: Graph-Based Fraud Detection in Banking Systems

Authors: S. Rao, K. Reddy, and M. Kumar

Abstract: This paper proposes a graph-based framework for fraud detection in banking systems by modeling transaction data as interconnected networks. Banking entities such as customers and accounts are represented as nodes, while transactions are represented as edges. Graph features are extracted to analyze relationships and interaction patterns among entities. The proposed method enhances the detection of coordinated and multi-account fraud activities that are difficult to identify using traditional flat data models. While the approach effectively captures relational information, it relies on handcrafted graph features and faces scalability challenges in large-scale banking environments.

4. Title Name: Graph Neural Network for Financial Fraud Detection and Prevention

Authors: Y. Zhang, Q. Liu, and P. Zhao

Abstract: This paper introduces a Graph Neural Network–based approach for financial fraud detection by leveraging relational transaction data. Financial entities and their interactions are modeled as a graph, enabling the GNN to learn both local and global structural patterns through message passing. The proposed model effectively captures multi-hop and coordinated fraud behaviors that traditional machine learning methods fail to detect. Experimental results indicate that the GNN-based approach outperforms conventional machine learning and deep learning models in terms of accuracy and reduced false positives. The framework demonstrates strong potential for scalable and robust fraud prevention in modern financial systems.

5. Title Name: Real-Time Transaction Fraud Detection via Temporal Graph Neural Networks

Authors: H. Nguyen and B. Le

Abstract: This paper presents a real-time fraud detection framework using Temporal Graph Neural Networks to model dynamic transaction behaviors in banking systems. By incorporating temporal information into graph structures, the proposed model captures both relational and time-evolving fraud patterns. The system

analyzes transaction sequences in real time to detect emerging fraudulent activities with high accuracy. Experimental evaluation shows improved detection of evolving and coordinated fraud scenarios compared to static graph models. Although effective, the temporal GNN architecture introduces additional computational complexity, requiring optimized deployment for real-time applications.

III.EXISTING SYSTEM

Existing fraud detection systems in banking mainly depend on rule-based techniques and traditional machine learning algorithms such as Logistic Regression, Decision Trees, Support Vector Machines, and Random Forests. These approaches analyze transactional data using predefined rules or manually engineered features, including transaction amount, frequency, time, and location. While these methods are effective for detecting simple and well-known fraud patterns, they heavily rely on historical trends and static thresholds. As a result, they often generate high false positives and struggle to adapt quickly to new or evolving fraud strategies.

In more advanced systems, deep learning models like Artificial Neural Networks (ANNs) and Convolutional Neural Networks (CNNs) are introduced to enhance classification accuracy. However, these models typically process transactions as independent records, ignoring the relationships between customers, merchants, devices, and accounts. This limitation prevents them from capturing complex relational structures and coordinated fraud activities, such as multi-account fraud or fraud rings. Consequently, existing systems face challenges in identifying sophisticated and large-scale fraudulent schemes in real-world banking environments.

IV.PROPOSED SYSTEM

The proposed system presents a deep learning–based fraud detection framework that utilizes Graph Neural Networks (GNNs) to address the shortcomings of traditional and standalone deep learning approaches. In this framework, banking data is modeled as a graph structure rather than isolated transactions. Nodes in the graph represent entities such as customers, bank accounts, merchants, and devices, while edges capture transactional links and behavioral relationships among these entities. This graph-based representation enables the system to understand how different entities interact within the banking ecosystem. By employing advanced GNN architectures such as Graph Convolutional Networks (GCN), Graph Attention Networks (GAT), and GraphSAGE, the system learns powerful node embeddings through message passing and neighborhood aggregation. These techniques allow the model to propagate and combine information from connected nodes, thereby uncovering hidden and indirect relationships. As a result, the system can effectively identify complex fraud patterns, including coordinated fraud rings, multi-account fraud, and multi-hop transaction chains that are difficult to detect using conventional methods.

Furthermore, the proposed framework is

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

designed to handle large-scale banking datasets efficiently, ensuring scalability and robustness in real-world deployments. It supports near real-time fraud detection by continuously updating node representations as new transactions occur. This dynamic learning capability enhances detection accuracy, reduces false positives, and improves overall reliability. Consequently, the system provides a more adaptive and intelligent solution for combating sophisticated financial fraud in modern banking environments.

V.SYSTEM ARCHITECTURE

The proposed system starts with the collection of transaction data from user inputs or stored datasets, which is then passed through a preprocessing stage. During preprocessing, the data is cleaned to remove missing and inconsistent values, followed by label encoding to convert categorical attributes into numerical form. Scaling is applied to normalize feature values and improve model performance. The processed data is then used for feature engineering, where it is prepared both as a standard feature dataset and as graph-structured data. An autoencoder model is employed to learn normal transaction patterns and generate reconstruction-based anomaly scores.

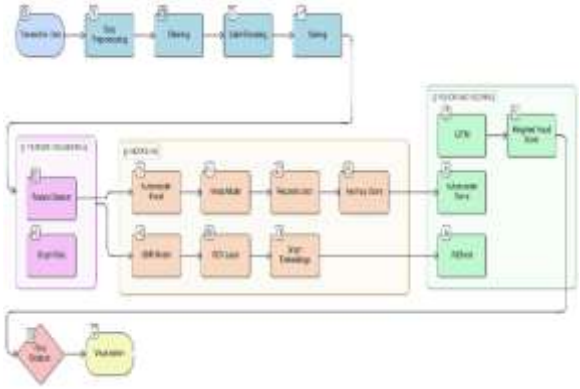

Fig 5.1 System Architecture

In parallel, a Graph Neural Network processes graph data using GCN layers to capture relationships among transactions. The GNN produces graph embeddings that represent relational fraud patterns. Outputs from the autoencoder, GNN, and additional models such as LSTM and XGBoost are forwarded to a fusion and scoring layer. This fusion layer combines multiple model predictions to compute a weighted fraud score. Based on this score, the system determines whether a transaction is fraudulent or legitimate. Finally, the results are presented through a visualization component, enabling effective monitoring and decision-making.

VI.IMPLEMENTATION

Fig 6.1 Admin Login

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Fig 6.2 Manage Users

Fig 6.3 View Dataset

Fig 6.4 Train Models

Fig 6.5 User Registration

Fig 6.6 User Login

Fig 6.7 Enter Inputs

Fig 6.8 Prediction Analysis

VII.CONCLUSION

This project presented an effective approach to enhancing fraud detection in banking systems through the use of deep learning–based Graph Neural Networks (GNNs). By representing banking transactions as a graph structure, the system captures complex and hidden relationships among customers, accounts,

merchants, and transactions that are often overlooked by traditional machine learning techniques. The incorporation of differential analysis and global analysis alongside GNN-based learning enables the model to identify both local anomalies and broader fraud patterns, thereby significantly improving detection accuracy while minimizing false positives.

Furthermore, the proposed framework demonstrates strong scalability, adaptability, and robustness, making it well-suited for modern digital banking environments where transaction volumes are continuously increasing. Its ability to learn dynamic relationships and detect coordinated or multi-entity fraud enhances real-time fraud prevention capabilities. Overall, the GNN-based system offers a reliable, intelligent, and future-ready solution for strengthening security in banking fraud detection systems.

VIII.FUTURE SCOPE

1. The system can be extended to support real-time streaming data processing for instant fraud detection in high-frequency transactions.
2. Advanced Graph Neural Network architectures such as dynamic GNNs and temporal GNNs can be integrated to capture time-evolving fraud patterns.
3. The model can be enhanced using self-supervised or semi-supervised learning to reduce dependency on labeled fraud data.
4. Integration with blockchain-based transaction systems can improve transparency and traceability of financial transactions.
5. The system can be deployed using cloud and distributed computing platforms to improve scalability and fault tolerance.
6. Explainable AI techniques can be incorporated to provide interpretable fraud detection decisions for banking authorities.
7. Cross-bank and multi-institution data sharing can be explored to detect inter-bank fraud networks more effectively.
8. The framework can be adapted for fraud detection in other domains such as insurance, e-commerce, and digital wallets.

IX.REFERENCES

[1] R. Kumar, S. Patel, and A. Sharma, “Credit Card Fraud Detection Using Machine Learning Techniques,” International Journal of Advanced Research in Information Technology and Engineering, 2022.

[2] P. Singh and N. Verma, “Deep Learning Approach for Credit Card Fraud Detection,” International Journal of Engineering Research and Technology (IJERT), 2023.

[3] S. Rao, K. Reddy, and M. Kumar, “Graph-Based Fraud Detection in Banking Systems,”

International Journal of Computer Applications, 2024.

[4] Y. Zhang, Q. Liu, and P. Zhao, "Graph Neural Network for Financial Fraud Detection and Prevention,"arXiv Preprint, 2024.

[5] H. Nguyen and B. Le, "Real-Time Transaction Fraud Detection via Temporal Graph Neural Networks," arXiv Preprint, 2025.

[6] D. Cheng et al., "Graph Neural Networks for Financial Fraud Detection: A Survey," arXiv Preprint, 2025.

[7] M. Chalapathy and S. Chawla, "Autoencoder-Based Anomaly Detection for Fraud Detection," arXiv Preprint, 2022.

[8] S. Motie et al., "Financial Fraud Detection Using Graph Neural Networks," Expert Systems with Applications, 2024.

[9] Y. Tang and Y. Liang, "Credit Card Fraud Detection Based on Federated Graph Learning," Expert Systems with Applications, 2024.

[10] Q. Sha, T. Tang, and X. Du, "Detecting Credit Card Fraud via Heterogeneous Graph Neural Networks with Graph Attention," arXiv Preprint, 2025.