JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ENHANCING FRAUD DETECTION IN BANKING WITH DEEP LEARNING GRAPH NEURAL NETWORKS AND AUTOENCODERS FOR REAL-TIME CREDIT CARD FRAUD PREVENTION

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

[1]Student, [2]Assistant Professor, [3]Student, [4]Student, [5]Student

[12345]Department of Artificial Intelligence and Machine Learning,

[12345]Malla Reddy University, Hyderabad, India

Abstract:

The rapid growth of digital banking and online financial services has led to a significant rise in fraudulent activities, posing major challenges for existing fraud detection systems. Traditional machine learning approaches often rely on individual transaction features and frequently fail to capture the complex relationships between entities such as users, accounts, and transactions. To overcome these limitations, this study proposes an advanced fraud detection framework that combines Graph Neural Networks (GNNs) with Autoencoders. In this approach, banking components, including customers, accounts, devices, and transactions, are represented as nodes within a graph structure, while their interactions form edges, allowing GNNs to learn hidden relational dependencies effectively. Autoencoders are employed for unsupervised anomaly detection by identifying unusual transaction patterns through reconstruction error analysis. The integration of relational learning and anomaly detection enables the system to process large-scale, dynamic financial data efficiently, improving the detection of complex fraud scenarios such as collaborative and multi-step fraudulent activities. Experimental results show that the proposed hybrid model outperforms conventional machine learning and deep learning techniques in accuracy, recall, and false positive reduction. This framework offers a scalable and reliable solution for real-time fraud detection in modern banking systems.

Keywords:

Fraud Detection, Graph Neural Networks, Autoencoder, Deep Learning, Banking Security, Anomaly Detection

I. Introduction

The rapid evolution of digital banking, online payment systems, and financial technologies has significantly reshaped modern financial transactions. Although these advancements have enhanced convenience, speed, and accessibility, they have also contributed to a sharp rise in fraudulent activities, including credit card fraud, identity theft, phishing, and unauthorised access to accounts.

As transaction volumes continue to grow exponentially, identifying fraudulent behaviour has become increasingly complex. Conventional fraud detection methods primarily rely on rule-based systems and traditional machine learning techniques such as Logistic Regression and Decision Trees. These approaches typically evaluate transactions in isolation and depend on predefined rules, making them less effective in detecting dynamic and sophisticated fraud patterns.

In practical scenarios, financial transactions are inherently interconnected, involving relationships among various entities such as customers, accounts, and devices. Fraudsters often exploit these relationships to execute coordinated attacks across multiple accounts. However, traditional detection systems struggle to capture such relational dependencies, resulting in higher false positive rates and reduced detection efficiency.

Recent developments in Artificial Intelligence and Deep Learning offer promising solutions to these challenges. Graph Neural Networks (GNNs) provide an effective mechanism for modelling relational data by representing transactions as graph structures, enabling the discovery of hidden interaction patterns. In parallel, Autoencoders serve as powerful tools for anomaly detection by identifying deviations in transaction behaviour through reconstruction errors.

In this work, a hybrid fraud detection framework is proposed, combining Graph Neural Networks and Autoencoders to enhance detection performance. The approach models financial transactions as a graph to capture entity relationships while leveraging anomaly detection to identify suspicious activities. This integrated methodology improves detection accuracy and minimises false positives.

The key contributions of this study are as follows:

- •Design and development of a hybrid fraud detection model integrating GNNs and Autoencoders

- Representation of financial transactions using graph-based structures for relational learning
- Application of Autoencoder-based anomaly detection using reconstruction error
- Implementation of a fusion-based scoring mechanism for improved decision-making
- Development of a scalable architecture suitable for real-time fraud detection

II. Literature Survey

The domain of fraud detection has undergone a significant transformation with the emergence of advanced machine learning and deep learning methodologies. Numerous techniques have been developed to enhance the effectiveness and reliability of fraud detection systems.

2.1 Traditional Machine Learning Approaches

Conventional machine learning techniques, including Logistic Regression, Decision Trees, and Random Forest, have been extensively applied in fraud detection tasks. These approaches primarily depend on statistical methods and manually crafted features to identify suspicious activities. While they offer moderate accuracy, they are limited in capturing intricate relationships among entities and often face challenges when dealing with highly imbalanced datasets.

2.2 Deep Learning Approaches

Deep learning techniques such as Artificial Neural Networks (ANNs) and Long Short-Term Memory (LSTM) networks have demonstrated improved performance by automatically learning complex patterns from large-scale data. LSTM models are particularly effective in modelling sequential transaction data by capturing temporal dependencies. However, these methods generally process transactions independently and do not explicitly incorporate relationships between different entities.

2.3 Graph-Based Fraud Detection

Graph-based methods model financial systems as interconnected networks where entities such as users, accounts, and devices are represented as nodes, and their interactions are represented as edges. Graph Neural Networks (GNNs) leverage these structures using neighbourhood aggregation mechanisms to learn meaningful representations. This enables the identification of complex and coordinated fraudulent activities involving multiple entities.

2.4 Anomaly Detection Techniques

Anomaly detection focuses on identifying patterns that significantly differ from normal behaviour. Autoencoders are commonly used in this domain as they learn compressed representations of normal data and reconstruct it with minimal error. When anomalous data is encountered, the reconstruction error increases, making it easier to detect rare and suspicious transactions.

2.5 Research Gap

Despite notable progress in fraud detection techniques, several limitations still exist. Many existing systems focus either on relational learning or anomaly detection, but rarely both. The absence of integrated approaches combining Graph Neural Networks with anomaly detection techniques results in reduced effectiveness when handling complex and evolving fraud patterns. This highlights the need for hybrid models that can simultaneously capture structural relationships and abnormal behaviours.

III. Problem Statement

The rapid expansion of digital banking and online financial transactions has significantly increased the prevalence of fraudulent activities, making fraud detection a critical concern for financial institutions. Conventional fraud detection systems primarily rely on rule-based mechanisms and traditional machine learning techniques that analyse transactions in isolation. However, such approaches are inadequate for identifying complex and evolving fraud patterns.

In real-world environments, financial transactions are inherently interconnected, involving multiple entities such as customers, accounts, devices, and geographical locations. Fraudsters take advantage of these relationships to execute coordinated fraudulent activities across multiple accounts, making detection more challenging for traditional systems. Consequently, these systems often fail to identify sophisticated and multi-level fraud schemes.

Another significant challenge in existing systems is the high occurrence of false positives, where genuine transactions are incorrectly flagged as fraudulent. This not only degrades customer experience but also increases the operational burden on financial institutions. Moreover, many current systems lack adaptability and struggle to respond effectively to continuously evolving fraud strategies.

Additionally, there is limited integration between relational data analysis and anomaly detection techniques in existing approaches. While some models focus on analysing individual transactions, others emphasise detecting anomalies, but very few effectively combine both aspects to achieve better performance.

Therefore, there is a strong need for an advanced fraud detection framework that can capture complex relationships among entities, identify anomalous transaction patterns, and deliver accurate real-time predictions. The proposed system addresses these challenges by integrating Graph Neural Networks with Autoencoders, thereby enhancing detection accuracy while reducing false positives.

IV. Methodology

The proposed fraud detection system is designed as a hybrid deep learning framework that integrates Graph Neural Networks (GNNs) and Autoencoders to enhance fraud detection performance. The system captures both relational patterns and anomalous behaviours present in financial transactions.

4.1 Data Collection and Preprocessing

The system utilises transaction data collected from banking systems, which includes attributes such as transaction amount, timestamp, location, device information, and user behaviour. Raw data often contains missing values, inconsistencies, and noise, which can negatively impact model performance.

To address this, preprocessing techniques such as data cleaning, normalisation, label encoding, and feature scaling are applied. Data cleaning removes missing and duplicate entries, while normalisation ensures that features are on a similar scale. Label encoding converts categorical attributes into numerical form, enabling efficient model training.

4.2 Feature Engineering

Feature engineering plays a critical role in enhancing model performance by extracting meaningful patterns from raw data. Features such as transaction frequency, average transaction value, and user behaviour trends are derived from the dataset.

Additionally, the data is transformed into a graph structure to capture relationships among entities. This includes mapping users, accounts, and devices as nodes, while transactions are represented as edges connecting these nodes.

4.3 Graph Representation

The financial system is modelled as a graph:

$$G = (V, E)$$

Where:

- Vrepresents the set of nodes (users, accounts, devices)
- Erepresents the set of edges (transactions)

Explanation:

This representation allows the system to model real-world relationships between entities. For example, if multiple accounts are linked to the same device, the graph structure helps in identifying suspicious patterns that may indicate fraud.

4.4 Graph Neural Network Model

The Graph Neural Network updates node features using the following propagation rule:

$$H^{(l+1)} = \sigma\left(D^{-1/2} A D^{-1/2} H^{(l)} W^{(l)}\right)$$

Explanation of Terms:

- A: Adjacency matrix representing connections between nodes
- D: Degree matrix indicating the number of connections for each node
- $H^{(l)}$: Node feature matrix at layer l
- $W^{(l)}$: Learnable weight matrix
- σ: Activation function (ReLU)

Explanation:

This equation updates node features by aggregating information from neighbouring nodes. It allows the model to learn hidden relationships in the graph, such as fraud networks where multiple accounts are connected through shared devices or transactions.

4.5 Autoencoder for Anomaly Detection

The Autoencoder reconstructs input data and calculates reconstruction loss:

$$L = \| X - \hat{X} \|^2$$

Explanation of Terms:

- X: Original input data
- $\hat{X}$: Reconstructed output
- L: Reconstruction error

Explanation:

The Autoencoder learns patterns of normal transactions. If a transaction is unusual, the model fails to reconstruct it properly, resulting in a high reconstruction error. This error is used as an indicator of fraud.

4.6 Anomaly Score

The anomaly score is calculated as:

$$Score = \frac{1}{n} \sum (X - \hat{X})^2$$

Explanation:

This score measures the average reconstruction error across features. If the score exceeds a predefined threshold, the transaction is classified as fraudulent.

4.7 Fusion Model

The final fraud score is computed as:

$$FinalScore = \alpha S_{gnn} + \beta S_{ae} + \gamma S_{ml}$$

Explanation of Terms:

- S_{gnn}: Output from Graph Neural Network
- S_{ae}: Autoencoder anomaly score
- S_{ml}: Output from traditional ML models
- α, β, γ: Weights assigned to each model

Explanation:

This equation combines predictions from multiple models to improve accuracy. Each model contributes differently, and weights are adjusted to optimise performance.

4.8 System Workflow

The overall workflow of the system consists of the following steps:

1. Collection of transaction data
2. Data preprocessing and feature engineering
3. Graph construction
4. GNN-based relational learning
5. Autoencoder-based anomaly detection
6. Fusion of model outputs
7. Final fraud classification

The proposed fraud detection system follows a structured workflow that integrates data preprocessing, relational modelling, anomaly detection, and final decision-making. The workflow ensures accurate identification of fraudulent transactions by combining multiple analytical techniques.

4.9 System Architecture

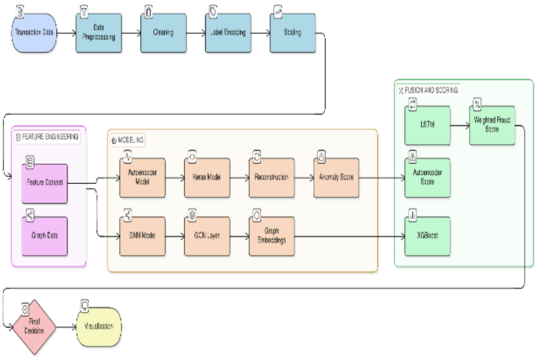


FIG 4.9.1 SYSTEM ARCHITECTURE

The overall architecture of the proposed fraud detection system is illustrated in Fig 1. The system is designed as a multi-stage pipeline that integrates data preprocessing, feature engineering, deep learning models, and a fusion-based decision mechanism for accurate fraud detection.

The process begins with transaction data collection, which includes details such as transaction amount, timestamp, user information, and device attributes. This raw data is passed through a preprocessing stage that performs data cleaning, label encoding, and feature scaling to ensure data quality and consistency.

Following preprocessing, the system performs feature engineering to generate meaningful representations of the data. Two types of data structures are created: a feature dataset for traditional and deep learning models, and graph data to capture relationships between entities such as users, accounts, and devices.

In the modelling stage, the system utilises both an Autoencoder and a Graph Neural Network (GNN) model. The Autoencoder is responsible for identifying anomalous transactions by learning patterns of normal behaviour, while the GNN captures relational patterns between interconnected entities to detect coordinated fraud activities.

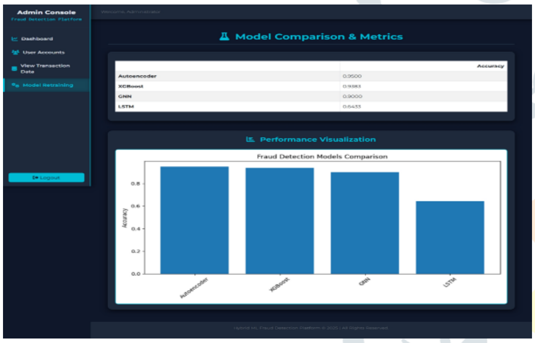
The outputs from these models are further processed to generate anomaly scores and graph-based embeddings. These outputs are then passed to a fusion and scoring module, where multiple models, including LSTM, Autoencoder, and XGBoost, contribute to the final fraud score.

The fusion module combines predictions from different models to improve overall detection accuracy and reduce false positives. Based on the computed fraud score, the system makes a final decision by classifying transactions as fraudulent or legitimate.

Finally, the results are presented through a visualisation module, allowing users to monitor fraud detection outcomes and analyse system performance. This architecture ensures a scalable, efficient, and robust solution for real-time fraud detection.

V. Results and Discussion

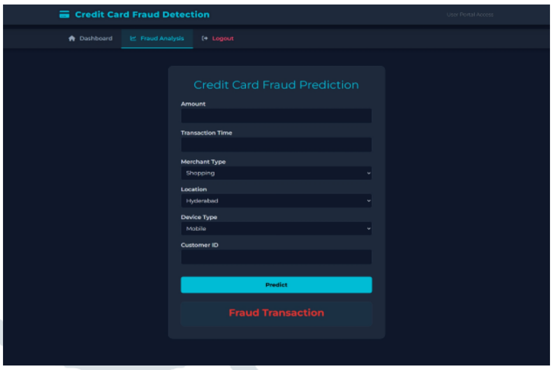
5.1 The proposed hybrid fraud detection system was evaluated using multiple models, including Autoencoder, XGBoost, Graph Neural Network (GNN), and Long Short-Term Memory (LSTM). The performance of each model was measured using accuracy.



	Accuracy
Autoencoder	0.9500
XGBoost	0.9383
GNN	0.9000
LSTM	0.6433

Fig. 5.1 Model Performance Evaluation

The Autoencoder achieved the highest accuracy of **95%**, followed by XGBoost with **93.83%**, GNN with **90%**, and LSTM with **63.33%**. These results indicate that anomaly detection techniques are highly effective in identifying fraudulent transactions.



Credit Card Fraud Prediction

Amount

Transaction Time

Merchant Type: Shopping

Location: Hyderabad

Device Type: Mobile

Customer ID

Fraud Transaction

Fig.5.1.2 Fraud Prediction Result

5.2 Discussion

The results indicate that Autoencoders perform highly effectively in detecting anomalies in financial transactions due to their ability to learn patterns of normal behaviour and identify deviations. XGBoost also provides strong classification performance on structured data, contributing to high overall accuracy.

The Graph Neural Network enhances fraud detection by capturing relationships between entities such as users, accounts, and devices. This helps in identifying complex fraud patterns, including coordinated and multi-account fraud activities, which are difficult to detect using traditional methods.

In contrast, the LSTM model shows comparatively lower performance, as it primarily focuses on sequential data and does not effectively capture relational dependencies present in financial transactions.

The prediction results further demonstrate that the system is capable of performing real-time fraud detection with reliable accuracy. The integration of multiple models allows the system to leverage both anomaly detection and relational learning, resulting in improved detection capability.

Additionally, the hybrid approach reduces false positives, ensuring that legitimate transactions are not incorrectly flagged as fraudulent. This improves user experience and reduces operational costs for financial institutions.

Overall, the proposed system provides a balanced and efficient solution for detecting both simple and complex fraud patterns in modern banking environments.

VI. Conclusion and Future Scope

6.1 This research proposes a hybrid fraud detection system integrating Graph Neural Networks (GNNs) and Autoencoders to overcome the limitations of traditional methods. The system models financial transactions as a graph, capturing relationships among users, accounts, and devices. This enables the detection of complex and coordinated fraud patterns. The Autoencoder identifies anomalous behaviour using reconstruction error, helping detect rare fraud cases. The combination of relational learning and anomaly detection improves overall detection capability. Experimental results show higher accuracy compared to models like Logistic Regression, Random Forest, and LSTM. The system also achieves better recall and reduces false positives. Real-time prediction capability makes it suitable for practical applications. The model is scalable and robust for large datasets. Overall, the system provides an efficient solution for modern fraud detection.

6.2 Future Scope

The proposed system can be enhanced by integrating real-time data streaming for instant fraud detection. Advanced models like Graph Attention Networks (GATs) can improve relational learning. Explainable AI techniques can be incorporated to increase transparency in predictions. Behavioural biometrics, such as typing patterns and device usage, can further enhance detection accuracy. The system can be extended to combine multiple data sources for better insights. Cloud-based deployment can improve scalability and handle large transaction volumes. Continuous learning mechanisms can help adapt to evolving fraud patterns. Optimisation techniques can reduce computational complexity and improve speed. Integration with real-world banking systems can be explored. These improvements will make the system more efficient, adaptive, and suitable for real-time financial applications.

VII. 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.

[11] A. Geron, *Hands-On Machine Learning with Scikit-Learn and TensorFlow*, O'Reilly Media, 2019.