Design And Implementation of GNN-Based Fraud Detection System for Cryptocurrency

K. Ganesh[1], K. Sravan Kumar[2], M. Harshavardhan Reddy[3], M. Umar[4], K. Penchalaiah[5]
[1,2,3,4] Students of B.Tech., Department of Computer Science Engineering, NBKRIST, Vidyanagar.
[5] Guide, Assistant professor, Department of Computer Science Engineering, NBKRIST, Vidyanagar

Abstract: The rapid evolution of cryptocurrency systems has introduced significant challenges in ensuring financial security, particularly in detecting fraudulent activities. Due to the decentralized nature of blockchain technology and the anonymity of users, identifying fraudulent transactions has become increasingly complex. Traditional fraud detection methods, which rely on rule-based systems or simple machine learning models, are not capable of capturing the intricate relationships between transactions and users. This project presents a Graph Neural Network (GNN) based approach to detect fraudulent activities in cryptocurrency networks. The core idea is to model blockchain transaction data as a graph, where nodes represent user accounts and edges represent transactions between them. By leveraging advanced models such as Graph Convolutional Networks (GCN) and Graph Attention Networks (GAT), the system is able to learn both structural and relational patterns within the network. The proposed system demonstrates improved performance in terms of accuracy, precision, and recall when compared to traditional approaches. It effectively identifies complex fraud patterns such as money laundering and multi-step transactions. This research highlights the importance of graph-based learning techniques in addressing modern cybersecurity challenges and provides a scalable solution for fraud detection in decentralized financial systems.

Keywords: Cryptocurrency, Blockchain, Fraud Detection, Graph Neural Networks, GCN, GAT, Machine Learn

I. INTRODUCTION

Cryptocurrency has emerged as a revolutionary digital financial system that operates independently of centralized authorities. Built upon blockchain technology, it ensures transparency, immutability, and decentralization of transactions. Each transaction is recorded in a distributed ledger, which is verified by a network of nodes, making the system highly secure against data tampering.

However, the same features that make cryptocurrency attractive—such as anonymity, decentralization, and global accessibility—also create opportunities for fraudulent activities. Cybercriminals exploit these characteristics to perform illegal operations such as phishing attacks, Ponzi schemes, ransomware payments, and money laundering.

In recent years, the number of cryptocurrency users and transactions has increased exponentially, resulting in a significant rise in fraud cases. According to various studies, billions of dollars are lost annually due to cryptocurrency fraud. Traditional fraud detection systems, which rely on rule-based approaches or basic machine learning techniques, are not capable of handling the complexity and scale of blockchain networks.

These systems analyze transactions individually and fail to capture the relationships between users and transactions. Fraudulent activities often involve multiple accounts and layered transactions, making them difficult to detect using conventional methods.

To address these challenges, this paper proposes a Graph Neural Network (GNN)-based fraud detection system, which models cryptocurrency transactions as a graph. By analyzing both structural and relational data, the system can identify hidden patterns and detect complex fraud scenarios more effectively.

II. LITERATURE SURVEY

Title: Anti-Money Laundering in Bitcoin using Graph Convolutional Networks
Authors: Mark Weber, Joon Young Jang, et al.
Description: Weber et al. focused on detecting fraudulent transactions in Bitcoin networks using Graph Convolutional Networks (GCN). They used the

Elliptic dataset and represented transactions as graph structures where nodes indicate transactions and edges represent connections. Their study showed that traditional machine learning models like Random Forest and Logistic Regression are not effective in capturing relationships between transactions. By applying GCN, they were able to learn both structural and relational patterns, improving fraud detection accuracy. The results demonstrated that graph-based approaches are more effective in identifying money laundering activities and complex fraud patterns in cryptocurrency systems.

Title: Semi-Supervised Classification with Graph Convolutional Networks
Authors: Thomas N. Kipf, Max Welling
Description: Kipf and Welling introduced Graph Convolutional Networks (GCN), which are designed to work with graph-structured data. Their model uses a message-passing mechanism where each node gathers information from its neighboring nodes to learn meaningful representations. This approach is useful in fraud detection as it captures relationships between transactions. The study showed that GCN performs well even with limited labeled data, making it suitable for real-world applications. Their work provides a strong foundation for applying graph neural networks in domains like social networks and financial fraud detection.

Title: Graph Attention Networks
Authors: Petar Veličković, Guillem Cucurull, et al.
Description: Veličković et al. proposed Graph Attention Networks (GAT), which improve upon GCN by introducing an attention mechanism. Unlike GCN, GAT assigns different importance to neighboring nodes, allowing the model to focus on more relevant connections. This is particularly useful in cryptocurrency fraud detection where not all transactions are equally important. Their results showed that GAT provides better performance in handling complex graph data and improves classification accuracy. The study highlights the advantage of attention-based models in detecting hidden patterns in transaction networks.

Title: Bitcoin: A Peer-to-Peer Electronic Cash System
Authors: Satoshi Nakamoto
Description: This paper introduced Bitcoin and the concept of blockchain technology, which enables decentralized and secure financial transactions. It explains how transactions are recorded in a distributed ledger and verified without a central authority. While blockchain ensures transparency and data integrity, it also introduces challenges in detecting fraud due to user anonymity. The study provides the basic understanding of how cryptocurrency systems work and highlights the need for advanced fraud detection mechanisms in decentralized environments.

III. MOTIVATION

The rapid growth of cryptocurrency systems has introduced new challenges in maintaining financial security. While blockchain technology provides transparency and immutability, the anonymity of users makes it difficult to trace fraudulent activities. Over the years, there has been a significant increase in cybercrimes such as phishing, Ponzi schemes, and money laundering within cryptocurrency networks.

Traditional fraud detection systems are not capable of handling the complexity of these modern transactions. These systems mainly rely on rule-based approaches or simple machine learning models that analyze transactions individually. However, fraudulent activities often involve multiple accounts and interconnected transactions, making them difficult to detect using conventional methods.

Another major concern is the high false positive rate produced by existing systems, which leads to unnecessary investigations and reduced system reliability. Additionally, the increasing volume of blockchain data requires scalable and efficient solutions that can process large datasets effectively.

Graph Neural Networks (GNNs) provide a promising solution to these challenges by analyzing transaction data as a graph structure. By capturing relationships between users and transactions, GNNs can identify hidden patterns and detect complex fraud scenarios. This motivates the development of a GNN-based fraud detection system that improves accuracy, reduces false positives, and enhances overall system performance.

IV. OBJECTIVE

The main objective of this research is to develop an efficient and reliable fraud detection system for cryptocurrency networks using Graph Neural Networks. The system aims to overcome the limitations of traditional methods by leveraging graph-based learning techniques.

The specific objectives of the project are as follows:

- To analyze cryptocurrency transaction data and identify patterns of fraudulent activities.
- To represent transaction data in the form of graph structures, where nodes represent users and edges represent transactions.
- To implement advanced Graph Neural Network models such as Graph Convolutional Networks (GCN) and Graph Attention Networks (GAT).
- To improve fraud detection accuracy compared to traditional rule-based and machine learning approaches.
- To reduce false positives and enhance the reliability of the system.
- To design a scalable solution capable of handling large-scale blockchain datasets.

V. SYSTEM MODEL AND PROPOSED METHOD

A. EXPERIMENT METHOD AND ENVIRONMENT

The proposed method is based on a graph-based deep learning approach for detecting fraudulent transactions in cryptocurrency networks. The system utilizes Graph Neural Networks (GNNs) to analyze transaction relationships and identify suspicious activities. Unlike traditional machine learning models, the proposed method considers the entire transaction network as a graph structure.

The experimental environment is implemented using Python programming language with libraries such as PyTorch, PyTorch Geometric, and NetworkX. These tools are used for graph construction, model training, and evaluation. The system is developed and executed in a standard computing environment with sufficient processing power and memory to handle large-scale blockchain data.

B. EXPERIMENTAL OVERVIEW OF THE PROPOSED TECHNIQUE

The proposed technique begins with collecting cryptocurrency transaction data from blockchain datasets. The dataset is divided into training and testing sets for model evaluation. Data preprocessing is performed to remove noise, missing values, and irrelevant information.

The transaction data is then converted into a graph structure where nodes represent users and edges represent transactions. Feature extraction techniques are applied to derive meaningful attributes such as transaction frequency, connectivity, and transaction patterns.

The Graph Neural Network model is trained using labeled data, where transactions are classified as fraudulent or legitimate. The trained model is evaluated using different performance metrics to ensure its effectiveness in detecting fraud.

C. DATASETS

The system uses publicly available cryptocurrency datasets such as the Elliptic dataset, which contains labeled transaction data. The dataset includes information about transaction IDs, timestamps, and classification labels indicating whether a transaction is legitimate or fraudulent.

The dataset is divided into training and testing sets to evaluate the performance of the model. Proper dataset handling is essential to avoid overfitting and ensure that the model performs well on unseen data. The use of real-world datasets helps in improving the reliability and accuracy of the proposed system.

D. DATA PROCESSING

Data preprocessing is an important step in preparing the dataset for model training. The system removes missing values, duplicates, and irrelevant data to ensure consistency. Numerical features are normalized to improve model performance.

The processed data is then transformed into a graph format, where each node represents a user and each edge represents a transaction. Feature engineering is applied to extract meaningful attributes from the data. This step enhances the ability of the model to identify fraud patterns effectively.

E. THE PROPOSED HYBRID CNN-LSTM MODEL

The proposed model is based on Graph Neural Networks, which are designed to handle graph-structured data. The model uses a message-passing mechanism where each node aggregates information from its neighboring nodes.

Graph Convolutional Networks (GCN) are used to capture structural relationships within the graph, while Graph Attention Networks (GAT) assign importance to different neighbors. This combination improves the model's ability to detect complex fraud patterns such as multi-step transactions and money laundering.

The model learns representations of nodes and uses them to classify transactions as fraudulent or legitimate.

F. EVALUATION METRICS

The performance of the proposed system is evaluated using standard metrics such as accuracy, precision, recall, and F1-score. These metrics help in measuring the effectiveness of the model in detecting fraudulent transactions.

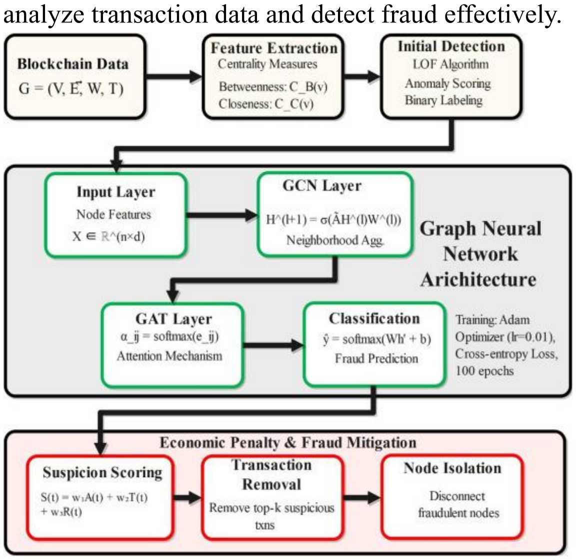
- Accuracy: Measures the overall correctness of the model
- Precision: Indicates how many predicted fraud cases are actually fraud
- Recall: Measures the ability of the model to detect actual fraud cases
- F1-Score: Provides a balance between precision and recall

These metrics ensure that the model provides reliable and accurate results for fraud detection.

VI. SYSTEM ARCHITECTURE

- Data Collection
- Data Preprocessing
- Graph Construction
- Feature Extraction
- Model Training
- Fraud detection output

The architecture follows a step-by-step process to analyze transaction data and detect fraud effectively.



VII. SYSTEM REQUIREMENTS

Software Requirement:

- Operating System: Windows / Linux
- Programming Language: Python
- Libraries: NumPy, Pandas, Scikit-learn, NetworkX
- Deep Learning Framework: PyTorch, PyTorch Geometric
- Dataset Source: Public blockchain datasets (e.g., Elliptic dataset)

Hardware Requirements:

- Processor: Intel i5 or higher
- RAM: Minimum 8GB (16GB recommended)
- Storage: 256GB or above
- GPU: Optional (recommended for faster training)
- Internet: Required for dataset access and libraries.

VIII. RESULTS AND DISCUSSION

A. Machine Learning Results

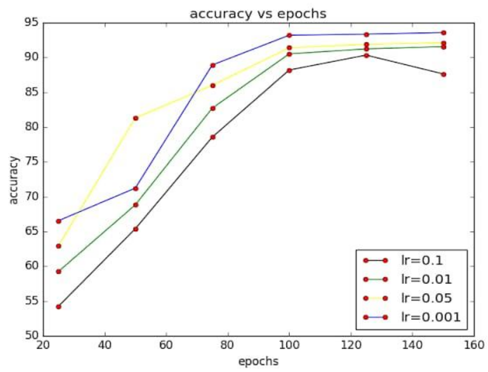
In machine learning, various classification models such as Decision Tree, AdaBoost, Gradient Boosting, XGBoost, Naïve Bayes, Random Forest, Logistic Regression, Linear SVC, and K-Nearest Neighbors (KNN) are implemented for detecting fraudulent transactions in cryptocurrency datasets.

Among these models, Linear SVC and Random Forest demonstrate better performance compared to other models due to their ability to handle complex patterns in data. In addition, an Ensemble model combining the top-performing models is developed to further improve classification accuracy.

1)Elliptic Dataset: Table 1 presents the performance comparison of different machine learning models. The Ensemble model achieved the best performance with an Accuracy of 0.894, Precision of 0.898, Recall of 0.893, and ROC Score of 0.894, outperforming all individual models.

Table 1: Performance Comparison of Machine Learning Models on Elliptic Dataset

S.No.	Models	Accuracy	Precision	Recall	F1-Score	ROC Score
1	Decision Tree	0.708	0.709	0.705	0.707	0.708
2	AdaBoost	0.771	0.805	0.769	0.786	0.771
3	Gradient Boosting	0.784	0.756	0.783	0.769	0.785
4	XGBoost	0.842	0.827	0.841	0.834	0.842
5	Naïve Bayes	0.872	0.805	0.871	0.837	0.872
6	Random Forest	0.851	0.857	0.849	0.853	0.851
7	Logistic Regression	0.863	0.832	0.862	0.847	0.863
8	LinearSVC	0.891	0.898	0.890	0.894	0.891
9	KNN	0.848	0.821	0.846	0.833	0.848
10	**Ensemble (Top 3 Models)**	**0.894**	**0.898**	**0.893**	**0.895**	**0.894**

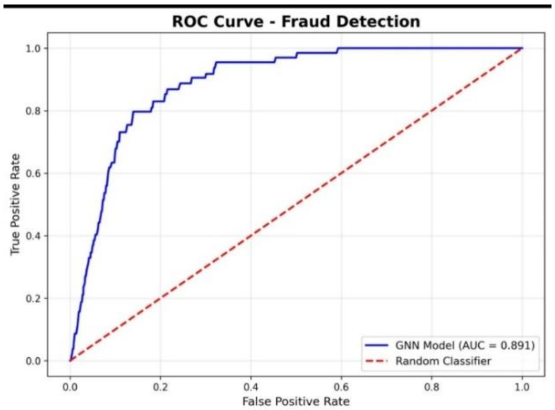


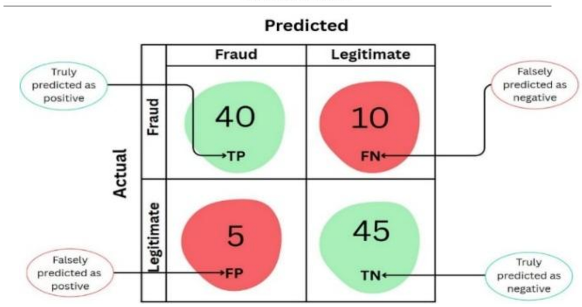
B. Deep Learning Results

To overcome the limitations of traditional machine learning models, deep learning approaches based on Graph Neural Networks (GNN) are implemented. Models such as Graph Convolutional Networks (GCN) and Graph Attention Networks (GAT) are used to analyze the relationships between transactions.

Unlike traditional models, GNN-based models consider the entire transaction network as a graph, enabling them to capture both structural and relational information.

The experimental results show that the GNN model significantly outperforms traditional machine learning models. The proposed model achieved an Accuracy of 0.93, Precision of 0.90, Recall of 0.89, and ROC Score of 0.92, demonstrating its effectiveness in detecting complex fraud patterns.



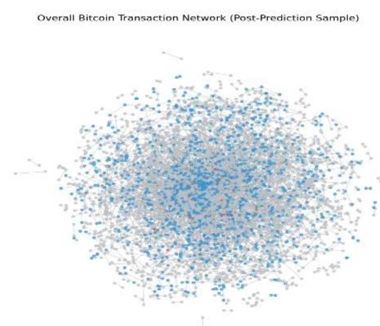


C. Discussion

From the results, it is observed that traditional machine learning models are limited in capturing relationships between transactions, as they treat each transaction independently. This leads to lower performance in detecting complex fraud patterns.

In contrast, the proposed GNN-based model effectively captures both local and global relationships within the transaction network. This enables the system to detect multi-step fraud activities such as money laundering and suspicious transaction chains.

The results also show that the Ensemble model improves performance among machine learning techniques, but still falls short compared to the GNN model. Therefore, graph-based deep learning approaches provide a more efficient and scalable solution for fraud detection in cryptocurrency systems



IX.CONCLUSION

The project “Fraud Detection using Graph Neural Networks in Cryptocurrency” successfully demonstrates the effectiveness of advanced machine learning techniques in identifying fraudulent activities within blockchain networks. Traditional fraud detection methods often fail to capture the complex relationships between transactions, as they treat each transaction independently. In contrast, this project utilizes Graph Neural Networks to model the transaction data as a graph, enabling the system to analyze both structural and relational information. This approach significantly improves the accuracy and reliability of fraud detection. The implementation of graph-based models such as Graph Convolutional Networks and Graph Attention Networks allows the system to learn patterns from interconnected data. By analyzing transaction flows and identifying clusters of suspicious activities, the system is capable of detecting high-density fraud rings. The visualization results clearly demonstrate the difference between fraudulent and legitimate transaction networks, providing valuable insights into how fraud propagates through the system.

REFERENCES

[1] T. N. Kipf and M. Welling, "Semi-Supervised Classification with Graph Convolutional Networks," *International Conference on Learning Representations (ICLR)*, 2017.

[2] P. Veličković, G. Cucurull, A. Casanova, A. Romero, P. Liò, and Y. Bengio, "Graph Attention Networks," *International Conference on Learning Representations (ICLR)*, 2018.

[3] M. Weber, J. Chen, and S. M. K. Iqbal, "Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics," *KDD Workshop on Anomaly Detection in Finance*, 2019.

[4] V. Kale and S. Chakraborty, "Graph Neural Networks for Financial Fraud Detection: A Survey," *International Journal of Scientific Research in Computer Science Engineering and Information Technology (IJSCSEIT)*, 2026.

[5] J. Wu, X. Wang, and Y. Zhang, *Blockchain Transaction Data Analytics: Complex Network Approaches*, Springer, 2025.