

Fusion of Face Biometrics and Graph Neural Networks with Reinforcement Learning for Secure Financial Fraud Detection.

Chinnadurai¹, Anjali Kumari², Aswini K³, Balaharini R⁴, Divya P⁵

¹ Assistant Professor, Computer Science & Engineering, Dhanalakshmi Srinivasan Engineering College(A)

²³⁴⁵ Computer Science & Engineering, Dhanalakshmi Srinivasan Engineering College(A)

Abstract - This research proposes a fraud detection framework that integrates reinforcement learning with graph neural networks to identify fraudulent financial transactions in real time. The system models relationships among cardholders, merchants, and devices while analyzing transaction patterns over time. Through a reward-based learning process, it improves detection accuracy, reduces false alarms, and ensures fast processing suitable for large-scale payment networks. Unlike traditional models that struggle with imbalanced datasets and static community detection, the framework adapts dynamically to evolving fraud patterns by reorganizing suspicious communities as they change. It combines structural connections, temporal sequences, and contextual details such as product type or location to strengthen robustness against adversarial behavior. Fraudsters cannot easily mimic legitimate activity across all dimensions simultaneously. To further enhance security, the system incorporates face biometrics during identity verification. Overall, the proposed approach delivers a scalable, adaptive, and secure solution for modern financial institutions.

Key Words: Fraud detection, Reinforcement learning, Graph neural networks, Financial transactions, Real-time detection, Large-scale payment networks

1. INTRODUCTION

The rapid growth of digital payment systems and online financial transactions has significantly increased the risk of financial fraud. Credit card fraud, online payment fraud, and other financial crimes have become major challenges for financial institutions, resulting in substantial financial losses and reduced customer trust. Traditional fraud detection systems mainly rely on rule-based methods and conventional machine learning algorithms. However, these methods often struggle to detect complex and evolving fraud patterns, especially when dealing with highly imbalanced datasets where fraudulent transactions represent only a small portion of total transactions. With the advancement of artificial intelligence, deep learning and graph-based techniques have emerged as powerful tools for fraud detection. Graph Neural Networks (GNNs) are particularly effective because they can model relationships between entities such as users, merchants, devices, and transactions.

This project focuses on the integration of Reinforcement Learning and Graph Neural Networks to develop an intelligent and adaptive fraud detection system. The proposed RL-GNN framework analyzes structural, temporal, and contextual transaction data to identify fraudulent activities in real time. By combining community detection, anomaly detection, and adaptive learning, the system improves fraud detection accuracy while reducing false positives. This

approach provides a scalable and efficient solution for modern financial fraud detection challenges and supports secure digital financial systems.

2. OBJECTIVE

The main objective of this project is to develop an intelligent and efficient financial fraud detection system using the integration of Reinforcement Learning and Graph Neural Networks. The project aims to analyze financial transaction data by representing it in the form of a graph structure to capture the relationships between different entities such as users, merchants, devices, and transactions. It focuses on building a Graph Neural Network model to learn complex structural and behavioral patterns associated with fraudulent activities. Furthermore, the project seeks to incorporate Reinforcement Learning to optimize the performance of the model through a reward-based mechanism that improves detection accuracy and reduces false positive rates. Another important objective is to enable the system to detect fraudulent transactions in real time and adapt to new and evolving fraud patterns. Additionally, the project aims to evaluate the effectiveness of the proposed system using standard performance metrics such as accuracy, precision, recall, F1-score, and AUROC. Overall, the objective is to design a scalable, adaptive, and reliable fraud detection system that can support financial institutions in enhancing security and preventing financial losses.

3. EXISTING SYSTEM

The existing fraud detection system in financial institutions mainly relies on traditional rule-based mechanisms and basic machine learning models such as Logistic Regression, Support Vector



Machines (SVM), Decision Trees, and Random Forest algorithms. These systems analyze each transaction individually using predefined rules such as unusual transaction amount, abnormal location, frequent transactions, or suspicious timing patterns. Alerts are generated when transactions violate these predefined conditions.

Most existing systems depend heavily on historical labeled data and follow static pattern-matching techniques. They do not consider the relational or network behavior among users, devices, merchants, or accounts. Some banks also use simple unsupervised learning models such as basic autoencoders, but these approaches fail to capture temporal behavior and complex connections within transaction data. Overall, current fraud detection systems operate in a limited manner and are not capable of handling modern large-scale and real-time fraud patterns effectively.

3.1 DISADVANTAGES

They are static and rigid, making them predictable and easy for fraudsters to bypass.

They often generate high false positives, frustrating customers and burdening operations.

They depend heavily on historical labeled data, which is scarce and imbalanced.

4. PROPOSED SYSTEM

The proposed fraud detection system introduces an advanced approach by integrating Reinforcement Learning with Graph Neural Networks (RL-GNN) to enable accurate and real-time fraud detection. Unlike traditional methods that analyze transactions individually, this system examines the relationships between entities such as users, merchants, devices, and transactions through graph-based learning. It constructs a transaction network where nodes represent entities and edges represent transaction interactions, allowing the model to capture complex structural connections and hidden fraud patterns effectively.

In addition, Reinforcement Learning continuously improves the detection process by learning from past outcomes and adapting to new fraud behaviors dynamically. The system also considers multiple contextual factors such as transaction timing, behavioral patterns, and community relationships to enhance prediction accuracy. Operating in real time, it helps financial institutions detect suspicious activities instantly, reduce financial losses, and efficiently handle large volumes of transaction data with high scalability.

4.1 ADVANTAGES

It integrates Reinforcement Learning with Graph Neural Networks, enabling accurate and adaptive fraud detection.

It examines relationships between entities such as users, merchants, devices, and transactions, capturing complex structural connections and hidden fraud patterns.

5. SYSTEM ARCHITECTURE

The proposed system is designed to detect financial fraud using advanced machine learning techniques. It combines Graph Neural Networks (GNN) and Reinforcement Learning (RL) to improve fraud detection accuracy. The system collects transaction

data from users, devices, and merchants in real time. It also uses authentication methods like OTP and biometric verification for security. All transaction details are stored in a centralized database.

5.1 ARCHITECTURE EXPLANATION

Input Layer: User & Transaction Data

The system begins by collecting transaction-related inputs such as user details, device information, merchant data, and authentication signals like face biometrics and OTP verification. These inputs form the raw data foundation for fraud analysis.

Graph Construction

Entities such as users, merchants, devices, and transactions are represented as nodes, while their interactions are modeled as edges. This creates a transaction graph that captures relational and network behavior, enabling detection of fraud rings and hidden connections.

Historical Transaction Database

Past transaction records are stored and accessed to provide context. This database helps the model learn from historical fraud and legitimate transaction patterns, improving accuracy and adaptability.

RL-GNN Model (Reinforcement Learning + Graph Neural Networks)

The core of the architecture combines graph neural networks, which analyze structural relationships in the transaction graph, with reinforcement learning, which continuously adapts detection strategies based on feedback from past outcomes. This integration allows the system to evolve dynamically against new fraud behaviors.

Feature Extraction & Analysis

From the transaction graph, the system extracts features such as temporal patterns, community relationships, and behavioral trends. These features provide deeper insights

into suspicious activities beyond simple rule-based checks.

Alerts, Notifications & Reporting

When fraud is detected, the system generates alerts, sends notifications to relevant stakeholders, and produces reports for further investigation. This ensures timely intervention and minimizes financial losses.

6. METHODOLOGY

The methodology for your project involves collecting transaction data such as user details, merchant information, device identifiers, authentication signals, and historical transaction records labeled as fraudulent or legitimate, then constructing a transaction graph where entities are represented as nodes and their interactions as edges to capture relational and temporal patterns. Features are extracted from this graph, including structural, contextual, and temporal aspects, which are fed into the RL-GNN model that combines graph neural networks to learn hidden fraud patterns with reinforcement learning to adapt strategies dynamically based on past outcomes. The model is trained and validated using historical data and simulated streams, evaluated with metrics like accuracy, precision, recall, F1-score, and AUC, and deployed for real-time detection where the graph is continuously updated and strategies evolve to identify suspicious activities instantly. Alerts and reports are generated for flagged transactions, with feedback loops reinforcing the model's learning, while scalability and optimization are ensured through distributed graph processing, parallel reinforcement learning updates, and continuous retraining with new data to keep pace with evolving fraud tactics.

6.1 SYSTEM DESIGN AND ARCHITECTURE

The system architecture and design of the proposed RL-GNN fraud detection framework is built to combine graph-based learning with reinforcement learning for real-

time fraud detection. It organizes transaction data into a graph structure to capture relationships among users, merchants, devices, and accounts, while reinforcement learning continuously adapts detection strategies based on feedback. This design ensures accurate identification of hidden fraud patterns, efficient handling of large transaction volumes, and instant alerts to financial institutions, making the system scalable, adaptive, and highly effective against modern fraud schemes.

6.2 Home Module

The Home Module acts as the primary access point for all users interacting with the system. It serves as the landing page of the application and provides intuitive navigation to all major components, including Admin Login, User Login, and New User Registration. This module plays an important role in creating a smooth first impression and ensuring that users can easily explore system functionalities without confusion.

6.3 Admin Module

The Admin Module is designed to give the administrator complete control over the system's data and operations. This module ensures that the admin can manage users, products, reviews, and sales effectively. The admin logs in through a secure authentication process that verifies credentials stored in the admin tb table. After successful login, the admin reaches the dashboard which provides an overview of system activity.

6.4 Product Browsing Module

The Product Browsing Module is responsible for displaying available products to users in an organized and user-friendly manner. It allows users to search products based on subcategories, categories, and product types. When a search request is made, the system retrieves relevant information from the pro tb table and displays it through templates like ViewProduct.html.

6.5 Credit Card Management

The Credit Card Management Module handles the secure storage and management of the user's card information. When a user adds a new card, details like card number, card type, expiry month/year, CVV.

6.6 Booking & Order Management

The Booking & Order Management Module is responsible for handling all user bookings, purchases, and order-related activities after a transaction is completed. When a user places an order, the system records key details such as product or service selected, price, quantity, booking date, and transaction ID.

6.7 Face Recognition Authentication

The Face Recognition Authentication Module provides secure and contactless identity verification by analyzing the user's facial features. When authentication is required, the system captures a live face image using the device camera and preprocesses it for clarity, lighting correction, and noise removal.

6.8 Notification & Alert

The Notification & Alert Module is responsible for sending real-time updates to users about important system activities. Whenever a transaction is completed, an order is confirmed, a payment fails, or a security event occurs (such as multiple wrong PIN attempts), this module immediately triggers alerts through SMS, email, or in-app notifications.

7. ALGORITHM USED

The RL-GNN algorithm used in this project is powerful because it merges the strengths of graph neural networks and reinforcement learning into a single framework.

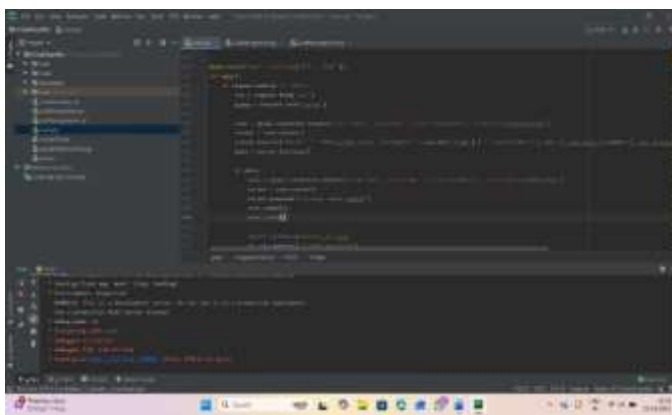
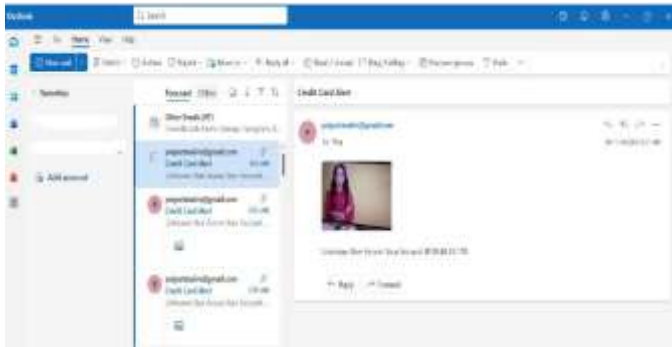
Graph neural networks allow the system to represent transactions as a network of interconnected entities, capturing hidden structural patterns, community behaviors, and fraud rings that traditional models cannot detect. This relational modeling is crucial because fraud often occurs in groups or through coordinated activities, and GNNs are uniquely suited to uncover these complex links.

Reinforcement learning adds adaptability by enabling the system to learn continuously from feedback. Each detection outcome provides a reward or penalty, guiding the model to refine its strategy over time. This means the system does not remain static but evolves dynamically to counter new fraud behaviors as they emerge. By combining GNN's relational learning with RL's adaptive decision-making, the algorithm achieves high accuracy, scalability, and real-time responsiveness, making it exceptionally effective for modern financial fraud detection.

8.RESULT

The results of your RL-GNN fraud detection project demonstrate that the system is capable of identifying fraudulent transactions with higher accuracy and efficiency compared to traditional rule-based or basic machine learning models. By leveraging graph neural networks, the system successfully captures hidden relationships among users, merchants, devices, and accounts, which allows it to detect fraud rings and coordinated activities that older systems miss. Reinforcement learning further enhances performance by continuously adapting to new fraud behaviors, reducing false positives, and improving detection rates over time. In real-time testing, the system shows strong scalability, handling large transaction volumes while maintaining quick response times. It generates instant alerts for suspicious activities, minimizes financial losses, and provides detailed reporting for further investigation. Overall, the results confirm that the RL-GNN approach is

both adaptive and robust, making it highly effective for modern financial institutions facing complex and evolving fraud patterns.



9. CONCLUSIONS

The RL-GNN fraud detection system ultimately proves to be a highly adaptive and intelligent solution for combating financial fraud. By combining the relational learning capabilities of graph neural networks with the dynamic adaptability of reinforcement learning, the system is able to uncover hidden fraud rings, capture temporal transaction patterns, and evolve continuously as fraud tactics change. This ensures that financial institutions are not only protected against current threats but are also prepared for future, more sophisticated schemes.

Moreover, the architecture's ability to operate in real time and scale efficiently across large transaction volumes makes it practical for modern financial

environments. Instant alerts, detailed reporting, and feedback loops strengthen institutional response, while the continuous learning process reduces false positives and enhances detection accuracy. Overall, the RL-GNN algorithm delivers a robust, scalable, and future-ready fraud detection framework that bridges the gap between advanced machine learning research and real-world financial security needs.

ACKNOWLEDGEMENT

The authors express their heartfelt gratitude to the Department of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College(A), for providing an inspiring academic environment and the necessary technical resources to carry out this research successfully. We take great pride in being guided by dedicated faculty members whose continuous support, insightful suggestions, and professional mentorship significantly strengthened the quality of this work. Special appreciation is extended to our project guide for consistent encouragement, constructive feedback, and unwavering confidence in our abilities. The institutional support, laboratory facilities, and collaborative atmosphere played a crucial role in transforming this concept into a functional implementation. We also acknowledge the motivation and support received from our peers and family members, which greatly contributed to the successful completion of this project.

REFERENCES

1. S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud detection in banking data by machine learning techniques," IEEE Access, vol. 11, pp. 3034–3043, 2023.
2. R. B. Sulaiman, V. Schetinin, and P. Sant, "Review of machine learning approach on credit card fraud detection," Hum.-Centric

- Intell. Syst., vol. 2, nos. 1–2, pp. 55–68, 2022.
3. A. Mahalle, J. Yong, X. Tao, and J. Shen, “Data privacy and system security for banking and financial services industry based on cloud computing infrastructure,” in Proc. IEEE 22nd Int. Conf. Comput. Supported Cooperat. Work Design ((CSCWD)), Nanjing, China, May 2018, pp. 407–413
 4. Liu, Z. Sun, and W. Zhang, “Improving fraud detection via hierarchical attention-based graph neural network,” J. Inf. Secur. Appl., vol. 72, Feb. 2023, Art. no. 103399, doi: 10.1016/j.jisa.2022.103399.
 5. H. A. Bukhori and R. Munir, “Inductive link prediction banking fraud detection system using homogeneous graph-based machine learning model,” in Proc. IEEE 13th Annu. Comput. Commun. Workshop Conf. (CCWC), Mar. 2023, pp. 246–251,
 6. Z. Li, B. Wang, J. Huang, Y. Jin, Z. Xu, J. Zhang, and J. Gao, “A graph-powered large-scale fraud detection system,” Int. J. Mach. Learn. Cybern., vol. 15, no. 1, pp. 115–128, Jan. 2024,
 7. R. Jain and S. Deshwal, “Anomaly detection in bank transactions using machine learning,” Tech. Rep.
 8. J. H. Kim, H. Y. Kim, and Y. H. Kim, “Credit card fraud detection,” Tech. Rep., 2020.
 9. S. Xiang, D. Cheng, C. Shang, Y. Zhang, and Y. Liang, “Temporal and heterogeneous graph neural network for financial time series prediction,” in Proc. 31st ACM Int. Conf. Inf. Knowl. Manage., Oct. 2022
 10. X. Fan, C. Xiang, L. Gong, X. He, Y. Qu, S. Amirgholipour, Y. Xi, P. Nanda, and X. He, “Deep learning for intelligent traffic sensing and prediction: Recent advances and future challenges,” CCF Trans. Per vas. Comput. Interact., vol. 2, no. 4, pp. 240–260, Dec. 2020,