Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

Enhancing Fraud Detection in Banking with Deep Learning Graph Neural Networks and Auto Encoders for Real-Time Credit Fraud Prevention

Y Venkata Subbaiah[1], R Chaitanya Lakshmi[2], N Kusuma[2], S Yasin[2], S Harsha Vardhan Reddy[2]

[1]Assistant professor, Dept. of CSE, Sai Rajeswari Institute of Technology, Kadapa – 516360.

[2]UG Scholar, Dept. of CSE, Sai Rajeswari Institute of Technology, Kadapa – 516360.

Correspondence

Y Venkata Subbaiah

Assistant Professor, Dept. of CSE, Sai Rajeswari Institute of Technology, Kadapa – 516360.

- Received Date: 25 Jan 2026
- Accepted Date: 14 Mar 2026
- Publication Date: 20 Mar 2026

Keywords

Banking Fraud Detection, Credit Card Fraud, Deep Learning, Graph Neural Networks (GNN), Autoencoders, Lambda Architecture, Temporal Graph Attention Network (TGAT), Anomaly Detection, Business Intelligence, Real-time Fraud Prevention, Imbalanced Dataset Handling, Node Embedding, Reconstruction Error, Precision–Recall, Financial Cybersecurity..

Abstract

Under the umbrella of artificial intelligence (AI), deep learning enables systems to cluster data and provide incredibly accurate results. This study explores deep learning for fraud detection, utilizing Graph Neural Networks (GNNs) and Autoencoders to enhance business practices and reduce fraudulent activities in large organizations. For real-time fraud detection, we propose Graph neural network with lambda architecture while for credit card fraud detection, we use an autoencoder, validated through case studies from two banks. The findings demonstrate that these methods effectively detect fraud with balance of precision and recall, improving the efficiency of banking systems. Python is employed for analysis, emphasizing the ability of deep learning to manage and prevent fraud in real-time on dynamic datasets. In the end, this study concludes that by using deep learning algorithms, we can control online credit card fraud detection in banks, improve the efficiency of the banking system. We can manage fraudulent activity in real-time and on dynamic datasets by utilizing deep learning algorithms, which allows for ongoing improvement of the fraud detection and prevention system.

Introduction

Banking fraud has emerged as a major concern in the digital financial landscape, including activities such as identity theft, credit card fraud, phishing, and account takeover. With the rapid growth of online banking and e-commerce, fraud attempts have become more frequent and sophisticated, posing significant risks to financial institutions and customers. Traditional rule-based fraud detection systems struggle to keep pace with evolving fraud patterns and the increasing volume of transaction data, often resulting in inefficiencies and high false positive rates.

To address these challenges, advanced artificial intelligence techniques, particularly deep learning, have gained prominence in fraud detection. These methods can analyze large-scale transactional data, learn complex patterns, and identify anomalies indicative of fraudulent behavior in real time. Among them, Graph Neural Networks (GNNs) effectively capture relationships between entities, while autoencoders enable efficient anomaly detection by learning data representations.

Furthermore, model-free and uncertainty-aware AI approaches enhance detection performance by eliminating rigid assumptions and improving robustness against noisy and dynamic data. Multi-dimensional constrained optimization further refines the learning process by incorporating multiple objectives and constraints.

This study proposes a hybrid framework combining Graph Neural Networks and autoencoder-based anomaly detection for credit card fraud detection. By integrating deep learning with data mining and business intelligence, the approach aims to improve fraud detection accuracy, reduce false positives, and strengthen the overall security of financial systems

Literature Survey

Recent studies have explored various machine learning and deep learning techniques to enhance credit card fraud detection.

S. K. Hashemi et al. (2023) focused on handling imbalanced datasets using class weight tuning and Bayesian optimization. Their approach combined ensemble models such as CatBoost, XGBoost, and LightGBM with deep learning-based hyperparameter tuning, achieving significant improvements in performance metrics such as ROC-AUC, precision, and recall.

Graph-based approaches have also gained attention in fraud detection. H. A. Bukhari and R. Munir (2023) proposed a homogeneous graph-based model for inductive link prediction, demonstrating superior performance over traditional tree-based models

Citation: Venkata Subbaiah Y, Chaitanya Lakshmi R, Kusuma N, Yasin S, Harsha Vardhan Reddy S. Enhancing Fraud Detection in Banking with Deep Learning Graph Neural Networks and Auto Encoders for Real-Time Credit Fraud Prevention. GJEIIR. 2026;6(3):200.

by capturing relationships between entities, albeit with increased computational cost.

Additionally, R. Achary and C. J. Shelke (2023) presented a machine learning-based approach using resampled datasets to address class imbalance. Their work emphasized the role of AI in improving fraud detection accuracy and reducing financial losses through early detection.

P. Tiwari et al. (2021) proposed a fraud detection framework for streaming transaction data by clustering cardholders based on transaction behavior and applying a sliding window approach. Multiple classifiers were trained on grouped data, and a feedback mechanism was introduced to handle concept drift, improving adaptability to evolving fraud patterns.

Overall, existing research highlights the effectiveness of machine learning, ensemble methods, and graph-based models in fraud detection. However, challenges such as data imbalance, evolving fraud patterns, and computational complexity remain, motivating the need for more adaptive and scalable solutions.

System Analysis

Existing System

Existing fraud detection systems utilize machine learning, deep learning, and graph-based models to identify fraudulent activities in large-scale financial data. Studies such as those by Bao et al. demonstrate the effectiveness of classifiers like Random Forest in achieving high accuracy, while A. Mahale et al. highlight the role of ML and DL in handling massive datasets for business intelligence. Advanced approaches like Hierarchical Attention-based Graph Neural Networks (HAGNN) improve fraud detection by capturing complex relationships between entities using attention mechanisms. Similarly, works by Kanan and Baguette emphasize the superiority of graph-based models over traditional methods, although they involve higher computational costs. Despite these advancements, existing systems still face challenges such as scalability, data imbalance, and adapting to evolving fraud patterns.

Proposed System

The proposed system introduces an advanced fraud detection framework that integrates Graph Neural Networks (GNNs) and autoencoder-based anomaly detection with model-free and uncertainty-aware artificial intelligence techniques. The system is designed to enhance the accuracy, adaptability, and robustness of fraud detection in online banking transactions.

The model-free approach enables the system to learn directly from complex and high-dimensional transaction data without relying on predefined assumptions, making it suitable for dynamic and evolving fraud patterns. In addition, uncertainty-aware AI methods are incorporated to handle noise and variability in data, improving the model's generalization capability and reducing false positives. Multi-dimensional constrained optimization is applied to effectively control the learning process by considering multiple objectives such as accuracy, precision, and recall simultaneously.

For real-time fraud detection, the system employs a Graph Neural Network integrated with a lambda architecture, allowing continuous processing of streaming transaction data. This helps in capturing relationships between customers, transactions, and behavioural patterns. Alongside this, autoencoders are utilized for credit card fraud detection by identifying anomalies through reconstruction errors, enabling the detection of previously unseen fraudulent activities.

The proposed framework is further evaluated using real-world banking datasets, providing insights into the gap between traditional fraud detection methods and modern AI-driven approaches. By combining deep learning with business intelligence, the system enhances decision-making processes, improves predictive analytics, optimizes business operations, and strengthens cybersecurity measures.

Overall, the proposed system aims to provide a scalable, efficient, and intelligent solution for fraud detection, improving the security and performance of banking systems while supporting advanced business practices.

System Design

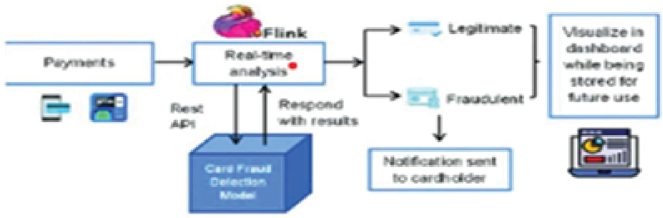


Figure 1: *System Architecture*

The overall system architecture integrates:

Graph Neural Networks (GNN) + Lambda Architecture → Real-time fraud detection

Autoencoder Model → Credit card anomaly detection

The system is divided into two major frameworks:

1. GNN + Lambda Architecture (Real-Time Fraud Detection)
2. Autoencoder-Based Anomaly Detection (Credit Card Fraud) GNN + Lambda Architecture A. Batch Layer Purpose: Train fraud detection model using historical data. Components:

- Historical Transaction Database
- Graph Construction Engineer
- GNN Model Training
- Fraud Pattern Mining
- Node Embedding Storage

Working:

1. Collect historical credit card transactions.
2. Construct a graph:
   - Nodes → Accounts, Cards, Devices, Merchants
   - Edges → Transactions, IP relationships
3. Train GNN model to:
   - Learn node embeddings
   - Detect abnormal patterns
4. Store learned embeddings for serving layer.

Speed Layer

Purpose: Detect fraud instantly when transaction occurs.

Components:

- Real-Time Data Stream (Kafka)
- Incremental Graph Updater
- Pre-trained GNN Model • Fraud Alert Engine

Working:

1. Incoming transaction arrives.
2. Graph updated dynamically.

3. GNN performs real-time inference.
4. If fraud probability > threshold:
   - Block transaction
   - Trigger alert
   - Send for manual review

Serving Layer

Purpose: Combine batch + real-time insights.

Components:

- Query Interface
- Risk Scoring Engine
- Decision Support System
- Dashboard for Analysts

Output Decisions:

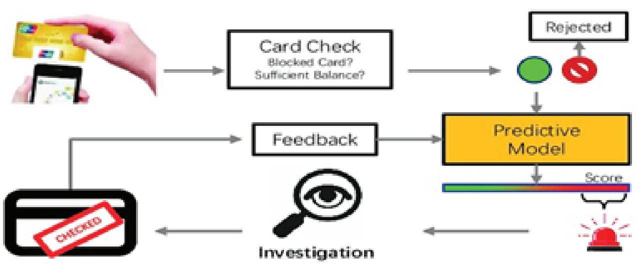
- Approve Transaction
- Flag for Review
- Reject Transaction

Temporal Graph Neural Network

Key Modules:

1. Attribute Embedding Layer
2. Temporal Graph Attention Network (TGAT)
3. Gated Residual Mechanism
4. Two-Layer MLP Fraud Risk Predictor

Autoencoder-Based Credit Card Fraud Detection



Working Principle

1. Train autoencoder only on normal transactions.
2. Learn compressed latent representation.
3. Reconstruct input.
4. If reconstruction error > threshold → Fraud.

Complete System Workflow

Step 1: Data Collection

- Historical banking transactions
- Real-time transaction streams

Step 2: Preprocessing

- Min-Max Scaling
- Handling imbalance
- Train-test split

Step 3: Model Training

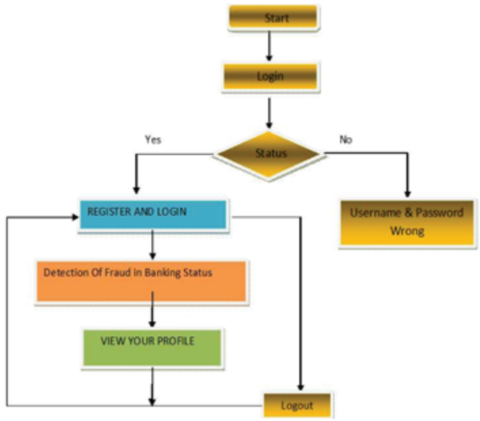
- GNN trained on transaction graph
- Autoencoder trained on normal transactions.

Step 4: Real-Time Detection

- Transaction arrives
- Graph updated
- Fraud risk predicted

Step 5: Decision Engine

- Risk score generated
- Alert or block triggered



Experimental Results and Discussion

The proposed fraud detection framework was experimentally evaluated using real-world credit card transaction data collected from two Pakistani private banks (Meezan Bank and UBL).

The dataset consists of:

- 284,807 total transactions
- 492 fraudulent transactions
- Highly imbalanced class distribution

Experimental Environment:

- Deep learning models implemented using neural network frameworks
- Semi-supervised learning for Graph Neural Network (GNN)
- Unsupervised anomaly detection for Autoencoder • Performance evaluated using classification metrics

Results of Graph Neural Network (GTAN Model):

The fraud detection problem was modelled as a semi-supervised node classification task on a temporal transaction graph.

Semi-Supervised Learning Performance

The percentage of labeled data was varied from 10% to 80% to test robustness.

Observations:

- Even with limited labeled data, the GTAN model achieved strong performance.
- Performance improved as labeled data increased.
- The model effectively captured temporal relationships between transactions.

The experimental results validate that:

Temporal Graph Attention Networks significantly improve fraud detection.

Autoencoders effectively detect anomalous transactions.

The hybrid deep learning approach enhances robustness.

The system achieves approximately 99.75% overall accuracy.

It is suitable for real-time credit card fraud detection in banking systems. The study demonstrates that combining graph-based relational learning with anomaly detection provides a scalable and reliable fraud detection solution.

Conclusion

This work presents a hybrid fraud detection framework that integrates Graph Neural Networks (GNNs) with Autoencoder-based anomaly detection for real-time credit card fraud detection. By modelling transactions as a temporal graph, the proposed Graph Temporal Attention Network (GTAN) effectively captures complex relational dependencies, enabling the detection of sophisticated fraud patterns beyond the capability of conventional methods.

The semi-supervised learning strategy demonstrates strong performance under limited labelled data, achieving high AUC (≈0.98) with stable precision–recall trade-offs across varying label ratios. Complementarily, the Autoencoder enhances detection of unseen fraud through reconstruction error-based anomaly scoring, yielding high classification accuracy (≈99.75%) with minimal misclassification.

Overall, the proposed framework effectively addresses class imbalance, leverages temporal-relational structures, and combines supervised and unsupervised learning to deliver a scalable and robust solution suitable for real-time deployment in modern banking systems.

References

1. P. Tiwari, S. Mehta, N. Sakhuja, J. Kumar, and A. K. Singh, 'Credit card fraud detection using machine learning: A study,'' 2021, arXiv:2108.10005.
2. T. Micro, ''Deep security? Software,'' Tech. Rep., 2020.
3. G. Kulatilaka, ''Challenges and complexities in machine learning based credit card fraud detection,'' 2022, arXiv:2208.10943.
4. 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.
5. 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.
6. E. Boush, X. Zhou, R. Gururaian, K. Chan, and X. Tao, ''A survey on credit card fraud detection techniques in banking industry for cyber security,'' in Proc. 8th Int. Conf. Behave. Social Compute. (BESC), Oct. 2021, pp. 1–7.
7. Y. Bao, G. Hilary, and B. Ke, ''Artificial intelligence and fraud detection,'' in Innovative Technology at the Interface of Finance and Operations, vol. 1, 2022, pp. 223–247.
8. 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, doi: 10.1109/CSCWD.2018.8465318.
9. N. Karkashadze, G. Shanidze, M. Shalamberidze, and S. Mikabadze, ''Modern challenges in agribusiness,'' Int. J. Innov. Technol. Economy, vol. 2, no. 38, Jun. 2022, doi: 10.31435/rsglobal_ijite/30062022/7828.
10. F. Manessi, A. Rozza, and M. Manzo, ''Dynamic graph convolutional networks,'' 2017, arXiv:1704.06199.
11. T. Kanan, A. Mughaid, R. Al-Shalabi, M. Al-Ayyoub, M. Elbes, and O. Sadaqa, ''Business intelligence using deep learning techniques for social media contents,'' Cluster Comput., vol. 26, no. 2, pp. 1285–1296, Apr. 2023, doi: 10.1007/s10586-022-03626-y.
12. A. Bouguettaya, H. Zarzour, A. Kechida, and A. M. Taberkit, ''Machine learning and deep learning as new tools for business analytics,'' in Handbook of Research on Foundations and Applications of Intelligent Bus. Analytics, 2022, doi: 10.4018/978-1-7998-9016-4.ch008.