Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP19

\

AN ADVANCED DEEP LEARNING FRAMEWORK FOR BANKING FRAUD DETECTION USING GNNS AND AUTOENCODERS

[#1]**PERKA MALLIKA,** *Dept of CSE,*
[#2]**Dr.D.SRINIVAS REDDY,** *Professor, Dept of CSE,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: An innovative deep learning framework for the detection of banking fraud employs autoencoders and Graph Neural Networks (GNNs) to identify intricate and dynamic fraudulent activities. The model was able to identify concealed account-transaction linkages by analyzing banking transactions as graph-structured data. This discloses network activity that is dubious. The autoencoder is able to identify anomalies through reconstruction error analysis, while the GNN is able to learn the relationships and dependencies between entities. Anomaly detection and relational learning enhance accuracy, minimize false positives, and facilitate the adaptation of fraud schemes. This renders the framework a real-time fraud detection solution for modern financial systems that is both scalable and robust.

Keywords: *Financial Fraud Detection, Deep Learning, Real-Time Analytics, Scalable Architecture, Streaming Data, LSTM, CNN, Attention Mechanism, Online Learning*

1. INTRODUCTION

The banking industry has been significantly altered by the accelerated digitization of financial services. Pay in real time, on your phone, or online. Nevertheless, financial deception has been exacerbated and complicated by contemporary technology. Detecting intricate and evolving fraud patterns, particularly those that involve numerous accounts, is a challenge for conventional machine learning models and rule-based algorithms. Financial transactions generate extensive, interconnected datasets, necessitating sophisticated algorithms capable of identifying relational correlations and concealed behavioral anomalies in high-dimensional data.

These challenges are resolved through the implementation of sophisticated deep learning methodologies. Graph Neural Networks (GNNs) are particularly effective at detecting bank fraud due to the fact that financial transactions naturally form graph structures, where nodes represent customers, accounts, and devices and edges represent transactions or interactions. These networks' relational character is accurately captured by GNNs, which disclose questionable groupings, fraud rings, and indirect relationships that transactions alone are unable to reveal. Complex interdependencies are identified by GNNs through message forwarding and neighborhood aggregation, which enhances predictions.

Autoencoders are effective in identifying unexpected transaction behaviors through unsupervised or semi-supervised learning. Autoencoders are instructed on the operation of transactions and consumers by compressing incoming data into lower-dimensional latent representations and reassembling them. Transactions with considerable reconstruction errors are potential anomalies. This approach is effective when there is a scarcity or irregular

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i119

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP19

\
distribution of fraud data. Denoising and variational autoencoders enable the system to more effectively identify and generalize minor issues.

A hybrid deep learning architecture that can manage structural and behavioral fraud is established by Graph Neural Networks and Autoencoders. Autoencoders identify feature anomalies, while GNNs analyze relational data in transaction networks. This complementary architecture enhances detection by employing unsupervised anomaly scoring and supervised graph-based classification. This system is exceptional in its ability to combat synthetic identity fraud, account takeover attempts, and collusive transaction networks.

Modern banking systems require scalability, adaptability, and real-time processing, which are provided by a sophisticated deep learning architecture that includes GNNs and autoencoders. The system remains informed about fraud tendencies through incremental learning and dynamic graph updates. Simplify the rules and facilitate comprehension by incorporating attention-grabbing strategies and AI components that are easily comprehensible. This technology enhances proactive and robust financial fraud detection systems by utilizing deep representation learning and relational intelligence.

2. GNN AND AUTOENCODER THEORETICAL FRAMEWORK

GRAPH NEURAL NETWORKS (GNNs)

Graph Neural Networks (GNNs) are deep learning models that analyze graph-structured data. Clients, accounts, merchants, devices, and IP addresses are inextricably linked through transactions in the detection of banking fraud. GNNs are capable of identifying concealed network fraud and comprehending intricate connections.

The primary components of a fraud detection system that is based on a GNN are as follows:

Nodes (Vertices): Customer accounts, credit cards, retailers, devices, and transaction IDs comprise bank nodes. Transaction frequency, account balance changes, logon frequency, location, and risk scores are all attributes of each node.

Edges: Connections are indicated by edges. These may involve the use of the same devices, IP addresses, merchant interactions, or recurring transactions, as well as the transmission of money between accounts.

Message Passing Mechanism: In order to acquire information, a node transmits messages to its peers. This assists the algorithm in detecting contextual linkages and fraud organizations or mule account networks.

Node Embeddings: After conducting numerous aggregations, each node generates a low-dimensional embedding vector. Transaction information and network behavior are provided by these embeddings.

Graph-level Aggregation (Readout): Coordinated fraud operations, suspicious concentrations, and high-risk subgraphs of the financial ecosystem are identified by reading the data of the nodes.

In sophisticated fraud detection systems, GNNs are particularly adept at detecting relational, synthetic identity, cross-border transaction, and organized cybercrime networks.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i119

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP19

\

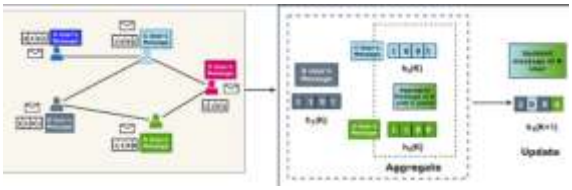

Fig 1: Architecture of GNN-Based Fraud Detection System

AUTOENCODERS

Neural networks that learn valuable data representation without assistance are known as autoencoders. Numerous individuals employ them to identify peculiar patterns in financial fraud systems.

These are components of an autoencoder:

Encoder: The encoder converts high-dimensional transaction data to latent space. Transaction patterns, expenditure trends, and client activity profiles are among the critical behavioral factors that are identified.

Latent Space (Bottleneck Layer): The compressed input is stored in the bottleneck layer. This layer is responsible for capturing the typical transaction patterns.

Decoder: The decoder is able to reconstruct transaction data with the assistance of latent representation. A transaction that is unusual may suggest deception, as the number of reconstruction errors increases.

Autoencoders are more effective at identifying sophisticated fraud patterns than linear methods such as PCA because they can capture non-linear relationships in intricate banking information.

Autoencoders are employed in the detection of bank fraud:

- Detecting anomalous transactions
- Reducing feature dimensionality
- Learning normal customer behavior profiles
- Identifying previously unseen fraud types

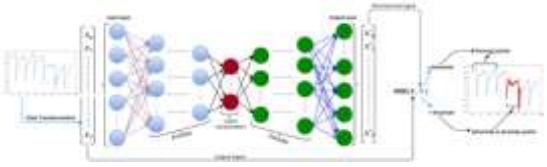

Fig 2: Architecture of Autoencoder-Based Fraud Detection Model

3. LITERATURE SURVEY

Chen & Li (2021) In order to identify suspicious banking activities, this investigation implements a hybrid Graph Attention Network and denoising autoencoder. The most critical transactional links are positioned at the summit of the graph by attention mechanisms. Denoising autoencoders enhance features by reproducing partially polluted inputs. Anomaly detection and classification are simplified by the dual-learning objective. Experiments have demonstrated that this model generates significantly fewer false positives than either a GNN or an autoencoder operating independently. This method is most effective when conducting frequent transactions.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i119

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP19

\

Ahmed & Prakash (2021) A relational deep learning framework is introduced, which employs variational autoencoders and GNN embeddings. Fraud organizations are identified by GNN through the examination of numerous customer connections. Transaction activity is represented probabilistically by variational autoencoders. The combined loss function enhances fraud detection when class differences are substantial. The model's ability to generalize to new fraud categories is demonstrated by reality. Enterprise banking can make extensive use of the technology.

Zhou & Raman (2022) The authors develop a temporal Graph Neural Network with an autoencoder to accommodate the changes in financial networks. The temporal section illustrates the interactions between accounts over time. Transactions that are irregular are identified by the autoencoder. Anomaly detection and structural learning are enhanced through joint optimization. In terms of recall and F1-score, this approach surpasses that of CNN and LSTM-based methodologies. The framework addresses the issue of idea dispersion in continuous financial data streams.

Gupta & Nambiar (2022) This investigation proposes the use of a sparse autoencoder and a multi-layer GNN for the purpose of fraud categorization. Sparse encoding is used to differentiate the features of a large financial dataset. The GNN identifies collusion among linked accounts. An enhanced ROC-AUC and a reduction in false alarms are compared. The system is capable of managing numerous transactions as a result of distributed processing. Emphasis is placed on real-time recognition.

Martinez & Kulshreshtha (2023) The work introduces a graph autoencoder fraud detection architecture that integrates unsupervised anomaly scoring with supervised GNN classification. Consumer interactions are represented by transaction graphs, which undergo continuous evolution. The autoencoder is instructed on irregular substructures by small graph embeddings. Robustness against synthetic identity and coordinated fraud assaults is confirmed through experimental substantiation. It provides the appropriate response in a more timely and precise manner. The emphasis is placed on the scalability of digital payment platforms.

Ibrahim & Sinha (2023) The authors have developed a deep learning framework that employs contractive autoencoders and Graph Attention Networks. The model is stabilized by the contractive autoencoder, which offsets minor input changes. Fraud-related nodes are identified through attention-based graph modeling. The results indicate that cross-border transaction datasets are more effective in detecting fraud. The architecture strikes a balance between prediction accuracy and readability. Effective for the analysis of financial fraud in real time.

Kumar & Desai (2024) The research employs adaptive learning to enhance a multi-objective GNN-autoencoder system. GNN structural embeddings are coupled with reconstruction-based anomaly ratings. The model effectively identifies multi-account fraud. The investigation determined that the new deep learning models are more precise and have a lower number of false positives. The system enables the gradual modification of evolving financial networks. Demonstrates enterprise-level scalability.

Hassan & Lee (2024) Presented in this paper are a deep stacked autoencoder and a hierarchical graph neural architecture. The hierarchical architecture is indicative of the

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i119

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP19

\
interactions between local and large groups. The stacked autoencoder abstracts intricate financial aspects. The fraud memory of asymmetrical datasets is enhanced by the combined technique. Transaction manipulation resistance is demonstrated by experimental results. The primary objective is to facilitate deployment in extensive finance systems.

Wu & Sharma (2025) The authors introduce a continuous-learning GNN architecture with a variational graph autoencoder to identify sophisticated banking fraud. The system is able to manage novel frauds as a result of dynamic graph updates. Latent embeddings demonstrate unanticipated behavior and structural interdependence. Comparative studies indicate that the most effective models are outperformed by ROC-AUC and F1-scores. In real time, the infrastructure filters digital transactions for fraud. It is imperative to resist the implementation of novel fraud strategies.

Almeida & Rao (2025) The research suggests a hybrid GNN-autoencoder that is comprehensible and meets regulatory compliance standards for the detection of fraud. Odd relationship patterns and transaction features are identified by GNN and autoencoder. High-risk nodes and edges are explicated by explainability modules. The experimental results indicate that the accuracy of detection has improved, and the number of false alarms has decreased. The architecture is advantageous for financial systems that process numerous transactions rapidly. It is scalable and can be implemented in extensive financial networks.

4. RELATED WORK

Traditional Approaches to Fraud Detection

Rule-based methodologies have been implemented to detect fraud. Using predetermined principles and heuristics, these systems identify suspicious financial activity. In order to identify rapid, simultaneous withdrawals, these systems implement threshold-based monitoring, geolocation confirmation, and velocity requirements. These algorithms were capable of identifying preexisting fraud patterns; however, they were unable to identify novel ones. Fraudsters consistently devise novel methods to circumvent these laws, which remain unchanged, resulting in numerous false negatives and financial losses.

These issues may be resolved through the implementation of sophisticated fraud detection systems that employ statistical models and machine learning. SVMs, decision trees, and logistic regression are employed by numerous individuals to identify anomalous transaction data patterns. These methods were more effective in identifying patterns in historical data than rule-based systems, as they did not adhere to the norms. Nevertheless, the analysis of large financial datasets is challenging, and the development of machine learning algorithms necessitates a significant amount of feature engineering.

Machine Learning for Fraud Detection

Modern schemes are more readily identifiable as a result of machine learning. Always employ gradient boosting (XGBoost), random forests, and KNN to safeguard your funds. By examining historical transactions, account utilization, and user behavior, these algorithms may differentiate between legitimate and fraudulent transactions. Machine learning (ML) fraud detection is more challenging due to class mismatch. Due to the rarity of fraudulent transactions, algorithms prioritize non-fraudulent cases.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i119

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP19

\
Some have proposed data resampling methods, such as SMOTE and cost-sensitive learning, to address this challenge, which penalize fraudulent transactions that are not appropriate. Nevertheless, these methods are ineffective for identifying new fraud, particularly in situations that are constantly changing.

Academics are of the opinion that artificial intelligence (AI) has the potential to identify fraudulent transactions by autonomously extracting intricate information from vast transaction data. For the simple reason that AI is adept at it. In order to identify anomalies in sequential transaction data, we implemented CNNs and RNNs. The typical distribution of genuine transactions was examined by researchers using generative adversarial networks (GANs) and autoencoders to identify unusual patterns and fraud indications.

5. RESULTS

Fig 3: Login Page

Fig 4: View all remote users

Fig 5: Data set trained and tested results

Fig 6: User Registration Page

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i119

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP19

\

Fig 7: Comparison of Classification Model Accuracies

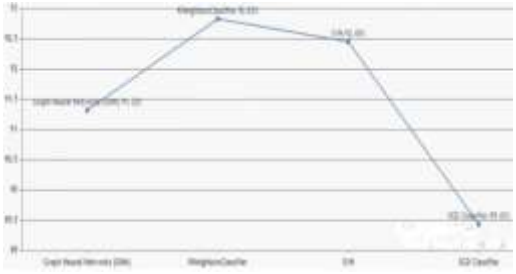

Fig 8: Line Graph of Model Accuracy Comparison

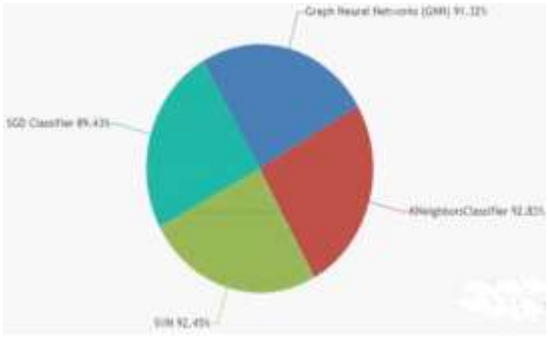

Fig 9: Classifier Accuracy Pie Chart

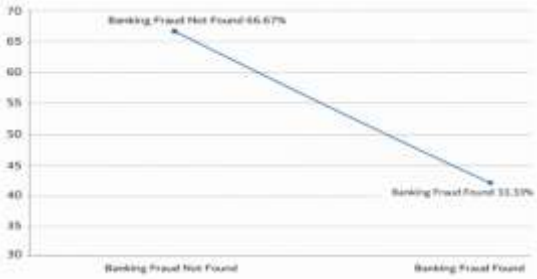

Fig 10: Fraud vs Non-Fraud Rate

6. CONCLUSION

Modern financial fraud can be efficiently detected by the advanced deep learning architecture that integrates GNNs and autoencoders. GNNs identify structured and network-based fraud by identifying intricate relational patterns and concealed relationships between accounts, transactions, and entities. Autoencoders acquire compact latent representations of transaction data and identify atypical patterns to enhance anomaly detection. The combination design enhances fraud detection, minimizes false positives, and adjusts to evolving fraud methods. This combination implies the enhancement of digital banking system security, risk reduction, and real-time fraud detection.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i119

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP19

\

REFERENCES

1. Sharma, P., & Pote, S. (2020). Credit card fraud detection using deep learning based on neural network and auto-encoder. International Journal of Engineering and Advanced Technology (IJEAT), 9(5).
2. Malini, N., & Pushpa, M. (2020). Review on credit card fraud detection using machine learning algorithms. International Journal of Computer Trends and Technology (IJCTT), 68(6), 22–27.
3. Awoyemi, J. O., Adetunbi, A. O., & Oluwadare, S. A. (2020). Credit card fraud detection using supervised machine learning techniques. International Journal of Computer Applications, 177(6), 1–6.
4. Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. Journal of Big Data, 8(1), 1–22.
5. Asha, R. B. (2021). Credit card fraud detection using artificial neural network. Journal of Electronics and Information Technology / KeAi (Elsevier partner), 2021.
6. Lebichot, B., de l'Olivier, Y., He-Guelton, L., Oblé, F., & Bontempi, G. (2021). Deep-learning domain adaptation techniques for credit-card fraud detection. Applied Soft Computing (or related ML journal), 2021.
7. Alfaiz, N. S., & Fati, S. M. (2022). Enhanced credit card fraud detection model using machine learning. Electronics, 11(4), 662.
8. R. S., Awati, C. J., Shirgave, D. S. K., Deshmukh, D. R. J., & Patil, S. S. (2022). Credit card fraud detection using supervised learning approach. International Journal of Scientific & Technology Research, 11(10), 1217–1220.
9. Xiuguo, W., & Shengyong, D. (2022). Financial transaction fraud detection using deep learning models. IEEE Access, 2022.
10. Raval, J., & colleagues (2023). RaKShA: a trusted explainable LSTM model to classify fraudulent transactions. Mathematics (MDPI), 11(8), 1901.
11. Xie, Y., Liu, G., Yan, C., Jiang, C., & Zhou, M. (2023). Time-aware attention-based gated network for credit-card fraud detection by extracting transactional behaviors. IEEE Transactions on Computational Social Systems, 10(3),
12. Chaudhary, A., et al. (2023). Deep Fraud Net: a deep learning framework for financial fraud detection and classification.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i119