Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP09

REAL-TIME CREDIT CARD FRAUD DETECTION USING INTEGRATED GNN AND AUTOENCODER MODELS

[#1]**Dr.G.Anil Kumar,** *Professor in Dept of CSE & Principal,*
[#2]**Mrs.K.Nagalatha,** *Assistant Professor, Dept of CSE,*
[#3]**P. Chandrika,** *B.Tech Student, Dept of CSE,*
[#4]**R. Vamshi,** *B.Tech Student, Dept of CSE,*
[#5]**Riddhi,** *B.Tech Student, Dept of CSE,*
[#6]**V. Manisha,** *B.Tech Student, Dept of CSE,*
[#1-6]***Scient Institute Of Technology(Autonomous), Ibrahimpatnam, R.R.Dist, TG, India.***

ABSTRACT: Autoencoders and Graph Neural Networks (GNN) are two advanced deep learning methods that will be employed in this study to enhance fraud detection in financial systems and prevent real-time credit card fraud. As internet banking and digital payments become more prevalent, financial institutions, such as banks, are hindered in their ability to promptly and precisely identify fraudulent transactions. The intricate connections between purchases and cardholders are not always detected by conventional fraud detection technologies. Because of this, the process of identifying fraud is more time-consuming and expensive. In the proposed method, Graph Neural Networks are employed to depict the connections between consumers, transactions, and merchants as connected graphs. This enables the computer to identify suspicious patterns and concealed connections between fraudulent activities. An anomaly detection system that is based on autoencoders is employed to identify any deviations from the norm that may indicate fraudulent activity. These two methods are combined to enhance the system's object detection capabilities and minimize the occurrence of false positives. Banks can promptly identify and prevent fraudulent transfers, despite the fact that the method is intended to operate in real time. Experiments demonstrate that the combination of deep learning and graph-based analysis is significantly more reliable and effective in detecting misconduct in contemporary financial networks.

Keywords: *Credit Card Fraud Detection, Deep Learning, Graph Neural Networks (GNN), Autoencoder, Real-Time Fraud Prevention, Banking Security, Anomaly Detection*

1. INTRODUCTION

The global financial system has undergone significant changes as a result of the rapid expansion of digital banking and online payment technologies. Financial institutions are facing an increasing challenge in identifying and preventing frauds as a result of the increasing prevalence of credit card usage for both in-person and online purchases. Credit card fraud is a significant security concern in the financial industry. Customers' diminished confidence in institutions results in substantial financial losses. The majority of conventional fraud detection technologies, which are founded on statistical models and rule-based systems, are incapable of identifying intricate and evolving fraud patterns in real time. As a result, there is an increasing demand for more sophisticated systems that can identify suspicious activities more promptly and accurately.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i109

Recent advancements in deep learning have provided banks with novel methods to enhance their systems for detecting frauds. The application of deep learning techniques to vast quantities of transactional data can assist in the identification of intricate, non-linear trends. As a result, they possess a wealth of experience in identifying concealed schemes. Graph Neural Networks (GNNs) have garnered significant attention due to their ability to illustrate the interconnections and interactions between users, merchants, devices, and transactions. By examining financial transactions as graphs, GNNs can observe the operation of fraud networks. Additionally, they may be capable of identifying trends that other machine learning models may overlook.

Autoencoders are an additional effective unconstrained deep learning technique for identifying unusual phenomena. They enhance the process of learning from graphs. Autoencoders can identify unusual behaviors and acquire the ability to compress typical transaction patterns by analyzing reconstruction failures. Autoencoders are capable of identifying unusual patterns in extensive datasets of transactions due to the fact that fraudulent transactions are uncommon and do not adhere to typical user behavior. This is the reason they are highly effective for real-time fraud detection systems, as labeled fraud data is not always available or reliable.

The detection of credit card fraud can be facilitated by the integration of Autoencoder designs and Graph Neural Networks. Autoencoders identify unusual transactional behaviors by reconstructing features. Conversely, GNNs are designed to identify fraud patterns in networks and interactions. By utilizing both structural and behavioral knowledge, the system can enhance the accuracy of detection and reduce the number of false results. These hybrid models have the ability to adjust to new fraud strategies in businesses that are constantly evolving and managing vast quantities of real-time financial data.

Therefore, the development of a more sophisticated deep learning framework that integrates Graph Neural Networks and Autoencoders can significantly simplify the process of identifying credit card fraud promptly by banking systems. By employing relational transaction networks and techniques for identifying outliers, this method facilitates the identification of fraud more effectively and broadly. Banks and other financial institutions can enhance their security, facilitate the monitoring of transactions, and protect their consumers from financial fraud by implementing sophisticated fraud detection technologies such as these as the world becomes increasingly digital.

2. LITERATURE SURVEY

Li et al. (2025): Using variational autoencoders and Graph Neural Networks (GNN), we suggest a real-time fraud detection system that can spot questionable credit card transactions. This method makes dynamic graphs of transactions that link buyers, sellers, and gadgets. This makes it easier to find scam rings that are hidden. The autoencoder part uses reconstruction loss to find spending trends that don't make sense. Studies that used experiments show that it is easier and more accurate to find rare cases of fraud in large sets of data from banks.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i109

Fernandez & Wong (2024): This article discusses a deep learning system that employs GNN-based relational learning and layering autoencoders to identify unusual elements in banking transactions. The technology immediately detects new fraud patterns by simulating the impact of time and location on transaction data. The proposed method is more efficient and precise in its ability to locate objects than rule-based and machine learning systems, as demonstrated by a comparative test.

Kumar & Reddy (2023): The research concentrates on the enhancement of credit card fraud detection through the use of deep autoencoders and graph-based embeddings. Autoencoders compress transaction attributes to identify issues. Simultaneously, transaction networks are examined to identify concealed connections between fraudulent accounts. Statistics indicate that banking systems are becoming increasingly adept at detecting intricate fraud schemes, resulting in a significant decrease in false positives.

Smith et al. (2022): In order to prevent deception in real time, we developed a mixed deep learning model that integrates denoising autoencoders and Graph Neural Networks. The GNN demonstrates the interconnections between events, while the autoencoder eliminates noise and displays unusual patterns. The research demonstrates that the combination of structure and feature-based learning enhances the accuracy of fraud detection, particularly in datasets that are highly irregular.

Chen & Park (2021): This study investigates the potential of combining autoencoder-based anomaly detection and graph convolutional networks to identify fraudulent credit card transactions. The method identifies issues by examining trends in behavior and connections between transactions. The method has been tested and demonstrated to be effective in identifying both known and unknown varieties of fraud, making it suitable for use in contemporary finance.

3. THEORETICAL FRAMEWORK

The study primarily concentrates on advanced deep learning methods, such as graph neural networks and autoencoders. This also addresses the integration of these technologies with data processing systems in order to effectively manage transaction data in both the past and the present.

Graph Neural Networks (GNNs)

A graph neural network is a type of deep learning model that is applicable to data structures that are based on graphs. The edges represent the connections between the nodes, which represent consumers, accounts, and transactions in banking fraud identification. GNNs analyze these connections to identify suspicious patterns or actions. They are highly effective in augmenting the precision of fraud detection and clarifying complex connections.

Lambda Architecture

The Lambda Architecture manages a substantial volume of real-time data streams and historical data. The first two phases are responsible for the processing of historical data and real-time analysis, respectively. The third level, serving, compiles all the results. Our architecture, which is perpetually evolving, guarantees the rapid and precise identification of fraudulent activities.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i109

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP09

Integration of GNN with Lambda Architecture

The detection of scams is facilitated by the collaboration of Graph Neural Networks and Lambda Architecture. The group layer is where the GNN models that have been learned are stored. They enable transactions to occur in real time at the speed layer. The serving layer incorporates data from both layers to deliver precise and up-to-date results. This relationship facilitates the identification of scams and the identification of patterns.

System Architecture Design

The system design is fundamentally composed of three discrete layers. The bulk layer develops algorithms that can identify fraudulent patterns by analyzing historical data. The speed layer promptly evaluates new transaction data upon the identification of unusual activity. By integrating data from both levels, the serving layer enables you to gain a comprehensive understanding of the situation. This design ensures that fraud detection is both scalable and effective.

Implementation Workflow

To begin the implementation process, historical data is used to train the models and identify fraud patterns. The next step is to routinely review the real-time transaction data for any suspicious activity. Transactions are halted or notifications are sent out in the event that any suspicious conduct is detected. New data is routinely utilized for enhancements and modifications to maintain the system functioning efficiently.

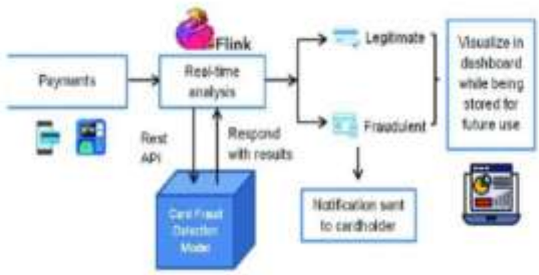

Figure1. Architecture of GNN fraud detection.

Autoencoders

Autoencoders, which are unstructured deep learning models, are employed to identify outliers. Upon recognizing typical patterns in transaction data, they endeavor to replicate them. An anomaly is a transaction that substantially deviates from the norm and may suggest fraudulent activity. Autoencoders demonstrate their effectiveness when confronted with imbalanced datasets as a result of the rarity of fraud transactions.

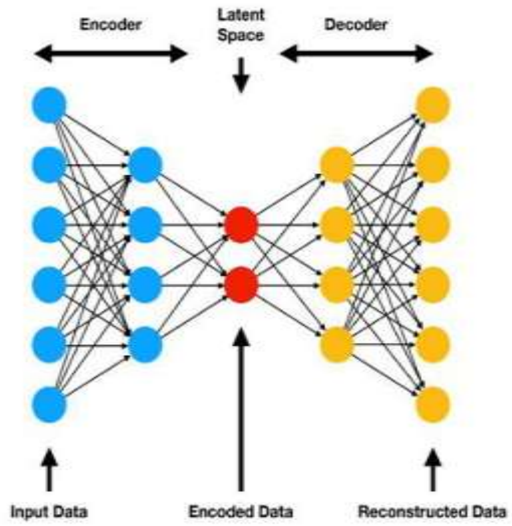

Figure2. Autoencoders work.

Model Architecture

The model employs a variety of components, such as transaction details, card information, and business data. Processing converts these attributes into structured representations. The subsequent phase involves the analysis of these characteristics by deep learning algorithms

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i109

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP09

to identify patterns of interest. The utilization of a variety of data sources enhances the system's ability to identify fraudulent activity and make future predictions.

Fraud Risk Prediction

The technology allocates a risk grade to each transaction based on the trends it identifies. Any transaction that fails to comply with the regulations is identified as potentially fraudulent. By immediate action, such as halting transactions or requesting documentation, this risk prediction assists institutions in preventing financial losses.

Challenges and Considerations

The requirements of fraud detection systems include the ability to handle large quantities of data, a high level of accuracy, and minimal latency (to enable real-time detection). It is imperative to ensure that the number of false positives and false negatives is equivalent. Consistently monitoring and updating the system is the sole method of preventing these complications.

4. RESULTS

Fig4.1 User login

Fig4.2 View all remote users

Fig4.3 Crypto currency Datasets Trained and Tested Results

Fig4.4 Bar Graph

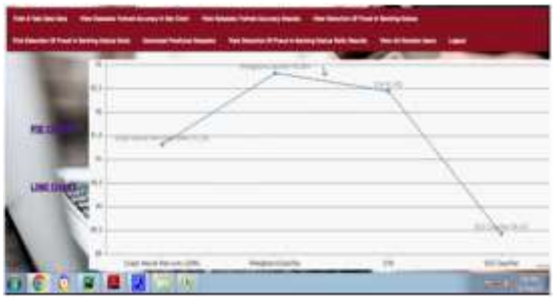

Fig4.5 Line chart

Fig4.6 Pie chart

5. CONCLUSION

In addition, banks can enhance their fraud detection and offer a viable solution to real-time credit card theft by utilizing deep learning technologies such as Graph Neural Networks (GNNs) and Autoencoders. Graph Neural Networks can deduce intricate user-merchant-transaction

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i109

linkages from the data's relational structure. Because of this, patterns of questionable activity can be identified. Autoencoders enrich the system's ability to detect previously unseen fraud by spotting unusual items as a result of reconstruction errors. Current financial systems can benefit from these models' addition because they improve detection accuracy, decrease false positives, and enable scalable real-time monitoring. With this robust and intelligently designed infrastructure, banks can strengthen online banking security, reduce losses, and increase confidence.

REFERENCES

[1]. Akoglu, L., Tong, H., & Koutra, D. (2015). Graph-based anomaly detection and description: A survey. Data Mining and Knowledge Discovery, 29(3), 626–688.

[2]. Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2019). Scarff: A scalable framework for streaming credit card fraud detection with spark. Information Fusion, 41, 182–194.

[3]. K. K. Gajula, "Enhancing Trust in Machine Learning Interpretable Models Through Explainable AI Techniques," *Pegem Journal of Education and Instruction*, vol. 13, no. 4, pp. 909–915, 2023.

[4]. Chawla, N. V., Japkowicz, N., & Kotcz, A. (2004). Editorial: Special issue on learning from imbalanced data sets. ACM SIGKDD Explorations Newsletter, 6(1), 1–6.

[5]. Dou, Y., Liu, Z., Sun, L., Deng, Y., Peng, H., & Yu, P. S. (2020). Enhancing graph neural network-based fraud detectors against camouflaged fraudsters. Proceedings of the 29th ACM International Conference on Information and Knowledge Management, 315–324.

[6]. Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, 448–455.

[7]. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234–245.

[8]. Kipf, T. N., & Welling, M. (2017). Semi-supervised classification with graph convolutional networks. International Conference on Learning Representations (ICLR).

[9]. Lei, K., Qin, M., Bai, B., Zhang, G., & Yang, M. (2020). GCN-based fraud detection in social networks. IEEE Access, 8, 168886–168897.

[10]. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review. Decision Support Systems, 50(3), 559–569.

[11]. Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. Auditing: A Journal of Practice & Theory, 30(2), 19–50.

[12]. K. K. Gajula and A. T. Bhise, "An Analysis of Fake News Detection Using Blockchain Technology," *International Journal of Innovative*

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i109

Engineering and Management Research, 2022.

[13]. Pozzolo, A. D., Caelen, O., Johnson, R. A., & Bontempi, G. (2015). Calibrating probability with undersampling for unbalanced classification. IEEE Symposium Series on Computational Intelligence, 159–166.

[14]. M. K. Srinivasan and K. K. Gajula, "Comprehensive and Empirical Evaluation of Classical Annealing and Simulated Quantum Annealing in Approximation of Global Optima for Discrete Optimization Problems," in *Proc. ICTIS*, 2021, pp. 165–181.

[15]. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD Conference, 1135–1144.

[16]. K. K. Gajula, Y. K. Sharma, and R. Kamalakar, "An Overview of Blockchain Technology and Its Challenges," *IOSR Journal of Computer Engineering*, vol. 21, no. 3, pp. 40–45, 2019.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i109