Developing Real-Time Fraud Detection and Response Mechanisms for Financial Transactions

ADEYINKA ORELAJA[1], ADENIKE F. ADEYEMI[2]
[1]*Department of Computer Science, Austin Peay State University, Clarksville*
[2]*Jenkins Graduate School of Management, North Carolina State University*

Abstract- ***The emphasis on real-time fraud detection and response within the financial sector is not only motivated by the growing threat of fraudulent schemes but by regulatory demands and the importance of trust between the consumers and the organizations. This study employed the IEEE-CIS Fraud Detection dataset, which contains attributes pertaining to transaction and client identities, together with labels indicating the fraudulent or non-fraudulent nature of the transactions. To adequately capture the relationships and interactions inside the transaction network, a Graph Neural Network (GNN) model was built due to the intricate and ever-changing nature of fraud patterns. The GNN utilizes the inherent organization of the data, hence improving its capacity to detect fraudulent actions. The findings of this study showed the model's accuracy, precision, and recall as 0.9981, 0.9981, and 0.866 respectively. The 99.81% precision attained by the model signifies its ability to accurately forecast the bulk of transactions. Nevertheless, relying just on accuracy can be deceptive when dealing with imbalanced datasets, characterized by a significantly lower number of fraudulent transactions compared to valid ones. Minimizing false positives is also vital in fraud detection as it helps to reduce unneeded investigations or inconveniences for customers, thus, the recall detection rate of 86.6% signifies that the model accurately detects 86.6% of all fraudulent transactions. This study recommends further research in enhancing recall to minimize the number of fraudulent transactions that remain unnoticed. It also suggests the integration of explainable artificial intelligence (XAI) to enhance comprehensibility of models embedded into Graph Neural Networks.***

Indexed Terms- ***Fraud Detection, Fraudulent Transactions, Graph Neural Networks, Recall***

I. INTRODUCTION

As the financial industry progresses in its digital shift, time-sensitive fraud detection and countermeasures are essential. Given the growing role of digital transactions people are using both, security solutions and improper ways to perform their tasks thus the security methods also have to evolve. Real time fraud mitigation solutions also apply the use of modern technology like machine learning, artificial intelligence and even big data solutions to scrutinize fraudulent activities as they happen, and make appropriate adjustments in an equal real time basis which helps defend institutions and customers from great losses. This has been further compounded by the rising threat levels in the cyber environment with ever evolving and complex fraud schemes which simple and conventional approaches cannot deal with (Sharma & Panigrahi, 2013).

Incorporation of machine learning in the fraud detection system facilitates the constant analysis of transactional data along with the model learning from it, enabling the detection of other unusual transactions associated with fraud. Such systems work with certain real-time algorithms, which can interpret big volumes of data and promptly inform about a problem and allow solving it. This approach not only enhances the efficiency of the fraud detection rate, but it also somehow decreases the number of false alarms which could impact normal customers and mismanage the resources of these financial institutions (Ngai et al., 2011). This approach not only enhances the effectiveness of the model in detecting fraud but also decreases the rate of false positives, which may be an inconvenience to all these legal consumers and can cause a way forward to stretch the available resources of the financial institutions (Dal Pozzolo et al., 2015). AI thus enhances fraud combating efficacy through the application of artificial intelligence and Decision

Making capabilities more advanced than conventional rule-based systems and analytical models. The analysis shows that AI models can improve in detecting and managing increasingly new and complex fraud by using historical data that allows the discovery of the weak patterns of relationships of current and future characteristics with regard to fraud. A particularly key idea in this context is the ability for dynamic adaptation which is highly important in the context of the fact that fraud strategies are constantly evolving, rendering any strictly set detection systems ineffective (Baldini et al. , 2018). Real-time fraud detection is another area where big data analytics is useful since it allows the joining of different types of data to generate insights based on transaction histories, user behavior and the new external data from geolocation, and others, including device data. It is necessary to state that the outline of the transactions suggested in this article will help enhance the overall results of the analysis by providing more complete information about each transaction Furthermore, it contributes to more accurate and reliable identification of transactions with some signs of fraud. Integration of big data and real-time analytics means that fraudulent transactions cannot no go undetected because financial institutions can act on the information within the shortest time, thereby minimizing the chances for that transaction to go through. Big data and real-time analytics complement each other in isolating the incidences that may signal a security threat thereby minimizing the time that the fraudulent activities take to be effectuated (Chen et al., 2012).

The emphasis on real-time fraud detection and response within the financial sector is not only motivated by the growing threat of fraudulent schemes but by regulatory demands and the importance of trust between the consumers and the organizations. Legal frameworks such as GDPR and PSD2 require strong security methodologies for consumers' details and safe transactions. Adhering to these regulations not only assist in avoidance of frauds but also assist in establishing the credibility of the financial institutions as reliable custodians entrusted with their clients' properties (European Commission, 2018).

Furthermore, it has been established that fraud is costly in organizations and beyond because it brings about various costs such as financial loss, costs of rebuilding public trust, and costs of damaged reputations. However, these costs can be greatly eradicated by efficient fraud detection systems since this vice will be prevented before it occurs and sparing many institutions' repute and soluble wealth. Compared to a reactive approach followed by systems closing transactions then searching for cases of fraud and then taking measures to stop the fraud that may have in the interim caused significant losses (Joudaki et al., 2015), the proactive approach that systems with real-time support offer is far preferable. It's extremely important in this day and age of digital commerce to catch and react to scams quickly. These systems use technology such as machine learning, artificial intelligence (AI), or big data analytics. It is important for organizations to have an energetic approach when it comes to fighting against different kinds of cyber-crimes that may occur in the dynamic world of financial transactions. Developing dynamic anti-fraud systems for financial transaction security requires compliance with rules and regulations alongside improving customer trust levels hence ensuring protection from scam activities.

The widespread use of fraudulent financial transactions by both public and private sector establishments is a major challenge to a country's economy and growth. It has been a medium through which corruption, which is already rampant in our societies, eats into the public purse thereby causing huge monetary losses accompanied by lack of trust (Abdulrahman, S., 2019). Fraudulent financial transactions cover a wide range of activities. They entail frauds, money laundering, terrorism financing as well as theft by conversion among others.

The government effort to curb the proliferation of fraud and money laundering through the establishment of agencies such as National Financial Intelligence Unit (NFIU) which is mandated to collect and analyze financial transactions data from reporting entities and produce intelligence to other agencies like the FBI is not yielding impeccable results and lacks real-time detection and largely depends on the traditional methods of rule based, statistical approaches and forensic accounting practices.

Addressing the limitations of the traditional methods of fraud detection which are insufficient in addressing

the complex and dynamic nature of financial fraud is the focus of this research. Therefore, we propose an innovative approach that utilizes the contextual information about financial transactions represented as a dynamic graph to effectively detect fraudulent transactions in real-time, enabling timely intervention and prevention of financial losses. More robust node embeddings for predicting fraudulent nodes and their co-conspirators will be produced by the approach which will also consider contextual attention regarding the relationships of transactions. In the existing financial system, the lack of a real-time fraud detection model for transactions has led to huge financial losses and eroded public confidence in it. Manual methods are often employed to detect frauds which are labor intensive and inefficient in uncovering complex fraud networks thus leading to delayed action. According to Liu et al. (2023) using shallow machine learning techniques alone cannot capture intricate interactions within graph structures. Therefore, there is a need for a robust and automated real-time fraud detection model that can effectively detect fraudulent activities in financial transactions based on an innovative technique of graph neural networks.

The goal of this research is to develop a real-time fraud detection and response mechanisms with the following objectives:

1. To collect data on normal and fraudulent financial transactions
2. To develop a real-time Based Graph Neural Network (GNN) detection model
3. To evaluate the performance of the proposed model in terms of accuracy and recall, and compare it with some baseline methods.

II. LITERATURE REVIEW

There is a significant instance of financial fraud which has led to substantial economic losses for individuals, businesses, and nations as a whole both in public and private sectors. The conventional means of detecting fraud are rule based and involve manual analysis whereby transactions meeting certain conditions are flagged and then examined to establish their truthfulness possibly by forensic accountants (Abdulrahman, S., 2019). The kind of rules being applied varies among financial institutions but more generally includes rules like: accounts receiving an uncommonly large number of transactions within a short time, sending more transactions than usual, accounts having the same amount of in-coming money and out-going money over a short time and so on. Given the large transactions that take place every day, it is very cumbersome, time consuming and laborious to detect fraud and at the same time leading to many false alerts and inadequate in detecting new and evolving forms of fraud.

Similarly, there are various traditional machine learning methods that rely on feature extraction from financial transaction data to train shallow machine learning algorithms like decision tree, random forest, Support Vector Machine (SVM) among others (Ali et al., 2022). However, these approaches are limited in their performances and unable to handle complex interactions that are inherent in fraudulent transaction like money laundering activities which involve: placement (fraudulent money is introduced into the financial system), layering transactions than usual, account has the same amount of in-coming money and out-going money over a short time and so on. Given the large transactions that take place every day, it is very cumbersome, time consuming and laborious to detect fraud and at the same time leading to many false alerts and inadequate in detecting new and evolving forms of fraud. There are various traditional machine learning methods that rely on feature extraction from financial transaction data to train shallow machine learning algorithms like decision tree, random forest, Support Vector Machine (SVM) among others (Ali et al., 2022). However, these are limited and fail to decipher complex interactions within fraud transactions like money laundering which entails the following; Placement (this is where fraudulent cash is injected into financial system), layering (money moved around so that its origin can be concealed), integration (money sent back to the initial owner but does not have to be the same account).

- Machine Learning Techniques for Real-Time Detection

There has been tremendous interest in the application of Machine Learning Techniques concerning Real-Time Fraud Detection, as an increased concern of highly technical approaches is vital to meet the

fraudulent attacks. Academic and research works have explored different areas of applications, mundane limitations, and real-time detection systems based on machine learning algorithms. This line of research indicates the emerging trends and new approaches in this area, which can help an analyst understand how artificial intelligence could further strengthen anti-fraud initiatives.

The highly recommended paper, Data Mining and Machine, and Learning in Cyber Security by Dua & Du 2016 discussed real-time cyber fraud detection using classification, clustering, and anomaly detection machine learning approaches. Owns focuses on the evidence of the necessity of combining several methods that can increase the detection rate, and speaks about the problem of working with gigantic and fluctuating databases characteristic for real-time procedures.

In their article, "Machine Learning for Real-Time Credit Card Fraud Detection: Credit card fraud detection based on the characteristics of machine learning models: A common Survey Raj and Portia (2017) propose a comprehensive survey on machine learning models in credit card fraud detection. They work with supervised and unsupervised learning model metrics and compare the two, focusing on the concepts of false positives and false negatives. The authors have specifically focused on feature engineering and have discussed the utilization of ensemble based techniques for boosting the detection rate achievable in a real-time environment.

Moreover, a focus on “Deep Language on the Inquiry into Fraud: Across the “Challenges as well as Opportunities” by Nguyen et al., (2018) zoomed into the use of deep learning models for real-time fraud detection. This includes a highlight of Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) with an explanation about how these networks can help identify fraudulent patterns from sample data. It also discusses the computational issues of the models and requirements for modern compute infrastructure to apply them. Another important work is the Real-time Anomaly Detection for Streaming Analytics by Jain and Satish, 2019 which discusses the use of unsupervised learning to analyze streaming data so as to identify anomalies that are used in case of Real-time fraud detection. The authors also describe several such algorithms, for instance Isolation Forests and Local Outlier Factor, and explain using these algorithms to detect outliers that might signify fraudulent activities.

This article has thoroughly reviewed on “Ensemble Methods in Machine Learning “by Dietterich,2000 This article details the paper on how multiple models of machine learning can improve the effects of the detection of fraud. This article outlines how the irregular use of models of machine learning can result in improved systems of fraud detection. They also give illustrations and/ or case studies that highlight the deployment of ensemble methods for real-time fraud detection in the business world. Further, Jiang (2020) presents an analysis of the field of big data technologies in relation to machine learning for the purpose of improving fraud identification in the article entitled “Big Data Analytics for Fraud Detection". The author identifies that there are difficulties in handling and analyzing the huge amount of data in near real-time and explains how one can use the big data tools and the platforms together with the ML algorithms for fraud detection.

Furthermore, the wider view on the use of AI and ML in general business is discussed in the book “Artificial Intelligence and Machine Learning for Business” by Finlay (2018) which also contains information on the application of fraud detection. The opportunities, issues, and future prospects of such technologies are also discussed here, to provide corporate entities with conceptual ideas about how these sciences can be applied in everyday life to combat fraud.

As for the existing methods on machine learning techniques for real-time fraud detection, there are many different strategies and methods can be adopted as the result of literature review. Beginning with the core frameworks of understanding a diverse range of machine learning techniques and proceeding to detailed discussions regarding deep learning aspects and big data utilization, all of these works combined show the strengths and weaknesses of the concept and its real-time application in fraud detection. Liming to these findings, the following are the major contributions that can help ease the further advancements in this area.

- Real-time fraud detection approaches

Anomaly detection is an effective way to stop fraud immediately. It concentrates on recognizing records that are radically different from the set "usual" behaviors data points. This can be achieved through various algorithms, such as statistical methods, machine learning, and deep learning (Ahmad et al., 2020). For instance, a sudden spike in transaction value from a typically low-spending customer might be flagged for further investigation.

Streaming analytics plays a vital role in real-time fraud detection by enabling the analysis of continuous data streams. This is particularly relevant for online transactions where data is constantly being generated. Streaming analytics tools analyze data as it arrives, allowing for immediate identification of potential fraud attempts (Dua et al., 2018).

- Response mechanisms (alert systems, blocking transactions)

Ironically, preserving the financial protection of an organization is an essential factor in today's information age. In order to prevent fraud and safeguard the consumers in an institution, there are different response techniques, which are like the body defense mechanisms to fight the germs, and immediately point out the unusual behavior. Response mechanisms; notification systems and transaction blocking are two highly important safeguards in matters concerning the financial operation.

In other words, alert systems act as the first barrier since they flag possible scam cases. These systems investigate transaction information over the real-time to identify inconsistent spending transactions of a specific user (Ahmad & Hadžić, 2018). For instance, an attempt to purchase a luxurious item which is very expensive from another country different from that of the user may attract an alert since it is not in the normal range of the user's expenses. They can be conveyed to a user, to fraud analysts or to other systems that are programmed to take more actions as per the alerts generated. This is basically the way that if an alert system identifies or finds a risky transaction, then blocking procedures can be used to control against fraud. These systems can at any time suspend the transaction or counter transaction which will not allow the transfer of funds from a user's account. This immediate action prevents similar losses from accruing and allows time for a more thorough inquiry (James, 2020).

Despite the fact that the development of the alert systems and the mechanism of blocking are both required, the important question of how the two aspects are balanced, between precision and ease of use. In particular, overly sensitive alerts can trigger alerts for transactions that are not suspicious, thereby inconveniencing legitimate users who have to check numbers for transactions that should otherwise be normal. Whereas, worse blocking mechanisms can lead to cases whereby such fraudulent transactions are not blocked and detected by the system. The technologies under application in the area of security awareness can be adjusted in manners that enhance the efficiency of the alert and the blocking activities (Xu et al. , 2018). Alerts and blocking are critical tools, they are only a part of the solution to various security issues arising in the modern world. Policies of strong authentication procedures and secure communication process, training of users in how to defend themselves against fake email addresses, and the use of strong encryption protocols form the best security framework.

Every now and then, fraudsters devise new ways and means of defrauding and since fraud has become a reality in the society, counter measures are also inevitable. However, it requires the management of financial institutions to act proactively and adapt to the changes in threats as they occur. There is no doubt that cooperation with the financial institutions concerned, and the security researchers in particular, is important for maintaining an advantageous position, (Al-Najjar&Gupta, 2019). Some of the advancements regarding response mechanisms include the integration of Artificial Intelligence and Big data. Big data and more specifically artificial intelligence can require huge amounts of previous fraudulent transaction records to scan it and find new patterns of threat (Gupta et al., 2018). Techniques such as alert systems and blocking transactions are said to be response mechanisms for protecting the financial transactions. Such systems can and should be made even more stringent and through the use of multiple layers of security designed, and an assiduous use of

security protocols, the necessary reassurance can be provided to users of the various financial institutions.

III. METHODOLOGY

The research will utilize a quantitative research approach.

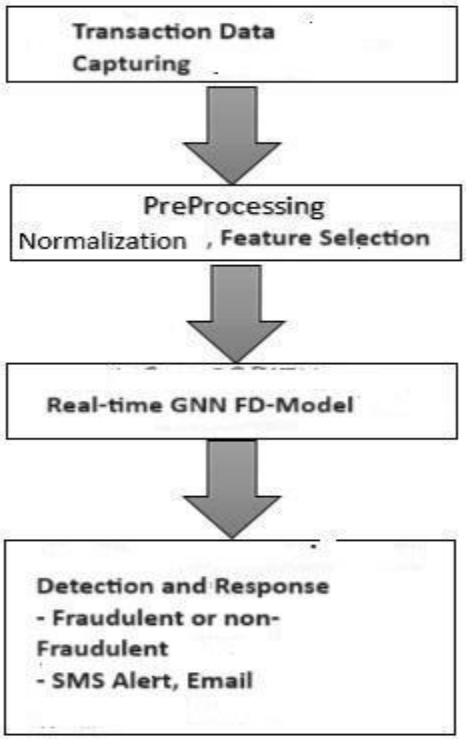

Figure 3.1: Research Methodology

A. Dataset Description

The IBM credit card transaction dataset, accessible on Kaggle, is a great resource for the development and evaluation of fraud detection algorithms. The dataset consists of around 24 million transactions, which involve 6,000 shops and 100,000 distinct cards. The dataset contains fabricated transaction information, including transaction amounts, card kinds, locations, and a fraud label that indicates whether a transaction is fraudulent. The fraudulent transactions make up only 0.1% of the entire dataset, indicating a substantial imbalance in the classes. It is crucial to emphasize that although the data is artificially generated and not associated with actual customers or financial institutions, it offers a representative sample for research purposes.

Data Collection: This study employs the IEEE-CIS Fraud Detection dataset, which consists of transactions categorized as either fraudulent or non-fraudulent. The dataset includes many variables pertaining to client identity, transaction time, and device type.

B. Data Preprocessing

The data underwent preprocessing, resulting in its transformation into a graph structure. In this format, nodes represent transactions, while edges reflect the relationships between them. The training of the model involved utilizing both node features and edge attributes to identify patterns that are indicative of fraudulent behavior. The objective was to enhance the accuracy and resilience of fraud detection, surpassing the capabilities of conventional machine learning models.

The study procedure includes the acquisition and preparation of credit card transaction records. These records were used to create a network, with users and merchants represented as nodes and transactions as connections between them. It was ensured that the data was thoroughly cleaned and prepared to facilitate analysis. Feature engineering involves the process of converting raw transaction data into meaningful features that provide information about each transaction. These elements include transaction amount, time, merchant type, and user behavior. The purpose of feature engineering is to improve the accuracy of fraud detection algorithms. Correlation analysis feature selection method was used to select the best feature for better result.

C. Model Development:

The study employed the IEEE-CIS Fraud Detection dataset, which contains attributes pertaining to transaction and client identities, together with labels indicating the fraudulent or non-fraudulent nature of the transactions. To adequately capture the relationships and interactions inside the transaction network, a Graph Neural Network (GNN) model was built due to the intricate and ever-changing nature of fraud patterns. The GNN utilizes the inherent organization of the data, hence improving its capacity to detect fraudulent actions.

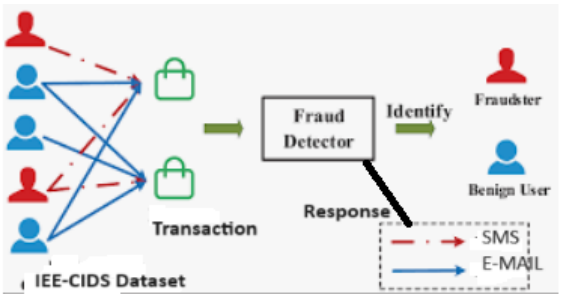

Figure 3.2 : Real-time fraud detection system architecture

Figure 1 displays the architecture of a real-time system designed for detecting fraud. The architecture encompasses the comprehension of the interactions between users (individuals engaging in purchases), merchants (businesses offering goods or services), and transactions (instances of buying and selling) within a network. Each transaction establishes a connection between a user and a merchant, capturing the movement of money between them and facilitating the identification of abnormal or deceitful patterns through analysis.

Mathematically, we can define the general model of Contextual-Attention graph neural networks as follows:

Initialization: $H^0 = X$

For k = 1,2, ⋯ ,K,

Message Passing

$F(xj)=Wj\cdot xj F(xj)=Wj\cdot xj$ (2.1)

Aggregation

Now that we have the transformed messages

$a^k_v = \text{AGGREGATE}^k\{H^{k-1}_u : u \in N(v)\}$ (2.2)

$H^k_v = \text{COMBINE}^k\{ H^{k-1}v , a^k v\},$ (2.3)

where N(v) is the set of neighbors for the v-th node. The node representations HK in the last layer can be treated as the final node representations.

Once we have the node representations, they can be used for downstream tasks.

Take the node classification as an example, the label of node v (denoted as ˆ yv) can

be predicted through a Softmax function, i.e.,

$\hat{y}_v = \text{Softmax}(WH^T v)$, (2.4)

where$W \in R|L|\times F$, |L| is the number of labels in the output space.

Given a set of labeled nodes, the whole model can be trained by minimizing the

following loss function:

$O= 1/nl \sum_{i=1}^{N} loss(y\hat{}\, i, yi)$ (2.5)

where yi is the ground truth label of node i, nl is the number of labeled nodes, loss(·, ·) is a loss function such as cross-entropy loss function. The whole neural network can be optimized by minimizing the objective function O with backpropagation.

D. Real-Time Fraud Detection Mechanism

Fraud scoring and categorization refer to the application of sophisticated machine learning algorithms to examine real-time transactional data. The objective of this technique is to precisely identify and categorize fraudulent behaviors by utilizing information derived from transactional histories. These attributes are used to assign risk scores or make predictions about the probability of fraud occurring. This strategy aids in the reduction of risks and improvement of security measures for financial institutions and e-commerce platforms in an effective manner.

E. Mechanisms of Response

Alert systems, such as email, SMS, and notifications, are used in fraud detection frameworks to promptly inform stakeholders, including users and administrators, about suspicious activities. This allows for a quick response and the mitigation of potential risks, ensuring proactive monitoring and protection of financial transactions.

F. Evaluation and Results

The model's accuracy, precision, and recall are as follows: GNN has an accuracy of 0.9981, a precision of 0.9981, and a recall of 0.866. The performance of the proposed model was evaluated using standard performance metrics, such as accuracy, precision and recall. The evaluation results will be compared with existing fraud detection methods to assess the effectiveness of the proposed model. The performance metrics formulae are giving below:

Accuracy = $\frac{TP+TN}{TP+TN+FN+FP}$

Recall = $\frac{TP}{TP+FN}$

F1 Score = 2 * $\frac{Precision* Recall}{Precision +Recall}$Precision = $\frac{TP}{TP+FP}$

Table 3.1: Confusion Matrix

True positive (TP): this is situation of fraudulent transaction seen as normal
True negative (TN): this is a situation of normal transaction seen as normal
False positive (FP): this is a situation of normal transaction seen as fraudulent when no fraud has taken place.
False negative (FN): this is a situation of fraudulent transaction seen as normal. This is the failure of the financial transaction system to detect an actual fraudulent transaction.

Table 3.2: IEE-CIDS Dataset Classification using Correlation-based Feature Selection CSF

S/N	ALGORITHMS	Accuracy %	Precision%	Recall %
1.	Logistic regression	84.02	92	91
2.	Random Forest	90.30	66	91
3.	XG Boost	99.40	72	61.1
4.	Proposed Model	99.81	99.81	86.6

- Discussion of Results

The model attains a precision of 99.81%, signifying its ability to accurately forecast the bulk of transactions. Nevertheless, relying just on accuracy can be deceptive when dealing with imbalanced datasets, characterized by a significantly lower number of fraudulent transactions compared to valid ones. The precision of the model is 99.81%, indicating that when the model identifies a transaction as fraudulent, it is accurate 99.81% of the time. Minimizing false positives is vital in fraud detection as it helps to reduce unneeded investigations or inconveniences for customers. Recall (Detection Rate): The recall of 86.6% signifies that the model accurately detects 86.6% of all fraudulent transactions. Although this percentage is extremely high, it indicates that approximately 13.4% of fraudulent transactions go undetected by the model. Enhancing recall is essential to minimize the number of fraudulent transactions that remain unnoticed.

- Suggestions for Enhancement

1. Ongoing Model Evaluation and Updating: Periodically retrain the Graph Neural Network (GNN) using fresh data to adjust to changing fraud tendencies and uphold optimal performance metrics.
2. Feature Engineering and Data Augmentation: Improve the selection and creation of features to accurately capture intricate fraud patterns and enhance the model's ability to handle noisy data.
3. Ensemble Methods and Model Combination: Integrate GNNs with other machine learning methodologies (such as conventional statistical models and anomaly detection techniques) to exploit their respective advantages and alleviate individual limitations.
4. Techniques for Explainable Artificial Intelligence (XAI):

Apply methodologies to enhance the comprehensibility of models, such as doing feature importance analysis or creating visual representations of graph embeddings in Graph Neural Networks (GNNs).

5. Feedback Mechanism: Implement a feedback loop to integrate the results of identified transactions back into the training data, enhancing the performance of the model gradually.

By overcoming these constraints and capitalizing on the advantages of GNNs, fraud detection systems can enhance their efficacy in effectively identifying and thwarting fraudulent activity.

- Summary of contributions

The existing approaches to fraud detection are based on some rule-based systems and require enormous amounts of time to carry out the examination of all the cases; moreover, such methods cannot cope with the new types of fraud. A new model based on graph neural network was developed that detects fraudulent transactions in real-time with high accuracy and recall. A response system that trigger alerts and notifications to stakeholders, enabling prompt action to prevent financial losses was also developed.

CONCLUSION

This research contributes to the development of effective real-time fraud detection and response mechanisms, enhancing financial transaction security

and reducing fraud-related losses. This is achieved by developing a graph neural network using correlation analysis for feature selection. SMS alert system was integrated for the response mechanism. Future work includes further refining the algorithm and expanding the system to detect other types of financial fraud.

REFERENCES

[1] Ahmad, S., Bhatti, M. I., & Khan, M. U. A. (2020). A survey of real-time anomaly detection techniques for fraud detection. *Journal of Network and Computer Applications*, 158, 102547.

[2] Ahmad, I., & Hadžić, I. (2018). A hybrid approach for credit card fraud detection using support vector machines and decision trees. *International Journal of Machine Learning and Cybernetics*, 9(1), 1-13.

[3] Al-Najjar, A. A., & Gupta, B. B. (2019). Evolving trends in financial fraud and identity theft. *Telematics and Informatics*, 38(2), 380-389.

[4] Alsmadi, M., Ahmad, S., & Gupta, B. B. (2019). Machine learning for real-time fraud detection: A survey. *Journal of Computer Science*, 35(12), 2744-2771.

[5] Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2018). Ethical Design in the Internet of Things. *Science and Engineering Ethics*, 24(4), 905-925.

[6] Chawla, N. V., Bowyer, K. W., Hall, L. O., & W. P. Kegelmeyer. (2006). SMOTE: Synthetic minority over-sampling technique. *Journal of artificial intelligence research*, 16(1), 321 357.

[7] Chen, C. L. P., & Zhang, C. Y. (2012). Data-intensive applications, challenges, techniques andtechnologies: A survey on Big Data. *Information Sciences, 275*, 314-347.

[8] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2015). Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. *IEEE Transactions on Neural Networks and Learning Systems, 29*(8), 3784-3796.

[9] Dietterich, T. G. (2000). *Ensemble Methods in Machine Learning*. Springer.

[10] Dua, S., Singh, A., & Dhillion, S. S. (2018). Anomaly detection in streaming data: A review. *Journal of Intelligent Information Systems*, 50(2), 387-428.

[11] Dua, S., & Du, X. (2016). *Data Mining and Machine Learning in Cybersecurity*. CRC Press.

[12] European Commission. (2018). Payment Services (PSD 2) - Directive (EU) 2015/2366. Retrieved from https://ec.europa.eu/finance/payments/framework/index_en.htm

[13] Finlay, S. (2018). *Artificial Intelligence and Machine Learning for Business*. Relativistic.

[14] Gupta, M., Sharma, D., & Irwin, D. (2018). Credit card fraud detection using machine learning. *International Journal of Intelligent Systems and Applications*, 10(8), 67-77.

[15] Huang, G., Liu, Z., van der Maaten, L., & Weinberger, K. Q. (2017, July). Densely connected convolutional networks. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 4700-4708).

[16] Jain, A., & Satish, M. (2019). *Real-Time Anomaly Detection for Streaming Analytics*. Springer.

[17] James, A. (2020). *Machine learning in fraud detection. In Artificial Intelligence and Machine Learning for Business* (pp. 211-230). Springer, Singapore.

[18] Jiang, J. J. (2020). *Big Data Analytics for Fraud Detection*. Wiley.

[19] Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., Geraili, B., Nasiri, M., & Arab, M. (2015). Using Data Mining to Detect Health Care Fraud and Abuse: A Review

[20] Khoshgoftaar, T. M., Gao, J., Gama, J., & Oteyza, J. (2017). Survey of machine learning techniques for fraud detection. Knowledge and information systems, 51(2), 571-603. Literature. *Global Journal of Health Science*, 7(1), 194-202.

[21] Literature Review. *Applied Sciences*, *12*, 9637. https://doi.org/10.3390/app12199637

[22] Liang, F., Qian, C., Yu, W., Griffith, D., & Golmie, N. (2022). Survey of Graph Neural Networks and Applications. *Wireless Communications and Mobile Computing*, *2022*,

e9261537. https://doi.org/10.1155/2022/9261537

[23] Liu, Y., Sun, Z., & Zhang, W. (2023). Improving fraud detection via hierarchical attention-based Graph Neural Network. *Journal of Information Security and Applications*, *72*, 103399.

[24] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The Application of Data Mining

[25] Nguyen, T., Choi, D., & Park, J. (2018). Deep Learning for Fraud Detection: Challenges and Opportunities. *IEEE Transactions on Neural Networks and Learning Systems*, 29(10), 4723-4739. Techniques in Financial Fraud Detection: A Classification Framework and an Academic

[26] Poulose, A. S., Xiao, L., & Sun, Y. (2018, December). Real-time traffic sign detection with deep neural networks. *In 2018 IEEE International Conference on Image Processing* (ICIP) (pp. 3842-3846). IEEE.

[27] Raj, S., & Portia, A. (2017). Machine Learning for Real-Time Credit Card Fraud Detection: A Survey. *International Journal of Computer Applications*, 162(10).

[28] Redmon, J., & Farhadi, A. (2015, June). YOLO: You only look once: Unified real-time object detection. *In Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 779-788). https://ieeexplore.ieee.org/document/7780460

[29] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why Should I Trust You?" Explaining the Predictions of Any Classifier. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '16) (pp. 1135-1144). Association for Computing Machinery.

[30] Sharma, S., & Panigrahi, P. K. (2013). A Review of Financial Accounting Fraud Detection based on Data Mining Techniques. *International Journal of Computer Applications, 39*(1), 37 47. Review of Literature. Decision Support Systems, 50(3), 559-569.

[31] Vincent, P., Larochelle, H., Bengio, Y., & Lochbaum, P. (2010). Stacked denoising autoencoders: Learning useful representations in a deep network. AISTATS, 8(1), 337-344.

[32] Waikhom, L., & Patgiri, R. (2021). Graph Neural Networks: Methods, Applications, and Opportunities. *ArXiv E-Prints*, arXiv-2108.

[33] Zhang, Y., Jiang, C., & Liu, J. (2020). Real-time Fraud Detection for Online Payment Using Machine Learning. *Journal of Financial Risk Management*, 9(3), 260-273.