International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 13 Issue 02 February 2026

An Adaptive Federated Graph Neural Network Framework for Real-Time Financial Fraud Detection

Aashish Panwar[1], Mohit Jain[2]
Research Scholar[1], HOD CSE[2]
BM College of Technology, Indore (M.P.), India[1, 2]
aashishpanwar72@gmail.com[1], bmctmohitcs@gmail.com[2]

Abstract: *As financial systems grow increasingly complex and interconnected, traditional fraud detection methods struggle to keep up with sophisticated and evolving fraudulent activities. This paper introduces FraudGNN-RL, an innovative framework that combines Graph Neural Networks (GNNs) with Reinforcement Learning (RL) to enable adaptive and context-aware financial fraud detection. By modeling financial transactions as a dynamic graph—where entities such as users and merchants are nodes and transactions are edges—our novel Temporal-Spatial-Semantic Graph Convolution (TSSGC) captures temporal patterns, spatial relationships, and semantic information simultaneously. The RL component, implemented via a Deep Q-Network (DQN), dynamically adjusts fraud detection thresholds and feature importance, allowing the model to adapt in real time to changing fraud tactics while minimizing detection costs.To further enhance privacy and collaboration, we integrate a Federated Learning scheme that enables multiple financial institutions to jointly train the model without sharing sensitive data. Extensive experiments on a large-scale, real-world dataset demonstrate that FraudGNN-RL achieves a 97.3% F1-score and reduces false positives by 31% compared to the best-performing baselines. Additionally, the framework exhibits strong resilience against concept drift and adversarial attacks, maintaining robust performance over extended periods. These results suggest that FraudGNN-RL offers a powerful, adaptive, and privacy-preserving solution for modern financial fraud detection challenges.*

Keywords: *Financial Fraud Detection, Graph Neural Networks (GNN), Reinforcement Learning (RL), Deep Q-Network (DQN), Federated Learning, Temporal-Spatial-Semantic Graph Convolution (TSSGC), Transaction Graph Analysis, Privacy-Preserving Machine Learning.*

1. INTRODUCTION

Credit card transactions have skyrocketed alongside the expansion of online shopping and other digital payment methods. In order to analyze consumer data and identify and avoid fraud, machine learning (ML) has proven crucial. But most real-world credit card data has irrelevant and redundant information, which makes ML classifiers not work as well. [1]Using a combination of filter and wrapper feature-selection procedures, this study proposes a hybrid feature-selection approach to identify the best features for ML. The features graded by the information gain (IG) technique are passed on to a genetic algorithm (GA) wrapper, which uses the extreme learning machine (ELM) as its learning algorithm. While doing so, the proposed GA wrapper is adjusted to handle imbalanced classification by displacing the conventional accuracy metric with the geometric mean (G-mean). Outperforming other baseline procedures and methodologies in the recent literature, the proposed strategy acquired a sensitivity of 0.997 and a specificity of 0.994, respectively [2].

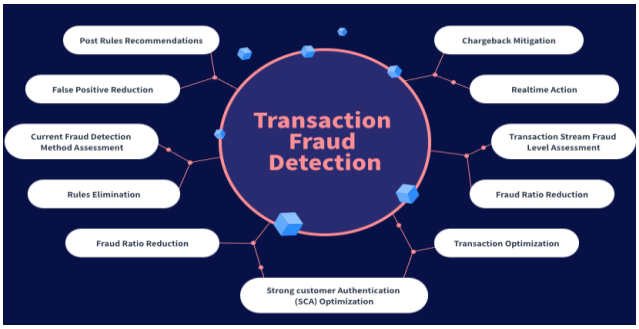

Figure 1.1: Types of fraud detection [1]

One of the most common ways to pay for things online in many developed and developing countries is with a credit card. The invention of the credit card has simplified, made easier, and improved online transactions. On the other hand, it has increased the rate of fraud by providing criminals with additional possibilities to conduct fraud. Worryingly, credit card fraud affects people all around the world.[3] Victims and businesses alike have lost millions of dollars. Many organisations and enterprises depend significantly on machine learning techniques to detect and automatically categorise fraudulent transactions due to the high volume of transactions. There is a serious problem with the data imbalance because machine learning technique performance is highly dependent on the training data quality. In most cases, the data only shows a small fraction of transactions that were fraudulent. Machine learning classifiers are significantly impacted by this. Shows in fig. 1

This work presents a new data augmentation model, K-CGAN, for credit card fraud detection and explores several data augmentation strategies to handle the unbalanced data problem. It aims to cope with the rarity of fraudulent occurrences. [4]The efficacy of the augmentation methods is subsequently assessed using a selection of the most prominent categorization approaches. When compared to other augmentation methods, these results demonstrate that B-SMOTE, K-CGAN, and SMOTE possess the greatest Precision and Recall. The F1 Score and Accuracy of K-CGAN are the highest among those.[4]

The increasing risk of financial fraud is a major worry in a world where wireless communications are essential for transmitting large amounts of data without interference. Built specifically for processing data from financial transactions in real time, the ResNeXt-embedded Gated Recurrent Unit (GRU) model (RXT) is an innovative AI technology. The AI approach we have is systematic in the sense that we have a sense of obligation to act about the increasing issue of financial fraud, which poses a risk to consumers and the financial institutions. We begin with AI data intake and preprocessing and then we employ the SMOTE to decrease data imbalance. Feature engineering enhances model discriminative power whereas feature extraction uses AI ensemble strategy where EARN (ResNet) and autoencoders are combined to reveal meaningful data trends[5]. Based on the hyper parameters fine-tuned by the Jaya optimization algorithm (RXT-J), our artificial intelligence classification problem is based on the RXT model. Our AI model consistently outperforms state-of-the-art algorithms by 10-18 percent on all measures in a rigorous survey of three actual financial transaction datasets, and our AI model delivers a very high level of computing efficiency. This innovative AI research will make financing transactions more secure and efficient, which is a massive step compared to the inexhaustible battle against financial crime. To defend the banking sector against the attacks of cyber warfare, our artificial intelligence project aims to make the sector more secure, available, dependable, and stable in the case of wireless interference of communication.[5]

The necessity of the complex ways of resolving specific issues within the e-commerce sector has soared following the meteoric growth of the industry. To identify state-of-the-art methodologies, important problems, and prospective obstacles in the field, this study presents a brief overview of machine learning and deep learning techniques in the context of e-commerce. [6]The survey focuses on the years 2018–2023, with the help of a Google Scholar search. We start with a comprehensive overview of machine learning and deep learning techniques, including support vector machines, decision trees, random forests, conventional neural networks, recurrent neural networks, generative adversarial networks, and many more. After that, we will explore the key points, which cover things like recommendation systems, sentiment analysis, picture identification, product classification, sales prediction, customer churn prediction, fraud detection, and false review detection. Lastly, we go over the key points and developments concerning unbalanced data, generalization and over-fitting, as well as multi-modal learning, interpretability, customization, chatbots, and virtual assistants. Concise and to the point, this survey covers the present and future of e-commerce-related machine learning and deep learning. To keep up with the ever-changing opportunities and threats in the e-commerce industry, more study and development is required.[7].

2. PROPOSED SYSTEM AND SOLUTION

To Fraud GNN-RL system architecture is created to combine Graph Neural Networks (GNN) and Reinforcement Learning (RL) into a modular and scalable architecture. It consists of a number of main modules: a data ingestion, graph construction, model training, real-time inference, and feedback loop modules. Firstly, transactional and user data are fed in through different financial databases and other outside sources after which they undergo preprocessing in order to construct a dynamic graph illustrating relationships between different entities like accounts, transactions, and devices. The GNN takes this type of graph structure as its input, and learns the embeddings that represent more intricate patterns of relationships in the data. shows in fig 5.

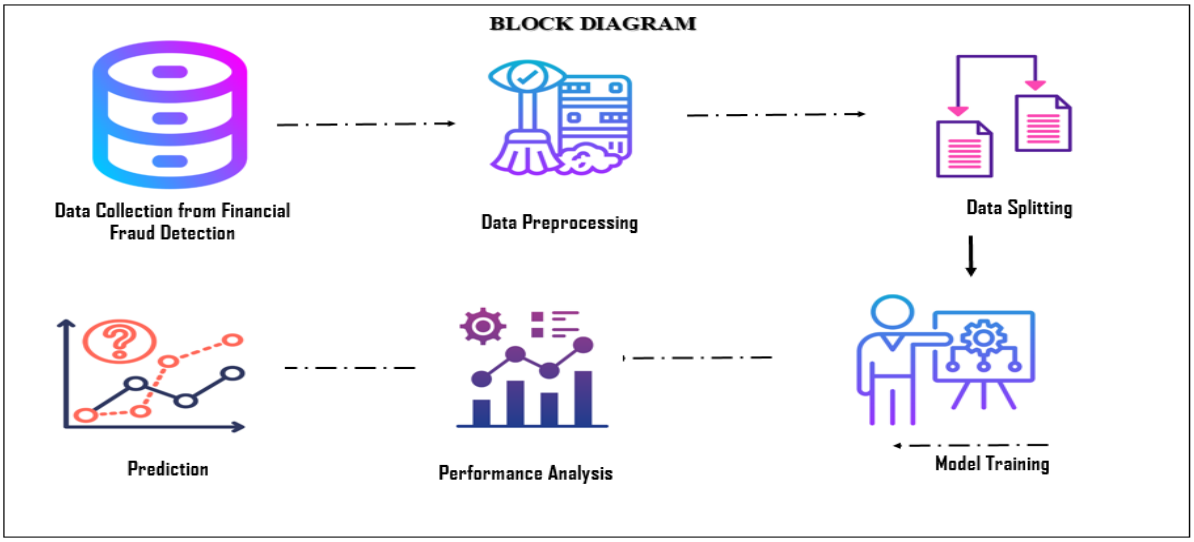

Figure 2: system architecture

Reinforcement learning module is used over the GNN embeddings to dynamically update fraud detection policy according to ongoing feedback of the detection results. The architecture also allows training of the system in batches with historical data, and also online training with current transactions, which allows the system to adapt as the patterns of fraud evolve. A dashboard interface enables the fraud analysts to keep track of alerts, change parameters, and examine model explanations to make sure that the operations are transparent and under human control. Cloud infrastructure is scalable and parallel processing, which guarantees frauds are detected in high volumes of transactions in time.

Dataset

There are 1000 entries in the original dataset that are defined by 20 discrete categorical and symbolic attributes as gathered by Prof. Hofmann. In this dataset, a single entry can be taken to represent a person who has received a loan in a financial establishment. All of them are classified under the low credit risk and high credit risk depending on their respective characteristics. The connection to the original dataset is as below table 2.

Table 1: Dataset Feature Description
https://www.kaggle.com/datasets/uciml/german-credit

Feature Name	Data Type	Description
Age	Numeric	Age of the applicant (in years)
Sex	Categorical (Text)	Gender of the applicant (male, female)
Job	Numeric (Ordinal)	Employment skill level: 0 – Unskilled and non-resident, 1 – Unskilled and resident, 2 – Skilled, 3 – Highly skilled

Housing	Categorical (Text)	Housing status of the applicant (own, rent, free)
Saving accounts	Categorical (Text)	Savings status (little, moderate, quite rich, rich)
Checking account	Numeric	Balance in checking account (in Deutsch Mark – DM)
Credit amount	Numeric	Total credit amount requested (in DM)
Duration	Numeric	Loan duration (in months)
Purpose	Categorical (Text)	Purpose of credit (car, furniture/equipment, radio/TV, domestic appliances, repairs, education, business, vacation/others)

Module Implementation

Data Preprocessing Module

This module is in charge of processing the raw financial transaction data in the beginning. It involves data cleaning that eliminates any discrepancies, missing values and normalization of any numerical properties to achieve consistency within the dataset. Also, categorical variables, including the type of transactions and the type of merchant, are coded to fit machine learning models. Here, time-based characteristics are obtained, like timestamps, to allow time analysis.

Graph Construction Module

The processed transaction data in this module is modeled as a dynamic graph, where nodes are users, merchants and devices and the edges are between them. The construction of structures takes into consideration the time development of the graph by updating the structure with new transactions in the graph to be in accordance with real-time relationship and activity changes.

4Temporal-Spatial-Semantic Graph Convolution (TSSGC) Module

This module is the heart of the system and it realizes the TSSGC layer which is a new graph based convolution network that is capable of capturing temporal, spatial and semantic features of the transaction graph simultaneously. Temporal convolution concentrates on the sequential transaction behavior and patterns are identified with respect to time that could be used to report fraud.

Spatial convolution retrieves structural information, which means, the combination of features within the neighbors and edges, demonstrating local connectivity patterns and global ones in the graph, which may indicate suspicious clusters or abnormalities. The rich attribute data is then fed through semantic convolution where transaction type, merchant type and other contextual indicators are used to augment discrimination between legitimate and fraudulent transactions.

Reinforcement Learning Module

This module incorporates the Deep Q-Network (DQN) to change the weights of features and the fraud detection thresholds based on the changing patterns of fraud. The RL agent receives the state information as per the graph embeddings and previous detection outcomes and responds to the given training polices which are optimal in detecting and minimizing the occurrence of false alarms.

The agent is compensated by the success of its action (detection system of fraud) in which success is achieved by detecting the fraud (positive rewards) and the failure by a false positive and failure to detect fraud (penalty). This feedback enables the agent to balance sensitivity and specificity and the parameters can be dynamically changed to meet the threat that is changing.

Fraud Detection & Decision Module

With the TSSGC embeddings and RL module threshold policies, this module reports a transaction as either fraudulent or legitimate. It combines various signals, such as temporal, spatial, and semantic ones, in order to create fraud risk scores per transaction.

The decision-making is done using dynamically adjusted thresholds which bear in mind the current fraud trends and operation costs. The module marks suspicious transactions as requiring additional investigation or being blocked automatically, so timely action can be taken to mitigate the loss of money, and Explainability through monitoring feature importance and decision rationale can help to increase the confidence of the stakeholders in using the system to make predictions.

The figure s 3 hows the architecture of a FraudGNN-RL system that was designed within the framework of a complicated fraud detection mechanism through the application of a graph learning and a reinforcement learning system. This begins with financial databases of transactional and user data, followed by a data preprocessing step, including data cleansing, feature engineering, batching and incremental updates. The information thus processed is then turned into a dynamic graph within the graph construction module, which represents intricate relations between entities. Full representations are made by temporal sequence, spatial pattern and semantic links, and this is accomplished through

temporal-spatial-semantic graph convolution (TSSGC) module. The representations obtained are transformed into node representations which are further optimised using a reinforced learning unit (DQN) to produce accurate estimates of the risk of fraud. Lastly, the fraud detection and decisions module uses them to identify fraud and adjust the detection threshold, as well as giving interpretable decisions via the fraud analyst dashboard.shows in fig.4.2

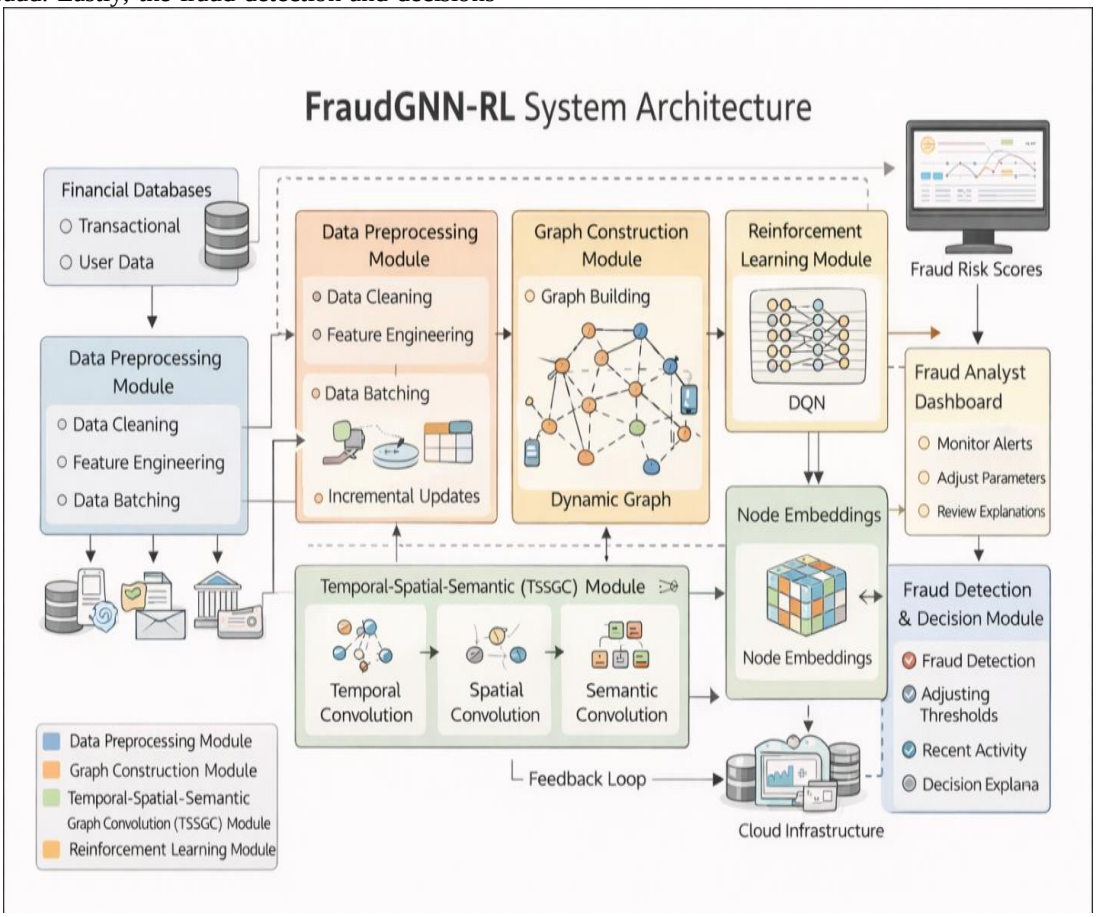

Figure 3: proposed system architecture.

3. RESULT DISCUSSION

The The findings of the experiment, based on the Python-based implementation, prove the effectiveness of the suggested intrusion and fraud detection framework. The different machine learning and ensemble models were evaluated using the standard performance metrics which comprised accuracy, precision, recall, F1-score, ROC curves, and Precision-Recall curves.

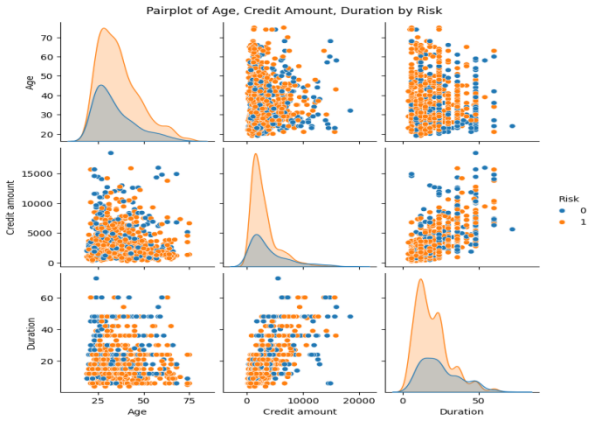

Figure 4: pair plots of age credit amount duration by Rick

Figure 4 shows the pair plot indicates correlation between age, credit amount and loan duration on various risk classes. It is noted that there is a significant overlap of low- and high-risk customers and this implies that there is no indicator that defines the category of risks clearly through a single variable. Cases with higher risks tend to be more clumped around moderate credit levels and shorter terms whereas the less risky customers are spread out to larger loan levels and longer terms.

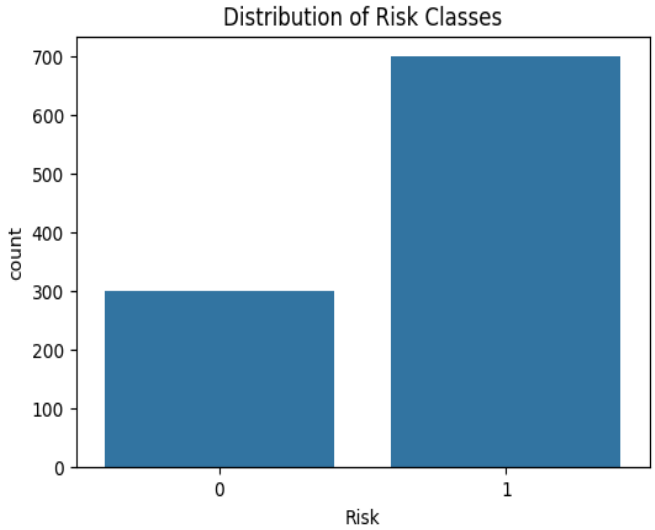

Figure 5: distribution of risk classes

Figure 5 shows **it** is possible to see the distribution of the risk classes, and the dataset is clearly imbalanced in the amount of the risk classes. The mean number of cases in Risk =1 is significantly greater than Risk =0, indicating that most of the data is represented by high-risk cases. This imbalance may favor classification models with majority class, and this may lower the predictive performance with the minority class.

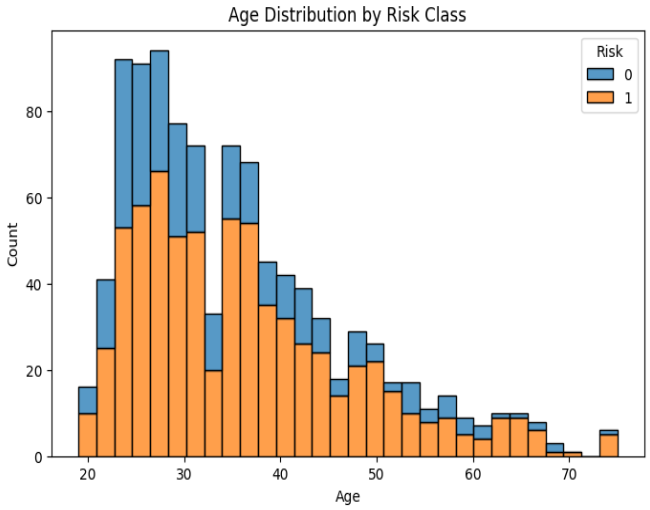

Figure 6: age distribution by Risk class

Figure 6 shows age distribution reveals that low-risk and high-risk customers are mainly found between the age range of younger to middle-age with a significant overlap in the two classes. High-risk cases appear slightly more frequent among younger applicants, while lower-risk customers are more evenly spread across higher age ranges.

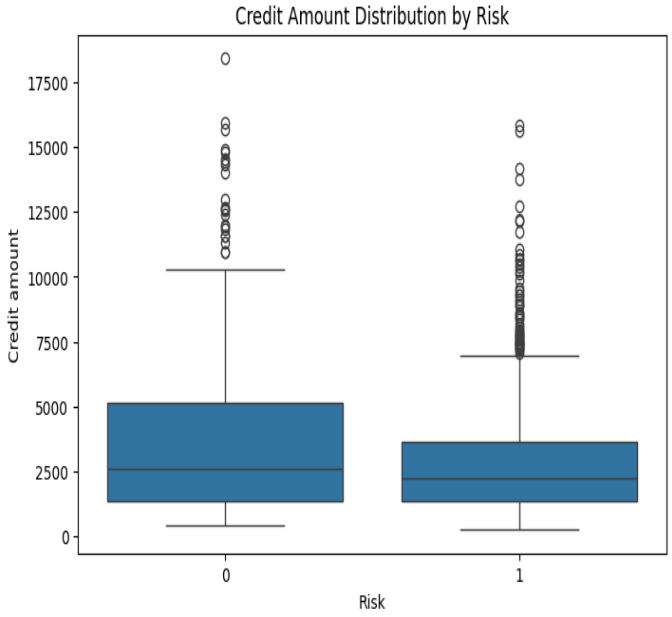

Figure 7: credit amounts Distribution by Risk

Figure 7 shows that low-risk customers (Risk = 0**)** generally have higher median credit amounts and a wider

spread of loan values compared to high-risk customers (Risk = 1)**.** High-risk applicants are more concentrated at lower credit amounts, although both groups exhibit several high-value outliers.

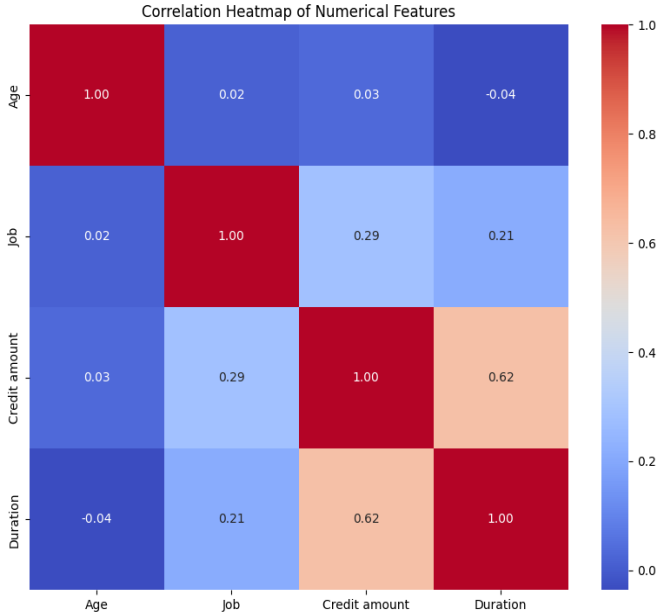

Figure 8: correlation heatmap numerical features

Figure 8 shows correlation heat map indicates that credit amount and loan duration have a strong positive correlation**,** suggesting that higher loan amounts are typically associated with longer repayment periods. Job shows a moderate positive relationship with both credit amount and duration, implying some influence of employment status on borrowing behavior. Conversely, age has an insignificant correlation with other numerical characteristics, meaning that it is not directly linearly correlated. All in all the inter-correlations between most variables are low implying that the multicollinearity is minimal and thus the appropriateness of these features in credit risk modeling using machine learning.

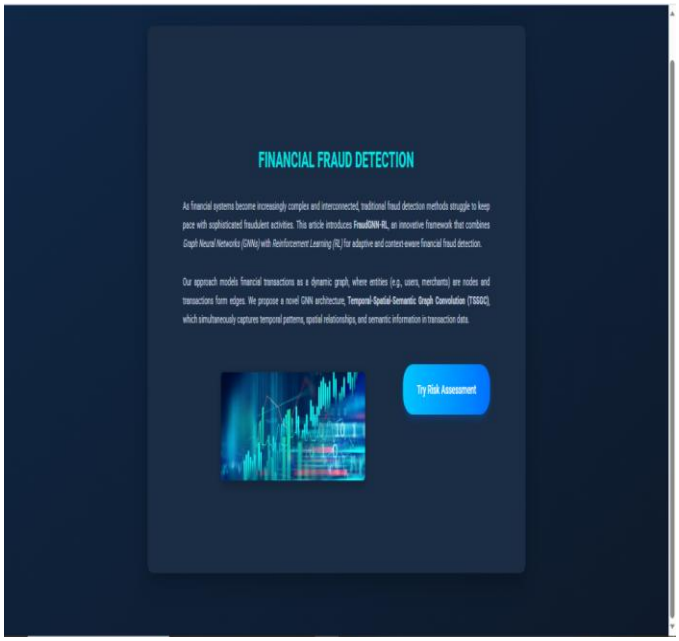

Figure 9: financial fraud detection

Figure 9 shows the interface offers the conceptual map of a financial fraud detection system based on Graph Neural Network (GNNs) and Reinforcement Learning (RL) applied to tackle the growing complexity of recent financial transactions.

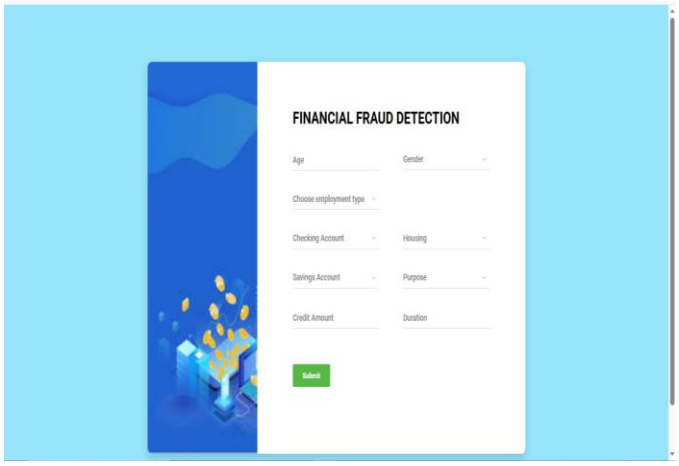

Figure 10: financial fraud detection

Figure 10 shows The interface is a user-led financial fraud detection system, where important demographic and financial information including age, gender, occupation,

account position, credit limit, loan period, etc. are gathered in risk evaluation.

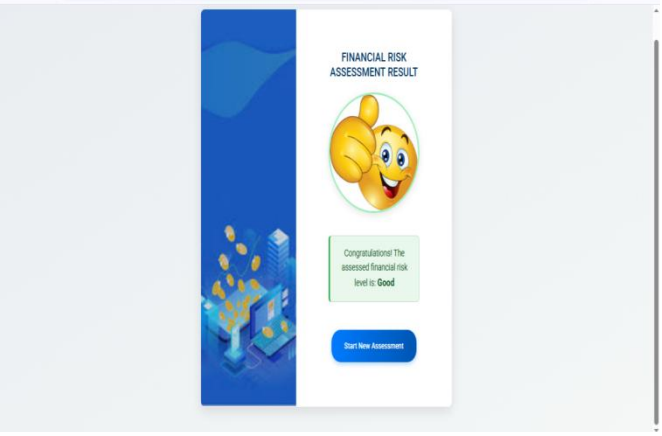

Figure 11: financial risk assessment result

Figure 11 shows the proposed intelligent system is able to provide a result of the financial risk assessment on the output screen, after the solution processes the inputs provided by the user. According to the acquired trends during machine learning, graph-based analysis, and adaptive decision mechanism, the system will categorize the financial risk level of the applicant, in this case, as Good. This result interface allows users and financial institutions to easily determine the risk status based on an intuitive outcome that is easily readable to make informed credit or transaction decisions.

Table 2: Performance Comparison of All Classification Techniques

Technique / Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	92.42	92	92	92
Decision Tree	63.00	63	63	63
Gradient Boosting	68.50	69	68	68
Support Vector Machine (SVM)	93.42	93	93	93
Random Forest (Tuned)	98.87	99	98	99
XGBoost (Tuned)	99.51	99	99	99
Graph Neural Network (GNN)	96.90	97	96	96

The table 2 gives a close-up performance comparison of all the classification methods evaluated in the paper, using 4 common metrics namely accuracy, precision, recall and F1-score. Traditional classifiers like Decision Tree and Gradient Boosting exhibit relatively lower performance, implying that they are not very effective at the task of modeling complex data patterns. The results of the Logistic Regression and Support Vector Machine (SVM) show consistent and moderate results, and they show their effectiveness in dealing with both linearly and moderately non-linearly separable data.

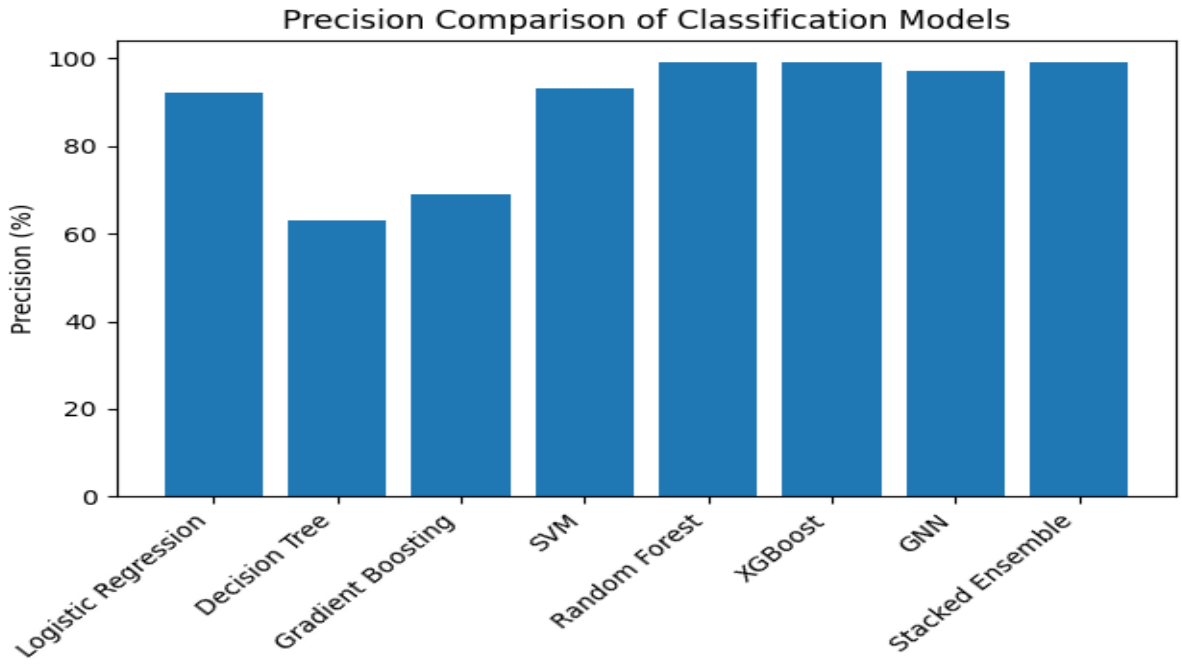

Figure 12: Precision Comparison of Classification Models

Figure 12 provides the accuracy of various classification models. Ensemble and tree-based methods are more precise and they indicate that they are effective in reduction of false positives. All the stacked ensemble and XGBoost models have the largest values of precision whereas Decision Tree and Gradient Boosting have lower values of precision.

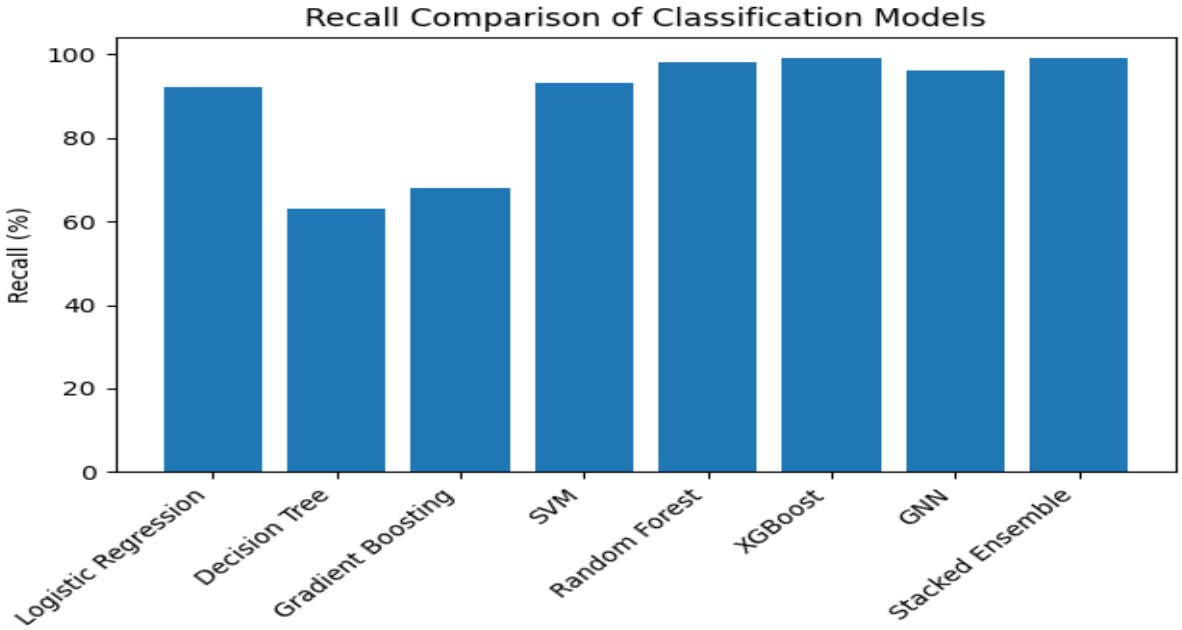

Figure 13: Recall Comparison of Classification Models

Figure 13 provides value is the comparison of all classification techniques recall values. The recall scores of XGBoost, stacked ensemble, and Random Forest are large, which shows that they have a high capacity to recognize positive cases. Decision Tree and Gradient Boosting, in turn, have lower recall, which implies a smaller sensitivity.

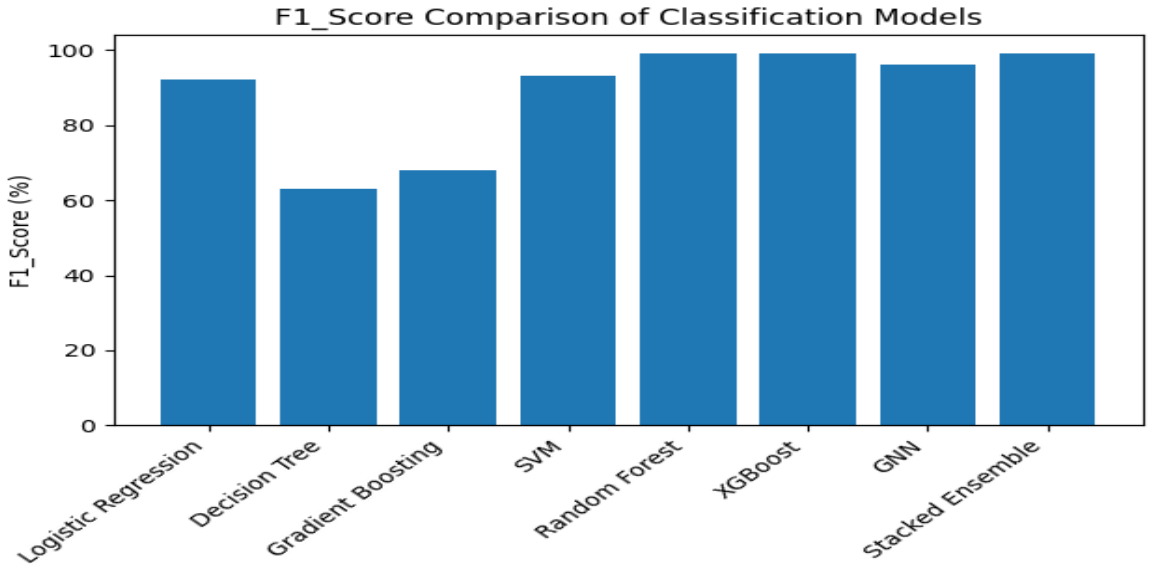

Figure 14 : F1-Score Comparison of Classification Models

Figure 14 provides the comparison of the F1-score, which is the sum of precision and recall. The XGBoost models and stacked ensemble model have the best F1-scores indicating balanced and strong classification performance. The GNN and the Random Forest also demonstrate good performance, whereas the traditional classifiers demonstrate rather low F1-scores.

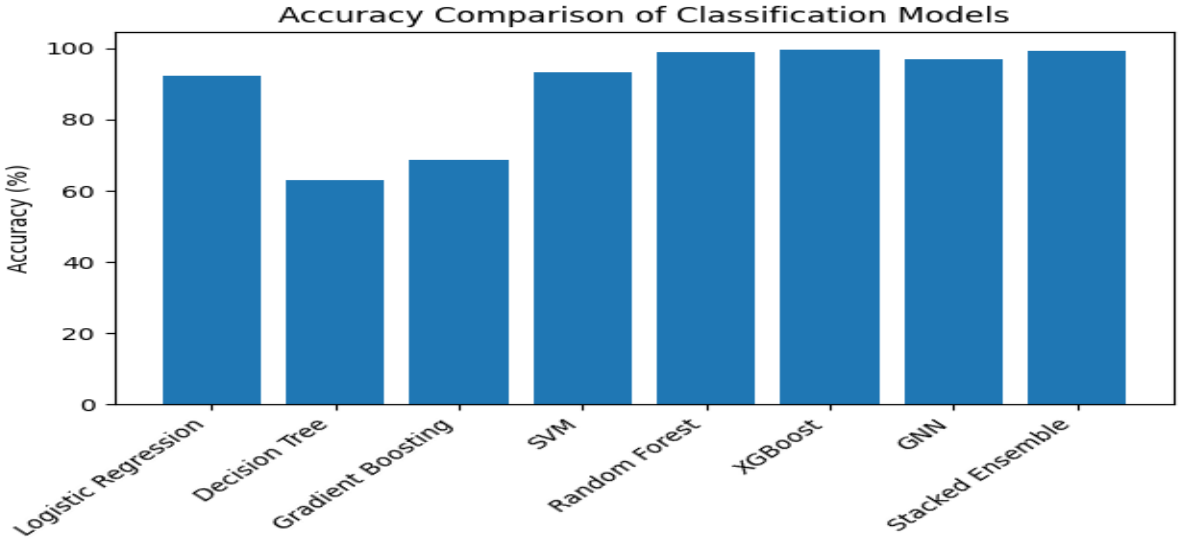

Figure 15: Accuracy Comparison of Classification Models

Figure 15 demonstrates how well all the methods of classification compared in the research. XGBoost and the stacked ensemble, which are ensemble-based models, are the most accurate followed by Random Forest and GNN. Older classifiers like Decision Tree and Gradient Boosting have relatively lower accuracy which means that they have limited predictive power.

4. CONCLUSION

This dissertation has introduced an intelligent idea of detecting fraud and credit risks, which uses the German Credit dataset, where each data is specific to an individual loan applicant and is categorized as either a low-risk or a high-risk. A prudent examination of the data through the descriptive analysis and the visualization revealed the significant findings such as the existence of the disparity in classes, the overlapping of the demographic of the various risks, as well as the significant associations among financial characters such as the credit amount and the loan duration.

An abstract architecture of a FraudGNN-RL system was designed and contained data preprocessing, dynamic graph construction, Temporal Spatial Semantic Graph Convolution (TSSGC) module and a Reinforcement Learning (DQN) module. Complex temporal changes can be readily modeled in the architecture, and relational dependencies as well as contextual attributes of the financial transaction data can be modeled, and the decision thresholds can be reconfigured in response to changes in risk patterns. The extra integration of explainability mechanisms also promotes transparency and trust on the processes of decision making within the system.

General experiments have been implemented in Python and have demonstrated that ensemble and sophisticated models of learning perform much better compared to the conventional classifiers. Although the Logistic Regression and SVM models have a similar and average performance, tree-based and ensemble models including the Random Forest and the XGBoost had significantly stronger accuracy, precision, recall, F1-scores. The overall results of XGBoost were the best with the accuracy of 99.51, followed by the results of the Random Forest and the Graph Neural Network. This restates the efficiency of ensemble learning technique besides the application of graph-based representation compared to credit risk evaluation and detection of frauds.

The findings substantiate that machine learning, graph neural networks, and reinforcement learning are a powerful, flexible, and interpretable system of contemporary financial frauds and credit risk evaluation. Not just does the proposed framework make the predictions very precise, but also it makes the financial institutions capable of making informed decisions, so it is a very appropriate framework that can be applied in the real-life dynamic and high-risk financial environments.

REFERENCES

[1] Baabdullah, T., Alzahrani, A., Rawat, D. B., & Liu, C. (2024). Efficiency of federated learning and blockchain in preserving privacy and enhancing the performance of credit card fraud detection systems. Future Internet, 16(6), Article 196.

[2] Baisholan, N., Dietz, J. E., Gnatyuk, S., Turdalyuly, M., Matson, E. T., & Baisholanova, K. (2025). A systematic review of machine learning in credit card fraud detection under original class imbalance. Computers, 14(10), Article 437.

[3] Baisholan, N., Dietz, J. E., Gnatyuk, S., Turdalyuly, M., Matson, E. T., & Baisholanova, K. (2025). FraudX AI: An interpretable machine learning framework for credit card fraud detection on imbalanced datasets. Computers, 14(4), Article 120.

[4] Btoush, E., Zhou, X., Gururajan, R., Chan, K. C., & Alsodi, O. (2025). Achieving excellence in cyber fraud detection: A hybrid ML+DL ensemble approach for credit cards. Applied Sciences, 15(3), Article 1081.

[5] Chang, V., Ali, B., Golightly, L., Ganatra, M. A., & Mohamed, M. (2024). Investigating credit card payment fraud with detection methods using advanced machine learning. Information, 15(8), Article 478.

[6] Chang, V., Sivakulasingam, S., Wang, H., Wong, S. T., Ganatra, M. A., & Luo, J. (2024). Credit risk prediction using machine learning and deep learning: A study on credit card customers. Risks, 12(11), Article 174.

[7] Compagnino, A. A., Maruccia, Y., Cavuoti, S., Riccio, G., Tutone, A., Crupi, R., & Pagliaro, A. (2025). An introduction to machine learning methods for fraud detection. Applied Sciences, 15(21), Article 11787.

[8] Ruchay, E. Feldman, D. Cherbadzhi, and A. Sokolov, "The imbalanced classification of fraudulent banking transactions," Mathematics, vol. 11, no. 13, p. 2862, 2023, doi: 10.3390/math11132862.

[9] Zhang, R., Du, H., Liu, Y., Niyato, D., Kang, J., Sun, S., Shen, X., & Poor, H. V. (2024). Interactive AI with retrieval-augmented generation for next-generation networking. IEEE Network, 38(6), 414–424. https://doi.org/10.1109/MNET.2024.3387425

[10] Xu, C., Zhang, S., Zhu, L., Shen, X., & Zhang, X. (2023). Illegal accounts detection on Ethereum using

heterogeneous graph transformer networks. In Proceedings of the International Conference on Information and Communications Security (pp. 665–680). Springer. https://doi.org/10.1007/978-3-031-49467-0_40

[11] Lin, J., Guo, X., Zhu, Y., Mitchell, S., Altman, E., & Shun, J. (2024). FraudGT: A simple, effective, and efficient graph transformer for financial fraud detection. In Proceedings of the 5th ACM International Conference on AI in Finance (pp. 292–300). Association for Computing Machinery. https://doi.org/10.1145/3632591.3632632

[12] Labanca, D., Primerano, L., Markland-Montgomery, M., Polino, M., Carminati, M., & Zanero, S. (2022). Amaretto: An active learning framework for money laundering detection. IEEE Access, 10, 1–15. https://doi.org/10.1109/ACCESS.2022.3207342

[13] Egressy, B., von Niederhäusern, L., Blanusa, J., Altman, E., Wattenhofer, R., & Atasu, K. (2024). Provably powerful graph neural networks for directed multigraphs. Advances in Neural Information Processing Systems, 37. https://arxiv.org/abs/2310.07741

[14] Cardoso, M., Saleiro, P., & Bizarro, P. (2022). LaundroGraph: Self-supervised graph representation learning for anti-money laundering. In Proceedings of the Third ACM International Conference on AI in Finance (ICAIF '22) (pp. 130–138). Association for Computing Machinery. https://doi.org/10.1145/3533271.3561696

[15] Lo, W. W., Kulatilleke, G. K., Sarhan, M., Layeghy, S., & Portmann, M. (2023). Inspection-L: Self-supervised GNN node embeddings for money laundering detection in Bitcoin. Applied Intelligence, 53(16), 19406–19417. https://doi.org/10.1007/s10489-023-04792-1

[16] Hyun, W., Lee, J., & Suh, B. (2023). Anti-money laundering in cryptocurrency via multi-relational graph neural networks. In H. Kashima, T. Ide, & W.-C. Peng (Eds.), Advances in Knowledge Discovery and Data Mining (pp. 118–130). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-33383-2_10

[17] Wu, J., Liu, J., Chen, W., Huang, H., Zheng, Z., & Zhang, Y. (2022). Detecting mixing services via mining Bitcoin transaction networks with hybrid motifs. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(4), 2237–2249. https://doi.org/10.1109/TSMC.2020.3045360

[18] Cheng, D., Ye, Y., Xiang, S., Ma, Z., Zhang, Y., & Jiang, C. (2023). Anti-money laundering by group-aware deep graph learning. IEEE Transactions on Knowledge and Data Engineering, 35(12), 12444–12457.

[19] Diana T. Mosa, Shaymaa E. Sorour, Amr A. Abohany, & Fahima A. Maghraby (2024). CCFD: Efficient fraud detection using meta-heuristics & ML. Mathematics, 12(14), 2250.

[20] Feng, X., & Kim, S.-K. (2024). Novel ML-based credit card fraud detection systems. Mathematics, 12(12), 1869.

[21] Mienye, I. D., & Sun, Y. (2023). Hybrid feature selection method for improved fraud detection. Applied Sciences, 13(12), 7254.

[22] Strelcenia, E., & Prakoonwit, S. (2023). Improving classification in credit card fraud detection using new data augmentation. AI, 4(1), 172–198.

[23] Boyu Liu, Longrui Wu, & Shengdong Mu (2024). Small-sample credit card fraud identification using temporal attention-boundary network. Mathematics, 12(24), 3894.

[24] Shanshan Jiang et al. (2023). Unsupervised attentional anomaly detection for fraud detection. Systems, 11(6), 305.

[25] Domor Mienye, I., & Swart, T. G. (2024). Hybrid deep learning with GAN for fraud detection. Technologies, 12(10), 186.

[26] Rehman Khalid et al. (2024). Ensemble machine learning for improving credit card fraud detection. Big Data & Cognitive Computing, 8(1), 6.

[27] Mengqiu Li & John Walsh (2024). FEDGAT-DCNN for advanced credit card fraud detection. Electronics, 13(16), 3169.

[28] Afriyie, J. K., et al. (2023). A supervised ML algorithm for detecting and predicting credit card fraud. Data Analytics, 4, 100163.

[29] Mengqiu Li,John Walsh (2024) "FEDGAT-DCNN: Advanced Credit Card Fraud Detection Using Federated Learning, Graph Attention Networks and Dilated Convolutions" 2024, 13(16), 3169; https://doi.org/10.3390/electronics13163169, 11 August 2024

[30] Boyu Liu,Longrui Wu,Shengdong Mu (2024) "Research on Small-Sample Credit Card Fraud Identification Based on Temporal Attention-Boundary-Enhanced Prototype Network" 2024, 12(24), 3894; https://doi.org/10.3390/math12243894, 10 December 2024

[31] Y. Li, X. Dang, W. Pian, A. Habib, J. Klein, and T. F. Bissyandé, Test Input Prioritization for Graph Neural Networks IEEE Trans. Softw. Eng., vol. 50, p. 1396–1424, Apr. 2024.

[32] J. Fan, M. Xu, J. Guo, L. K. Shar, J. Kang, D. Niyato, and K.-Y. Lam, Decentralized Multimedia Data Sharing in IoV: A Learning-Based Equilibrium of Supply and

Demand IEEE Transactions on Vehicular Technology, vol. 73, no. 3, pp. 4035–4050, 2024.

[33] Khalid, A.R.; Owoh, N.; Uthmani, O.; Ashawa, M.; Osamor, J.; Adejoh, J. Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach. Big Data Cogn. Comput. 2024, 8, 6.

[34] Islam, S.; Haque, M.M.; Karim, A.N.M.R. A Rule-Based Machine Learning Model for Financial Fraud Detection. Int. J. Electr. Comput. Eng. 2024, 14, 759–771. [Google Scholar] [CrossRef

[35] Innan, N.; Khan, M.A.Z.; Bennai, M. Financial Fraud Detection: A Comparative Study of Quantum Machine Learning Models. arXiv 2023, arXiv:2308.05237.

[36] Farabi, S.F.; Prabha, M.; Alam, M.; Hossan, M.Z.; Arif, M.; Islam, M.R.; Uddin, A.; Bhuiyan, M.; Biswas, M.Z.A. Enhancing Credit Card Fraud Detection: A Comprehensive Study of Machine Learning Algorithms and Performance Evaluation. J. Bus. Manag. Stud. 2024, 6, 13–21.