



Article

A Systematic Review of Machine Learning and Graph-Based Approaches for Financial Fraud Detection

Showive Hasan Shuvo¹, Jarin Nuran Rahman², Al Amin³, Shoumya Hassan Shurovi⁴

1. San Francisco Bay University, USA BSc (Hons) Computer Science
2. San Francisco Bay University, USA BSc (Hons) Computer Science
3. Ravensbourne University London, United Kingdom BSc (Hons) Computer Science
4. University of Liberal Arts Bangladesh (ULAB), Bangladesh BSc (Hons) Computer Science

*Correspondence: shuvoshuvo123@gmail.com, jarinnuranrahman@gmail.com,
alaminanto729@gmail.com, sumaiyashurovi1@gmail.com

Abstract: The growing complexities of digital transactions and the rise in digital fraud pose a significant threat to financial transactions. In this research, a systematic review is presented on financial fraud detection using machine learning and graph-based methods. The survey discusses the related works of the AI techniques, feature engineering techniques, behavior analysis and graph based fraud detection techniques. Financial transaction data is analyzed using exploratory data analysis to detect fraud patterns in terms of geographical location, amount of financial transaction, risk score and the distribution of financial transactions. The results show that there are salient behavioral characteristics and risk related attributes that offer important clues in detecting suspicious activities. The study emphasizes the benefits of machine learning methods for better fraud detection in automated systems, as they can be used to learn from previous transactions, and of graph-based methods as they can be used to identify relationships between financial entities. The study offers an overview of the potential benefits of combining machine learning with graph-based techniques for financial fraud detection, as well as the potential drawbacks of traditional methods.

Keywords: Digital transaction, AI techniques, Financial Transaction, Machine Learning Methods, Graph-based Fraud Detection.

Citation: Shuvo S. H. A Systematic Review of Machine Learning and Graph-Based Approaches for Financial Fraud Detection. American Journal of Economics and Business Management 2026, 9(10), 867-879.

Received: 10th Jul 2026
Revised: 11th Aug 2026
Accepted: 11th Sep 2026
Published: 21th Oct 2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>)

1. Introduction

Background of the Study

The financial sector has seen a significant change with digital transactions and is becoming one of the most convenient banking methods for people to use with online banking, digital payment and electronic fund transfer growing in numbers [1]. As digital financial services have become more popular, cybercriminals have also started to exploit them to conduct fraud such as unauthorized transactions, identity theft and payments fraud. With the ongoing rise in financial transactions worldwide, traditional fraud detection techniques are no longer effective in detecting complex and evolving fraud patterns. Financial institutions are in need of sophisticated automated detection systems that are able to process vast amounts of data from transactions and provide the fast identification of suspicious activity. Machine learning and artificial intelligence techniques are effective solutions as they learn from historical patterns of transactions and identify abnormal behaviour. These innovations contribute to enhancing security, mitigating financial loss, and creating safer digital payment spaces for banks and financial

institutions. Thus, the design of intelligent fraud detection systems has emerged as a key research area to enhance financial security and tackle the new problems of financial fraud.

Problem Statement

The traditional financial fraud detection systems are primarily based on the rule-based methods, which detect fraud based on the set rules and patterns. However, it has drawbacks as they cannot effectively identify new and more sophisticated forms of fraud, which constantly evolve in response to the changing digital landscape [2]. Fixed rules can become less accurate and less adaptable as fraudsters create new methods to come up with a positive identification. Fixed rules can become ineffective as fraudsters devise new ways and means to achieve a positive ID. Financial fraud behavior is constantly evolving and poses difficulties in the detection of hidden relationships, abnormal transaction trends, and sophisticated financial fraud. With a higher number of transactions, financial institutions need sophisticated techniques to be able to analyse large volumes of data to deliver accurate real-time fraud detection. Hence, new machine learning and graph-based methods that could enhance fraud identification and address the drawbacks of traditional fraud detection methods need to be investigated.

Objectives of the Study

The accomplishment of this research work fulfills many essential objectives as mentioned below:

- To analyze the currently used machine learning approaches for predicting financial fraud.
- To inspect the graph-based fraud detection techniques to recognize the complicated transaction relationships.
- To identify the transactions pattern encountered with financial fraud using the exploratory techniques
- To investigate the performance of machine learning models used for determining the fraudulent activities
- To determine the challenges and contribution of research in future in the field of AI-based financial fraud detection systems.

Research Question

Question 1. How does the effectiveness of algorithms in a machine learning model play a crucial role in determining financial fraud?

Question 2. What is the contribution of graph-based approaches in improving the fraud detection mechanism in comparison to conventional methods?

Question 3. What barriers are responsible for preventing the application of AI techniques for detecting financial fraud?

Significance of the Study

The study is relevant because it brings to light the significance of advanced technologies in enhancing financial security and minimizing risks associated with fraud. With more and more transactions going digital, it is essential to have reliable systems which can detect suspicious activities in a timely and accurate manner. Financial institutions can gain enhanced capabilities by applying machine learning and graph-based approaches for analyzing patterns of transactions, identifying irregular activity, and mitigating financial losses. This study could contribute to the comprehension of the role AI tools can play in improving banks and other financial institutions' fraud detection mechanisms. The results of this study could be used to facilitate better decision-making, improve customer protection, and increase trust in digital financial services.

Financial Fraud Detection and Evolution of Detection Methods

With the ongoing expansion of digital financial services and fraudulent activity becoming more complex, financial fraud detection has evolved quite a bit. As mentioned by Soyombo et al. [3] AI has emerged as a crucial technology in financial fraud detection as it is able to analyse the vast amounts of transaction data that a financial institution receives and to detect suspicious transactions more efficiently. The author noted that traditional fraud detection systems using pre-defined rules have constraints as they are mainly relying on known fraud patterns and could miss new types of financial crimes. It highlighted that AI-based methods are more flexible, as they learn from past transactions and detect any irregularities in user activity. The research is primarily focused on the general aspect of using AI to stop fraud, however, and there is not much discussion of comparing the performance of various more advanced detection techniques.

Beemamol [4] has witnessed a shift from a traditional accounting-based investigation approach to financial fraud detection research towards highly analytical and computational approaches. The author examined the evolution of financial statement fraud detection and found that most of the early studies were based on statistical techniques and manual analysis of financial statements. Later developments added data mining and machine learning methods, which enhanced the ability to uncover hidden patterns in financial information. The study highlighted the change in fraud detection from reaction to prediction. Beemamol [4] offers a more historical perspective on fraud detection methodologies by outlining the evolution in the field, as contrasted to the approach outlined by Soyombo et al. [3]. The study, however, primarily addresses financial statement fraud, and transaction level fraud detection using the latest AI techniques is not given much attention.

However, with the emergence of advanced financial fraud detection algorithms in recent years, deep learning algorithms have become more and more the focus of the algorithms in financial fraud detection because they have the capacity to process high dimensional and complex financial data [5]. The authors performed systematic literature review to analyze the evolution of deep learning-based fraud detection techniques and pointed out the increased utilization of neural networks, deep learning models, and automated feature learning techniques. The study proposed that deep learning models can address some of the challenges of traditional machine learning techniques by being able to automatically uncover intricate relationships in transactional data. The authors also mentioned some data availability issues, model interpretability and computation requirements. Although Chen et al. [5] give great detail on advanced learning techniques, they need large quality datasets, which may present issues for smaller financial institutions.

The reviewed literature shows that the financial fraud detection has shifted from the rule-based approach to the intelligent approach using machine learning and deep learning techniques. Soyombo et al. [3] emphasized the relevance of AI to fraud prevention, and Beemamol [4] detailed the evolution of fraud detection studies. This was further developed by Chen et al. [5] who highlighted recent progress in deep learning. These strategies offer enhanced detection capabilities, but available studies suggest that challenges like behavior shifts in fraudsters, lack of explainability in fraud detection, and complicated financial connections persist. So, advanced machine learning techniques combined with relationship-based techniques like graph-based fraud detection can offer better solutions to detect intricate financial fraud patterns.

Machine Learning Approaches for Detecting the Financial Fraud

Ali et al. [6] state that one of the most relevant financial fraud detection techniques is the use of machine learning, due to its ability to process vast amounts of financial data and detect patterns relating to financial fraud. The authors systematically reviewed the existing literature to explore various machine learning approaches for fraud detection and

emphasized the significance of algorithms like decision trees, support vector machines, random forests, and neural networks. The study notes that machine learning models are more adaptable than traditional rule-based models, as they can learn from past transaction patterns and enhance their ability to detect transactions accurately. But the authors also found problems such as data imbalance, feature selection and the need for good-quality datasets. While the research offers an overview of machine learning-based fraud detection, it primarily examines the current strategies and systems for fraud detection rather than developing a specific detection system.

As stated by Njoku et al. [7] in financial institutions, machine learning methods can be used to build automated fraud detection models that can detect fraudulent transactions. The authors have designed a web-based fraud detection system with machine learning techniques in order to enhance the efficiency of fraud monitoring process. Their research was primarily focused on the real-world application of machine learning models and showcased the ability of automated systems to assist financial institutions in combating fraudulent activities. The study carried out by Ali et al. [6] is more systematic while the study by Njoku et al. [7] is more application oriented as it shows how machine learning is applied in a real system environment. But these systems can be effective only if they receive accurate financial information and are continuously refined to adapt to evolving fraud trends.

Deep Learning methods offer sophisticated tools for financial fraud detection in the context of Udayakumar et al. [8] by discovering intricate patterns and relationships in large and complex datasets. The authors suggested a deep learning-based method for cyber security and financial fraud detection and classification, Deep Fraud Net. The study emphasized that the deep learning model can automatically capture key features from transactions and enhance the ability to detect complex fraud schemes. The deep learning approach outperforms the traditional machine learning approach discussed in [6] and the practical application presented in [7] in the case of complex fraud scenarios. But deep learning models also need large amounts of data, more computing power and more methods for obtaining interpretability. The reviewed studies show that machine learning and deep learning techniques have been effective in enhancing fraud detection in financial services, but there are still several challenges to address, such as data quality, the transparency of ML models, and the evolving nature of fraudulent activity.

Feature Engineering and Behavior Evaluation in Fraud Detection

Alamri and Ykhlef [9] stated that feature engineering is a key aspect of the fraud detection algorithms as it is important to transform the raw transaction data into meaningful patterns that are related to the customer behavior. The authors suggested a hybrid feature engineering method with the consideration of customer spending behavior to detect credit card anomaly and fraud activity. They studied the spending habits, transaction behavior, and user attributes to look for any atypical transactions and spending behavior. It also showed that machine learning models can be significantly enhanced in distinguishing between normal and suspicious transactions by carefully designing the behavioral features. The approach, however, was primarily concerned with credit card transaction behavior and needs to be studied in greater detail in various financial fraud situations. The study identifies that user behavior is important, with fraudulent transactions sometimes resembling deviations from user's normal spending habits.

Kumar et al. [10] have indicated that feature engineering can enhance fraud detection systems by identifying relevant features from the complex data patterns. The authors examined fraudulent review detection by studying emotional expressions and the explicit features, and demonstrated that other behavioral and contextual features help improve the classification performance. The purpose of the study was not to review fraud but financial transaction fraud, but valuable insights are provided on the use of feature extraction techniques to detect hidden features of fraudulent behavior. In the same way, Esenogho et

al. [11] introduced a NN ensemble method along with feature engineering to enhance the credit card fraud detection. The authors noted that the use of proper selection of features and the use of multiple learning models to enhance the accuracy of classification of frauds is important to note. Esenogho et al. [11] concentrated more on improving the performance of the model by using advanced learning techniques, as compared to Alamri and Ykhlef [9]. But feature engineering can be very complicated and can necessitate the selection of the most relevant features. Overall, these studies confirm that feature engineering and behavior evaluation are crucial in fraud detection due to their ability to help machine learning models grasp the patterns of transactions, detect any anomalies, and enhance the precision of financial fraud prediction systems.

Graph-Based Approaches for Financial Fraud Detection

Financial fraud detection is an effective use of graph-based approaches because financial activities tend to have complex relationships between financial users, transactions, accounts, and other entities [12]. According to the authors, the models that are based on graphs can be used to represent financial data as a network of nodes and edges, with nodes representing financial entities, and edges representing the relationships between them. This helps in uncovering hidden links and strange patterns that may not be obvious with conventional machine learning techniques. The study revealed that analyzing graphs can help in fraud predictions based on relationships and not just on transaction features. The methodology, however, primarily gives a conceptual idea about how fraud detection can be achieved using a graph and needs to be validated with real large scale financial data.

Based on Li et al. [13] graph learning algorithms can be used to enhance the detection of financial fraud in the internet by analyzing complex transaction relationships and behavioral connections. To detect fraudulent activities the authors suggested a graph learning based approach, which captures interactions among various financial entities. Their research proved that graph-based models can be applied to identify fraud patterns involving multiple interconnected users or transactions. Graph learning offers extra information as it incorporates the structure of the relationships in financial networks, complementing the traditional machine learning methods used in earlier research. The performance of graph learning models, however, requires detailed relationship data and good quality graph construction, which may not be readily available in reality.

GNNs with anomaly detection algorithms can be used to assist financial fraud detection in real-time by analyzing transaction networks and detecting abnormal patterns, as identified by Zakaria et al. [14] and Rasul et al. [15]. The authors concentrated on Graph Neural Networks (GNNs) in the context of fraud detection in dynamic transaction systems. Their research showed that graph neural networks can automatically learn more complex relations and enhance the detection of suspicious behavior, compared to the conventional way. Zakaria et al. [14] and Rasul et al. [15] have focused on more practical research on real time fraud detection scenarios. These methods, however, might possess computational complexity, real time processing demands and model interpretability issues. The studies reviewed in this paper suggest that graph-based approaches offer substantial benefits for financial fraud detection, as they can detect fraud patterns that are based on relationships and can be integrated into more sophisticated AI based security systems. The combination of graph-based methods with machine learning techniques can yield more precise and flexible answers to financial fraud detection which is a complex issue.

Literature Gap

The use of machine learning, deep learning, feature engineering and graph-based techniques for detecting financial fraud has been studied in the past, but few studies have considered combining these techniques for a more complete financial fraud analysis. The

ability to explain models, detect fraud in real time, and the inherent challenges of dynamic fraud behavior and complex transaction relationships are still under investigation.

2. Methodology

Research Design

The research approach of this research is quantitative research, which is used to analyze the patterns of financial fraud in a scientific manner by applying data-driven techniques. The methodology is based on exploratory data analysis and machine learning based investigation to get the insights of transaction behaviors related to fraudulent activities. The study employs statistical analysis and computational techniques to uncover meaningful patterns, relationships, and anomalies in financial transaction data. This research aims to assess the applicability of machine learning methods in fraud detection with the analysis of parameters related to transactions, user behavior, and the risk level. The approach offers a structured procedure to conduct an investigation on fraud detection issues and assess the effectiveness of AI-based solutions.

Description of Dataset

For the purpose of this research, the Fraud Detection Transactions Dataset is used, which consists of financial transactions with various attributes related to customer activity, transaction details, security factors, and fraud patterns [16]. The data set contains information at the transaction level such as transaction amount, user identification details, device type, geographical location, risk score, authentication method, previous fraudulent transaction and fraud classification labels. Fraud Label is the main variable, indicating the legitimacy of the transaction or fraud. They offer an appropriate baseline to base financial fraud pattern analysis and machine learning classification and prediction models. The dataset is designed for exploratory analysis and fraud detection modelling, including the features that are needed to detect suspicious activities [16].

Data Preprocessing

Data preprocessing is carried out to enhance quality and reliability of the data set for further analysis and modelling. Data is checked for accuracy by first looking for missing data, duplicate entries and inconsistent data. Encoding techniques are applied to categorical variables like device type, location, transaction type, and authentication method to convert them into numerical values that can be used by machine learning algorithms. If necessary numerical features are scaled for consistency across the variables and to enhance the performance of the model. Irregularities are removed, and the data set is cleaned up for effective exploratory analysis and predictive modelling.

Exploratory Data Analysis with the Help of R Studio

The analysis of these data, known as Exploratory Data Analysis (EDA), is carried out in R Studio to discover important trends, relationships and behavioral patterns for financial transactions. The distribution of fraud, changes in transaction amounts, fraud risk score behavior and correlations between transaction attributes are analyzed using various statistical and visualization methods. The analysis is conducted by examining the frequency of fraud transactions, comparing fraud and legitimate transactions, examining fraud location patterns, and examining fraud device behavior. The patterns are hidden and revealed using visualizations like bar charts, histograms and correlation analysis to gain insight into factors that affect the occurrence of financial fraud. The results of the EDA yield valuable information about relevant characteristics that help fraud detection.

Machine Learning Framework

A framework for machine learning is designed for the purpose of assessing the effectiveness of models used for predicting fraud in financial transactions. Logistic Regression, Random Forest, and XGBoost are chosen as supervised learning algorithms because they are suitable for classification tasks and for detecting complex fraud patterns. Models are trained on processed transaction data and tested based on the accuracy,

precision, recall and F1 scores. Accuracy is the degree of accuracy of all predictions, and precision and recall measure the ability of the model to accurately say whether a transaction is fraudulent or not. F1-Score is a good measure for evaluating fraud detection because it takes into account the balance between precision and recall. This framework helps determine the capability of machine learning approaches in improving automated financial fraud detection systems.

Conceptual Framework

The conceptual framework of this research shows the relationship between the problems of financial fraud detection, machine learning approaches, graph-based methods, and analysis of results. The framework starts with financial transaction data, which includes behavioral and contextual information like the risk score, location and user activity patterns. These features are then subjected to data preprocessing and exploratory analysis to discover important indicators of fraud. The next step is to leverage machine learning algorithms and graph-based methods to uncover hidden relationships and suspicious activities in the financial networks. Effectiveness of these approaches is assessed in the framework by fraud classification and performance assessment. The goal of this framework is to create a new and better concept of an intelligent mechanism for detecting fraud, which will help financial institutions to mitigate fraud risks. The proposed conceptual framework emphasizes the need to combine AI methodologies and behavioral analytics to develop accurate, adaptive, and reliable fraud detection systems in today's digital financial landscape and services.

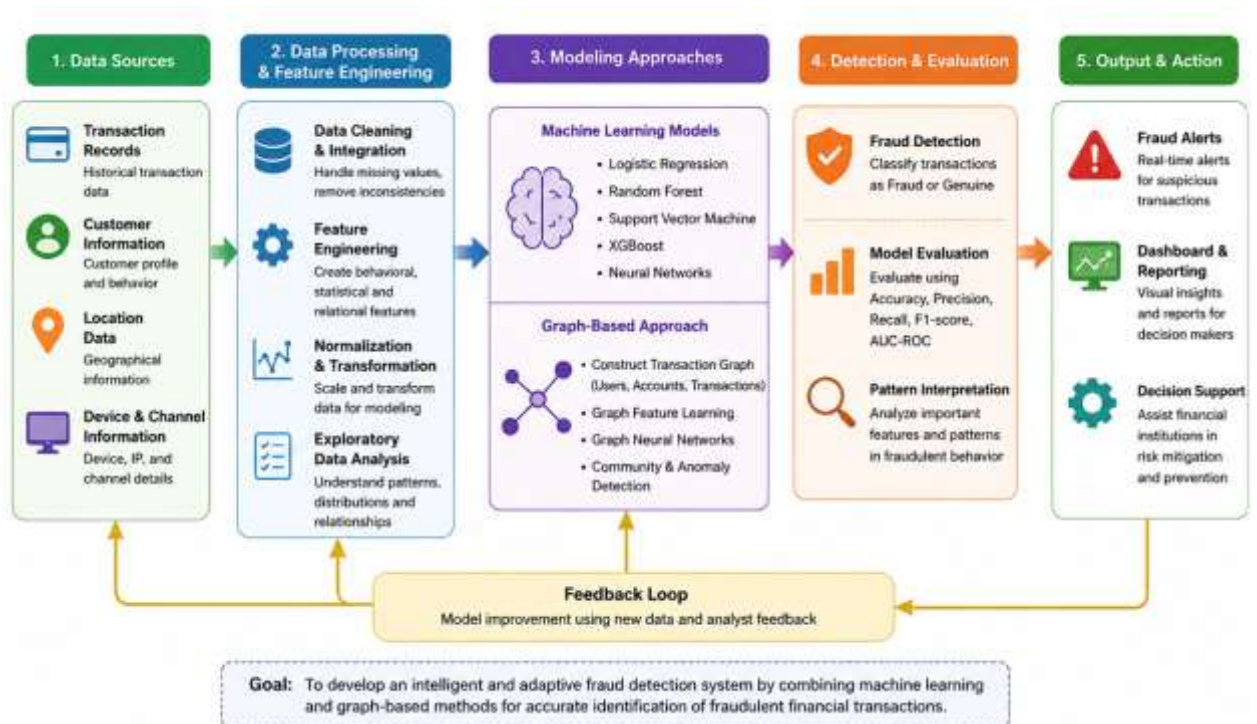


Figure 1. Conceptual Framework for Financial Fraud Detection and Machine Learning Integration

(Source: Created by learner)

3. Result

Data Distribution Analysis

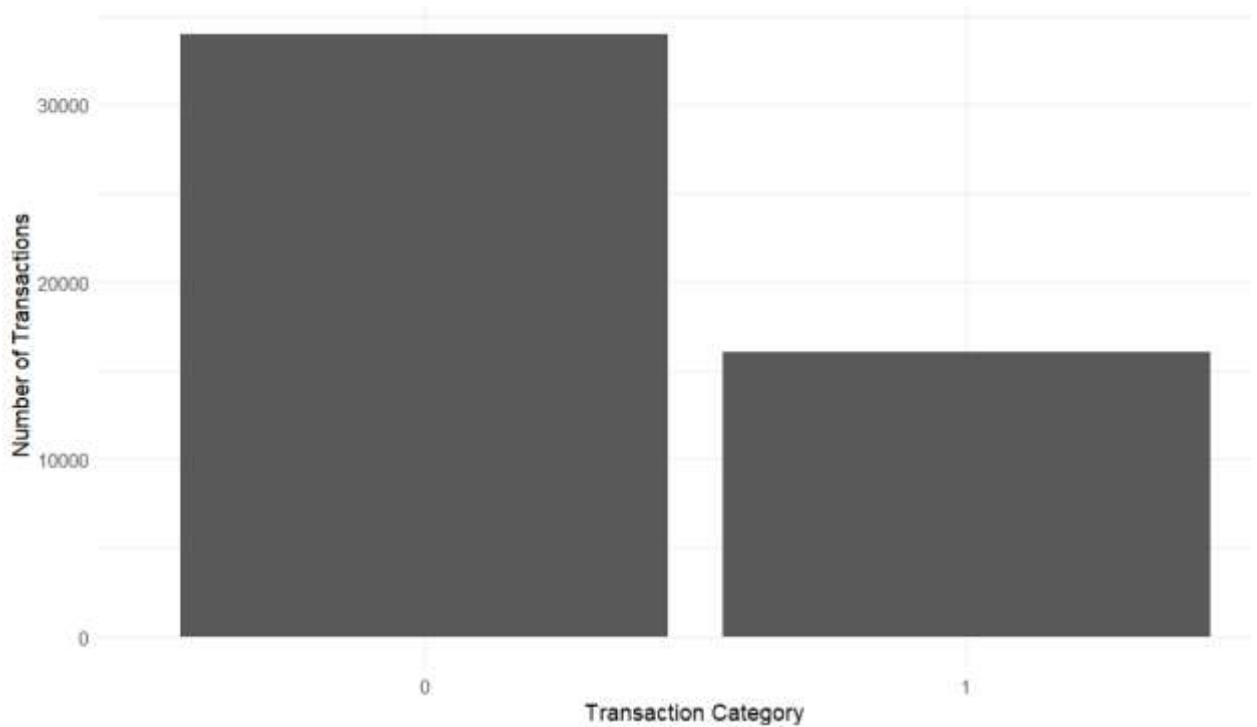


Figure 2. Distribution of Fraudulent and Genuine Transaction

(Source: Created by learner)

The visualization shows what percentage of the dataset represents fraudulent transactions and what percentage represents genuine transactions. It is seen that there is an imbalance between the genuine transactions and the fraudulent transactions. This is the typical situation in financial fraud detection that frauds are less frequent than normal transactions. The distribution shows that the effectiveness of machine learning techniques is essential to accurately detect minority fraud cases.

Transaction Behavior Analysis

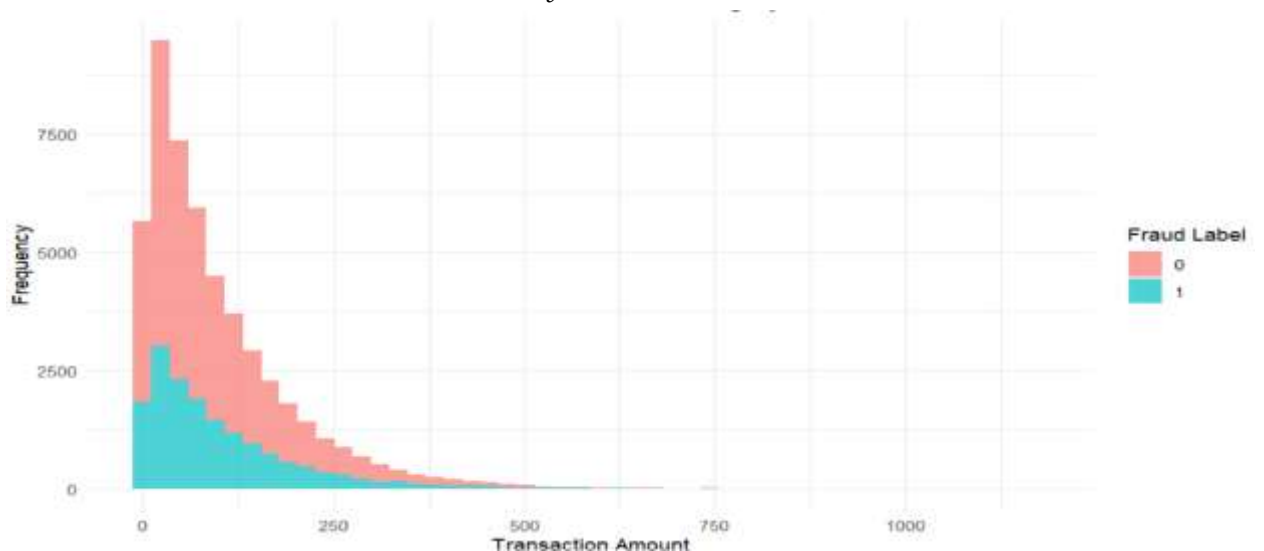


Figure 3. Transaction Amount Distribution Based-on Fraud Category

(Source: Created by learner)

The amount of the transaction distribution reveals that both fraudulent and legitimate transactions have a skewed distribution across lower ranges of transaction amounts. Fraudulent transactions, however, show varying distributions as compared to genuine

transactions, which show variations in spending behaviour. The results indicate that transaction amount is a potentially useful attribute to consider when using it as part of the identification process of unusual financial activity and to boost fraud detection results.

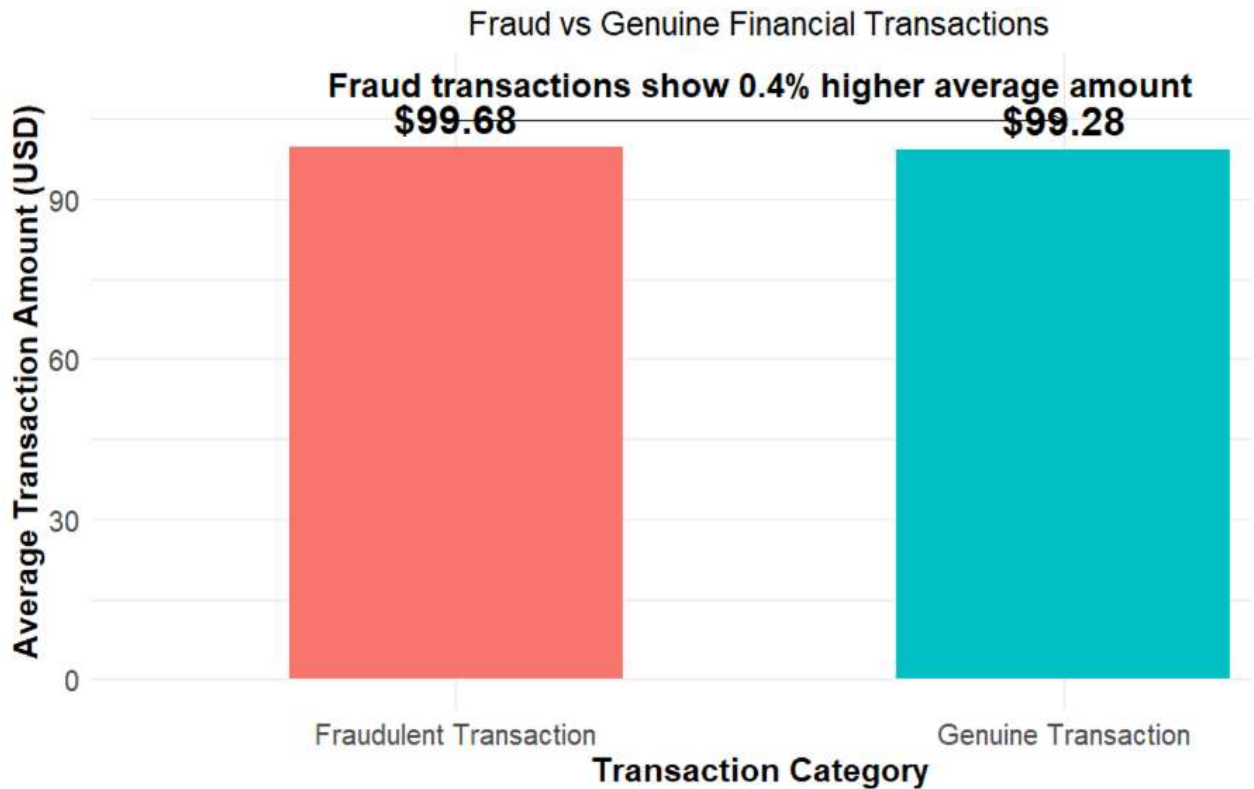


Figure 4. Average Transaction Amount Comparison

(Source: Created by learner)

Average transaction values suggest that the fraudulent transactions have a slightly higher average value than authentic transactions. The gap is not a huge one, but it does indicate that transaction value itself might not be enough to identify fraud. Using transaction amount along with other behavioral characteristics can improve the accuracy of machine learning models.

Feature Relationship Analysis

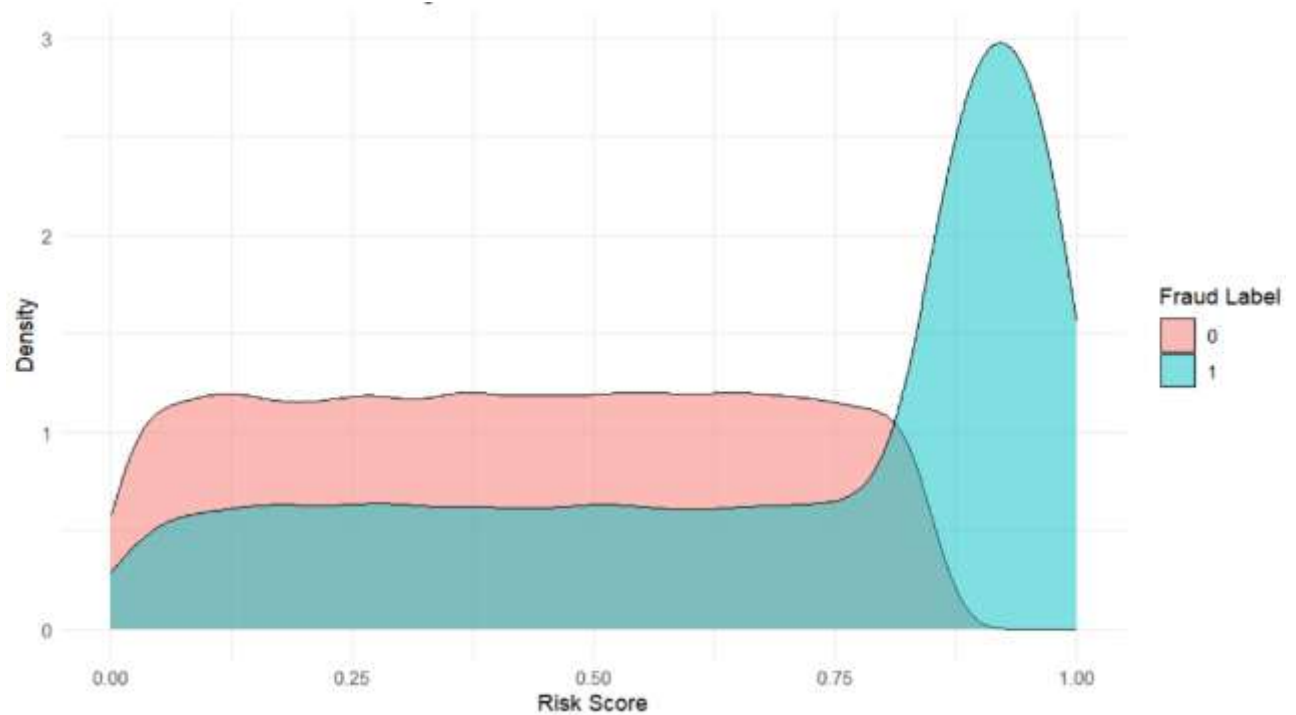


Figure 5. Risk Score Distribution Among Fraud and Genuine Transaction

(Source: Created by learner)

In the risk score distribution graph, there is an obvious difference between the fraudulent and legitimate transactions. Fraudulent transactions have higher risk score values; valid transactions are predominantly in the lower ranges of risk score values. This discovery suggests that risk score is an important feature to detect suspicious transactional activity and can be used to enhance fraud classification models.

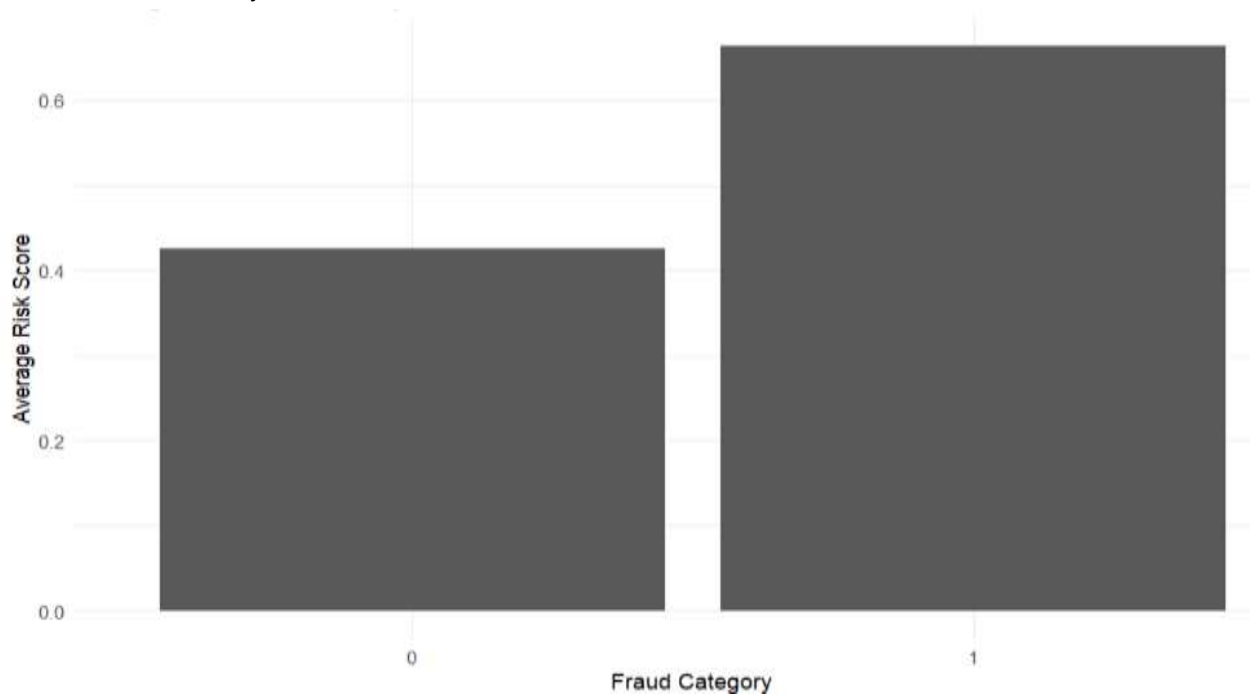


Figure 6. Average Risk Score Comparison

(Source: Created by learner)

The average risk score comparison shows that fraudulent transactions have a higher average risk score than non-fraudulent transactions. This result suggests that risk assessment features can provide valuable information for detecting potential fraud cases.

The differences between the two categories illustrates the need to include risk related attributes in fraud detection systems.

Fraud Detection Model Results

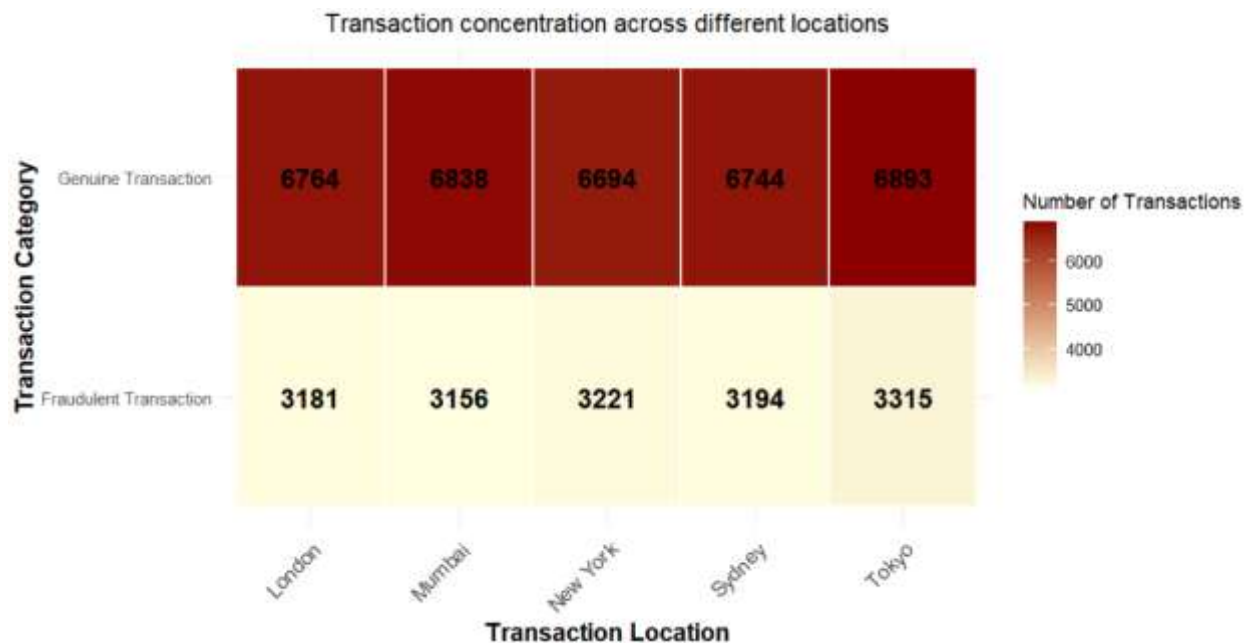


Figure 7. Geographical Fraud Risk Distribution

(Source: Created by learner)

Geographical fraud risk distribution visualization gives a visualization of transaction patterns across geographical locations. The results indicate that both authentic and phony transactions are spread out among the all the examined sites, while the phony ones seem to be regularly found in each area. This indicates that location-based information alone may not completely identify fraud but can provide additional contextual information. The combination of machine learning, graph-based analysis, and geographical characteristics can enhance the detection of intricate fraud schemes.

4. Discussion of Results

The findings gathered from the exploratory analysis are useful to gain insights on the patterns of financial fraud and supplement the findings from the literature review. The data distribution analysis indicates that there are more genuine transactions than fraudulent transactions, illustrating the typical class imbalance issue in fraud detection studies. In financial datasets, Ali et al. [6] have explained that there is an imbalance due to the limited number of fraudulent transactions in comparison to the normal transactions. Thus, the accurate classification of minority fraud cases is still a key factor to the design of good fraud detection systems.

Transaction behavior analysis suggests that the fraudulent transactions exhibit different behavior in terms of transaction amount and risk score, as compared to the genuine transactions. The results indicate that higher transaction value and risk scores are associated with fraudulent transactions. As reported by Alamri and Ykhlef [9] that the spending behavior and transaction patterns are crucial features to identify the abnormal activities are in line with the findings in this paper. Likewise, Esenogho et al. [11] pointed out that feature engineering is important to enhance fraud detection since it chooses meaningful attributes from the transactional data. The risk score analysis also corroborates the results of Soyombo et al. [3] which indicated that AI techniques could detect suspicious behaviors when analyzing financial data patterns.

Results of the geographical analysis reveal that fraudulent activities are distributed throughout space, suggesting that location-based information could be used to give further context to fraud detection. This discovery is related to the graph-based methods mentioned by Chakraborty and Sharov [12] which involve building relationships between entities like users, transactions, and locations, to uncover hidden fraud patterns. Similarly, Li et al. [13] have demonstrated that graph learning techniques can enhance the detection process by considering relationships among financial entities, and not just individual financial transaction features. In conclusion, the findings showed that the integration of behavioral attributes, machine learning techniques, and graph-based methods can enhance the effectiveness of financial fraud detection in identifying complex fraud activities. The study findings corroborate the literature and highlight the need for intelligent and adaptive fraud detection systems.

Future Work

Future research can be directed towards developing hybrid fraud detection systems that can integrate together machine learning models and graph-based approaches. The analysis presented here is useful for detecting important transaction patterns, but sophisticated techniques like graph neural networks can be used to discover customer relationships, account relationships, device relationships, and more. These methods can enhance the identification of sophisticated financial fraud schemes and networks.

There are also further studies that can be conducted regarding real-time fraud detection, explainable AI, and financial data sets. Real time systems can enable financial institutions to detect suspicious transactions as they occur, and explainable models can enhance the level of trust and transparency in automated decision-making. Further studies can explore other deep learning approaches and compare the performance of various models to create even more precise, trustworthy and flexible fraud detection systems.

5. Conclusion

This study explored the financial fraud detection process using machine learning and graph-based methods by conducting exploratory data analysis on transaction patterns. It is clear from the results that aspects of transaction amount, risk score and location information can offer useful information on fraudulent activity. The results of the study align with the previous research which emphasizes the significance of AI in improving fraud detection accuracy. Machine learning models and graph-based techniques offer enhanced possibilities for fraud pattern detection over traditional approaches. But there are issues about data imbalance, fraud behavior evolution and transparency that need further research. In conclusion, intelligent fraud detection systems can help decrease financial losses from fraud and enhance financial security as a whole.

REFERENCES

- [1] A. Hazar and Ş. Babuşcu, "Financial technologies: Digital payment systems and digital banking. Today's dynamics," *Journal of Research, Innovation and Technologies*, vol. 2, no. 4, pp. 162–178, 2023.
- [2] O. Ilori, "The effectiveness of data mining in detecting financial fraud: A review and applications."
- [3] O. T. Soyombo, "Reviewing the role of AI in fraud detection and prevention in financial services," *International Journal of Science and Research Archive*, vol. 11, no. 1, pp. 2101–2110, 2024.
- [4] M. Beemamol, "Mapping the trends of Financial Statement Fraud detection research from the historical roots and seminal work," *Journal of Economic Criminology*, vol. 6, p. 100096, 2024.

- [5] Y. Chen, C. Zhao, Y. Xu, C. Nie, and Y. Zhang, "Year-over-year developments in financial fraud detection via deep learning: A systematic literature review," *arXiv preprint arXiv:2502.00201*, 2025.
- [6] A. Ali, S. Abd Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, et al., "Financial fraud detection based on machine learning: A systematic literature review," *Applied Sciences*, vol. 12, no. 19, p. 9637, 2022.
- [7] D. O. Njoku, V. C. Iwuchukwu, J. E. Jibiri, C. T. Ikwuazom, C. I. Ofoegbu, and F. O. Nwokoma, "Machine learning approach for fraud detection system in financial institution: A web base application," *Machine Learning*, vol. 20, no. 4, pp. 01–12, 2024.
- [8] R. Udayakumar, A. Joshi, S. S. Boomiga, and R. Sugumar, "Deep fraud Net: A deep learning approach for cyber security and financial fraud detection and classification," *Journal of Internet Services and Information Security*, vol. 13, no. 3, pp. 138–157, 2023.
- [9] M. Alamri and M. Ykhlef, "Hybrid feature engineering based on customer spending behavior for credit card anomaly and fraud detection," *Electronics*, vol. 13, no. 20, p. 3978, 2024.
- [10] A. Kumar, R. D. Gopal, R. Shankar, and K. H. Tan, "Fraudulent review detection model focusing on emotional expressions and explicit aspects: Investigating the potential of feature engineering," *Decision Support Systems*, vol. 155, p. 113728, 2022.
- [11] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," *IEEE Access*, vol. 10, pp. 16400–16407, 2022.
- [12] S. Chakraborty and S. Sharov, "Graph based approach on financial fraudulent detection and prediction," in *Applied Graph Data Science*, pp. 25–37, Morgan Kaufmann, 2025.
- [13] R. Li, Z. Liu, Y. Ma, D. Yang, and S. Sun, "Internet financial fraud detection based on graph learning," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 3, pp. 1394–1401, 2022.
- [14] R. M. Zakaria, M. M. Rahman, H. Rahman, M. A. Rafi, A. Minto, M. S. Hossain, and S. I. Saimon, "Detecting financial fraud in real-time transactions using graph neural networks and anomaly detection techniques," *Journal of Economics, Finance and Accounting Studies*, vol. 7, no. 6, pp. 01–13, 2025.
- [15] I. Rasul, S. I. Shaboj, M. A. Rafi, M. K. Miah, M. R. Islam, and A. Ahmed, "Detecting financial fraud in real-time transactions using graph neural networks and anomaly detection," *Journal of Economics, Finance and Accounting Studies*, vol. 6, no. 1, pp. 131–142, 2024.
- [16] B. A. Arbab, *Fraud Detection Transactions Dataset*, Kaggle, 2025. [Online]. Available: <https://www.kaggle.com/datasets/barkataliarbab/fraud-detection-transactions>