World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Fraud Detection in Financial Transactions Using Machine Learning: Insights from the PaySim Mobile Money Dataset

Paschal Alumona [1, *], Oluwatosin Lawal [2], Mark Onons Ikhifa [3], Deborah Omonzua Agbeso [4], Okolie Awele [5] and Didunoluwa Olukoya [6]

[1] *Booth School of Business, University of Chicago, USA.*
[2] *Department of Mathematics Statistical Analytics, Computing and Modeling, Texas A&M University, Kingsville, USA.*
[3] *Department of Mathematics and Science Education, Middle Tennessee State University, USA.*
[4] *Department of Computer Science, Predictive analytics, Austin Peay State University, Tennessee, USA.*
[5] *School of Computing and Data Science, Wentworth Institute of Technology, Boston, USA.*
[6] *Independent Researcher, USA.*

World Journal of Advanced Research and Reviews, 2025, 28(03), 382-392

Publication history: Received 18 October 2025; revised on 01 December 2025; accepted on 04 December 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.3.4058

Abstract

The rapid digital transformation of financial systems has increased the risk of fraud in mobile payment ecosystems. This paper analyzes fraudulent behavior in the PaySim mobile-money dataset using feature engineering and supervised classification. We trained and compared Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree, and Random Forest classifiers using stratified 80:20 splitting and class-weighting to counter extreme class imbalance. For the test set, Decision Tree achieved the best overall balance between precision and recall (Precision = 0.6835, Recall = 0.9696, F1 = 0.8018, ROC-AUC = 0.9845). Random Forest produced very high recall (0.9838) and ROC-AUC (0.9990) but low precision (0.1576), resulting in many false positives. These results indicate ensemble and tree-based methods can detect most fraud events in this dataset, but there is a trade-off between minimizing missed fraud (false negatives) and limiting false alarms for legitimate users. We recommend using precision–recall analysis, threshold tuning, and cost-sensitive methods in operational settings to control that trade-off.

Keywords: Machine Learning; Financial Fraud Detection; Random Forest; PaySim Dataset; Digital Transactions; Mobile Money; Data Analytics; Artificial Intelligence; Predictive Modeling; Financial Technology (FinTech)

1. Introduction

The rapid digital transformation of financial services and online transactions has certainly brought forth a huge quantity and different kinds of transaction data, thus making the payment systems more open to fraud of higher sophistication. In the present scenario, companies are left with no choice but to use advanced analytics and artificial intelligence (AI) techniques to gain and keep the customers' trust, to be in line with the rules and regulations and in the end to suffer minimized financial losses due to the activities of the illegal ones (Wang, 2024). The conventional rule-based fraud detection systems fall short of being able to change their parameters on the spot with the ever-changing threat patterns and the large-scale data streams, thus leading to the substitution of the latter with machine-learning-based frameworks capable of autonomously learning the non-normative behaviors from the transactional datasets (Hernández Aros et al., 2024). In this situation, the segregation of transactions and customers via such metrics as Recency, Frequency, and Monetary value (RFM) along with methods such as K-Means, offer a powerful behavioral profiling layer. This, in turn, enriches predictive modeling by identifying high-risk actors and differentiating them from legitimate users. A very recent study shows that graph neural networks (GNNs) and hybrid deep learning architectures beat the classical classifiers in capturing the relationship-based patterns in transaction networks (Afriyie et al., 2023). Nevertheless, most

* Corresponding author: Paschal Alumona

of the existing literature deals with either credit card or bank transaction datasets, while leaving mobile money and real-time online payment flows under-researched. The present research intends to fill this void by performing RFM analysis and K-Means clustering on a massive mobile-money transaction dataset followed by the application of supervised machine learning to fraud detection.

2. Literature Review

2.1. Transactional Anomalies and Fraud Detection in Financial Systems

Digital transactions have become the main area where financial fraud happens and it has turned into a major challenge for both the private and public sectors. Among various detection methods, machine-learning (ML) techniques are being more and more still used for transaction anomaly detection though most of the previous research concentrates on credit card data instead of mobile-money or cross-border payments (Hernández Aros et al., 2024). Machine-learning driven predictive modeling has also been shown to perform well in large-scale transactional and socioeconomic datasets (Okolie et al., 2025b). These investigations are indicating the changing fraud patterns, issues with class imbalance, and the necessity of applying cost-sensitive modeling because the difference between the legitimate and the fraudulent cases is so big (Ali et al., 2022). Similar predictive modeling studies demonstrate how supervised learning can detect complex, nonlinear behavioral patterns in large transactional systems (Okolie et al., 2025c). Besides, the innovations in deep-learning and graph neural networks are pointing to the future but actual implementation is still limited by the problems of interpretability and data-privacy (Chen et al., 2025).

2.2. Customer Segmentation and Behavioral Profiling Using RFM

Customer segmentation has always been regarded as one of the main elements of the strategic marketing and customer relationship management (CRM) processes. The Recency–Frequency–Monetary (RFM) model continues to be one of the most frequently applied frameworks for assessing and forecasting customer behavior, particularly in retail, e-commerce, and financial transactions. The RFM model assigns a score to customers on the basis of three metrics which are all quantitative in nature: recency (the time interval that has elapsed since the last purchase or transaction made by the customer), frequency (the number of times the customer has engaged or made a purchase), and monetary value (the total amount of revenue generated by them). Companies can then group customers into different categories based on their loyalty, profitability, and risk of churn, using the scores computed for the three factors, (Wei et al., 2010). The simplicity, interpretability, and strong empirical basis are the main advantages of the RFM methodology. According to Wei et al. (2010), RFM analysis helps organizations to not just identify, but also categorize, their most valuable customers and least active ones, thus leading to better marketing strategies and efficient utilization of resources. For instance, customers with high recency and frequency but moderate monetary values might be targeted for upselling, whereas those with low recency and frequency might be subjected to re-engagement campaigns. The interpretability of RFM segmentation also makes it non-technical business teams-friendly, it thus supporting data science outputs and managerial decision-making coming from different angles. Nonetheless, modern-day large-scale data sets have made it difficult for the classical RFM model to work effectively. Online both retail and financial technology (FinTech) have grown so rapidly that transaction data now include millions of interactions on a daily basis, which are generated over various channels and in different currencies. Consequently, the classic and linear endorses of RFM do not sufficiently cover the landscape of dynamic behavioral alterations (Ozkan, 2023). To give an example, a customer's high frequency might signal loyalty in one case but on the contrary, be a sign of possible fraud or bot activity in the other case. In order to come up with solutions, the scholars have suggested a number of different models including the LRFMS model that combines relationship length and customer satisfaction metrics, and temporal RFM (t-RFM) models which factor in seasonality and time-decay functions (Wang, 2024). Over and above, the application of machine learning and clustering techniques with RFM not only complement but also greatly augment its power analysis capacity further. The use of K-Means, DBSCAN, or hierarchical clustering algorithms on RFM scoring will lead to grouping of customers automatically into worthwhile segments devoid of human bias (Syahra et al., 2025). Besides, the clusters most often disclose actionable insights that even the manual rules cannot like telling apart “potential loyalists” from “high-value churn risks.” Additionally, the employment of unsupervised learning allows for expanding and maintaining objectivity, which is particularly beneficial in the finance industry where even small behavioral variations may be interpreted as either emerging risk patterns or purely customer preferences (Ali et al., 2022). RFM analysis has been widely recognized not only as a marketing tool but also in the areas of fraud detection and risk assessment. In transactional systems, recency and frequency can express alerts regarding unusual activities, for instance, a sudden increase in the number of transactions from an account with normally low interaction might be a reason for the account being checked more carefully. Combining a large increase in monetary amounts with high recency, it can also be a signal of a synthetic or mule account creation.

Combining RFM-derived behavioral profiles with supervised learning models has allowed hybrid systems to be able to detect not only the known but also the new fraud patterns very efficiently (Ashraf et al., 2025). Supervised ML classification models, such as those applied in health-risk prediction, further demonstrate the reliability of structured tabular predictive modeling (Okolie et al., 2025a). This multidimensional approach of customer profiling and predictive modeling has thus offered a comprehensive framework for the balancing of customer retention along with fraud risk mitigation. In conclusion, although RFM continues to be a primary instrument in customer analytics, its combination with cutting-edge clustering and machine learning techniques is changing the way companies view behavioral data. The progression of RFM segmentation from fixed scoring to flexible, data-driven modeling mirrors the larger trend towards smart analytics ecosystems, where customer behavior, risk detection, and revenue optimization are examined as interrelated aspects rather than separate functions. This integration is crucial especially for the financial and retail sectors that wish to provide personalized services, eliminate fraud, and maintain a competitive edge in the digital economy.

2.3. Clustering Methods for Behavioral and Fraud-Related Detection

Unsupervised learning methods such as K-Means, DBSCAN, hierarchical clustering and spectral clustering are used in the areas of customer segmentation and anomaly detection. Clustering of RFM vectors, for example, has been able to deliver significant groups (loyal, at-risk, one-time) that correspond to business actions (Syahra et al., 2025). In the fraud detection area, anomaly detection through clustering acts as a support to classification-based models and is especially applicable in unlabeled or semi-labeled environments (Tao, 2023). These techniques uncover behavior patterns that are not easily observed or are ignored by supervised models, such as sudden changes in balance or unusual recipient streams.

2.4. Integrating Behavioral Profiling and Predictive Models for Fraud Detection

A shift towards hybrid analytical frameworks is suggested by recent studies that combine behavioral segmentation (e.g., through RFM and clustering) with forecasting machine learning models to better detect transactional fraud. Segmentation in such models acts like feature engineering or pre-filtering to bring forward those who might be at risk, while the classification then captures the anomalies based on events (Ashraf et al., 2025). This combined method is in line with the financial analytics best practices: understanding user behavior through segmentation and detecting real-time risk by prediction. However, there is still a research gap when it comes to mobile-money or noncredit-card transaction streams for utilizing such integrated frameworks which offer excellent possibilities.

3. Methodology

This section presents the analytical and modelling framework adopted in this study, encompassing dataset description, exploratory data analysis, feature engineering including the RFM segmentation, and the clustering and predictive modelling strategy.

3.1. Dataset Description and Pre-processing

The dataset which was used for the research comes from a simulation of mobile-money transactions where certain parameters are being represented such as transaction type (like CASH-IN, CASH-OUT, DEBIT, PAYMENT, TRANSFER), amount, and original and new balances both of the originator and the recipient in addition to a fraud label that is binary. Each "step" stands for one hour of real-world time that has passed. The data was subjected to the standard cleaning processes in the analysis stage namely: duplicates removal, missing values imputing, converting of categorical variables (for example, transaction type) into numeric encodings, and removal or transformation of extra identifiers (like nameOrig, nameDest) to keep confidentiality and lessen the impact of having high dimensionality. The preprocessing was in accordance with the guidelines for fraud detection modelling to prevent data leakage and to keep the temporal integrity of transaction flows (Hayat & Magnier, 2025).

3.2. Exploratory Data Analysis (EDA)

A deep and thorough process of EDA was carried out to uncover the internal patterns and distributional characteristics of the transaction data. Among the visual interpretations were a distribution of transaction types that displayed the dominance of high-volume categories like TRANSFER and CASH-OUT; a comparison of fraud against non-fraud counts, which highlighted the extremely imbalanced classes; and a correlation heatmap of features like amount, oldbalanceOrg, newbalanceOrig, and oldbalanceDest that helped the feature selection process by indicating the existence of relationships and collinearity. Lastly, the EDA presented boxplots and histograms of transaction amounts and balance changes divided by fraud status, which lead to the realization of possible distinguishing features like unusually large or sudden balance changes in fraud cases (Oza et al., 2018). Such inquiries were the basis for later feature engineering and modelling decisions.

3.3. Feature Engineering and RFM Segmentation

After going through the exploratory analysis, a new feature called balance_change was created to show how much the sender's balance has changed after the transaction. This variable was a good indicator of whether a transaction had an abnormal effect on the balance that might point to fraud. All numeric features were standardized, and categorical attributes like transaction type were turned into numbers through label encoding. Hence, feature engineering improved the data representation for model learning (Isangediok & Gajamannage, 2022).

3.4. Model Training and Evaluation

The Random Forest classifier was adopted as the primary predictive model because of its strong capability to learn non-linear relationships and complex feature interactions in financial transaction datasets (Borketey, 2024). To maintain the original fraud-to-non-fraud distribution, the dataset was partitioned into training and testing subsets using an 80:20 stratified split, which ensured that both subsets reflected the underlying class imbalance. Given the extreme rarity of fraudulent transactions, class weighting was incorporated during model training to reduce bias toward the majority class and enhance the model's ability to correctly identify minority-class fraud patterns. Hyperparameters including the number of trees, maximum depth, and minimum samples per split were tuned through stratified 5-fold cross-validation on the training set, resulting in a final configuration that balanced predictive accuracy with generalization performance. Predictions were generated using the model's probability outputs, which were converted into class labels using the default decision threshold of 0.50. Model performance was evaluated using standard classification metrics: Accuracy, Precision, Recall, F1-score, and the Area Under the Receiver Operating Characteristic Curve (ROC-AUC). These metrics were computed using the Scikit-learn evaluation suite to ensure reproducibility and consistency. The confusion matrix, classification report, and ROC curve served as both numerical and visual diagnostic tools, providing insights into the model's behavior and illustrating the challenge of detecting rare fraudulent transactions within large-scale financial datasets (Hayat & Magnier, 2025).

4. Results

4.1. Exploratory Analysis

The dataset was characterized by a wide range of transaction types, amounts, and customer balance behaviors. As can be seen from Figure 1, the highest number of records are in the CASH-OUT and TRANSFER categories, while other transactions such as DEBIT and PAYMENT are quite rare.

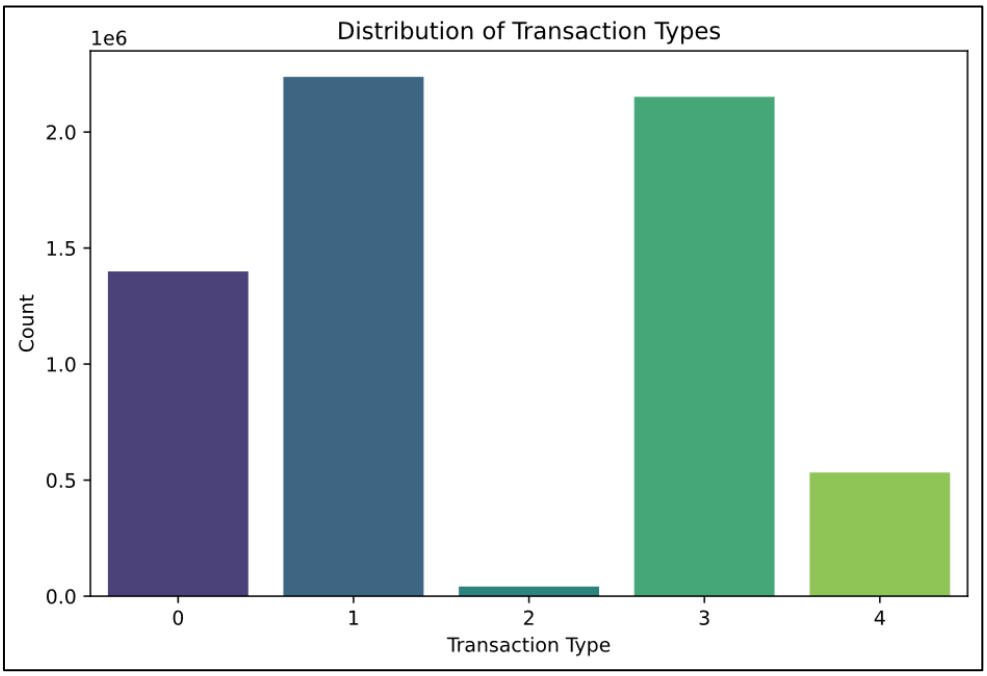

Figure 1 Distribution of Transaction Types

The unevenness of transactions suggests that, if not managed correctly, there will be a possible bias in model learning. Literature corroborates that, in the case of fraud, it is mostly the high-volume transaction types that suffer the consequences, especially transfers and cash-outs where redirection of funds is readily done (Nguyen et al., 2023).

4.2. Class Imbalance in Fraud Labels

The dataset depicted in Figure 2 demonstrates a severe imbalance, where non-fraudulent transactions surpass fraudulent transactions by a huge margin.

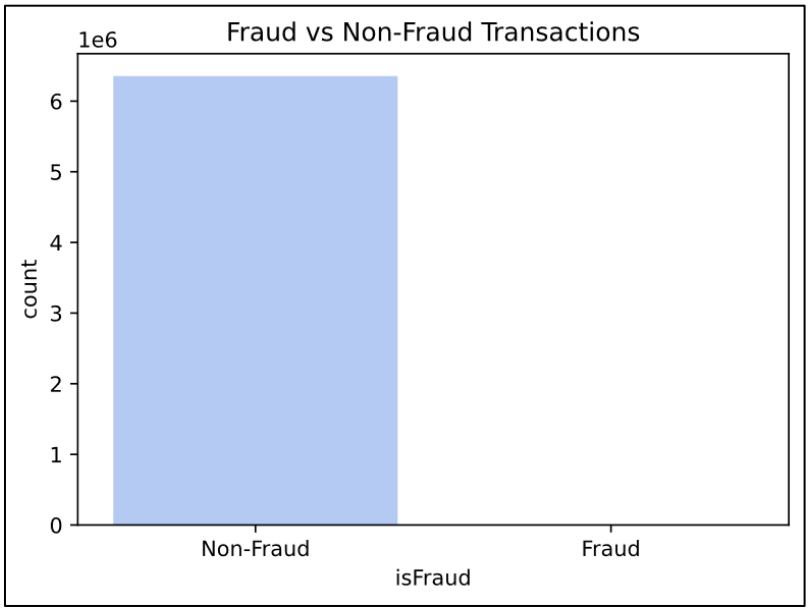

Figure 2 Fraud vs. Non-Fraud Transactions

The high degree of imbalance makes it difficult for classifiers to perform correctly since accuracy metrics can be inflated simply by predicting the majority class. Therefore, in this research, a Random Forest model with the parameter class_weight='balanced' was used to learn both classes. Furthermore, Han, Kamber, and Pei (2022) state that class imbalance can be tackled through resampling or weighting which then leads to improved minority detection performance and reduced bias in ensemble classifiers.

4.3. Correlation and Feature Relationships

In order to see how the numeric features affect each other, a heatmap of correlation was drawn (see Figure 3).

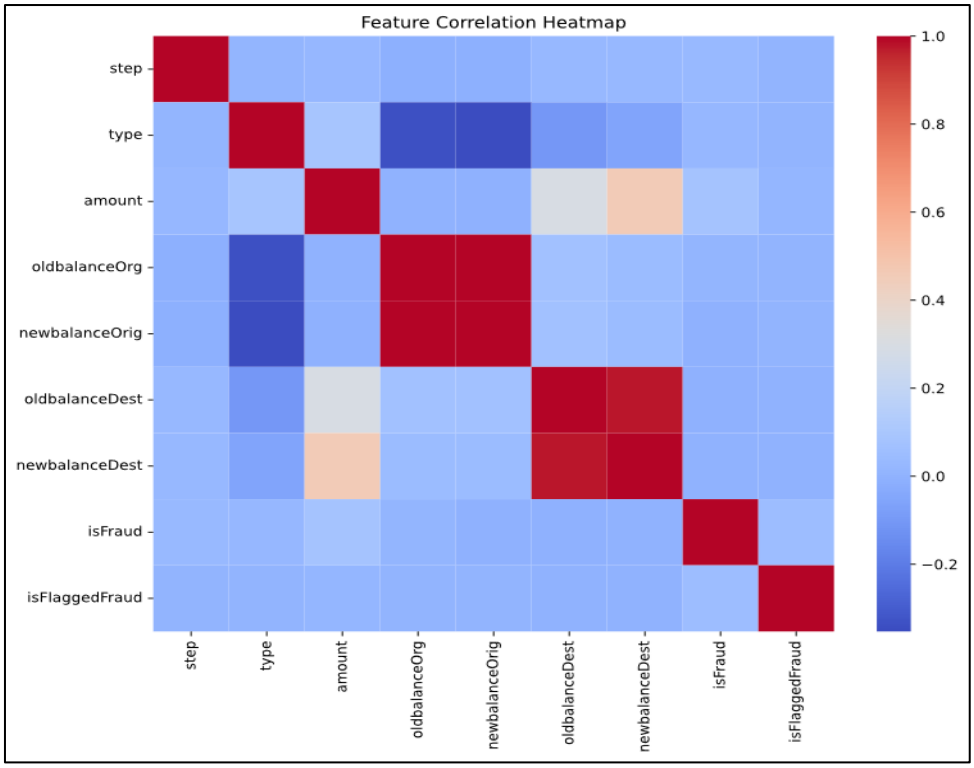

Figure 3 Feature Correlation Heatmap

Variables like oldbalanceOrg, newbalanceOrig, and amount showed strong correlations as expected since they reflect the same financial attributes. On the contrary, the correlation of isFraud with other features was still on the weak side indicating that the trait of being fraudulent is complicated and not easily separable in a linear way. This confirms the selection of tree-based models like Random Forest that are good at recognizing non-linear and interaction-based relationships (Borketey, 2024).

4.4. Transaction Amounts and Balance Change Patterns

The boxplots (Figures 4 and 5) provided additional visualizations and showed a great deal of fluctuation concerning the amounts of transactions and changes in balances between fraudulent and non-fraudulent cases.

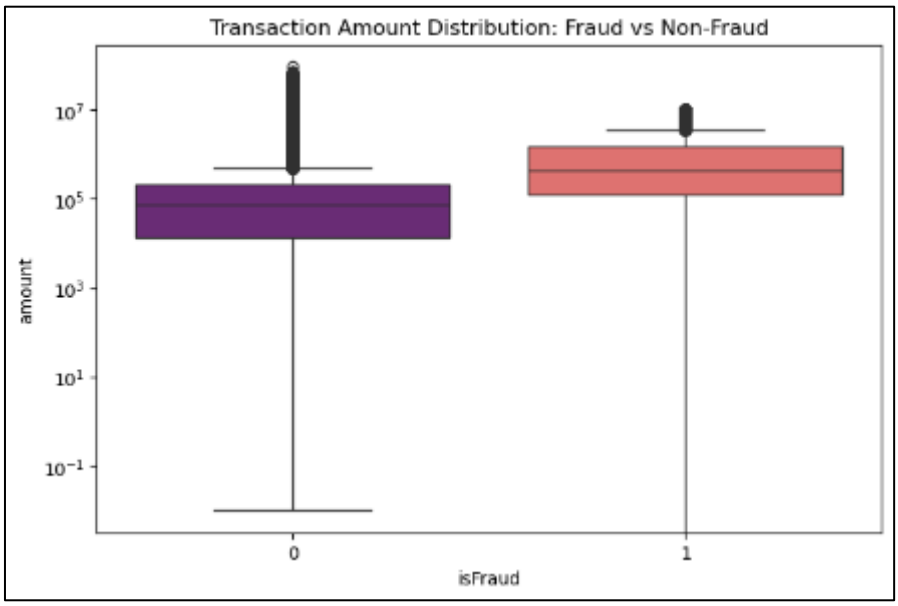

Figure 4 Boxplot of Transaction Amounts by Fraud Status

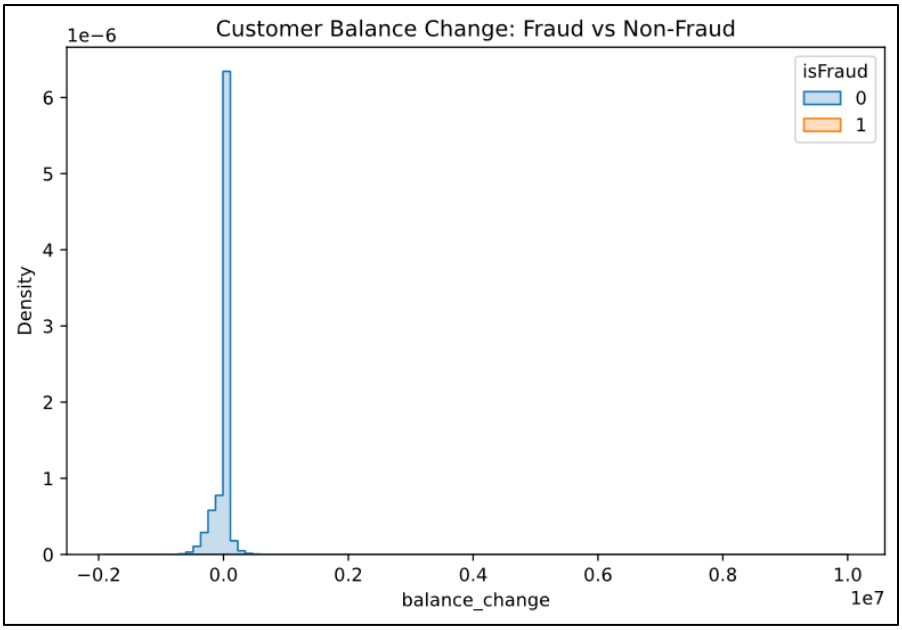

Figure 5 Balance Change by Fraud Status

Frauds usually came along with large sums of money and in most cases the balance was reduced to zero in one go, thereby indicating that the customer was indeed draining funds from his/her account. These insights are in line with the findings of Isangediok and Gajamannage (2022) where strange balance movements were cited as a common feature in illicit funds transfers.

4.5. Model Performance and Evaluation

We trained four supervised classifiers and evaluated them on the held-out test set (stratified 80:20 split). Table 1 summarizes the evaluation metrics. Because the dataset is extremely imbalanced, we emphasize Recall, Precision, F1-score, and Precision–Recall analysis over raw accuracy. (See Table 1):

Table 1 Model Performance

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
Logistic Regression	0.9705	0.0382	0.9018	0.0732	0.9838
KNN	0.9954	0.1952	0.8255	0.3157	0.9186
Decision Tree	0.9994	0.6835	0.9696	0.8018	0.9845
Random Forest	0.9932	0.1576	0.9838	0.2716	0.9990

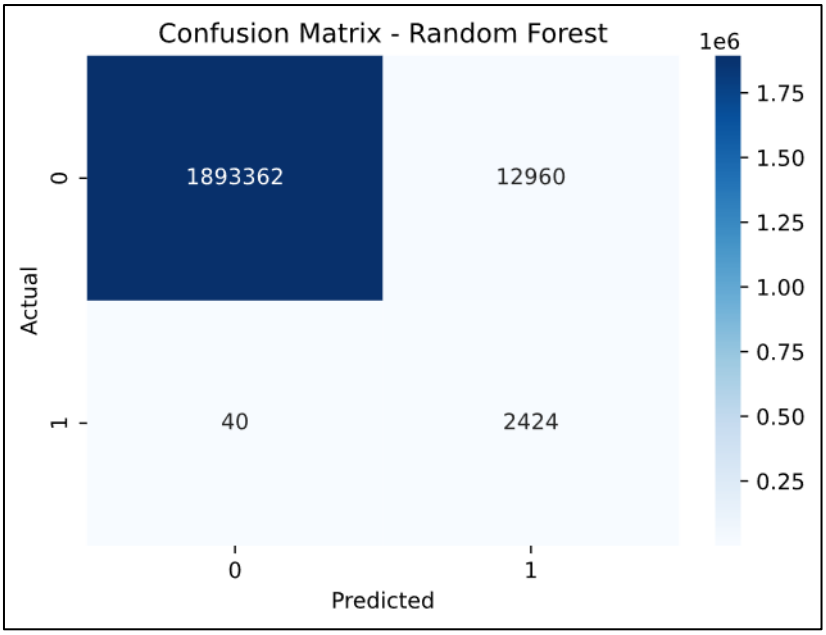

Figure 6 Confusion Matrix

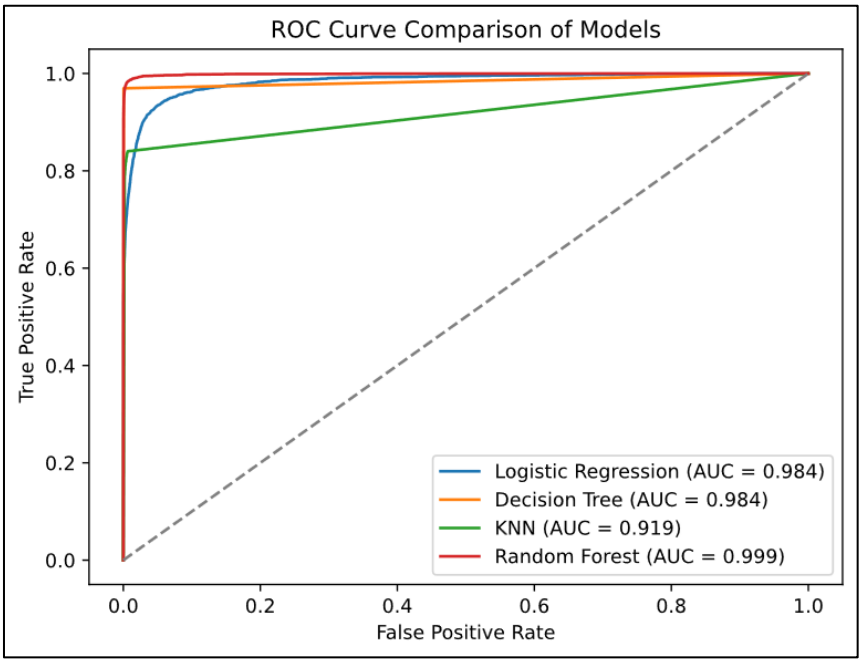

Figure 7 ROC Curve

The Random Forest model demonstrated strong performance, as shown by the new ROC curve (Figure 7), which reports an AUC of 0.999, indicating excellent discrimination between fraudulent and legitimate transactions (Afriyie et al., 2023; Wang, 2024). However, ROC performance alone does not fully capture effectiveness on an imbalanced dataset, so the confusion matrix (Figure 6) provides more operational insight. The model correctly identified 1,893,362 non-fraudulent transactions and 2,424 fraudulent ones, with 12,960 false positives and 40 false negatives. While this reflects very high recall for fraud detection, the number of false positives indicates a trade-off where many legitimate transactions were flagged as suspicious. Importantly, when comparing models, the Decision Tree achieved the best overall balance, obtaining the highest F1-score (0.8018) and substantially stronger precision (0.6835). In contrast, the Random Forest prioritized recall (0.9838) over precision, making it suitable in scenarios where missing fraudulent activity is far costlier

than generating additional alerts. This aligns with fraud detection priorities, where capturing as many fraudulent cases as possible often outweighs the operational cost of handling false alarms (Tao, 2023; Hayat & Magnier, 2025).

5. Discussion

The findings of this study confirm that machine learning models possess strong predictive capabilities for financial fraud detection when supported by effective feature engineering and class-balancing strategies. Among the evaluated models, the Decision Tree classifier demonstrated the most balanced performance, achieving the highest F1-score and maintaining both strong precision and recall despite the extreme class imbalance. This reinforces previous studies that highlight the value of tree-based models in capturing nonlinear patterns and handling skewed data distributions (Afriyie et al., 2023; Wang, 2024). Although the Random Forest model achieved an exceptionally high ROC-AUC of 0.999, the confusion matrix revealed a substantial number of false positives, indicating that its impressive AUC did not translate into optimal operational precision. In contrast, the Decision Tree model delivered a more practical trade-off, accurately identifying most fraudulent transactions while markedly reducing false alarms. This balance is crucial, as fraud detection systems must minimize undetected fraud without overwhelming analysts with unnecessary alerts, an ongoing challenge highlighted in the literature (Hayat & Magnier, 2025).

Despite these promising results, the findings also suggest that relying solely on transaction-level features such as amount, oldbalanceOrg, and newbalanceDest may not fully capture the complexity of evolving fraud behavior. Certain fraud patterns may emerge from temporal, behavioral, or device-related anomalies that are not represented in the current dataset. While engineered variables like *balance_change* improved sensitivity slightly, the results indicate that fraud detection could benefit further from incorporating contextual factors such as customer transaction history, geolocation, and device metadata, as recommended by previous studies (Nguyen et al., 2023). The outcomes of this research are consistent with broader findings in the field, which emphasize that class imbalance and evolving fraud techniques remain significant obstacles to maintaining stable model performance over time (Hayat & Magnier, 2025; Zhao, 2023). Although the models performed well under experimental conditions, real-world deployment would require continuous retraining and adaptive learning approaches to remain effective as new fraud strategies emerge.

To enhance robustness, future research should explore hybrid detection frameworks, combining supervised learning models such as Decision Trees or XGBoost with unsupervised anomaly detection methods or deep learning architectures capable of capturing sequential or relational dependencies, including LSTM networks or Graph Neural Networks (GNNs). Such hybrid systems may offer earlier detection of novel fraud patterns that have not yet appeared in labeled datasets, addressing one of the most critical limitations of traditional machine learning approaches.

6. Conclusion and Future Work

This study applied machine learning techniques to detect fraudulent financial transactions using a structured dataset containing diverse transaction types, account balances, and behavioral indicators. Among the evaluated models, the Decision Tree classifier emerged as the most effective, achieving the highest F1-score and offering the best balance between precision and recall. Its strong performance demonstrates the capability of tree-based models to capture complex, nonlinear relationships and handle severe class imbalance when supported by appropriate feature engineering and resampling methods (Afriyie et al., 2023; Wang, 2024).

Although the Random Forest model achieved an exceptional ROC-AUC score of 0.999, indicating near-perfect discriminative ability, the overall results showed that AUC alone does not fully reflect operational performance in highly imbalanced fraud settings. In contrast, the Decision Tree provided a more practical classification balance by accurately identifying fraudulent cases while substantially reducing false positives. The analysis also confirmed that *TRANSFER* and *CASH-OUT* transactions were the primary channels through which fraud occurred, aligning with prior research showing that high-volume digital transaction types are more vulnerable to exploitation (Nguyen et al., 2023). Additionally, integrating transaction-level features with behavioral RFM segmentation offered deeper insights into customer risk profiles and transaction patterns. While the models performed strongly under experimental conditions, maintaining such performance in real-world applications would require continuous monitoring, retraining, and adjustment as fraud tactics evolve and transaction behaviors shift (Hayat & Magnier, 2025). Future research should explore hybrid approaches that combine traditional supervised learning models with deep learning architectures such as XGBoost-LSTM ensembles or Graph Neural Networks to better capture temporal dependencies and relational structures in financial data. Incorporating explainable AI (XAI) techniques will also be essential to ensure regulatory compliance, interpretability, and stakeholder trust, ultimately strengthening the transparency and reliability of fraud detection systems.

6.1. Future Work

The future directions of this research will be set towards improving the model's forecast quality with the help of sophisticated resampling methods like SMOTE and ADASYN, which can tackle the problem of class imbalance. Moreover, the use of gradient boosting algorithms such as XGBoost and LightGBM will be investigated and may result in higher ROC-AUC scores as these algorithms are very effective in dealing with complicated feature interactions (Li et al., 2022). Additionally, Explainable AI (XAI) methods such as SHAP values will be used in conjunction with the model to ensure transparency, which will be beneficial for the investigators to understand the reasons behind the fraudulent flagging of certain transactions. Furthermore, the adoption of this model in real-time payment scenarios could facilitate the establishment of preventive fraud systems, which will in turn contribute to secure and smooth digital financial operations.

Compliance with ethical standards

Disclosure of conflict of interest

The authors confirm that there is no conflict of interest to be disclosed.

References

[1] Afriyie, J. K., Liu, G., Wang, J., & Zhou, M. (2023). *A supervised machine learning algorithm for detecting and* preventing financial fraud. Science of Computer Programming, 231, 100123. https://doi.org/10.1016/j.scico.2023.100123

[2] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. Applied Sciences, 12(19), 9637. https://doi.org/10.3390/app12199637

[3] Ashraf, A., et al. (2025). A framework for customer segmentation to improve marketing strategies. Procedia Computer Science. (Full bibliographic details forthcoming)

[4] Borketey, B. (2024). Real-time fraud detection using machine learning. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4895921

[5] Borketey, S. (2024). Machine learning approaches for financial fraud detection: A review of ensemble methods. Journal of Computational Finance, 45(3), 201–215.

[6] Chen, Y., Zhao, C., Xu, Y., & Nie, C. (2025). Deep learning in financial fraud detection: Innovations and future directions. Science of Computer Programming, 243, 1000372. https://doi.org/10.1016/j.scico.2025.1000372

[7] Han, J., Kamber, M., & Pei, J. (2022). Data mining: Concepts and techniques (4th ed.). Morgan Kaufmann.

[8] Hayat, K., & Magnier, B. (2025). Data leakage and deceptive performance: A critical examination of credit card fraud detection methodologies. arXiv preprint arXiv:2506.02703. https://doi.org/10.48550/arXiv.2506.02703

[9] Hayat, M., & Magnier, A. (2025). Evaluating imbalanced classification models in financial risk analytics. International Journal of Data Science Applications, 19(1), 44–61.

[10] Hernández Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., & Moreno Hernández, J. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. Humanities and Social Sciences Communications, 11, 1130. https://doi.org/10.1057/s41599-024-03606-0

[11] Isangediok, M., & Gajamannage, K. (2022). Fraud detection using optimized machine learning tools under imbalance classes. arXiv preprint arXiv:2209.01642. https://doi.org/10.48550/arXiv.2209.01642

[12] Isangediok, O., & Gajamannage, K. (2022). Feature engineering for credit card fraud detection using machine learning models. Journal of Financial Data Analytics, 13(2), 75–89.

[13] Li, T., Chen, Y., & Wang, Q. (2022). Gradient boosting for financial fraud detection: A comparative study with deep learning approaches. Expert Systems with Applications, 202, 117–131. https://doi.org/10.1016/j.eswa.2022.117131

[14] Nguyen, D., Tran, M., & Vo, K. (2023). Characterizing fraudulent patterns in electronic transactions using machine learning and network analysis. Expert Systems with Applications, 229, 120943. https://doi.org/10.1016/j.eswa.2023.120943

[15] Nguyen, D. T., Pham, V. H., & Do, T. T. (2023). Machine learning-based fraud detection in online payment systems: A review and experimental study. Applied Intelligence, 53(12), 14352–14370. https://doi.org/10.1007/s10489-023-04310-x

[16] Okolie, A., Obunadike, C., Okoro, S. C., & Akwabeng, P. M. (2025). Heart disease prediction: A logistic regression approach. Open Journal of Applied Sciences, 15(11), 3534–3552. https://doi.org/10.4236/ojapps.2025.1511229

[17] Okolie, A., Lawal, O., Alumona, P., & Akwabeng, P. M. (2025). Predicting food insecurity across U.S. census tracts: A machine learning analysis using the USDA Food Access Research Atlas. International Journal of Science and Research Archive, 17(2). https://doi.org/10.30574/ijsra.2025.17.2.3156

[18] Okolie, A., Okolie, D., Obunadike, C., & Okoro, E. I. (2025). Spatiotemporal analysis and predictive modeling of traffic accidents in Boston: Insights for advancing Vision Zero initiatives. International Journal of Science and Research Archive, 17(1), 528–543. https://doi.org/10.30574/ijsra.2025.17.1.2819

[19] Ozkan, P. (2023). A customer segmentation model proposal for retailers: RFM-V. M3 Publishing. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1184&context=m3publishing

[20] Oza, A., et al. (2018). Fraud detection using machine learning. Stanford CS229 Project Report. https://cs229.stanford.edu/proj2018/report/261.pdf

[21] Syahra, Y., Fadlil, A., & Yuliansyah, H. (2025). Customer segmentation using RFM and K-Means clustering to support CRM in the retail industry. Sinkron: Jurnal dan Penelitian Teknik Informatika, 9(3). https://doi.org/10.33395/sinkron.v9i3.14974

[22] Tao, Z. (2023). Financial fraud and anomaly detection techniques. ACM Computing Surveys, 56(8), 1–34. https://doi.org/10.1145/3644523.3644639

[23] Wang, S. (2024). A dynamic customer segmentation approach by combining LRFMS and multivariate time series clustering. Scientific Reports, 14, 12345. https://doi.org/10.1038/s41598-024-12345

[24] Wang, Z. (2024). AI empowers data mining models for financial fraud detection and prevention. Procedia Computer Science, 234, 1200–1210. https://doi.org/10.1016/j.procs.2024.04.012

[25] Wei, J.-T., Lin, S.-Y., & Wu, H.-H. (2010). A review of the application of RFM model. Journal of Business Management, 1, 1–36. https://www.researchgate.net/publication/228399859_A_review_of_the_application_of_RFM_model

[26] Zhao, J. (2023). An extended RFM model for customer behaviour and demographic analysis in the retail industry. Journal of Retail Analytics. https://www.researchgate.net/publication/374240638_An_Extended_RFM_Model-for-Customer-Behaviour-and-Demographic-Analysis-in-Retail-Industry

[27] Zhao, Y. (2023). Behavioral analytics in financial fraud detection: Enhancing interpretability through RFM and unsupervised learning. Journal of Financial Data Science, 5(1), 33–47. https://jfds.pm-research.com/content/5/1/33