Volume (1) No (10), 2025
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper/Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Performance Evaluation of Machine Learning Models Via Mobile Payment for Fraud Identification

Dr. Pradeep Laxkar,
Associate Professor,
ITM(SLS) University, Vadodara, Gujarat,
Department of Computer Science and Engineering
pradeep.laxkar@gmail.com

***Abstract*—Digital and mobile payments have not only led to a surge in fraudulent activities detected in financial systems but also made detecting fraud more difficult. The conventional rule-based methodology frequently lacks the ability to rely on complex patterns of fraud, and thus results in high FP and FN. Using the extremely skewed PaySim dataset, this research presents a machine learning model for detecting mobile money transfer fraud and laundering. A trained XGBoost classifier was then used to learn complex transactional relationships, and overfitting was checked by using regularization built in. The model was tested with accuracy (ACC), precision (PRE), recall (REC) and F1-score (F1) and ROC-AUC metrics all reaching 99.6%, 99.8%, 98.7% and 0.991%, respectively. The ROC curve and confusion matrix prove that there is a high ability to discriminate and low levels of false alarms. As compared with the recent methods like Bert and DenseNet, it is evident that XGBoost can perform significantly better. These findings indicate that the suggested XGBoost-based model is a highly scalable, dependable, and efficient model to detect real-time fraud in the mobile payment system and help a financial institution decrease losses and improve its anti-money laundering compliance.**

***Keywords*—Digital Payments, Mobile Money Fraud, Machine Learning, XGBoost, PaySim Dataset, SMOTE.**

I. INTRODUCTION

Digital transactions have transformed the financial sector by facilitating quick, convenient and inclusive mobile payment systems (MPS) and mobile money services. However, the rise of fraud and money laundering transactions, which threaten both financial integrity and consumer confidence, is equally attributable to this new digitalization [1][2]. The anonymity of transactions, the large volume of transactions, and the ability of transactions to be done across borders are exploited by the fraudsters who pose a big challenge to the traditional way of detecting frauds [3]. International control agencies, such as the Financial Action Task Force, are aware of mobile money as an increasingly popular avenue of money laundering and terrorist financing, and they call on financial institutions to ensure that they have proactive and technologically-focused strategies [4]. Traditional rule-based systems are prone to fail in keeping up with dynamic and changing trends of financial fraud which leads to high levels of false-positive and poor predictive capabilities [5]. As a result, a growing focus on data-driven methods that can learn based on the historical trends of transactions and spotting never-before-seen fraudulent activities is increasing [6].

In this regard, ML and AI have emerged as powerful fraud detectors and AML compliance tools. ML algorithms have the ability to extract complex non-linear correlations in transactional data and detect anomalous behavior in real time [7][8]. These techniques enable financial institutions to offer scalable, flexible and automated systems in tracking large volume of transactions to enhance efficiency in detection whilst minimizing human interventions [9][10]. The proposed research is dedicated to testing the effectiveness of several ML models when it comes to fraud detection in mobile payment systems. The study determines the models that give optimal tradeoffs between ACC, PRE, REC, and F1. The results are used to design smart, dynamic fraud detection systems, improve financial security, improve AML compliance, and increase the confidence of users in mobile payment systems.

A. Motivation and Contributions of the Study

As mobile payment systems are quickly adopted, security of transactions has been a major concern because of the increase in fraudulent activities. Cyber fraud is constantly developing and becoming more complex, making it difficult for traditional methods of fraud detection, like rule-based systems, to keep up, which results in a high rate of FP and incomplete detections. Despite the promising results of ML and DL models for detection, there are still obstacles to overcome in areas such as dealing with data imbalance, detecting fraud in real-time, and generalizing to other types of fraud. A desire to find effective, scalable, and trustworthy methods for mobile payment system fraud detection prompted this work to compare and analyze sophisticated ML models on the PaySim dataset. Contributions from this research primarily consist of:

- Designed a systematic preprocessing pipeline including label encoding for categorical features, and normalization.
- Used SMOTE to ensure that PaySim data had an even proportion of fraudulent and legitimate transactions.
- Proposed and implemented an XGBoost-based fraud detection model optimized for handling large-scale imbalanced transaction data.

- Exploratory data analysis and feature correlation research have proven that balance inaccuracy features are crucial for identifying fraudulent transactions.
- Ensuring rigorous and reliable performance analysis, conducted a systematic evaluation of the model utilizing metrics such as ACC, PRE, REC, F1, confusion matrix, ROC curve, and AUC.

B. Justification and Novelty

This study tackles the issues presented by highly imbalanced transaction datasets like PaySim by utilizing the XGBoost model for fraud detection in mobile payment systems. In comparison with traditional ML methods, XGBoost has the virtue of integrating scalability, feature selection and regularization which allow it to easily learn complex transactional patterns with minimal overfitting. This strict preprocessing step, such as label coding, normalization, and balancing via SMOTE, also increases its resistance to the problem of class imbalance. These methodology decision-making assurances lead to a low level of misclassifications, valid fraud detection, and adaptability to real-life mobile money ecosystems.

C. Organization of the Paper

The paper follows the following structure: Section II is a review of related work, Section III discusses the methodology, Section IV is a discussion of results and comparisons and Section V ends the study with future directions.

II. Literature Review

This section examines recent research endeavors that utilize ML, DL, and hybrid models to detect fraud in mobile payment systems. It concentrates on the methodologies, datasets, performance outcomes, and identified research gaps to offer insights into current advancements and future directions, as summarized in Table I.

U et al. (2025) used perceptron to identify specific objects and backpropagate error values in order to minimize error values, using the M-DBN model. Although the final model may have a convoluted initialization, it can learn some extremely appealing hierarchical features and enhance its prediction property by stacking Restricted Boltzmann Machines (Res-BMs) and fine-tuning the resultant deep network using gradient descent and back propagation. The model's confusion matrix shows that the M-DBN model attained F1=98.2%, REC=97.8%, PRE=98.1%, and ACC= 98.4% [11].

A, M and J (2025) explores the new approach through which an innovative algorithm, such as the Isolation Forest (IF) algorithm, has been used to combat it. It finds the unusual patterns within an imbalanced dataset without the support of labeled data. model has focused attention on analyzing transaction behaviors besides detecting anomalies in a given dataset. In this case, the remarkable ACC recorded is as high as 98%, far more than common usage of techniques like RF, SVM, and LR [12].

Ke et al. (2025) presented an innovative GAN-based model that detects minor alterations in payment photos, thereby improving the security of online payments. Pictures used for online payments in the real world and deep-fake images created with sophisticated GAN architectures like Style-GAN and Deep-Fake make up the dataset that the model is trained on. Based on the results, it is clear that the proposed model can detect deep-fakes with a sensitivity level above 95% and correctly identify genuine transactions [13].

C S et al. (2025) found that TLELM can detect online payment fraud by applying new approach TL and ELM improves DPFD procedures. The new metaheuristic TL excels at combinatorial optimization. TLELM efficacy was examined using multiple datasets. The recommended method was compared to top-tier algorithms for binary and multiclass data categorization. Experimental data shows that TLELM outperforms other models with 99.37% ACC [14].

Shdefat et al. (2024) ML is employed to enhance the PRE and efficacy of online payment fraud prediction. An established and renowned dataset that was created for the express purpose of studying online payment fraud was utilized. Trained and tested six algorithms: SVM, DT, NB, RF, KNN, and LR. Final results showed that Decision Tree had the best performance ACC at 98.58% after extensive testing [15].

Singh (2023) researches the performance of the KNN, NB, LR, and RF algorithms on a dataset that is severely skewed. Gathered from cardholder transactions in Europe, the dataset includes 2,84,807 transactins. Preprocessed and raw data were both subjected to the four methods, and specificity, ACC, sensitivity, and F1 were used to assess the outcomes. Optimal accuracy for NB, LR, KNN, and RF classifiers are 91.67%, 96.72%, and 52.34%, respectively, according to the results [16].

Despite high accuracies achieved by existing models, research gaps remain in real-time adaptability, generalization across diverse fraud scenarios, and model explainability. Most studies rely on specific datasets, limiting scalability, while data imbalance and lack of integration of temporal and behavioral features persist. Future work should focus on developing interpretable, adaptive, and cross-domain frameworks for robust fraud detection in dynamic mobile payment environments.

TABLE I. Comparative analysis related to Fraud Detection in Mobile Payment Systems using machine learning

Reference	Methodology	Results	Research Gaps	Recommendations
U et al. (2025)	M-DBN model using perceptron, stacked Restricted Boltzmann Machines (Res-BMs), fine-tuned via gradient descent and backpropagation.	ACC 98.4%, PRE 98.1%, REC 97.8%, F1 98.2%.	Initialization complexity and computational cost remain high; limited interpretability.	Optimize initialization; explore lightweight DBN variants for real-time fraud detection.
A, M & J (2025)	Isolation Forest applied on imbalanced dataset without labels to detect anomalies in transaction behaviors.	ACC 98%, better than RF, SVM, LR.	Focused only on anomaly detection; lacks comparison on labeled real-world fraud data.	Combine IF with semi-supervised or hybrid methods; validate on diverse datasets.
Ke et al. (2025)	Using GAN and both authentic and deep-fake payment images, a model was trained (Style-GAN, Deep-Fake). Spotting changes in photographs used for online payments.	Detection rate >95%, effectively distinguishes legitimate vs fake transactions.	Limited to image-based fraud, ignores transactional fraud patterns.	Extend model to multimodal data (images + transaction logs); evaluate robustness against evolving GAN attacks.

C S et al. (2025)	Transfer Learning + Extreme Learning Machine (TLELM). Compared across binary and multiclass fraud datasets.	ACC 99.37%, outperforming baseline models.	Limited explanation of model interpretability; applicability to streaming data not tested.	Apply TLELM in real-time fraud detection; enhance explainability for regulatory compliance.
Shdefat et al. (2024)	Trained SVM, DT, Naïve Bayes, RF, KNN, Logistic Regression on online payment fraud dataset.	DT achieved best ACC: 98.58%.	Comparative models limited to traditional ML; no hybrid/ensemble DL explored.	Explore ensemble/hybrid DL models; integrate feature engineering for better fraud detection.
Singh (2023)	Compared KNN, NB, LR, RF on European cardholder dataset. Used hybrid under-sampling + oversampling.	Naïve Bayes 98.72%, Logistic Regression 52.34%, KNN 96.89%, Random Forest 91.67%.	Limited scalability for larger datasets; ensemble techniques not fully exploited.	Incorporate advanced resampling + ensemble ML/DL methods; evaluate interpretability for financial institutions.

III. Methodology

This investigation's methodology is illustrated in Figure 1. Data statistics, outliers, label encoding, normalization using Min-Max scaling, and data balancing with SMOTE are all part of the preprocessing that happens after getting the PaySim dataset from Kaggle. Training uses 80% of the dataset, while testing makes use of the remaining 20%. Initial modelling and evaluation with XGBoost is done using F1 metrics, REC, ACC, and PRE.

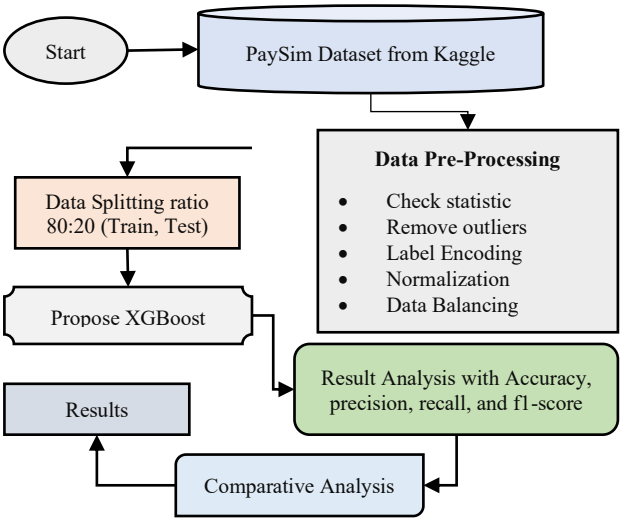

Fig. 1. Propose Flowchart for fraud detection

Each step of proposed methodology and implementation are explain in below:

A. Data Collection and Analysis

For this study, the PaySim dataset was utilized, obtained from the publicly available Kaggle repository, which provides unbalanced datasets for ML research. The dataset is widely recognized for simulating mobile money transactions and fraud detection scenarios. It contains a total of 6,362,620 card transactions, out of which 6,354,407 are legitimate and only 8,213 are fraudulent, highlighting the class imbalance challenge inherent in financial data. The correlated features of datasets are illustrate in below:

There are correlations among numerical and engineering factors, as shown in Figure 2 of the correlation heatmap of the PaySim dataset characteristics. Most features exhibit weak to moderate correlations, while stronger correlations are visible between derived balance difference features and their original counterparts. Transaction type and direction variables display minimal correlation with numerical attributes, confirming their independence. Overall, the heatmap indicates that the dataset provides diverse features with limited redundancy, making it suitable for effective fraud detection modeling.

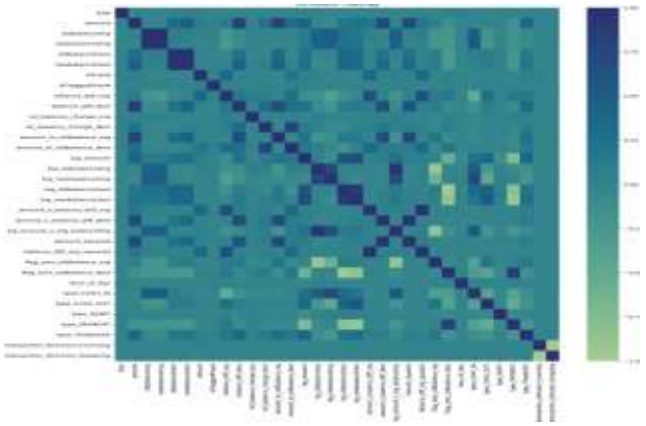

Fig. 2. Correlation Heatmap of dataset features

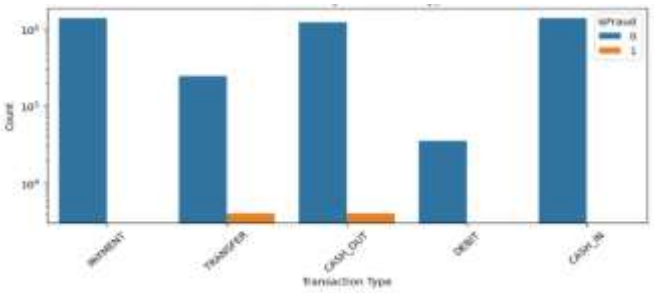

Fig. 3. Fraud count by Transaction Type

Figure 3 shows the breakdown of the PaySim dataset by transaction type in terms of fraudulent and non-fraudulent occurrences. Using a logarithmic scale for count, the bar chart reveals that PAYMENT and CASH_IN transactions dominate in volume but exhibit negligible fraud activity. In contrast, TRANSFER and CASH_OUT transactions show a significant presence of fraud, indicated by the orange bars, suggesting these types are more vulnerable to malicious behavior. DEBIT transactions appear infrequent and show minimal fraud. This visualization highlights the importance of transaction-type-specific analysis in designing targeted fraud detection strategies.

B. Data Preprocessing

Data preprocessing, cleansing, and preparation are the fundamental steps in data preparation before feeding it into ML algorithms to get high performance. Problems with categorical characteristics, class imbalance, and other similar issues arise in study. That could be affecting how well the chosen ML approach works. By utilizing several methods of preparation outlined below:

- **Check Statistics:** The summary statistics of the variables are presented before the analysis begins. The range of values at different percentiles, standard deviation, and mean are all used to evaluate numerical variables.
- **Remove outliers:** Reducing the model's ability to detect real fraud cases may result from removing outliers, which could remove important indicators of fraudulent activity.

C. Label-Encoding

The numerical value of each distinct textual value is determined by its sequence in this categorical data encoding approach. The integer value that represents each category is different from the other [17]. When dealing with ordinal relationships between categories or when utilizing algorithms that can directly handle integer inputs, label encoding is the way to go. Because it only involves replacing the categorical values with numerical labels, label encoding has the main benefit of not increasing the dataset size.

D. Normalization using MinMaxScaler

Attributes with very high or very low values can overwhelm the learning process if normalization is not used. A common method for normalizing data such that it can only take values between 0 and 1 or -1 and 1 is Min-Max Scaling. The normalization formula known as Min-Max is Equation (1):

$$X_{scaled} = \frac{x - x_{min}}{x_{maz} - x_{min}} \quad (1)$$

A feature's initial value is denoted by x, the minimum value is denoted as $\min(x)$, and the maximum value is $\max(x)$. Xnorm is the symbol for the normalized value.

E. Data balancing with SMOTE

Model performance in financial fraud detection can be hindered, particularly when it comes to detecting rare instances of fraud, by a class imbalance, which occurs when the quantity of genuine transactions greatly exceeds that of fraudulent ones. In order to cope with this, synthetic samples for the minority class are generated using SMOTE. This is achieved by interpolating between current instances and their closest neighbors in feature space.

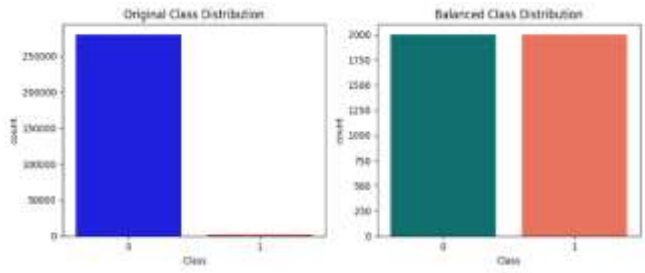

Fig. 4. Class Distribution Before and After Balancing

Data balance affects class distribution, as shown in Figure 4. The left panel shows the original distribution, where class "0" overwhelmingly dominates with over 275,000 instances, while class "1" is severely underrepresented highlighting a significant class imbalance. In contrast, the right panel presents the balanced distribution achieved through resampling techniques, where both classes are equalized to approximately 1,750 instances each. This preprocessing step is crucial for mitigating bias during model training and enhancing the classifier's ability.

F. Data Splitting

The term "data splitting" describes the process of dividing up a large dataset into two parts: a "training set" for training models and a "test set" for testing those models. The ratio was 80:20, meaning that using 80% of the dataset for training the model to make it better in the end, and 20% for evaluating it.

G. Proposed XGBoost Model

XGBoost is a gradient boosting decision tree ensemble that is very scalable. Like gradient boosting, XGBoost builds an additive extension of the objective function by minimizing a loss function [18][19]. The classifiers in XGBoost are built entirely on decision trees, therefore to control the complexity of the trees, a variation of the loss function is used, as shown in Equations (2), (3).

$$L_{xgb} = \sum_{i=1}^{N} L(y_i, F(X_i)) + \sum_{m=i}^{M} \Omega(h_m) \quad (2)$$

$$\Omega(h) = \gamma \mathbf{T} + \frac{1}{2}\lambda \|\boldsymbol{w}\|^2 \quad (3)$$

$\boldsymbol{w}$ are the leaf output scores, and $\mathbf{T}$ is the tree's leaf count. By including this loss function in the split criterion of decision trees, a pre-pruning strategy can be accomplished. As the value of γ grows, trees get simpler. The amount of γ determines the minimal gain needed to reduce loss in order to isolate an internal node.

H. Model Evaluation

Metrics for performance are crucial for gauging the ACC, efficiency, and dependability of a model. F1, REC, PRE, and ACC are some of the metrics used to quantify different parts of categorization performance. The four elements of a confusion matrix—TP, TN, FP, and FN are the basis for these. When evaluating the parameters, the most important things to bear in mind are:

- **True positive (TP):** Financial dealings that have been revealed to be dishonest.
- **True Negative (TN):** All transactions have been duly verified and acknowledged.
- **False positive (FP):** Honest deals that were falsely accused of fraud.
- **False Negative (FN):** unethical practices that are incorrectly thought of as legitimate.

Accuracy: ACC is the primary criteria used to assess DL classification models. It is calculated as follows Equation (4):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

Precision: Measures the proportion of samples identified as fraudulent that are fraudulent. It reflects the classifier's reliability when it predicts a positive result in Equation (5):

$$Precision = \frac{TN}{TN+FP} \quad (5)$$

Recall: It also known as Detection Rate, TPR, or Sensitivity. Identifies the fraction of valid samples that the classifier is able to identify using a specific Equation (6):

$$\text{Recall} = \frac{TP}{TP+FN} \quad (6)$$

F1-score: A fair compromise between PRE and REC, represented by their harmonic mean. It shines in cases where the given Equation (7) produces an uneven distribution of classes.

$$\text{F1} - \text{Score} = 2 \times \frac{(Precision \times Recall)}{Precision + Recall} \quad (7)$$

ROC curve: TPR and FPR are plotted against each other on the y-axis in the ROC-curve. Values close to 1 indicate a better model in the AUC measure of discrimination.

IV. Result Analysis and Discussion

The deployment of an XGBoost model to identify fraudulent transactions in mobile payment systems is the focus of this study. Studies were conducted using the PaySim dataset, which simulates the activities of real mobile money transfers. The experimental system ran Windows 11, had 16 GB of RAM, and was powered by an Intel(R) Core (TM) i7 processor running at 2.8 GHz. To analyze data, train the model, and assess the findings, Jupyter Notebook was utilized in a Python environment with libraries including Pandas, NumPy, Scikit-Learn, and TensorFlow. Table II shows, that the XGBoost model demonstrated high ACC, PRE, REC, and F1, which is in accordance with the fact that the XGBoost model is robust enough to identify fraudulent relationships and has few false alarms.

TABLE II. Propose Model Performance of XGBoost on Paysim Dataset

Matrix	XGBoost
Accuracy	99.6
Precision	99.8
Recall	98.7
F-1 score	99.8

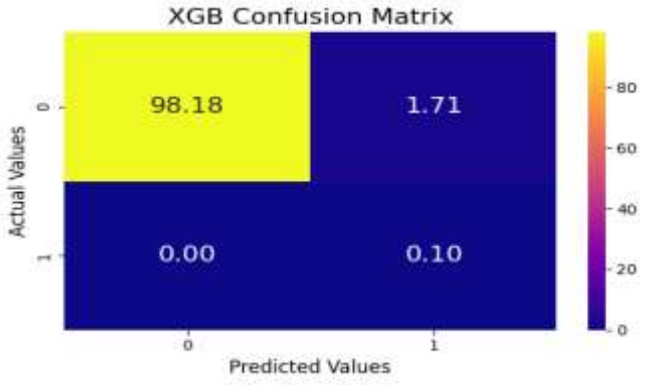

Fig. 5. Confusion matrix of XGBoost model

The XGBoost model's confusion matrix, shown in Figure 5, demonstrates its ability to classify fraudulent transactions. Based on the confusion matrix, it is clear that the XGBoost model has a low rate of false positives and negatives and can accurately identify both real and fraudulent transactions. Such high ACC and REC render it very reliable in detecting mobile payment fraud with a balance between protection and its ease of use.

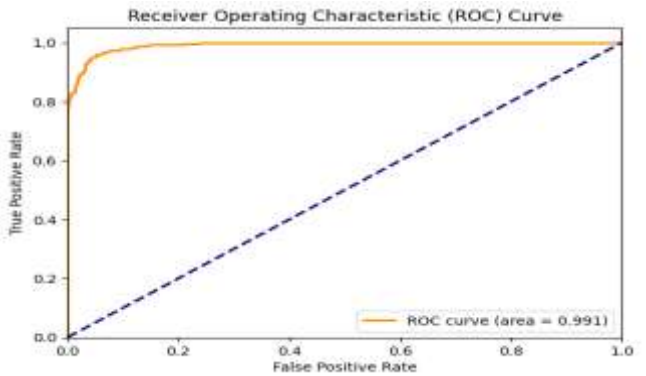

Fig. 6. ROC curve of XGBoost model

The ROC curve demonstrates that the XGBoost model has outstanding results, with the high TPR and the very low FPR. High discriminating power between good and poor transactions is shown by the curvature of the curve, which is closely directed towards the top-left corner. Having an AUC of 0.991 as presented in Figure 6, the model is virtually perfect in terms of classification and is thus quite useful in fraud detection tasks in which both of these errors are extremely important to minimize.

A. Comparison and Discussion

XGBoost on PaySim fraud detection data set dramatically outperforms both BERT and DenseNet in all evaluation metrics as demonstrated in Table III. In comparison, BERT performs moderately with the ACC of 89.6%, PRE of 89.6, and REC of 91.2% and F1 of 90.4%, whereas DenseNet performs slightly worse, with its ACC equal to 88.6, PRE equal to 83.7%, and REC equal to 88.2%. The findings underscore the strength and dependability of XGBoost in the fraud detection activities on transactional information.

TABLE III. Comparative Performance on PaySim dataset for fraud detection

Matrix	**BERT**[20]	**DenseNet** [21]	**XGBoost**
Accuracy	89.6	87.9	99.6
Precision	89.6	83.7	99.8
Recall	91.2	88.2	98.7
F1 Score	90.4	88.6	99.8

The XGBoost-based fraud detecting system suggested has significant benefits in regard to ACC, scalability, and efficiency in operation. It has the capacity to distinguish effectively between valid transactions and fraudulent transactions and as a result it is a good defense against financial threats in mobile payment systems. In comparison to DL models, XGBoost has better generalization and lower training times, which is why it is good to use in real-time. Combination of sound preprocessing measures such as normalization, label encoding, and data balancing improve the performance of the model and decrease bias. Altogether, the design of the framework facilitates high ACC of detection and low false alarms, which are part of safe and easy to use financial environments.

V. Conclusion and Future Scope

The modern growth of mobile payment systems has enhanced the threat of financial fraud that requires the elaboration of superior fraud detection methods and the alleviation of financial fraud in synthetic transaction networks, with a specific focus on the dynamic role of high-risk nodes. Based on the output of the PaySim simulator, a multistage fraud detection pipeline was developed which used complex ML. In the pipeline, the intensive preprocessing, class balancing using SMOTE and optimization of XGBoost classifier were used to learn intricate transactional patterns with a reduced number of false positives. It was experimentally validated that the proposed framework produced high ACC (99.6%), PRE (99.8%), REC (98.7%) and AUC (0.991%), which surpassed the existing models, including Bert and DenseNets. These findings demonstrate that blending graph-driven insights with powerful machine learning algorithms provides a scalable and reliable approach to identifying fraudulent behavior in mobile money ecosystems.

Future research can extend this work by incorporating real-time graph analytics and dynamic node-risk scoring to

track evolving fraud networks as transactions occur. Expanding evaluation to multi-source, real-world datasets and deploying the model within streaming environments will further validate its effectiveness, enabling proactive fraud prevention and improved anti-money-laundering compliance in rapidly changing digital payment landscapes.

REFERENCES

[1] S. Wawge, "A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 1–8, 2025.

[2] H. P. Kapadia, "API-Driven Banking: How COVID-19 Remote Work Boosted Open Banking and Fintech Integrations," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 10, pp. f514–f519, 2021.

[3] Z. Li, G. Liu, and C. Jiang, "Deep Representation Learning With Full Center Loss for Credit Card Fraud Detection," *IEEE Trans. Comput. Soc. Syst.*, vol. 7, no. 2, pp. 569–579, 2020, doi: 10.1109/TCSS.2020.2970805.

[4] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, "Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality," in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, IEEE, Aug. 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730334.

[5] M. E. Lokanan, "Predicting mobile money transaction fraud using machine learning algorithms," *Appl. AI Lett.*, vol. 4, no. 2, Apr. 2023, doi: 10.1002/ail2.85.

[6] L. Jia, X. Song, and D. Hall, "Influence of Habits on Mobile Payment Acceptance: An Ecosystem Perspective," *Inf. Syst. Front.*, vol. 24, no. 1, pp. 247–266, Feb. 2022, doi: 10.1007/s10796-020-10077-6.

[7] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 10, pp. 101–110, 2025, doi: 10.48175/IJARSCT-25619.

[8] V. Verma, "Deep Learning-Based Fraud Detection in Financial Transactions: A Case Study Using Real-Time Data Streams," *ESP J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 149–157, 2023, doi: 10.56472/25832646/JETA-V3I8P117.

[9] M. Lokanan and S. Liu, "Predicting Fraud Victimization Using Classical Machine Learning," *Entropy*, vol. 23, no. 3, 2021, doi: 10.3390/e23030300.

[10] K. B. Thakkar and H. P. Kapadia, "The Roadmap to Digital Transformation in Banking: Advancing Credit Card Fraud Detection with Hybrid Deep Learning Model," in *2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST)*, IEEE, Apr. 2025, pp. 1–6. doi: 10.1109/ICTEST64710.2025.11042822.

[11] R. U, M. P. Raj, J. N. Mithra, S. B. S, A. N. L, and J. M. Dass Y, "A Robust UPI Fraud Identification Scheme over Digital Money Transactions using Learning Powered Classification Principles," in *2025 International Conference on Electronics and Renewable Systems (ICEARS)*, 2025, pp. 1551–1558. doi: 10.1109/ICEARS64219.2025.10941576.

[12] K. S. A, P. M, and S. J, "Enhancing UPI Fraud Detection Accuracy Using Isolation Forest: A Novel Machine Learning Approach," in *2025 International Conference on Emerging Technologies in Engineering Applications (ICETEA)*, IEEE, Jun. 2025, pp. 1–5. doi: 10.1109/ICETEA64585.2025.11099839.

[13] Z. Ke, S. Zhou, Y. Zhou, C. H. Chang, and R. Zhang, "Detection of AI Deepfake and Fraud in Online Payments Using GAN-Based Models," in *2025 8th International Conference on Advanced Algorithms and Control Engineering (ICAACE)*, 2025, pp. 1786–1790. doi: 10.1109/ICAACE65325.2025.11020513.

[14] S. C S, S. Yadav, B. R. Kumar, S. Baranidharan, T. Vijayaraj, and P. K. Lakineni, "A Novel Network-Based Digital Payment Fraud Detection using OP-ELM Network," in *2025 3rd International Conference on Data Science and Information System (ICDSIS)*, 2025, pp. 1–6. doi: 10.1109/ICDSIS65355.2025.11070833.

[15] A. Y. Shdefat, M. Mohamed, S. Khaled, F. Hany, H. Fathi, and D. S. AbdElminaam, "Comparative Analysis of Machine Learning Models in Online Payment Fraud Prediction," in *2024 Intelligent Methods, Systems, and Applications (IMSA)*, 2024, pp. 243–250. doi: 10.1109/IMSA61967.2024.10652861.

[16] D. Singh, "Protecting Contactless Credit Card Payments from Fraud through Ambient Authentication and Machine Learning," in *ACCESS 2023 - 2023 3rd International Conference on Advances in Computing, Communication, Embedded and Secure Systems*, 2023. doi: 10.1109/ACCESS57397.2023.10200022.

[17] C. R. Kishore and H. S. Behera, "Malware Attack Detection in Vehicle Cyber Physical System for Planning and Control Using Deep Learning," in *Intelligent Systems Reference Library*, vol. 60, Springer Nature Switzerland, 2024, pp. 167–193. doi: 10.1007/978-3-031-54038-7_6.

[18] N. Prajapati, "The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications," *ESP J. Eng. Technol. Adv.*, vol. 5, no. 2, pp. 16–22, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[19] R. Q. Majumder, "Machine Learning for Predictive Analytics: Trends and Future Directions," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 04, pp. 3557–3564, 2025.

[20] A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," *IEEE Access*, vol. 11, no. December, pp. 137188–137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[21] H. Fanai and H. Abbasimehr, "A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection," *Expert Syst. Appl.*, 2023, doi: 10.1016/j.eswa.2023.119562.

