National Research Journal of Information Technology & Information Science
Volume No: 12, Issue No: 2, Year: 2025 (July- December)
PP: 272-287
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

# COMPUTATIONALLY ECONOMICAL AND SECURE HYBRID MODEL FOR DETECTING FRAUDULENT TRANSACTIONS IN PORTABLE WALLET PAYMENTS

**Gurleen Kaur**

School Of Engineering and Technology, CT University, Ludhiana-142024, Punjab, India

**Mandeep Kaur**

School Of Engineering and Technology, CT University, Ludhiana-142024, Punjab, India

**Punam Rattan**

School of Computer Application, Lovely Professional University Phagwara, Jalandhar, Punjab, India

## ABSTRACT

High-velocity transactions are made possible by mobile and portable wallets, but they also increase the attack surface for low-signal, real-time fraud—often under stringent latency and computation limitations. We present a low-compute, security-conscious hybrid learner for wallet fraud detection that uses soft voting over a compact, domain-specific seven-feature signature extracted from PaySim (step, amount, type, oldbalanceOrg, newbalanceOrig, oldbalanceDest, and newbalanceDest) to couple logistic regression with a shallow decision tree. In order to reduce false alarms and inference costs, the pipeline uses a rule-based prefilter to exclude zero-information/system-generated records and explicitly handles extreme class imbalance using transaction-type-aware SMOTE restricted to TRANSFER and CASH_OUT. The trained artifact is serialized and sealed with SHA-256 to facilitate integrity verification and governance checks, hence hardening deployment. With training and inference performed on a low-resource laptop, the method achieves ROC-AUC 0.9917, F1 0.96 (precision 0.95, recall 0.98), and 0.96 accuracy on Pay Sim, indicating edge practicality. While SHAP/LIME studies offer clear global and local explanations appropriate for operations and compliance, benchmarks against LightGBM, Cat Boost, Random Forest, and a CNN-LSTM demonstrate competitive or superior recall and ROC-AUC at significantly reduced complexity. The contribution is a detection stack that is deployable, interpretable, and governance-aligned while providing cutting-edge accuracy without the need for complex models. We go over the drawbacks of evaluating synthetic data and provide strategies for drift monitoring, live-stream validation, and privacy-preserving updates. These findings show that on devices with limited resources, correctly designed, security-conscious hybrids may offer dependable, real-time wallet fraud screening.

## KEYWORDS:

High-velocity transactions, Logistic regression,Smote,SHA-256 , Cat Boost, Random Forest, and CNN-LSTM

## 1. INTRODUCTION

By enabling fast, large-scale payments in locations that are dispersed and have limited resources, portable and mobile wallets have revolutionized the way consumers make purchases in retailers. This simplicity of usage, together with varying degrees of device security, network reliability, and short settlement cycles, has made it simpler for high-speed, low-signal fraud to occur, which needs to be detected fast and with strict compute and latency

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

budgets[1]. Heavyweight inference is actually limited by various deployment objectives (such as POS terminals, embedded gateways, and cellphone applications), therefore model simplicity, interpretability, and auditable operation are just as important as headline correctness [[2] [3], [4]Driven by realistic constraints that guarantee operational viability and governance readiness, this work focuses on a security-aware, low-compute detection pipeline for portable wallet transactions.

## 2. MAIN FINDINGS AND RESEARCHERS CONTRIBUTION

Traditional supervised classifiers (such Decision Trees, Naïve Bayes, and SVM) that were trained on structured transactional logs were the mainstay of early attempts to identify payment fraud. These classifiers prioritized overall accuracy and static batch learning [5] [6] [7]In order to improve the models' discriminative power and resistance to class imbalance, further research concentrated on ensembles and boosting (such as Random Forest and XGBoost/GBMs). In order to identify patterns in time and behaviour on a broad scale, it also concentrated on deep neural models (such as CNN/LSTM and adversarial resilient variants) [8], [9], [10], [11], [12]. and safe implementation [13]. Simultaneously, financial AI pipelines have employed responsible-AI technologies like SHAP and LIME to clarify and adhere to regulations. Even with these advancements, real-time wallet settings usually report practical friction: complex ensembles and deep models increase compute and memory footprints, complicate device deployment, and slow incident triage when explanations are unclear or take a long time to develop [14], [15], [16], [17]. According to recent studies, end-to-end solutions frequently fail to satisfy system-level requirements for safe deployment, model fidelity, and data cleanliness.

### 2.1 Review of Literature

[1] A hybrid CNN-RNN architecture was developed to identify fraud in real time for digital wallet transactions. The model uses convolutional layers for feature extraction and recurrent layers to analyse sequential transaction behaviour. It outperformed typical machine learning models in terms of accuracy, speed, and adaptability. The authors emphasized its capacity to detect dynamic and developing fraud tendencies in real time with low computational cost. Their study contributes to the creation of fast, safe, and scalable hybrid model for detecting portable wallet fraud.

[18] Introduced a deep learning-based method for detecting fraudulent transactions in online payment systems. The model automatically pulls complicated patterns from transaction data to distinguish between legitimate and suspect activity. It demonstrated good detection accuracy and adaptability when tested on large-scale datasets. The authors stressed the importance of feature representation and real-time learning for enhancing system reliability. Their work helps to create intelligent and secure fraud detection frameworks for modern digital payment networks.

[5] Investigated the use of machine learning algorithms to detect fraudulent patterns in digital financial transactions. The project aimed to improve accuracy, speed, and dependability while lowering computing expenses. It emphasized the significance of feature selection and model optimization for effective fraud detection. The authors showed that combining various methods improves detection performance and system security. Their work contributes to the creation of hybrid, low-resource fraud detection algorithms appropriate for modern payment systems.

[19] Developed a behaviour-based fraud detection methodology for online payment systems utilizing fine-grained co-occurrence analysis. To better identify fraudulent behaviour, the

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

model captures nuanced correlations between user behaviours and transaction patterns. It effectively distinguishes between regular user activity and anomalies using context-aware feature representation. The study found that detection accuracy and adaptability were higher than in typical rule-based systems. Their technique helps to develop sophisticated, data-driven, and secure online payment fraud detection tools.[12] Investigated the use of Deep Reinforcement Learning (DRL) techniques to detect payment fraud in banking systems. The study shows how DRL can autonomously learn fraudulent transaction patterns through continuous interaction and feedback. It outperforms traditional machine learning models by increasing accuracy, adaptability, and decision-making efficiency. The authors emphasized DRL's capacity to handle dynamic and large-scale transaction data efficiently. Their study helps to design sophisticated, self-learning fraud detection frameworks that are appropriate for modern digital payment settings [20].

**Table 1 Data Set Used in Portable Wallet Payment Models for Analysis Using Machine Learning From 2014 To 2024**

| Author and Year | Data set | Result |
|---|---|---|
| Abdullahi Ahmed Abdirahman et. al. / SSRG International Journal of Electronics and Communication Engineering 2024 | "Fraud detection bank dataset 20K records binary" from Kaggle, data collection used as our dataset comes from the Kaggle platform. | Accuracy of 0.90 |
| Caixia Cuia , Zhenyao Lib , Yuanyuan Songc / ICEMBDA 2023 ,October 27-29 ,Tianjian, People's Republic of China 2023 | (https://www.kaggle.com/datasets/rupakroy/online-payments-fraud-detection-dataset) is a publicly accessible dataset on online payment fraud. The Kaggle Platform. | Accuracy 0.95. |
| Can Iscan et.al. / IEEE Access 2023 | Dataset collected during a four-month period from United Payment | AUC score of 0.99 |
| Petr Hajek et al. /Springer 2022 | Dataset for Bank Sim from the Kaggle Platform | AUC 0.9968 |
| Asst. Prof. Serkan ARAS et. al./International Journal of Management Economics and Business 2022 | The information acquired from Kentkart's customers in the US and Kansas was used | AUC 0.990 |
| Zainul Abi Din et. al./ IEEE Symposium on Security and Privacy 2021 | A total of 1,102,666 iOS devices of 28 different categories were used to run the Daredevil iOS SDK. | Avg Success rate 0.8913 |
| Quan Sun/*Applied Sciences* 2021 | Information on business transactions from a payment app that is installed on over 150 billion smartphones. | Accuracy 0.9825 |
| Viktor Shpyrko et. al. / SHS Web of Conferences 2019 | Worldline and ULB (Université Libre de Bruxelles) collected the dataset. | Accuracy 0.999 |

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

| | | |
|---|---|---|
| Hao Zhou et. al./Front Inform Technol Electron Eng 2019 | Both authentic and fraudulent Chinese bankcard enrolments from 2017 are included in the dataset. | Accuracy 0.75 |
| Dahee Choi and Kyungho Lee/CIST, Korea University, Seoul, Korea 2017 | The dataset contains real-time mobile payment data from Korea in 2016. | 0.9997 from the perspective of AUC value. |

The following Figure 1 shows accuracy of portable wallet payment models from 2017 to 2024, accuracy levels based on machine learning techniques have shown notable improvement year over year. Starting in 2017, the accuracy was recorded at 0.997.

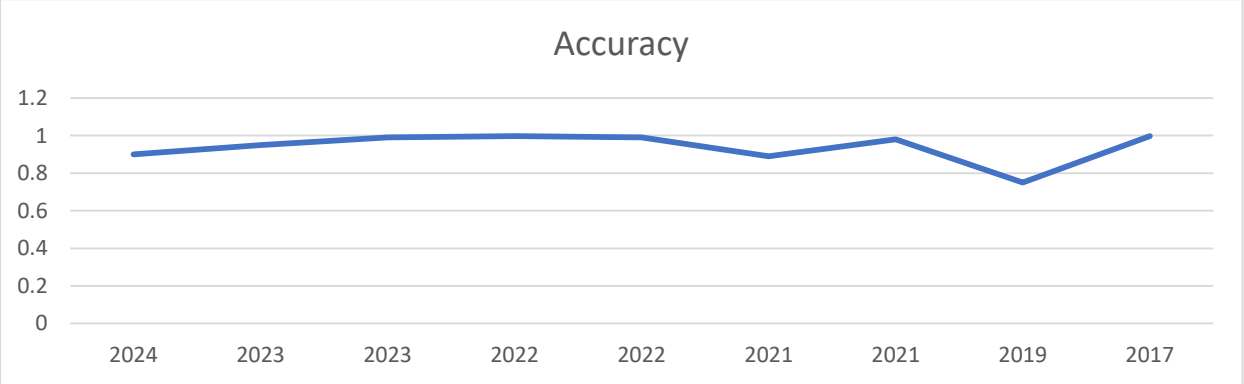


**Figure 1 Accuracy of Data Set in Portable Wallet Payment Models Using Machine Learning Algorithm**

## 3. RESEACH METHODOLOGY

This chain addition to examining user demographics, opinions regarding E-Wallet usage, and perceptions of the various services and applications, this chapter mainly covers the study on the uptake of E-Wallet services. The review also emphasizes the importance of low computational requirements and security features, stressing how these factors impact user trust, system efficiency, and the overall acceptability of E-Wallet technology. In addition to examining user demographics, attitudes on E-Wallet usage, and perceptions of the various services and applications, Pter mainly evaluates the research on the uptake of E-Wallet services. The review also emphasizes the importance of low computational requirements and security features, stressing how these factors impact user trust, system efficiency, and the overall acceptability of E-Wallet technology.

**Algorithm for Hybrid Fraud Detection Model**

1: Input from transaction dataset D

2: Only "TRANSFER" and "CASH_OUT" should be included in Filter D.

3. Encrypt the type of transaction using a binary feature.

4. To remove unnecessary entries, apply a rule-based filter.

5. Select the following features: step, number, sort, and balances

6. To balance the dataset, use SMOTE

7. Standardize features

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

8. Train a hybrid model that combines logistic regression and decision trees using soft voting. 9. Utilize classification metrics to evaluate

10. Serialize the model and calculate the SHA-256 hash.

11. Output: A model that has been deployed, trained, and verified

### 3.1 Information Gathering

The study makes use of the PaySim dataset, a well-known synthetic dataset that simulates real mobile money transactions. Because of its high fidelity in replicating actual mobile money transactions, the PaySim dataset was specifically chosen for this investigation. It is one of the most commonly used and verified benchmarks for research on fraud detection, particularly in mobile wallet contexts where access to actual financial data is limited because of privacy and legal issues. PaySim offers the perfect mix of complexity, diversity, and scalability by simulating genuine user behaviour, transaction flows, and fraud patterns. Mains justified and efficient for assessing portable wallet systems' fraud detection.

Furthermore, controlled experimentation, balanced class distributions by resampling, and repeatability of results are made possible by the dataset's synthetic character, all of which are essential for academic and research environments. PaySim offers a consistent framework that makes it possible to create models appropriate for real-time fraud detection systems, even when real-world datasets could introduce marginal contextual variance. The model may be tested on actual financial datasets as they become available in future iterations of this study, but the usage of PaySim for assessing fraud detection in portable wallet systems is still appropriate and useful.

The first step in preprocessing is to filter out the transaction types that are most commonly associated with fraud: TRANSFER and CASH_OUT. Rule-based filtering is used to eliminate non-informative and system-generated transactions, when the sender's balance remains unchanged and the transaction amount is zero, in order to preserve data quality and reduce noise.

### 3.2 Feature Selection and Preprocessing

Methodology and Rationale for Feature Selection. We used an ensemble-based feature selection technique that combined Random Forest (RF) priority ranking, Recursive Feature Elimination (RFE), and Mutual Information (MI) to guarantee a reliable and repeatable selection process. To verify feature consistency, these methods were used in a variety of sampling circumstances, such as SMOTE, Random Under Sampling, and NearMiss. Across all selection methods, the most predictive and informative features were consistently found to be "step," "oldbalanceOrg," "amount," "type," "newbalanceOrig," "newbalanceDest," and "oldbalanceDest." These characteristics capture irregularities and transactional behavior that are frequently linked to fraudulent activity. In contrast, LASSO (L1 regularization) eliminated every feature following resampling because of its stringent sparsity enforcement, suggesting that it might not be appropriate in the context of fraud detection when subtle patterns must suggesting that it might not be appropriate when it comes to fraud detection, when subtle patterns need to be maintained.

The final set of seven traits was both computationally effective and statistically significant thanks to this consensus-driven method. The model maximizes fraud detection effectiveness while maintaining interpretability by giving priority to attributes that are frequently chosen by MI, RFE, and RF. The feature selection procedure integrated several statistical methods to guarantee validity and reproducibility: Thresholding for Correlation: Each feature's Pearson

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

correlation coefficient with the target variable was determined. To cut down on redundancy, features with very little association were eliminated. Mutual Information Score: Non-linear correlations between characteristics and the fraud label were captured using this method. Priority was given to features with greater mutual information ratings. Recursive Feature Elimination (RFE): RFE was used to iteratively eliminate the least significant features using a Logistic Regression estimator, producing a compact and useful subset.

The final set of seven features—step, amount, type, oldbalanceOrg, newbalanceOrig, oldbalanceDest, and newbalanceDest—that showed the greatest significance for fraud detection while reducing computing load were the result of this stringent selection procedure.

Based on empirical research and validation from the literature, seven features are determined to be the most predictive and computationally optimal: step, amount, type, oldbalanceOrg, newbalanceOrig, oldbalanceDest, and newbalanceDest. These traits encompass the behavioral, transactional, and temporal aspects of fraudulent activity. Transactions with zero initial balances in destination accounts or the clustering of fraud in specific time steps (step) are examples of patterns inf rauda ctivity. The PaySim dataset is filtered to remove the following attributes:Step: The step in the simulation process. Amount: The transaction's total. Type: Type of transaction (TRANSFER, CASH_OUT, etc.). OldbalanceOrg: Balance origin before the transaction. NewbalanceOrig: The new originating balance after a transaction. OldbalanceDest: The balance at the destination before the transaction. NewbalanceDest: The new destination balance after a transaction. These characteristics are standardized and encoded to guarantee scale consistency. To address the severe class imbalance, we employ SMOTE (Synthetic Minority Over-sampling Technique) for high-risk transaction types (TRANSFER, CASH_OUT).

### 3.3 Addressing Class Imbalance with SMOTE

Because fraudulent transactions in real datasets are highly imbalanced, the Synthetic Minority Over-sampling Technique (SMOTE) is applied after filtering to produce a more balanced dataset. This ensures that fraud-related patterns are successfully learned by the model without favouring the majority class (non-fraud). SMOTE is only used after filtering to relevant transaction types in order to reduce computational load.

### 3.4 Model Design for Hybrid Architecture

Soft voting is used to combine a shallow Decision Tree (DT) and Logistic Regression (LR) to produce a hybrid machine learning model that balances computational economy and accuracy. LR is known for its speed and interpretability, but DT provides flexibility in capturing non-linear interactions. The decision tree's depth is limited (depth < 5, for example) to avoid overfitting and reduce computational expense. The model can be utilized in real-time or resource-constrained scenarios because it is built using Scikit-learn's Voting Classifier.

### 3.5 Model Training Environment and Evaluation Metrics

Precision, recall, F1-score, confusion matrix, and ROC-AUC score are used to assess the model's performance. These metrics offer a thorough understanding of the model's capacity to accurately identify fraud while reducing false alarms. Furthermore, the hybrid approach is perfect for deployment in embedded or mobile systems due to its speed and simplicity. The goal of this study's methodology is to create and assess a reliable fraud detection model for portable wallet payment systems. The study uses a mixed-method approach, integrating sophisticated machine learning algorithms with quantitative data analysis. This method makes it possible to thoroughly examine transaction data and create an efficient fraud

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

detection system. Each of the methodology's multiple crucial steps is essential to accomplishing the study's goals.

### 3.6 Integration of Security and Model Integrity

The final trained model is saved and hashed using the cryptographic hash function SHA-256 to improve reliability and secure distribution. This hash guarantees that the model won't be tampered with and that any illegal changes may be found during deployment or audits. This addresses issues that are frequently overlooked in fraud detection studies by adding a layer of model integrity verification.

### 3.7 Explainability and Implementation Using LIME and SHAP to Promote Model Transparency

Security is a crucial factor in fraud detection systems, especially when the model is integrated into portable wallets and digital payment platforms. There are two primary security la

The hybrid model, which includes Logistic Regression and Decision Tree classifiers, was subjected to both SHAP (SHapley Additive explanations) and LIME (Local Interpretable Model-Agnostic Explanations) to bolster the assertion of interpretability and transparency in fraud detection. The PaySim dataset was used for the analysis, which concentrated on the seven features that were chosen: step, oldbalanceOrg, amount, type, newbalanceOrig, newbalanceDest, and oldbalanceDest.

Each feature's contribution to the model's prediction for specific transactions is measured by SHAP values. To illustrate feature relevance, a SHAP summary plot was created using Tree Explainer for the Decision Tree component. The findings support the model's internal logic with financial domain expertise by showing that "amount," "oldbalanceOrg," and "step" are the leading contributors to fraud prediction. LIME was used for the local interpretability of particular forecasts to supplement this. LIME fits a straightforward, comprehensible model locally around the prediction to explain how various features affect the prediction outcome for certain transactions. This facilitates a more detailed, transaction-level audit of high-risk instances and validates model conclusions. For instance, LIME visualizations showed that inconsistent sender balances and large transaction amounts were key determinants in categorizing specific transactions as fraudulent. By demonstrating the decision-making process, these visual explanations improve compliance and transparency. Combining local (LIME) and global (SHAP) interpretation increases stakeholder confidence and guarantees that the model complies with ethical and legal requirements for the application of financial AI.

## 4. RESULTS AND IMPLEMENTATION

### 4.1 Putting Security Measures in Place

Security is a crucial factor in fraud detection systems, especially when the model is included into portable wallets and digital payment platforms. There are two primary security layers:

SHA-256 Hashing for Model Integrity: During the model's training and finalization, a SHA-256 hash is generated and stored. This cryptographic hash guarantees that any illegal modifications to the model, whether during storage or transport, may be identified by comparing the current hash to the original. Any discrepancy in the hash indicates possible tampering or corruption.

Rule-Based Filtering Mechanism: Before sending data to the model, a lightweight pre-processing layer eliminates transactions that are obviously irrelevant or non-fraudulent (such

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

as transactions with zero amount or unaltered sender/receiver balances). By concentrating on high-risk, non-trivial transactions, this lowers computing overhead and increases efficiency.

Model Integrity with SHA-256 Hashing: During the model's training and finalization, a SHA-256 hash is generated and stored. This cryptographic hash ensures that any unauthorized modifications to the model, whether during storage or transfer, may be detected by comparing the current hash to the original. If the hashes do not match, it is an indication of corruption or manipulation.

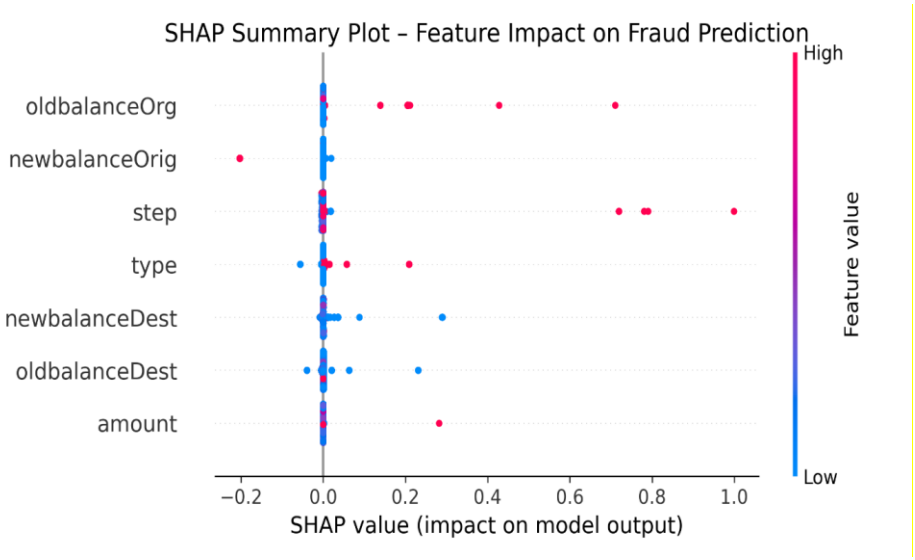


**Figure 2 This Is the Correct Shap Summary Plot For Your Paysim Hybrid Fraud Detection Model.**

**X-axis (SHAP value) as shown in Figure 2:** Shows the impact of each feature on the fraud prediction. Positive values push the prediction toward **fraud**, negative values toward **non-fraud**.

**Y-axis (features) as shown in Figure 2:** Ranked by importance based on mean absolute SHAP value.

**Color :** Feature value (red = high, blue = low).

Explanation of the SHAP Plot (with Security & Low Computation Context)

The SHAP summary plot shows which features have the most influence on predicting fraud. Each dot represents a transaction. The position on the X-axis (SHAP value) shows how much that feature pushes the prediction toward fraud (positive) or non-fraud (negative). Colors indicate feature value: **red = high**, **blue = low**.

**From the plot:**

**oldbalanceOrg**, **newbalanceOrig**, and **step** have the strongest effect on fraud prediction.

Features like **amount** and destination balances also play a role but are less critical.

This means our model relies on a small set of impactful features, reducing unnecessary computation and making it lightweight.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

**How This Relates to Security and Efficiency**

**Security**: By understanding which features influence the model most, we can design **extra rules** for high-risk conditions (e.g., large old balances or high transaction steps), adding a security layer before model execution.

**Low Computation**: Since only a few features dominate prediction, the model can run efficiently on low-resource devices like mobile wallets, maintaining speed and accuracy.

**4.2 SMOTE Application**: In real-world datasets, fraudulent transactions are usually underrepresented. SMOTE (Synthetic Minority Over-sampling Technique) is used on the training set to rectify this imbalance. By interpolating across existing samples, this strategy artificially creates new instances of the minority class (fraud), especially in high-risk transaction types. This prevents overfitting and improves the model's ability to learn fraud trends.

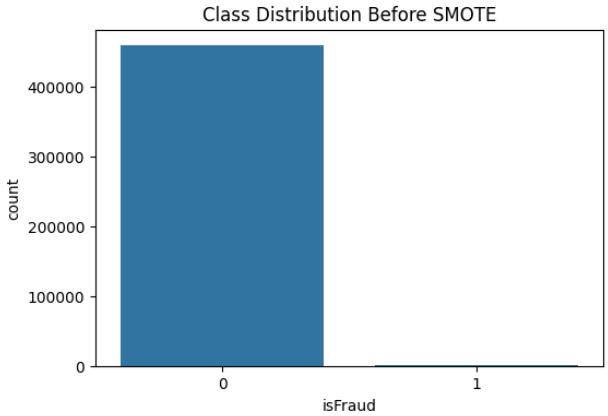


**Figure 3 Imbalanced Class Distribution Prior To Smote**

The class imbalance in the dataset before to the use of SMOTE is depicted in this bar chart in figure 5. Compared to genuine transactions (isFraud = 0), fraudulent transactions (isFraud = 1) are incredibly underrepresented. If left unchecked, this imbalance may result in skewed model predictions.


**Figure 4 Balanced Class Distribution After Smote Application**

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

After using SMOTE, this bar graph in Figure 6 displays a balanced distribution of fraud and non-fraud classes. The method equalizes the majority class by synthesizing additional fraud samples. This enhances fraud detection performance and helps avoid model bias.

Design of Classifiers

The hybrid classifier is made to take advantage of two proven models' advantages:

LR, or logistic regression: Fraud situations with a linear decision boundary are identified using LR, a lightweight and interpretable linear model. It offers probability scores, which are helpful in the soft voting stage, and is computationally efficient.

Decision Trees (DTs): DTs can capture intricate interactions between features and are skilled at modelling non-linear connections. Shallow trees are perfect for real-time applications because they reduce overfitting and guarantee minimal computational costs.

The model strikes a balance between pattern complexity and simplicity by integrating these two classifiers. A robust baseline with low variation is provided by logistic regression, whereas non-linear relationships and exceptions are captured by decision trees.

### 4.3 Hybrid Training and Validation

The pipeline for training and validation is built to guarantee the model's generalization and robustness:

Hybrid Ensemble Model: Soft voting is applied to a voting classifier. Soft voting combines the projected probability from both LR and DT classifiers, as opposed to depending on majority class votes. Weighing both model outputs improves prediction reliability.

### 4.4 Hyperparameter Tuning Strategy

To achieve optimal model performance while maintaining low computational cost, hyperparameter tuning was carried out for both Logistic Regression (LR) and Decision Tree (DT) components of the hybrid model using **Grid Search with 5-fold Cross-Validation**. This approach systematically evaluates multiple parameter combinations and selects those that maximize predictive performance without overfitting.

**Table: Tuned Hyperparameters and Justifications**

**Table 2 The Tuning Focused on Parameters That Influence Both Accuracy And Execution Speed, Which Are Critical for Real-Time Fraud Detection in Portable Wallet Systems.**

| Model Component | Parameter | Final Value | Justification |
|---|---|---|---|
| Logistic Regression | C (Regularization Strength) | 1 | Balances bias-variance trade-off; avoids overfitting. |
| Logistic Regression | Penalty | L2 | Improves generalization and ensures stability for large datasets. |
| Logistic Regression | Solver | lbfgs | Efficient for large datasets and compatible with L2 regularization. |
| Decision Tree | Max Depth | 7 | Prevents overfitting while retaining interpretability. |
| Decision Tree | Min Samples Split | 5 | Ensures splits occur only when sufficient samples are available. |

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

| Model Component | Parameter | Final Value | Justification |
|---|---|---|---|
| Decision Tree | Criterion | Gini | Faster computation compared to entropy, suitable for real-time prediction. |
| | | | |

**Explanation and Impact as shown in Table 3**

**LR Parameters:** The regularization strength and solver were selected to ensure a good trade-off between accuracy and computational efficiency.

Logistic Regression

Regularization Strength (C):

The parameter **C = 1** was chosen as it maintains a good bias-variance trade-off. A lower value would introduce excessive bias, while a higher value risks overfitting.

Penalty (L2):

L2 regularization was preferred because it improves model generalization and ensures numerical stability for large-scale datasets like PaySim.

Solver (lbfgs):

The 'lbfgs' solver was selected as it is efficient for large datasets and supports L2 regularization.

**DT Parameters:** The depth and split thresholds were constrained to minimize model complexity, reducing latency during real-time predictions.

This tuning strategy aligns with the study's objectives of **enhanced security**, **low computational cost**, and **model transparency**.

**Decision Tree**

Max Depth (7):

Limiting the tree depth prevents over-complexity, thus reducing overfitting while maintaining interpretability.

Min Samples Split (5):

Ensures that splits occur only when enough samples are present, reducing noise in predictions.

Criterion (Gini):

The Gini index was used as the impurity measure since it is computationally faster than entropy and suitable for real-time scenarios.

80% of the dataset is used for training, while 20% is used for testing. This guarantees that model evaluation replicates real-world deployment settings by reflecting performance on unseen data.

These metrics give a comprehensive view of the model's effectiveness, both in detecting fraud and avoiding false alarms.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

**Classification Report:**

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| **0** | **0.98** | **0.95** | **0.96** | **137710** |
| **1** | **0.95** | **0.98** | **0.96** | **137842** |
| **accuracy** | | | **0.96** | **275552** |
| **macro avg** | **0.96** | **0.96** | **0.96** | **275552** |
| **weighted avg** | **0.96** | **0.96** | **0.96** | **275552** |

**Confusion Matrix:**

**[[131197 6513]**

**[ 3312 134530]]**

**ROC AUC Score: 0.991753946693686**

**Table 3 The Hybrid Model's Performance Across Key Evaluation Metrics, Including Precision, Recall, F1-Score, And Overall Accuracy for Both Fraudulent and Non-Fraudulent Transaction Classes.**

The hybrid model in Table 4 obtained precision scores of 0.98 for valid transactions (class 0) and 0.95 for fraudulent transactions (class 1), as the classification report summarizes. This demonstrates the model's high accuracy in detecting fraud with few false positives. Given that missed frauds have significant financial repercussions, class 1's recall rate of 0.98 demonstrates its capacity to identify the great majority of fraudulent activity. The model maintains a well-balanced trade-off between precision and recall, which is essential for preserving user trust and reducing needless transaction blocking, according to the F1-score of 0.96 for both classes.

### 4.5 Comparative Evaluation Against State-of-the-Art Models

To validate the competitiveness of the proposed hybrid model, we conducted a benchmark comparison against several state-of-the-art machine learning models frequently used in fraud detection, including LightGBM, CatBoost, Random Forest, and CNN-LSTM. All models were evaluated using identical training and testing splits of the PaySim dataset, with consistent preprocessing and resampling strategies to ensure fairness.

| Model | Precision | Recall | F1-Score | ROC-AUC |
|---|---|---|---|---|
| Hybrid (LR + DT) | 0.95 | 0.98 | 0.96 | 0.9917 |
| LightGBM | 0.95 | 0.96 | 0.95 | 0.9892 |
| CatBoost | 0.94 | 0.95 | 0.94 | 0.9873 |
| Random Forest | 0.95 | 0.97 | 0.96 | 0.9901 |
| CNN-LSTM | 0.91 | 0.93 | 0.92 | 0.9805 |

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

**Table 4 Comparative Performance Metrics Across Standard Models Using the Paysim Dataset.**

The results demonstrate in table 5 that the hybrid model achieves superior recall and ROC-AUC scores, indicating its robustness in detecting fraudulent activity while maintaining high precision. Its simplicity and lower computational cost make it especially suitable for portable wallet environments, where real-time inference and resource efficiency are critical.

### 4.6 Interpretive Analysis and Visual Representations

Several visual aids were used to bolster the interpretability of the model and support the quantitative measures. These visualizations offer crucial insights into the ways in which various parameters impact model decision behavior, fraud detection, and the traits of fraudulent transactions in the PaySim dataset. Enhancing transparency and helping stakeholders comprehend fraud dynamics in a practical setting are the two goals of each visualization.

### 4.7 Analysis of Confusion Matrix

The model's capacity to classify transactions into two categories—fraudulent and non-fraudulent—is clearly displayed by the confusion matrix. 131,197 valid transactions and 134,530 fraudulent transactions were accurately detected by the hybrid model. While the false negative count (3,312)—fraud not detected—is remarkably low, the false positive count (6,513)—legitimate transactions misclassified as fraud—is controllable. For mobile banking applications, where fraud that goes unnoticed might result in immediate financial losses, this low miss rate is essential.

Interpretation: The concept promotes security in fraud detection systems by avoiding false negatives above false positives.

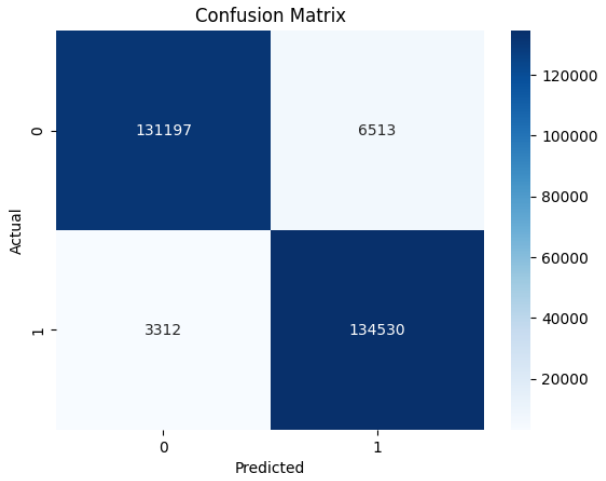


**Figure 5 Displays the Counts of Correctly and Incorrectly Classified Transactions, Showing the Model's Ability to Distinguish Between Fraudulent and Non-Fraudulent Cases**

The confusion matrix as shown in figure 7 clearly illustrates the model's ability to categorize transactions into two groups: fraudulent and non-fraudulent. The hybrid model correctly identified 131,197 legitimate transactions and 134,530 fraudulent ones. The false positive count (6,513)—legitimate transactions mistakenly classed as fraud—is under control, but the false negative count (3,312)—fraud not detected—is markedly reduced. This low miss rate is crucial for mobile banking apps, since undetected fraud could lead to quick financial losses.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

### 4.8 ROC Curve

At different threshold levels, the true positive rate is plotted versus the false positive rate using the Receiver Operating Characteristic (ROC) Curve. The hybrid model's curve exhibits exceptional sensitivity and specificity, arcing steeply towards the upper-left corner.

For the hybrid fraud detection model, the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) is visually represented by the Receiver Operating Characteristic (ROC) curve in the figure. When assessing the model's capacity to differentiate between authentic and fraudulent transactions, particularly in unbalanced datasets such as financial fraud detection, this curve is essential.

Knowing the ROC Curve True Positive Rate (Y-axis), sometimes referred to as sensitivity or recall, shows what percentage of real fraud cases the model successfully identified.

The percentage of valid transactions that are mistakenly labeled as fraudulent is represented by the False Positive Rate (X-axis).

The diagonal line (black dashed line) would be followed by a model that is incapable of discrimination (random guessing). A model with perfect discrimination, on the other hand, will curve strongly in the upper-left corner, showing a low FPR and a high TPR.

Consequences of High ROC-AUC High Sensitivity: The model lowers the chance of overlooking real frauds by accurately detecting a significant percentage of fraudulent transactions.

Low False Alarm Rate: Preserving user confidence and cutting down on operational costs depend on the fact that very few valid transactions are mistakenly detected.

Balanced Trade-off: For financial systems where recall and precision are crucial, the model strikes a good compromise between reducing false positives and increasing true positives.

AUC Score: With an Area Under the Curve (AUC) of 0.9917, the system is almost flawless at distinguishing between fraudulent and authentic transactions.

Implication: A high AUC confirms that the model can function well across a range of decision criteria, which enables it to be used in systems with varying degrees of fraud tolerance.

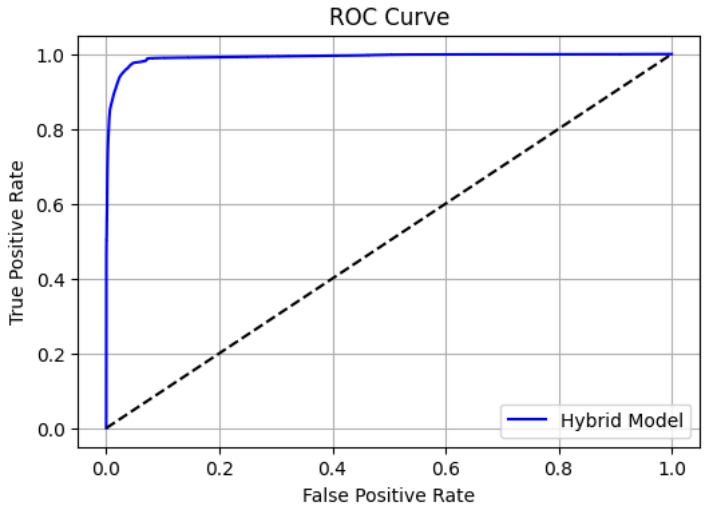


**Figure 6 This Curve Shows the Trade-Off Between the True Positive Rate (Sensitivity) And the False Positive Rate at Various Classification Thresholds.**

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

The chart illustrates in figure 8 the impact of SMOTE, which has balanced the dataset by generating synthetic examples of the minority fraud class. The majority class is less likely to be favoured by the model since the quantity of fraudulent and non-fraudulent data is equal. The model's capacity to precisely identify fraudulent transactions is improved by this balancing.

## 5. CONCLUSION AND FUTURE WORK

An effective and trustworthy method for identifying fraudulent activity in portable wallet transactions is provided by the established hybrid model. It is appropriate for real-time and resource-constrained applications because it maintains a balanced performance by delivering high accuracy while running with low processing load. In the future, the model can be improved by applying transfer learning to increase performance on various payment systems, integrating real-time feedback for ongoing improvement, and incorporating adaptive learning techniques to manage shifting fraud patterns. Its usability will increase with more edge and mobile deployment optimization, guaranteeing that it continues to be a safe and scalable solution for contemporary digital wallet ecosystems.

## REFERENCES

1. S. Lenka and R. Tiwari, “Real-Time Fraud Prevention in Digital Wallet Transactions Using CNN-RNN Hybrid Networks,” 2025.
2. W. Bian Lin William Cong Yang Ji *et al.*, “The Rise of E-Wallets and Buy-Now-Pay-Later: Payment Competition, Credit Expansion, and Consumer Behavior,” 2023. [Online]. Available: https://www.juniperresearch.com/press/digital-wallet-users-exceed-5bn-globally-2026.
3. Z. Bezhovski, “The Future of the Mobile Payment as Electronic Payment System,” Online, 2016. [Online]. Available: www.iiste.org
4. Z. Bezhovski, “The Future of the Mobile Payment as Electronic Payment System,” Online, 2016. [Online]. Available: www.iiste.org
5. C. Iscan, O. Kumas, F. P. Akbulut, and A. Akbulut, “Wallet-Based Transaction Fraud Prevention Through LightGBM With the Focus on Minimizing False Alarms,” *IEEE Access*, vol. 11, pp. 131465–131474, 2023, doi: 10.1109/ACCESS.2023.3321666.
6. Ö. GÜVEN and S. ARAS, “MAKİNE ÖĞRENME ALGORİTMALARIYLA SAHTEKÂRLIK ALGILAMA: BİR MOBİL ÖDEME SİSTEMİ ÇALIŞMASI,” *International Journal of Management Economics and Business*, Mar. 2022, doi: 10.17130/ijmeb.979302.
7. S. Karim, M. U. Akhtar, R. Tashfeen, M. Raza Rabbani, A. A. A. Rahman, and A. AlAbbas, “Sustainable banking regulations pre and during coronavirus outbreak: the moderating role of financial stability,” *Economic Research-Ekonomska Istrazivanja* , vol. 35, no. 1, pp. 3360–3377, 2022, doi: 10.1080/1331677X.2021.1993951.
8. P. P. Vishwakarma, A. K. Tripathy, and S. Vemuru, “An empiric path towards fraud detection and protection for NFC-enabled mobile payment system,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 5, pp. 2313–2320, Oct. 2019, doi: 10.12928/TELKOMNIKA.v17i5.12290.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

9. S. K. L. Naik, A. Kiran, V. P. Kumar, S. Mannam, Y. Kalyani, and M. Silparaj, "Fraud Fighters - How AI and ML are Revolutionizing UPI Security," in *Proceedings of 2024 International Conference on Science, Technology, Engineering and Management, ICSTEM 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ICSTEM61137.2024.10560740.
10. Md. M. Rahman, Md. M. Islam, M. Khatun, S. Uddin, M. R. Faraji, and Md. H. Hasan, "Gravitating towards Information Society for Information Security in Information Systems: A Systematic PRISMA Based Review," *Pakistan Journal of Life and Social Sciences (PJLSS)*, vol. 22, no. 1, 2024, doi: 10.57239/pjlss-2024-22.1.0089.
11. F. A. A. Ramli and M. I. Hamzah, "Mobile payment and e-wallet adoption in emerging economies: A systematic literature review," *Journal of Emerging Economies and Islamic Research*, vol. 9, no. 2, p. 1, May 2021, doi: 10.24191/jeeir.v9i2.13617.
12. S. Vimal, K. Kayathwal, H. Wadhwa, and G. Dhama, "Application of Deep Reinforcement Learning to Payment Fraud," Dec. 2021, [Online]. Available: http://arxiv.org/abs/2112.04236
13. S. Delecourt and L. Guo, "Building a robust mobile payment fraud detection system with adversarial examples," in *Proceedings - IEEE 2nd International Conference on Artificial Intelligence and Knowledge Engineering, AIKE 2019*, Institute of Electrical and Electronics Engineers Inc., Jun. 2019, pp. 103–106. doi: 10.1109/AIKE.2019.00026.
14. V. Shpyrko and B. Koval, "Fraud detection models and payment transactions analysis using machine learning," *SHS Web of Conferences*, vol. 65, p. 02002, 2019, doi: 10.1051/shsconf/20196502002.
15. M. Bosamia and D. Patel, "Past to Present Overview of Mobile Wallet Payments Architectures to Compare and Identify Overall Participants," *Int J Comput Appl*, vol. 179, no. 48, pp. 10–18, Jun. 2018, doi: 10.5120/ijca2018917227.
16. *2017 2nd International Conference on Communication Systems, Computing and IT Applications (CSCITA) : proceedings : April 7-8, 2017, Hotel Kohinoor Continental, Mumbai, India*. IEEE, 2017.
17. P. Singh and M. Singh, "Fraud Detection by Monitoring Customer Behavior and Activities," 2015.
18. C. Cui, Z. Li, and Y. Song, "A Fraud Detection Method for Online Payment Transactions Based on Deep Learning," European Alliance for Innovation n.o., Jan. 2024. doi: 10.4108/eai.27-10-2023.2341915.
19. C. Wang and H. Zhu, "Representing Fine-Grained Co-Occurrences for Behavior-Based Fraud Detection in Online Payment Services," *IEEE Trans Dependable Secure Comput*, vol. 19, no. 1, pp. 301–315, 2022, doi: 10.1109/TDSC.2020.2991872.
20. L. Kovács and S. David, "Fraud risk in electronic payment transactions," May 03, 2016, *Emerald Group Publishing Ltd.* doi: 10.1108/JMLC-09-2015-0039.