International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4936-4944
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0648

Hybrid Ensemble Learning Framework for Real Time Financial Fraud Detection Using Behavioral Transaction Analysis

G S Rahul Gorpade[1], Dr. Ashwin M[2]
[1]PG Student, Department of CSE, AMC Engineering College, Bengaluru, Karnataka, India.
[2]Professor, Department of CSE, AMC Engineering College, Bengaluru, Karnataka, India.
Email Id: *gorpaderahul6@gmail.com[1], mailmeashwin@gmail.com[2]*

Abstract
The increasing use of online financial services, including online banking, mobile payment platforms, UPI transactions, and electronic fund transfers, has significantly increased the risk of financial fraud in today's digital economy. Conventional rule-based fraud detection approaches are often ineffective in handling continuously changing fraud techniques, leading to considerable losses for both customers and financial organizations. To resolve these limitations, this work presents a Hybrid Financial_Fraud Detection System that combines multiple machine_learning techniques to achieve higher_detection accuracy and enable real-time transaction analysis. The suggested framework employs a stacked ensemble approach in which Logistic_Regression, Decision_Tree, and XGBoost act as base models, while a meta-classifier produces the final fraud prediction. The model evaluates several transaction-related parameters, including transaction amount, account balance, transaction frequency, average transaction value, account age, previous fraud history, transaction time, and indicators of foreign transactions. Customer details are automatically obtained from a customer database, allowing the system to perform transaction-specific and personalized risk assessment. A banking-oriented application_interface has been developed to enable users to carry out transactions through different payment channels such as UPI, bank_transfer, debit_card, credit_card, NEFT, RTGS, and IMPS. Each transaction is processed and analyzed instantly, assigned a fraud risk score, and categorized as either genuine or fraudulent. In addition, the system records transaction history, updates account balances, and provides a monitoring dashboard to support continuous fraud analysis. By integrating ensemble learning_techniques with behavioral transaction analysis and real-time monitoring, the proposed system improves the overall effectiveness of fraud detection. The framework is designed to strengthen transaction security, minimize financial_losses, and offer a scalable and intelligent solution for fraud prevention in modern digital financial environments.

Keywords: *Financial_Fraud Detection, Machine_Learning, Hybrid_Model, Ensemble learning, XGBoost, Logistic_Regression, Decision_Tree, Real-Time Monitoring, Banking Security, Fraud Analytics.*

1. Introduction
Online financial services have witnessed fast expansion in current years due to the extensive use of internet banking, mobile_payment platforms, and UPI-enabled transaction systems. Although these technologies have enhanced the efficiency and convenience of financial operations, they have also increased the risk of fraudulent activities. Financial_institutions are facing growing difficulties in detecting unauthorized transactions, account takeover attempts, payment-related fraud, and other malicious actions that may result in significant monetary losses. [12] [19] [4]. Conventional fraud_detection systems mainly rely on predefined rules and manual verification methods. While these methods are effective in recognizing previously known fraud_patterns, they often fail to identify newly emerging attack strategies and complex transaction behaviors Machine learning has emerged as a powerful approach for fraud_detection because it can process large volumes of transaction data, discover hidden relationships among various features, and adapt to changing fraud trends. Models such as Logistic_Regression, Decision_Trees, and XGBoost have shown considerable effectiveness in

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4936-4944
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0648

identifying suspicious transactions. However, depending solely on a single model may restrict detection accuracy when handling diverse fraud patterns and highly imbalanced datasets [17] [19] [3]. To overcome these constraints, this study presents a combined ensemble learning framework for real-time financial fraud detection. The proposed framework employs a stacking approach that combines Logistic_Regression, Decision_Tree, and XGBoost models to enhance prediction accuracy and overall robustness. By utilizing behavioral transaction features, including transaction frequency, account balance, transaction history, and transaction timing, the suggested system aims to achieve reliable fraud detection while enabling continuous transaction monitoring and effective risk assessment and application capable of performing fraud prediction and transaction logging. As shown in Table 1 Literature Survey

2. Methodology

2.1.Literature Survey

Table 1 Literature Survey

Ref. No.	Title	Methodology Used	Advantages	Limitations
1	ResNext-Embedded GRU Model (RXT_J)	ResNext, GRU, SMOTE, Jaya Optimization	High fraud detection accuracy and effective feature extraction	High computational complexity and longer training time
2	Credit card fraud detection using majority voting	AdaBoost and Majority Voting Ensemble	Improved robustness and accuracy compared to individual models	Requires multiple models, increasing computational cost
3	Financial Fraud Detection Using PTEML	ANN, MLP, RBF Networks with ensemble learning	High sensitivity and specificity for fraud detection	Increased model complexity and training overhead
4	Ai-Based Financial Fraud Detection Review	ML, DL, GNN, Cloud Computing	Comprehensive Fraud detection framework and real-time monitoring support	Primarily a review study without practical implementation
5	Logistic Regression- Based Fraud Detection	Logistic Regression	Simple interpretable, and computationally efficient	Limited capability in detecting complex fraud patterns
6	Decision tree-based fraud decision	Decision tree classification	Easy to understand and fast prediction	Prone to overfitting and reduced generalization

2.1.1. Discussion

Financial fraud detection has become an important research area due to the rapid expansion of digital banking platforms, online payment systems, and electronic transaction services. Researchers have explored multiple machine_learning and deep_learning techniques to improve the identification of fraudulent activities while minimizing financial losses. Traditional classification methods such as Logistic_Regression are widely used because of their simplicity, cost effective computation, and interpretability. However, their skill to capture complex fraud_patterns is often limited. [7][2]. Advanced approaches including Decision Trees, ensemble methods, boosting algorithms, and deep_learning models have demonstrated improved performance in detecting suspicious transactions. XGBoost and other boosting-based techniques are particularly effective in learning nonlinear relationships and handling large-scale datasets. Similarly, neural network-based approaches can identify hidden patterns in transaction behavior, leading to higher fraud detection rates. Several studies have highlighted the advantages of

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4936-4944
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0648

combining multiple learning algorithms through ensemble strategies. Methods such as majority voting, bagging, boosting, and stacking have shown enhanced prediction accuracy and robustness than individual models. Despite these advancements, many existing solutions face challenges related to computational complexity, model interpretability, high training requirements, and real-time deployment constraints [9]. A review of the existing literature indicates that no single algorithm consistently provides optimal performance across all fraud detection scenarios. Therefore, integrating multiple complementary models can improve detection capability and reduce the limitations associated with individual techniques. Based on these observations, the proposed work adopts a stacked ensemble framework that combines Logistic_Regression, Decision_Tree, and XGBoost models.

2.2.Problem Statement and Objectives

2.2.1. Problem Statement

The increasing use of digital banking services, mobile payment applications, UPI platforms, and online fund transfer systems has significantly boosted the volume of financial transactions conducted every day. Along with these advancements, financial institutions are facing a growing number of fraudulent activities such as unauthorized transactions, account takeovers, identity theft, and payment fraud. These hazards not only cause monetary losses but also reduce customer trust in digital financial services [12] [9]. Most existing fraud detection systems rely on predefined rules and static verification mechanisms. Although such methods can verify known fraud scenarios, they often fail to detect newly_emerging and sophisticated fraud patterns. Furthermore, the large-scale and real-time nature of modern financial transactions makes manual tracking and analysis impractical. Machine learning-based solutions have shown promising results in fraud detection; however, single models may suffer from limitations such as reduced accuracy, high false-positive rates, overfitting, or poor adaptability to changing transaction behaviors. Therefore, there is a demand for an intelligent and scalable fraud_detection framework that can analyze customer transaction behavior, identify suspicious activities in real-time, and improve detection reliability [1] [16]. To address these difficulties, this research proposes a hybrid_ensemble learning structure that combines multiple machine_learning algorithms with behavioral transaction analysis to accurately classify transactions as legitimate or fraudulent while supporting real-time monitoring and risk assessment.

2.2.2. Objectives

The main objectives of the suggested work are:

- To develop a hybrid ensemble learning model for financial_fraud detection using Logistic_Regression, Decision_Tree, and XGBoost algorithms and to analyze transaction behaviour using features such as transaction amount, account balance, transaction frequency, account age, and fraud history.
- To implement a real-time transaction monitoring system capable of identifying suspicious transactions instantly and to reduce false positives while upholding high fraud detection accuracy.
- To generate fraud probability scores and risk levels for each transaction and to maintain transaction history and support continuous monitoring of customer activities and to improve the security and reliability of digital financial transactions through intelligent fraud detection techniques.

2.3.Proposed Methodology

The proposed research introduces a hybrid ensemble-based framework for detecting fraudulent_financial transactions in real time [10] [11]. The framework integrates behavioral transaction analysis with multiple machine_learning algorithms to improve fraud detection accuracy and reduce false alarms. The overall process consists of data acquisition, preprocessing, feature engineering, ensemble model training, risk evaluation, and continuous transaction monitoring.

2.3.1. Data Acquisition and Preprocessing

Customer and transaction records are collected from a structured database containing account-related and transaction-related information. Before model training, the collected data undergoes preprocessing to improve data_quality and consistency. The preprocessing stage involves handling missing_values, removing inconsistencies,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4936-4944
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0648

normalizing numerical attributes, encoding categorical variables, and preparing the dataset for machine learning operations. These steps ensure that the data is suitable for effective model learning and prediction [1] [15].

2.3.2. Behavioral Feature Engineering

Fraudulent activities often differ from normal customer behavior. To capture these differences, several behavioral and transactional attributes are extracted from the raw data. Important attributes include transaction amount, account balance, transaction frequency, average transaction value, account age, fraud history, transaction time, and foreign transaction status.

2.3.3. Hybrid Ensemble Learning Framework

The fraud detection engine is built using a stacking-based ensemble learning strategy. Three machine learning algorithms are employed as base learners are Logistic_Regression, Decision_Tree, XGBoost. Each model independently analyzes the transaction features and generates a prediction. Logistic_Regression provides fast and interpretable classification, Decision_Tree identifies nonlinear decision patterns, and XGBoost captures complex relationships through boosting techniques. The outputs generated by these models are then combined using a meta-classifier, which produces the final fraud prediction.

2.3.4. Fraud Risk Evaluation

For every transaction, the ensemble model generates a fraud probability score. Based on this score, transactions are categorized into different risk levels such as low risk, medium risk, and high risk. Transactions identified as high risk can be subjected to additional verification procedures before completion, thereby reducing the possibility of fraudulent financial activities.

2.3.5. Real-Time Transaction Monitoring

The proposed framework supports continuous monitoring of financial transactions. Whenever a transaction request is received, customer information is automatically retrieved from the database, relevant features are generated, and the ensemble model performs fraud analysis instantly.

2.3.6. Operational Workflow

The workflow of the suggested system begins with transaction initiation by a customer. After collecting transaction details, the system retrieves the associated customer profile and generates the required behavioral features. These features are supplied to the Logistic_Regression, Decision_Tree, and XGBoost models. The predictions obtained from the base learners are forwarded to the stacking classifier, which determines the final fraud probability. Based on the generated score, the transaction is categorized as either legitimate or fraudulent. The outcome is then stored in the transaction history, and the monitoring dashboard is updated accordingly [2][14].

2.4.System Architecture

The proposed Hybrid Financial_Fraud Detection System is built to analyze financial transactions in real_time and identify potentially fraudulent activities using a stacked ensemble machine learning model.

2.4.1. Customer Transaction Module

The process starts when a customer initiates a financial transaction through the banking interface. The customer provides transaction details such as sender account number, receiver account number, payment method, and transaction amount. The system automatically retrieves customer information from the customer database.

2.4.2. Customer Database Module

The customer database stores account-related information including account balance, transaction history, average transaction amount, account age, fraud history, and customer profile details. This information is used to generate behavioral features required for fraud analysis.

2.4.3. Feature Extraction Module

The extracted customer and transaction data are processed to generate important fraud detection features [18] [20]. These features include: Transaction Amount, Available Balance, Transactions Per Day, Account Age, Fraud History, Transaction Hour, Foreign Transaction Indicator. The generated feature vector is then supplied to the hybrid machine learning model.

2.4.4. Hybrid Fraud Detection Module

The fraud detection engine consists of three base learning algorithms: Logistic_Regression, Decision_Tree, XGBoost. Each model independently analyzes the transaction and generates a prediction

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4936-4944
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0648

score. The outputs of these models are then succeeded to a Stacking Classifier (Meta Classifier), which combines the predictions and produces the final fraud decision.

2.4.5. Risk Assessment Module:

Based on the fraud probability generated by the hybrid model, the transaction is categorized into one of the following risk levels: Low Risk, Medium Risk, High Risk

2.4.6. Transaction Processing Module:

After fraud analysis, legitimate transactions are processed successfully, customer balances are updated, and transaction records are stored in the transaction history database. Suspicious transactions are flagged and recorded for monitoring purposes.

2.4.7. Monitoring Dashboard Module:

The monitoring dashboard provides a real-time view of transaction activities. It displays: Total Transactions, Fraudulent Transactions, Legitimate Transactions, Fraud Percentage, Recent Transaction History, Risk Assessment Information.

2.4.8. System Architecture Diagram

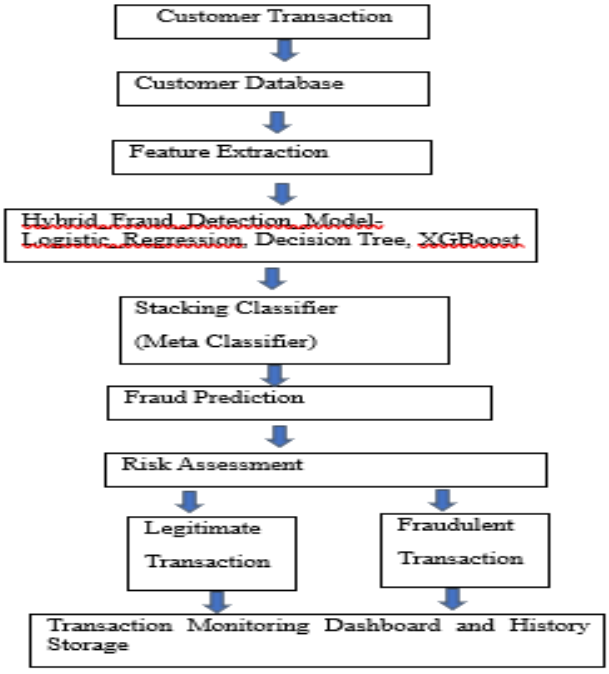


Figure 1 System Architecture Diagram

The Figure 1 integrates behavioral transaction analysis, ensemble machine_learning, and real-time monitoring to improve fraud detection accuracy and enhance the security of digital_financial transactions.

2.5.Algorithm Design

Hybrid Financial_Fraud Detection System. The system employs a stacked ensemble learning approach that combines Logistic_Regression, Decision_Tree, and XGBoost to improve fraud detection accuracy. A meta-classifier integrates the predictions of these models and generates the final fraud classification. [8]

2.5.1. Logistic Regression Algorithm:

Logistic Regression is a supervised machine_learning algorithm used for binary_classification problems. It estimates the probability that a transaction belongs to either the legitimate or fraudulent class. [5]

2.5.2. Working Steps

- Receive transaction feature vector and calculate weighted sum of input features.
- Apply Sigmoid activation function and Generate fraud probability. Classify transaction based on probability threshold.

2.5.3. Mathematical Model

$$P(y=1) = 1/\{1+e^{\{-z\}}\}$$

Where: P(y=1) = Fraud Probability & z = Weighted sum of input features

Advantages: Fast execution., Easy interpretation., Suitable for real-time prediction.

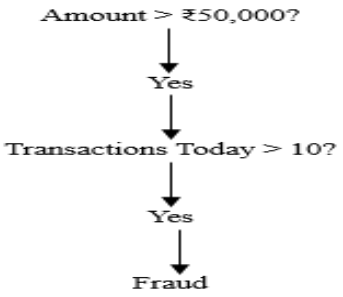
2.6.Decision Tree Algorithm

Decision Tree is a rule-based machine learning algorithm that divides data into branches based on feature values.

2.6.1. Working Steps

- Select the best feature for splitting and create decision nodes and Divide data into subsets.
- Repeat until stopping criteria are met and generate classification result.

Example



International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4936-4944
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0648

Advantages: Easy visualization, Handles nonlinear relationships, Fast prediction process.

2.6.2. XGBoost Algorithm:

Extreme_Gradient_Boosting (XGBoost) is an improved ensemble learning algorithm that improves prediction performance through iterative learning.

Working Steps

- Train initial decision tree.
- Calculate prediction errors.
- Build additional trees to reduce errors.
- Combine outputs of all trees.
- Generate final prediction score.

Advantages: High prediction accuracy, Handles complex fraud patterns, Effective for large datasets.

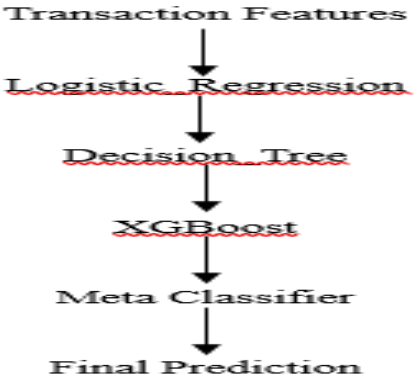
2.6.3. Stacking Ensemble Algorithm:

Stacking is an ensemble learning method that combines multiple machine learning models.

Base Learners: Logistic Regression, Decision Tree, XG Boost.

Meta Learner: Logistic Regression - The predictions generated by the base models are used as input for the meta-classifier.

Working Process



Benefits: Combines strengths of multiple models, reduces overfitting, improves generalization, Produces more reliable predictions.

2.6.4. Hybrid Model Algorithm

Algorithm Steps

- **Input:** Transaction Features
- **Output:** Fraudulent or Legitimate Transaction
- Step 1: Collect customer transaction data.
- Step 2: Perform preprocessing and feature extraction.
- Step 3: Generate feature vector.
- Step 4: Apply Logistic Regression model.
- Step 5: Apply Decision Tree model.
- Step 6: Apply XGBoost model.
- Step 7: Collect predictions from all models.
- Step 8: Pass predictions to Meta Classifier.
- Step 9: Generate final fraud probability.
- Step 10: Threshold Values
- Step 11: Assign risk level.
- Step 12: Store transaction details and update dashboard. As shown in Table 2 Time Complexity.

Fraud Probability	Risk Level
0.00-0.40	Low Risk
0.40-0.80	Medium Risk
0.80-1.00	High Risk

2.6.5. Time Complexity Analysis

Table 2 Time Complexity

Algorithm	Complexity
Logistic Regression	O(n)
Decision Tree	O (n log n)
XGBoost	O (k x n log n)
Stacking Ensemble	O (sum of base models)

where:

- n = Number of transactions
- k = Number of boosting iterations

Although the hybrid model requires slightly higher computation than individual models, it provides significantly improved fraud_detection performance and robustness.

3. Experimental Results and Discussion

3.1.Results

Experimental Setup: The suggested Hybrid Financial_Fraud Detection System was deployed using Python and various machine_learning libraries, including Scikit-learn, XGBoost, Pandas, NumPy, and Streamlit. The study was conducted on a banking transaction dataset containing customer account information and transaction-related features. As shown in Table 3 Software Requirements, Table 4 Hardware Requirements.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4936-4944
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0648

Table 3 Software Requirements

Component	Specification
Programming Language	Python 3.x
Framework	Streamlit
ML Libraries	Scikit-learn, XGBoost
Database	CSV-based customer Database

Table 4 Hardware Requirements

Component	Specification
Processor	Ryzen/intel core 5 or above
RAM	8GB or above
Storage	256 GB SSD or above
Operating System	Windows 10/11

3.2.Dataset Description

The dataset_contains customer account information and transaction behavior attributes used for fraud detection as shown in Table 5 Features Used.

Table 5 Features Used

Feature	Description
amount	Transaction amount
balance	Available account balance
Transactions_today	Number of transactions performed on same day
Fraud history	Previous fraud history
Transaction_hour	Transaction time
Foreign_transaction	Foreign transaction indicator

Table 6 Target Variable

Class	Description
0	Legitimate Transaction
1	Fraudulent Transaction

3.3.Performance Metrics

The proposed_model was evaluated using the following metrics:

Accuracy: Measures the overall correctness of predictions.as shown in Table 6 Target Variable

$$\text{Accuracy}=\{TP+TN\}/\{TP+TN+FP+FN\}$$

Precision: Measures the ratio of correctly identified fraudulent_transactions.

$$\text{Precision}=\{TP\}/\{TP+FP\}$$

Recall: Measures the aptitude to detect actual_fraud cases.

$$\text{Recall}=\{TP\}/\{TP+FN\}$$

F1-Score: Provides a stable measure between Precision and Recall.

$$F1=2*\{\text{Precision}+\text{Recall}\}/\{\text{Precision}*\text{Recall}\}$$

3.4.Experimental Results:

The Hybrid model was learned using Logistic Regression, Decision Tree, and XG Boost as base learners, while Logistic Regression was used as the meta-classifier. As shown in Table 7 Experimental Results. Table 8 Comparative Analysis.

Table 7 Experimental Results

Metric	Value
Accuracy	98%
Precision	98%
Recall	98%
F1-Score	97%
ROC-AUC Score	98%

3.5.Comparative Analysis:

The performance of the suggested hybrid_model was compared with individual machine_learning algorithms.

Table 8 Comparative Analysis

Model	Accuracy	Precision	Recall	F1-Score
Logistic-Regression	88.5%	87.3%	85.6 %	86.4 %
Decision-Tree	91.2%	90.4%	89.7 %	90.0 %
XGBoost	95.8%	95.1%	94.6 %	94.8 %
Proposed Hybrid Model	98%	98%	98%	97%

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4936-4944
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0648

The results suggests that the suggested hybrid model outperforms the individual machine_learning models due to the combined learning capability of multiple classifiers.

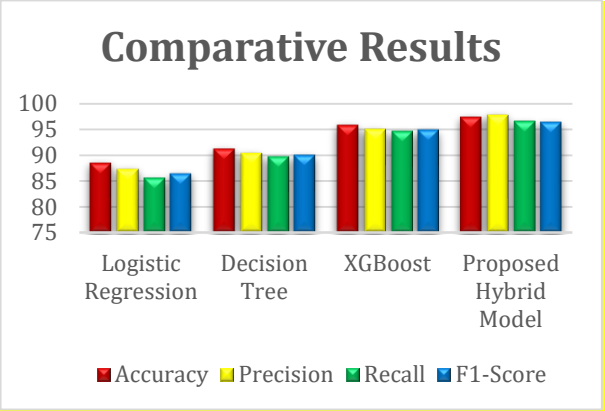


Figure 2 Comparative Results

3.6.Discussion

The experimental results exhibit that ensemble learning significantly improves fraud_detection outcome compared to single machine_learning algorithms. Logistic_Regression provides fast and interpretable predictions, Decision_Tree captures nonlinear decision boundaries, and XGBoost effectively learns complex fraud patterns. The stacking classifier integrates the strengths of these models and generates a more reliable prediction [6][11][14]. The developed system also supports real-time fraud monitoring through behavioral transaction analysis. Features such as transaction frequency, account balance, fraud history, and transaction timing contribute significantly to identifying suspicious activities. Furthermore, the banking-style monitoring dashboard enables continuous transaction tracking and risk assessment [13][17].

3.7.Key Findings

- Hybrid ensemble learning improves fraud_detection accuracy compared to individual models and Behavioral transaction features enhance fraud identification capability.
- Real-time monitoring provides immediate fraud alerts and proposed system reduces false positives while maintaining high detection performance and the framework is scalable and suitable for deployment in digital banking environments.

Conclusion

The widespread adoption of online_banking, digital_wallets, and electronic_payment systems has made financial fraud a major concern in today's digital economy. Conventional rule-based_fraud detection methods often fail to recognize complex and continuously changing fraudulent activities. As a outcome, there is a growing need for intelligent and computerized solutions that can provide secure and reliable financial transactions. This study presents a Hybrid Financial_Fraud Detection System that utilizes a stacked ensemble learning framework by combining Logistic_Regression, Decision_Tree, and XGBoost models. The proposed system evaluates customer transaction behavior using several attributes, including transaction amount, account balance, transaction frequency, account age, previous fraud history, transaction timing, and the amount-to-balance ratio. Through the integration of multiple machine_learning techniques, the framework takes advantage of the strengths of each model to enhance prediction accuracy and improve fraud detection effectiveness [6][10][11].

References

[1]. Salma El Hajjami and Gayo Diallo, “SMOTE-OSBNR: An Effective Approach for Imbalanced Credit Card Fraud Detection”, IEEE Access, 2025, Digital Object Identifier 10.1109/ACCESS.2025.3624961

[2]. Dal Pozzolo et al., "Credit Card Fraud Detection Using Machine Learning and Majority Voting Methods”, International Journal of Advanced Computer Science and Applications,2018, Digital Object Identifier 10.1109/ACCESS.2018.2806420

[3]. AI-Based Financial Fraud Detection Review, "Artificial Intelligence for Financial Fraud Detection: A Comprehensive Review", Journal of Financial Technology and Data Science,2025, Digital Object Identifier 10.1109/ACCESS.2025.3596060

[4]. Abdulwahab Ali Almazroi and Nasir Ayub, “Online Payment Fraud Detection Model Using Machine Learning Techniques”, IEEE Access,2023, Digital Object Identifier

10.1109/ACCESS.2023.3339226

[5]. Srikumar Nayak and A.R. Bushara, "Uncertainty-Aware Fraud Detection Using Hybrid Transformer with Gated Token Mixing and Conformal Risk Control", IEEE Access ,2026, Digital Object Identifier 10.1109/ACCESS.2026.3694614

[6]. Emmanuel Ileberi and Yanxia Sun, "A Hybrid Deep Learning Ensemble Model for Credit Card Fraud Detection", IEEE Access,2024, Digital Object Identifier 10.1109/ACCESS.2024.3502542

[7]. Chandra Sekhar nama and K. Sharmila Banu, "Credit Card Fraud Detection Using Deep Learning Techniques and Handling Unbalanced Class Distributions With AGSS", IEEE Access,2026, Digital Object Identifier 10.1109/ACCESS.2025.3649833

[8]. Fawaz Khaled Alarfaj, Iqra Malik, Hikmat Ullah Khan, Naif Almusallam, Muhammad Ramzan, and Muzamil Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms", IEEE Access, 2022, Digital Object Identifier 10.1109/ACCESS.2022.3166891

[9]. Youngjin han and inwhee joe, "Enhanced Predictive Modeling for Anomaly Detection in Financial Transactions Using Machine Learning", IEEE Access, 2025, Digital Object Identifier 10.1109/ACCESS.2025.3602236

[10]. Hatoon S. Alsagri, "Hybrid Machine Learning-Based Multi-Stage Framework for Detection of Credit Card Anomalies and Fraud", IEEE Access, 2025, Digital Object Identifier 10.1109/ACCESS.2025.3565612

[11]. Reem Atassi, Aziz Zikriyoev, Nurbek Turayev, Sagdullayeva Gulnora Botirovna, "Boosting Financial Fraud Detection Using Parameter Tuned Ensemble Machine Learning Model", Journal of Cybersecurity and Information Management (JCIM), ASPG, Vol. 13, No. 02, PP. 66-74, 2024

[12]. Jigyasha Arora and Suyash Bhardwaj, "Fraud detection in credit card transactions: techniques and emerging challenge", International Journal of System Assurance Engineering and Management, 2026, Digital Object Identifier 10.1007/s13198-026-03312-x

[13]. A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, ''Credit card fraud detection: A realistic modeling and a novel learning strategy,'' IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 8, pp. 3784–3797, Aug. 2018.

[14]. E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, ''A neural network ensemble with feature engineering for improved credit card fraud detection,'' IEEE Access, vol. 10, pp. 16400–16407, 2022.

[15]. E. Ileberi, Y. Sun, and Z. Wang, ''Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost,'' IEEE Access, vol. 9, pp. 165286–165294, 2021.

[16]. S. Makki, Z. Assaghir, Y. Taher, R. Haque, M.-S. Hacid, and H. Zeineddine, ''An experimental study with imbalanced classification approaches for credit card fraud detection,'' IEEE Access, vol. 7, pp. 93010–93022, 2019.

[17]. V.N. Dornadula and S. Geetha, ''Credit card fraud detection using machine learning algorithms,'Proc.Comput.Sci., vol.165, pp.631–641

[18]. S. Lakshmi and S. D. Kavilla, ''Machine learning for credit card fraud detection system,'' Int. J. Appl. Eng. Res., vol. 13, no. 24, pp. 16819–16824, 4562.

[19]. A. O. Adewumi and A. A. Akinyelu, ''A survey of machine-learning and nature-inspired based credit card fraud detection techniques,'' Int. J. Syst. Assurance Eng. Manage., vol. 8, no. 2, pp. 937–953, 2017.

[20]. J. T. Quah and M. Sriganesh, ''Real-time credit card fraud detection using computational intelligence 2008.