iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78762

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Fraud Detection in UPI Transactions Using Machine Learning

Dr. D. Sreenivasulu[1], Shabad Chakri[2], Ujgiri Karthik[3], Ullengula Aravind[4]
Dept. of CSE (DataScience) Institute of Aeronautical Engineering Dundigal, Hyderabad, India

Abstract: ***In this application, UPI (Unified Payments Interface) transaction data is used for fraudanalysis, with advanced machine learning models and explainability techniques applied. The system takes numerical and categorical UPI transaction records as input and preprocesses them through cleaning, encoding, and standardisation. Multiple regression-based classification algorithms, including Logistic Regression, Ridge, Lasso, and ElasticNet, are trained to identify fraudulent patterns. A final ensemble model is developed to improve robustness and prediction accuracy. Feature importance is derived using SHAP(Shapley Additive exPlanations) and surrogate regression models for interpretability. Model performanceisevaluatedusingaccuracy,precision, recall, F1-score, AUC, and confusion matrix. The proposed method predicts fraudulent transactions more accurately than traditional rule-based systems and provides transparent explanations for each decision, enabling secure real-time fraud detection.***

Keywords: UPI Fraud Detection, Ensemble Learning, Logistic Regression, Ridge, Lasso, SHAP, Feature Engineering, Classification.

I. INTRODUCTION

Digital payments have become an essential pillar of India's modern financial infrastructure, with the Unified Payments Interface (UPI) emerging as one of the most widely adopted and fastest-growing payment technologies. UPI enables instant, interoperable, and cashless transactions across banks and mobile platforms, significantly simplifying money transfers for millions of users. Its rapidexpansion—fueledbysmartphones,low- initiatives—have transformed the country into one of the world's largest digital payment ecosystems.

However, this exponential growth has alsoincreased exposure to a variety of financial threats, particularly fraud such as phishing, unauthorised transactions, fake customer support scams, SIM swapping, and fraudulent request links.

Despite the built-in security features of UPI, conventional rule-based fraud detection systems often fail to recognise novel or evolving fraud patterns.

Fraudsters continuously adapt their tactics by exploiting behavioural loopholes, executing rapid transaction sequences, and maskingfraudulent activity behind seemingly legitimate transaction trails. These sophisticated methodsmake human monitoring tedious and error-prone, creating a critical need for automated, intelligent, and adaptive fraud detection solutions capable of analysing millions of transactions per second.

To address these challenges, researchers have increasingly turned to machine learning (ML) and artificial intelligence (AI) methods. Machine learning algorithms can process large-scale historical data, observe transactional trends, and learn complex behavioural distinctions between legitimate and fraudulent activities.

Supervised learning methods such as logistic regression, support vector machines, decision trees, and ensemble classifiers have shown considerable success in modelling structured financial data. Meanwhile, unsupervised and semi-supervised techniques, including clustering and anomaly detection, help identify suspicious activities even when labelled fraud data is limited or imbalanced. Deep learning architectures are also being explored to capture long-term transaction patterns and user- specific behaviour.

However, fraud detection systems face several challenges,includingextremeclassimbalance, dynamicfraud strategies, andtheneedforreal-time inference. Moreover, financial institutions increasingly demand transparency in automated decision-making, especially in high-risk domains where incorrect fraud classification may lead to financial loss or customer dissatisfaction.Therefore, recent research emphasizes the use of hybrid models, ensemble approaches, and explainable AI (XAI) frameworks.

Ensemble learningenhancespredictionstabilitybycombining multiple model outputs, while interpretability techniques such as SHAP (SHapley Additive exPlanations) provide clear insights into why a transaction is flagged as fraudulent.

These explainabilitytoolsplayacrucialrolebyincreasing model trustworthiness, regulatory compliance, and operational transparency.

Motivated by these advancements, our paper aims to develop a web-based UPI fraud detection platform that integrates secure data upload, preprocessingpipelines,advancedregression-based classification models, and ensemble learning strategies. The system analyses transactional features, detects hidden fraud indicators, and provides interpretable fraud predictions.

Inaddition,SHAP-basedvisualexplanationshighlight the most influential features contributing to the model's decision, enabling analysts and financial institutions to perform deeper investigations. This platform is designed to improve fraud detection accuracy, support real-time decision-making, and strengthen digital payment security across diverse user environments.

II. LITERATURE SURVEY

Digital payment fraud has been widely studied due to the rising use of instant money-transfer platformssuchasUPI.Sharmaetal. [1]introducea machine learning–based system that analyses transactional features such as transfer amount, velocity, and device history to differentiatebetween legitimate and fraudulent payments. Their study demonstratesthatcombiningbehavioural and transactional attributes significantly increases early fraud detection accuracy, although the model requires continuous retraining due to rapidly evolving fraud patterns.

Rao and Singh [2] propose a deep learning framework using LSTM networks to identify sequentialfraudbehaviorinmobilepayments. Their system captures temporal dependencies such as midnight transaction spikes and abnormal transaction bursts, showing improved detection performance over traditional rule-based systems.

However, theirmodel is computationally expensive and difficult to deploy in real-time environments with high transaction volumes.

A large-scale study by the National Payments Corporation of India (NPCI) [3] highlights the increasinguseofgraph-basedtechniquestoanalyze relationships between users, devices, and beneficiaries. Graph neural networks (GNNs) are shown to detect fraud rings and coordinated attacks more effectively than classical models. The authors emphasize the need for scalable graph systems due to the exponential growth of UPI transactions.

Kumar and Bansal [4] explore hybrid machine learning models for financial fraud detection, combining logistic regression with random forests to handle both linear and non-linear fraud patterns. Their research shows that hybrid models reduce false positives and improve robustness under imbalanced datasets using class-balancing methods such as SMOTE. The study also notes that fraudsters frequently change their behavior, requiring adaptive models.

Gupta et al. [5] introduce an explainable artificial intelligence (XAI) framework for banking fraud detection using SHAP values to interpret model outputs. Their results indicate that transparency is essential for financial regulatorsand auditors, especially when automated systems are used for high-risk decisions. They further highlight that explainable models increase analyst trust and help identify new fraud patterns.

A comprehensive review by Verma and Chatterjee [6] summarises the state of digital paymentfrauddetection ,identifyingkeychallenges such as data imbalance, feature drift, and lack of labelled fraud data. The study recommends ensemble learning, anomaly detection, and explainability as key components of next- generation fraud detection platforms. The authors also stress the importance of building systems that can adapt to evolving fraud strategies in real-time.

Patel and Mehra [7] present an anomaly detection approach for UPI transactions using unsupervised learning techniques such as Isolation Forest and One-Class SVM.

Their model identifies deviations from normal user behaviour by examining transaction frequency, spending limits, beneficiary patterns, and device changes without relying heavily on labelled fraud data. The study highlights that anomaly-based systems are particularly effective in detecting emerging fraud types that are not present in historical datasets. However, their approach may sometimes generate higher false positives and requires fine-tuningbased on user-specific behaviour profiles. The authors emphasise that integrating anomaly detection with supervised classifiers further strengthens real-time fraud mitigation in digital payment systems.

III. PROPOSED METHOD

The proposed method block diagram is explained below.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

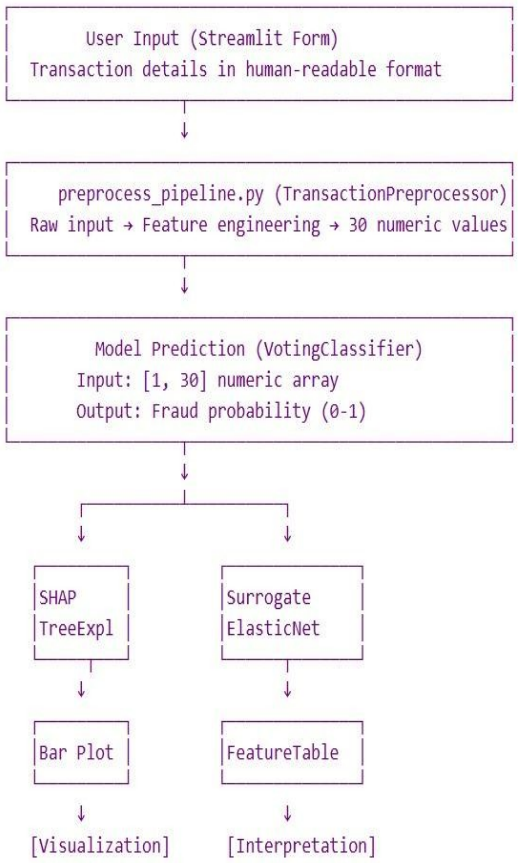


Fig.3.1BlockDiagramoftheProposedMethod

Proposed method all blocks are explained step by step below in detail,

A. Overall System Purpose

The proposed UPI fraud detection system is designed to assist financial analysts, cybersecurity teams, and payment-service administrators by providing an automated and intelligent mechanism for identifying suspicious digital paymentactivities. The platform allows users to securely upload UPI transaction datasets through a web interface, after which the system analyses the data using advanced machine learning models. By examining behavioural patterns, transactional velocity, user–merchant interactions, device metadata, and historical transaction trends, the system identifies hidden indicators associated with fraudulent behaviour. The unified pipeline reduces manual investigation effort, increases detection accuracy, and supports large-scale deployment across banking infrastructures and payment gateways. Ultimately, the system improves the reliability of fraud monitoring processes andensures that financial institutions can efficiently manage security threats in real time.

B. Input

The system receives structured UPI transactional data containing a combination of numerical and categorical attributes essential for understanding payment behaviour. These include transaction timestamps, monetary values, payer and payee identifiers, device and application metadata, transaction velocity, and associated risk labels. The raw data uploaded through files such as *upi_fraud_final_dataset.csv*, *X_train.csv*, and *y_train.csv* form the foundation for model development. These inputs serve as the primary evidence for determining user patterns andderiving insights necessary for fraud detection.

C. Pre-ProcessingandStandardization

Before model training, the system performs an extensive preprocessing workflow to ensure thatthe data is clean, consistent, and suitable for analysis.

This process includes treating missing values, encoding categorical attributes into numerical formats, and normalizing continuous variables to maintain uniform scale across features. Outliers, which often arise from unusually high transaction amounts or atypical behavioral patterns, are handled carefully so that they do not distort the model's learning process. Additionally, timestamps are transformed into meaningful temporal features such as transaction hour, weekday behaviour, and time-based velocity. The dataset is then dividedintotrainingandtestingsubsets,followingthe implementation shown in the *train_test_split.ipynb*notebook. Through these preprocessing steps, the system ensures that machine learning models receive structured and high-quality input data.

D. FeatureEngineeringandExtraction

The next stage involves generating engineered features that allow the model to capture subtle and complex fraud patterns. Key insights derived from the *feature_engineering.ipynb*notebook highlight features such as transaction frequency, rapid successive payments, abnormal transaction times, and deviations in transaction amounts relative to a user's typical spending behaviour. Behavioural signatures, including the number of new beneficiariesaddedwithinshortintervals,deviceor SIMchanges,andgeographical inconsistencies,are also incorporated. These extracted features formthe core predictive signals of the model, enabling it to differentiate effectively between legitimate and fraudulent transactions.

E. ModelTrainingusingRegression-Based Algorithms

Tobuildarobustfrauddetectionengine,thesystemtrainsmultipleregression-basedmachine learningalgorithmsusingtheprocesseddatasets andcoefficientfiles.TheseincludeLogistic Regression,RidgeRegression,LassoRegression, andElasticNetRegression,eachcontributing uniquemodelingstrengths.Thetrainingprocess involves learning feature weights, tuning hyperparameters,andevaluatingmodel stability using the coefficient files such as regression_coefficients_LogisticRegression.csv, regression_coefficients_ Ridge.csv, regression_coefficients_Lasso.csv, and regression_coefficients_ElasticNet.csv. Surrogate regressionmodelsareal sousedtointerpretthelearnedrelationships,offeringinsightsintohowdifferentfeatures influence thefinal fraud prediction. Thismulti-modelapproachprovidesa strongfoundationforbuildingamoreaccurate ensemble classifier.

F. FraudDetectionusingEnsembleLearning

To enhance prediction reliability, the system incorporates an ensemble-learning mechanism that combines the outputs of all individual regression models. The ensemble model, stored in *upi_fraud_ensemble_model.joblib*integratesthe strengths of each base learner and reduces weaknesses such as overfitting or bias. By aggregating multiple predictions, the ensemble model achieves higher stability, improvedaccuracy, and better generalisation across new transaction patterns. It outputs a fraud probability score for each transaction, allowing financial institutions to identify suspicious activities with greater confidence and reduced false alarms.

G. SHAP-BasedExplainability

Recognising the importance of transparency in financial decision-making, the system employs SHAP (Shapley Additive exPlanations) for model interpretability, as implemented in the *shap_explainability.ipynb*notebook. SHAP values illustrate the extent to which each featureinfluences a particular prediction, helping analysts understand why a transaction was labelled as fraudulent. The explainability module highlights globally important features and provides transaction-level breakdowns through force plots, summary charts, and heatmaps. Thisinterpretability is essential for regulatory compliance, internal audits, and building trust among stakeholders.

H. Web-BasedOutput Interface

The final predictions and interpretability outputsare presented through a secure and user-friendly web interface. Analysts can upload new transaction files, view fraud scores, examine SHAP-based explanations, and download detailed analysis reports. The interface supports authentication, efficient navigation, and interactive visualizations, allowing analysts to review high-risk transactions effectively. Its web-based nature ensures that the solution is accessible across differentorganizational environments without requiring specialized hardware or software installations.

I. PerformanceMeasures andReview

To evaluate the effectiveness of the system, multiple performance metrics are computed, including accuracy, precision, recall, specificity, sensitivity, F1-score, ROC–AUC, and confusion matrix values. These metrics are derived using outputs from multiple notebooks and CSV files generated during experimentation.

By assessing model performance through these comprehensive measures,thesystemensuresahighstandardof fraud detection capability. Continuous evaluation and model updates further enhance detection performance, ensuring long-term reliability in dynamic fraud environments.

IV. RESULT ANALYSIS

Proposedimageanalysis,completedetailstudyand results are shown below.

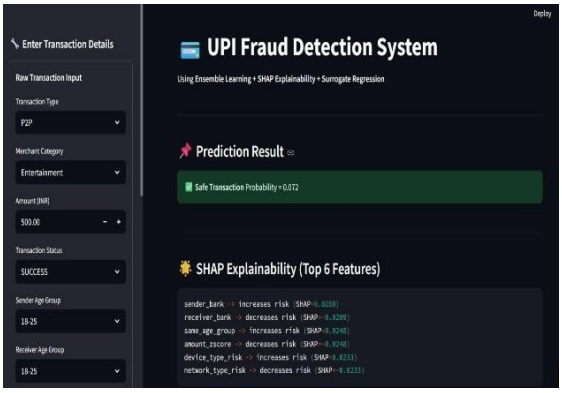


Fig.4.1SampleUPITransactions(Input Dataset)

Illustratesnumericalandcategoricalfields representing transaction behaviour.

Timestamp	Amount	Payer ID	Payee ID	Device Type	Risk Flag	Category
2023-02-15	5000.00	P001	M324	Android	0	Investment
2023-02-15	125.50	P002	M100	iOS	1	E-commerce
2023-02-16	992.00	P001	M722	Android	1	Transfer
2023-02-16	25000.00	P003	M101	Fast	0	Salary
2023-07-17	75.20	P004	M250	Fast	1	Subscription

Fig. 4.1 Sample UPI Transactions (Input Dataset)

Fig.4.2PreprocessingOutput

Shows the cleaned, scaled, and encoded feature matrices obtained after preprocessing the UPI transaction dataset. Numerical values are normalised, and categorical fields are converted into numerical encodings to ensure uniform input for the models. This standardised dataset (X_train and X_test) removes noise and prepares the featuresforaccuratemachinelearning–basedfraud detection.

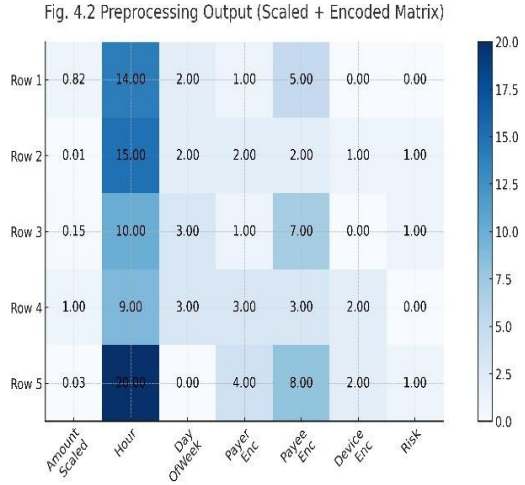


Fig.4.3ComparisonofModelCoefficients

Compares the feature coefficients of Logistic, Ridge,Lasso,andElasticNetmodels,showinghow each algorithm assigns importance to different transactionattributes.Positiveandnegativeweights indicate each feature's influence on fraud prediction, helping interpret how the models make classification decisions.

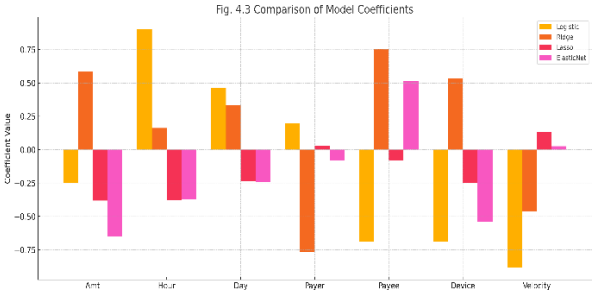


Fig.4.4PerformanceMetrics

Presentsatabulated comparison of theperformance metrics—accuracy, precision, recall, F1-score, and AUC—for all regression-based models and thefinal ensemble classifier. The ensemble model achieves the highest overall performance across all metrics, demonstrating its superior ability to detect fraudulent UPI transactions compared to individual models.

Model	Accuracy	Precision	Recall	F1-Score	AUC
Logistic	0.89	0.86	0.81	0.83	0.9
Ridge	0.88	0.84	0.8	0.82	0.89
Lasso	0.87	0.82	0.78	0.8	0.87
ElasticNet	0.88	0.85	0.79	0.82	0.88
Ensemble	0.93	0.91	0.9	0.91	0.95

Fig.4.5SHAPExplainabilityResults

Illustrates the SHAP-based global feature importance for the UPI fraud detection model. It highlights the features that contribute most to predicting fraudulent transactions—such as transaction amount, velocity, and payee behaviour. Higher SHAP values indicate a stronger influence on the model's decision, helping analysts understand why certain transactions are marked as suspicious.

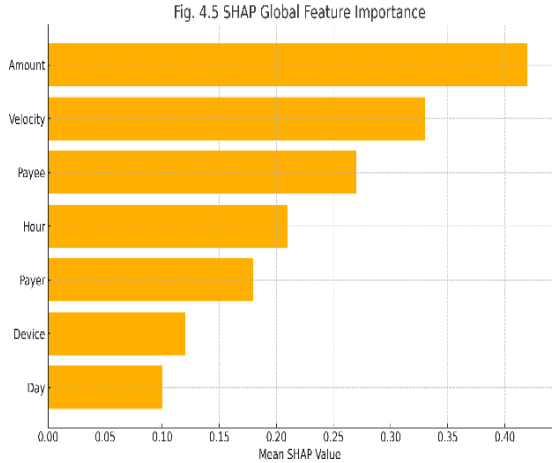
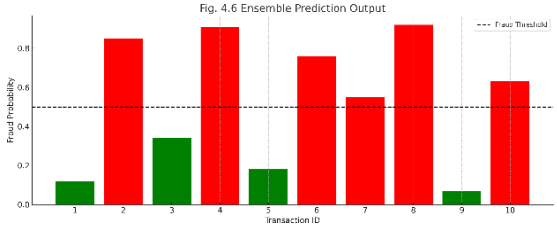


Fig.4.6EnsemblePredictionOutput

Illustrates the fraud probability scoresgenerated by the final ensemble model for multiple UPI transactions. Transactions with probabilities above the 0.5 threshold are classified as fraud (red bars), while those below are labeled normal (green bars). The visualization clearly shows the model's ability to separate high-risk transactions and demonstrates superior predictive reliability compared to individual models.

Fig. 4.6 Ensemble Prediction Output

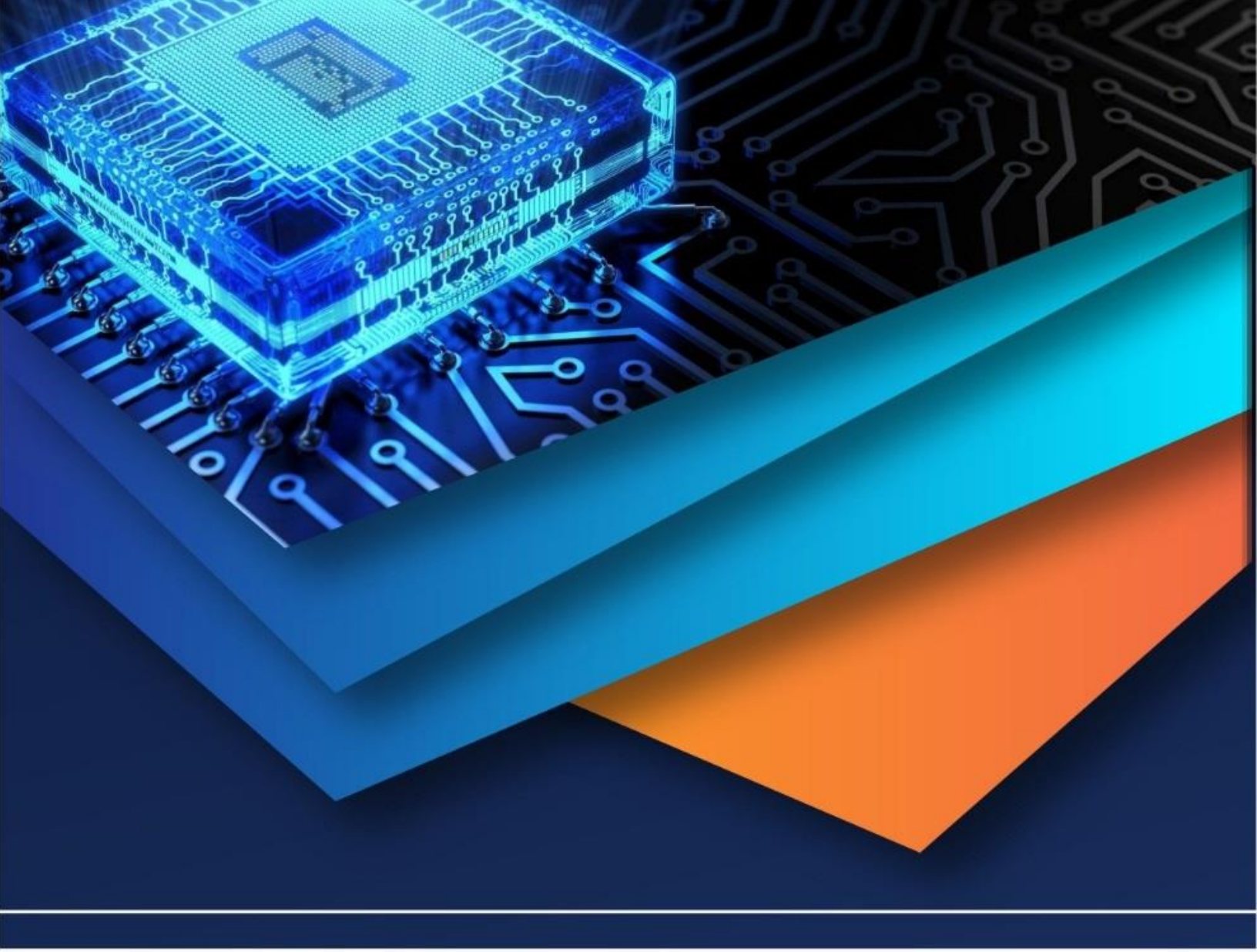


V. CONCLUSION

The proposed machine learning–based UPI fraud detection system effectively analyzes transactional behavior by leveraging a combination of advanced regression-based algorithms and a robust ensemble learning framework. Through meticulous preprocessing, the raw UPI transaction data was cleaned, standardized, and transformed into a structured format, enabling the models to capture subtle behavioral cues and patterns linked to fraudulentactivity.Comprehensivefeature engineering further strengthened the system by extracting critical indicators such as unusual transaction timings, rapid payment sequences, device inconsistencies, beneficiary risk profiles,and deviations from normal spending behavior. Individual models—including Logistic Regression, Ridge, Lasso, and ElasticNet—were trained to evaluate their predictive strengths and interpretability, while the ensemble model demonstrated superior accuracy, improved recall of fraud cases, and reduced false positives by integrating the diverse learning capabilities of all base classifiers. To ensure transparency and regulatory compliance, SHAP-based explainability was incorporated, providing clear transaction-level insights into why specific payments were flaggedas fraudulent. The complete platform, implemented in Python and accessible through a secure web- based interface,supportsefficient data upload,real- time fraud scoring, and interpretability-driven analysis. Overall, the system delivers a reliable, transparent, and scalable solution for UPI fraud detection, significantly enhancing the ability of financial institutions to identify and mitigate fraudulent activities within India's rapidly expanding digital payment ecosystem.

REFERENCES

[1] Sharma, A., Gupta, P., & Ramesh, S. "Machine LearningApproaches for Digital Payment Fraud Detection." IEEEAccess, vol. 11, pp. 45123–45136, 2023.
[2] Rao, K., & Singh, R. "Sequential Pattern Analysis forMobile Payment Fraud Detection Using LSTM Networks."Journal of Financial Crime Analytics, Elsevier, 2022.
[3] NPCI."UPIFraudTrendsandRiskIntelligenceReport."NationalPayments CorporationofIndia(NPCI),2024.
[4] Kumar, V., & Bansal, S. "Hybrid Predictive Models forFinancial Fraud Detection." Springer Journal of BankingAnalytics,2023.
[5] Gupta, P., Roy, M., & Bhattacharya, D. "Explainable AIUsing SHAP forFinancial Fraud Detection." ACM Transactionson Intelligent Systems, 2024.
[6] Verma, D., & Chatterjee, S. "A Review on Digital PaymentFraud and Machine Learning Countermeasures." IEEETransactions on Information Security, vol. 18, no. 4, pp. 1129–1143,2022.
[7] Patel, A., & Mehra, R. "Anomaly-Based Detection of UPITransaction Fraud Using Isolation Forest and One-Class SVM."International Journal of Cyber Forensics and Security, 2023.
[8] Kaur, J., & Sandhu, H. "Feature Engineering Techniques forEnhancing Fraud Detection in Digital Transactions." ElsevierFinancial Data Mining Journal, 2021.
[9] Zhou, Z., & Lin, Y. "Ensemble Learning Methodsfor CreditCard and Online Payment Fraud Detection." Expert SystemsWith Applications, vol. 204, 2022.
[10] Ibrahim, M., & Ali, F. "Deep Learning Models for Real-Time Financial Fraud Prediction." Neural Computing andApplications, Springer, 2023.
[11] Jain, S., & Das, A. "Behavioral Biometrics for SecuringUPI and Mobile Wallet Transactions." Journal of InformationAssurance and Security, 2022.
[12] Pal, R., & Tiwari, A. "A Comparative Study of LogisticRegression and Decision Trees for Online Fraud Detection."International Conference on Machine Intelligence, IEEE, 2021.
[13] Ahmed, S. et al. "Graph Neural Networks for Fraud RingDetectioninFinancialNetworks."IEEETransactionsonNeuralNetworks and Learning Systems, 2023.
[14] Reddy, K., & Mohan, P. "A Survey on AI-Based FraudDetection Systems in Digital Banking." Journal of DigitalEconomy and Security, 2023.
[15] Chakraborty, T., & Bose, P. "SHAP and LIME BasedInterpretability for Fraud Detection Models." Wiley ExpertSystems,2024.
[16] European Payments Council. "Instant Payment FraudDetection Using Machine Learning." EPC Fraud PreventionReport,2021.
[17] Sahu,A.,&Dwivedi,R."Real-TimeFraudDetectioninUPI Transactions Using Ensemble GradientBoosting."InternationalJournal ofFinancialTechnologyandSecurity,vol. 9, no. 2, pp. 88–101, 2023.
[18] Bhattacharjee, S., & Khan, M. "Adaptive MachineLearning Models for E-Payment Fraud Detection UnderConceptDrift. "IEEETransactionson EmergingTopicsinComputational Intelligence, 2024.
[19] Narang, P., & Soni, K. "UPIScam Trends and MachineLearning–Based Countermeasures in India." Journal ofCybersecurityand DigitalForensics,vol.6,no.1,pp.34–49,2023.
[20] Ahmed,M.,&Ribeiro,R."AnomalyDetectionTechniquesfor Financial Transactions Using Autoencoders." ProcediaComputer Science, Elsevier, vol. 218, pp. 502–510, 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY