iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79385

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 IV Apr 2026- Available at www.ijraset.com

Fraud Shield

Ms. Neha Kale, Ms. Pranali Siddhnath Chinchkar, Mr. Rahul Manish Kalambuskar, Mr. Sham Avinash Pathare
Department of Computer Engineering at New Horizon Institute of Technology and Management, Thane

Abstract: ***The rapid growth of digitalpayment systems has transformed financial transactions by enabling secure and instant money transfers through mobile platforms. Among these systems, Unified Payments Interface has gained widespread adoption due to its convenience and interoperability across banks. However, the increasing volume of digital transactions has also led to a rise in fraudulent activities, including identity theft, phishing attacks, and unauthorized fund transfers.Detecting fraudulent transactions in real time is challenging because of large-scale data generation and evolving fraud patterns. This research proposes a machine learning based fraud detection framework designed to analyse transaction behaviour and identify suspicious activities with high accuracy. The system examines multiple features such as transaction amount, frequency, time patterns, and device information to distinguish between legitimate and fraudulent transactions. Data preprocessing and feature engineering techniques are applied to enhance predictive performance. Experimental evaluation demonstrates that ensemble learning models provide improved detection rates while minimizing false alarms. The proposed solution aims to strengthen digital payment security by providing a scalable and efficient fraud detection mechanism.***

Index Terms: Digital payment security, fraud detection, machine learning, transaction analysis.

I. INTRODUCTION

The rapid advancement of digital payment technologies has significantly transformed the financial ecosystem by enabling secure, instant, and convenient transactions. In India, the Unified Payments Interface has emerged as one of the most widely adopted digital payment platforms due to its interoperability, real-time processing, and ease of use. The growing reliance on mobile-based transactions has accelerated financial inclusion and reduced dependency on cash-based systems. However, the exponential increase in transaction volume has also created new opportunities for fraudulent activities.

Digital payment fraud has evolved in complexity, involving techniques such as phishing, identity impersonation, social engineering, malicious application attacks, and unauthorized transaction requests. Fraudsters continuously adapt their strategies to bypass conventional rule-based security mechanisms. Traditional fraud detection systems rely on predefined rules and static thresholds, which are often ineffective against dynamic and evolving fraud patterns. As a result, there is a critical need for intelligent systems capable of detecting anomalies in real time while maintaining a low false positive rate.

Machine learning techniques offer a promising solution for fraud detection by analysing historical transaction data and identifying hidden behavioural patterns. Supervised learning algorithms such as Logistic Regression, Random Forest, and Gradient Boosting have demonstrated strong performance in classification tasks involving imbalanced datasets.

This research focuses on designing and implementing a machine learning based fraud detection framework specifically tailored for digital payment transactions. The proposed system emphasizes data preprocessing, feature engineering, model training, and performance evaluation using appropriate metrics such as precision, recall, accuracy, and F1-score. The objective is to develop a scalable and efficient fraud detection mechanism capable of strengthening transaction security while preserving user experience.

II. LITERATURE REVIEW

Digital payment fraud detection has attracted significant research attention due to the rapid growth of online and mobile-based financial transactions. Various approaches have been proposed to identify fraudulent activities using statistical analysis, machine learning, and hybrid models.

Early fraud detection systems were primarily rule-based, relying on predefined thresholds and expert-defined patterns. Although effective for detecting known fraud scenarios, these systems lacked adaptability to evolving fraud strategies and often resulted in high false positive rates. To overcome these limitations, researchers introduced data-driven techniques based on supervised learning algorithms.

Several studies have demonstrated the effectiveness of classification models such as Logistic Regression, Decision Trees, and Support Vector Machines in detecting fraudulent financial transactions.

These models analyse historical transaction data to identify distinguishing patterns between legitimate and fraudulent activities. However, class imbalance remains a major challenge in fraud detection datasets, as fraudulent transactions typically represent a small percentage of total transactions.

Recent research emphasizes the use of ensemble learning techniques such as Random Forest and Gradient Boosting, which combine multiple weak learners to improve predictive accuracy and robustness. These models have shown superior performance in handling high-dimensional data and reducing overfitting. Additionally, feature engineering techniques such as transaction frequency analysis, behavioural profiling, and anomaly detection have been widely adopted to enhance detection capability.

Deep learning approaches,including Artificial Neural Networks and Long Short-Term Memory networks, have also been explored for modelling sequential transaction patterns. While these methods provide improved accuracy in complex datasets, they require substantial computational resources and large-scale training data.

Based on the existing literature, it is evident that machine learning-based ensemble approaches combined with effective preprocessing strategies offer a promising solution for real-time fraud detection in digital payment systems.

III. PROBLEM STATEMENT

The rapid increase in digital payment transactions has significantly raised the risk of financial fraud in mobile-based payment systems. Traditional rule-based fraud detection mechanisms are limited in their ability to adapt to evolving fraud patterns and often result in high false positive rates. Additionally, the highly imbalanced nature of transaction data makes accurate fraud detection challenging. There is a need for an intelligent, scalable, and data-driven system capable of analysing real-time transaction patterns to accurately identify fraudulent activities while minimizing false alarms.

IV. PROPOSED METHODOLOGY

The proposed Fraud-Shield system adopts a machine learning based approach to detect fraudulent transactions in digital payment systems. The methodology consists of multiple stages including data collection, preprocessing, feature engineering, model training, and performance evaluation. The objective is to build a scalable and efficient fraud detection framework capable of analysing transaction behaviour in real time.

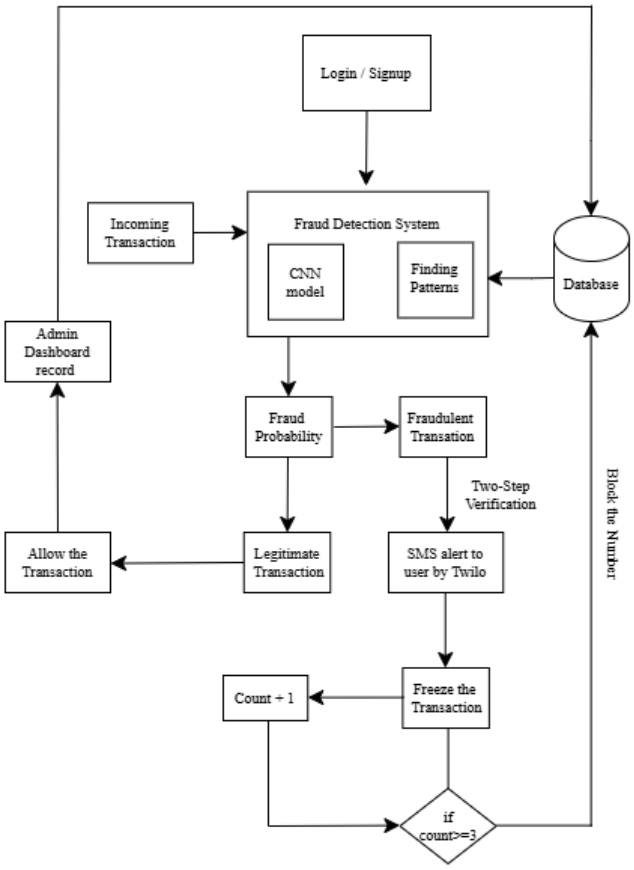
Initially, transactional data is collected from a structured dataset containing features such as transaction amount, transaction time, user identification, device information, transaction frequency, and location attributes. Since fraud datasets are typically imbalanced, preprocessing techniques such as data cleaning, normalization, and class balancing are applied to improve model reliability. Feature engineering is performed to extract meaningful behavioural indicators, including spending patterns and frequency-based metrics.

After preprocessing, supervised learning algorithms such as Logistic Regression, Random Forest, and Gradient Boosting are trained to classify transactions as legitimate or fraudulent. Ensemble models are preferred due to their ability to improve prediction accuracy and reduce overfitting. The dataset is divided into training and testing sets to evaluate model generalization capability.

Model performance is assessed using metrics such as accuracy, precision, recall, and F1-score to ensure effective fraud detection with minimal false positives. The best-performing model is selected for deployment within the Fraud-Shield framework to enable real-time fraud monitoring.

To further enhance system performance and reliability, the proposed framework incorporates real-time transaction monitoring and decision-making capabilities. Incoming transactions are processed dynamically, and the trained model evaluates each transaction instantly to determine its legitimacy. A threshold-based decision mechanism is used to classify transactions with higher confidence scores as fraudulent. Additionally, the system integrates an alert and notification module that informs users and administrators about suspicious activities for immediate action. The architecture is designed to be scalable, allowing integration with large-scale financial systems and continuous model updates based on newly observed fraud patterns, thereby improving adaptability to evolving threats.

V. SYSTEM ARCHITECTURE



VI. IMPLEMENTATION DETAILS

The Fraud-Shield system is implemented using a machine learning based framework designed to process and analyse digital transaction data efficiently. The implementation consists of data preprocessing, model training, model evaluation, and system integration phases.

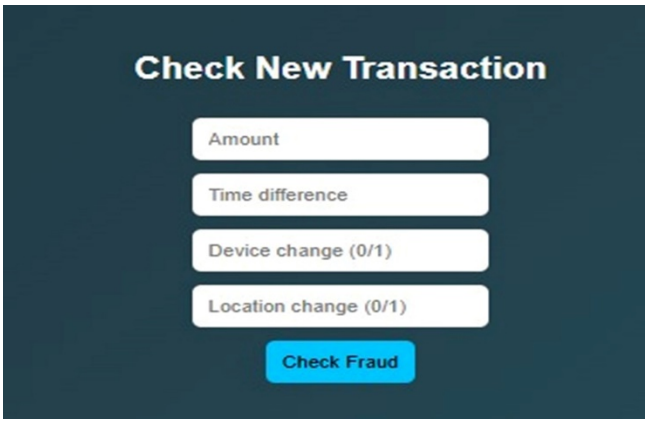
The dataset is first imported into the development environment and examined for missing values, inconsistencies, and redundant attributes. Data cleaning techniques are applied to remove null values and normalize numerical features to ensure uniform scaling. Since fraudulent transactions typically represent a minority class, class imbalance handling techniques such as resampling are applied to improve classification performance.

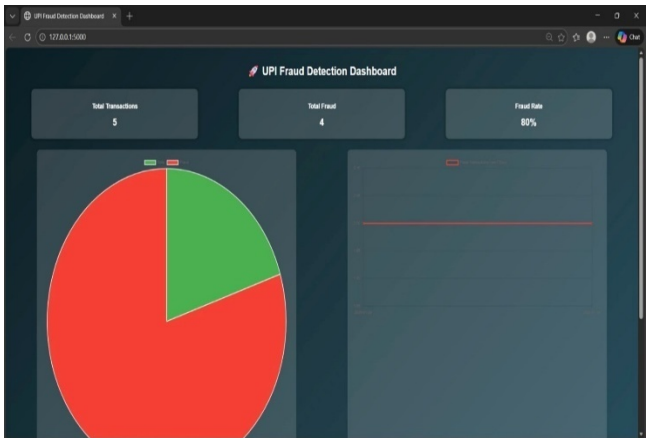
Feature engineering is performed to extract meaningful behavioural indicators, including transaction frequency, average transaction amount, time-based activity patterns, and location variance. These features enhance the predictive capability of the learning models.

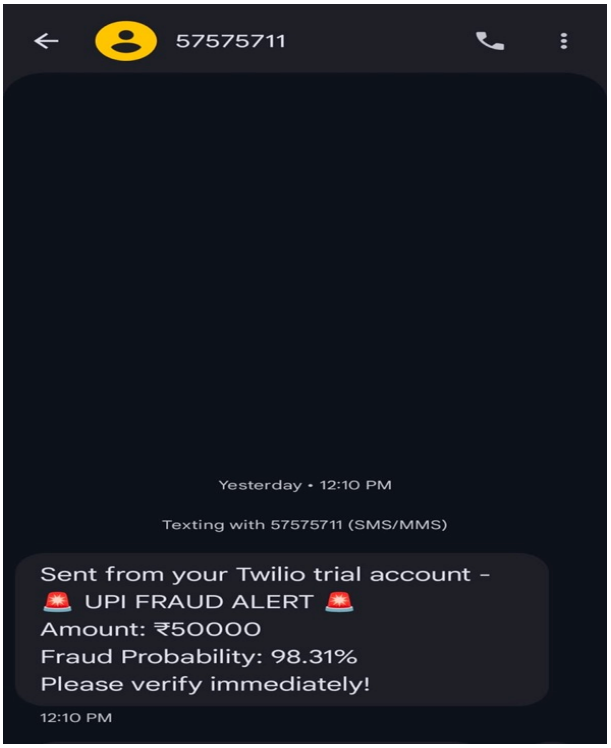
Supervised learning algorithms including Logistic Regression, Random Forest, and Gradient Boosting are implemented for classification. The dataset is divided into training and testing subsets to evaluate generalization performance. Model evaluation is conducted using metrics such as accuracy, precision, recall, and F1-score to ensure balanced fraud detection and minimal false positives.

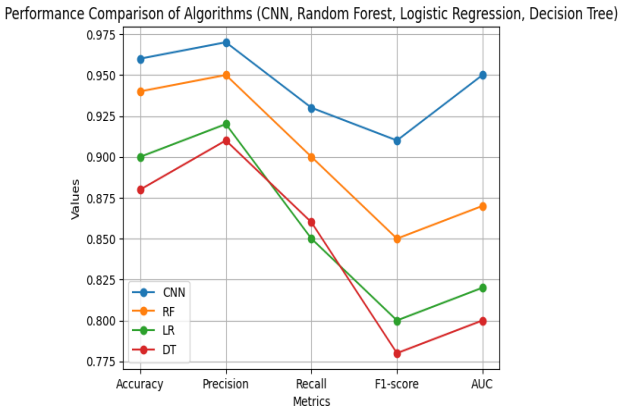
The best-performing model is integrated into the Fraud-Shield framework to enable real-time transaction monitoring. The system generates alerts for suspicious transactions and provides administrative monitoring capabilities through a dedicated dashboard.

VII. RESULTS AND ANALYSIS









VIII. CONCLUSION

The rapid expansion of digital payment systems has significantly increased the need for robust and intelligent fraud detection mechanisms. This research presented Fraud-Shield, a machine learning based framework designed to detect fraudulent transactions in real-time digital payment environments. The system integrates data preprocessing, feature engineering, and supervised learning algorithms to analyse transactional behaviour and classify suspicious activities effectively.

Experimental evaluation demonstrated that ensemble learning models such as Random Forest and Gradient Boosting outperform traditional classification approaches in terms of detection accuracy and reduction of false positives. The use of multiple evaluation metrics ensured balanced assessment, particularly in handling imbalanced transaction datasets. The proposed framework successfully identifies fraudulent patterns while maintaining operational efficiency.

The results confirm that data-driven fraud detection systems can significantly enhance the security and reliability of digital payment platforms. Fraud-Shield provides a scalable and adaptable solution capable of addressing evolving fraud strategies, thereby contributing to improved financial transaction safety.

IX. FUTURE SCOPE

Although the proposed Fraud-Shield framework demonstrates effective performance in detecting fraudulent transactions, there are several opportunities for further enhancement. Future work can focus on integrating deep learning models such as Artificial Neural Networks and Long Short-Term Memory networks to capture sequential transaction behaviour more effectively. These models can improve detection accuracy by identifying complex temporal fraud patterns.

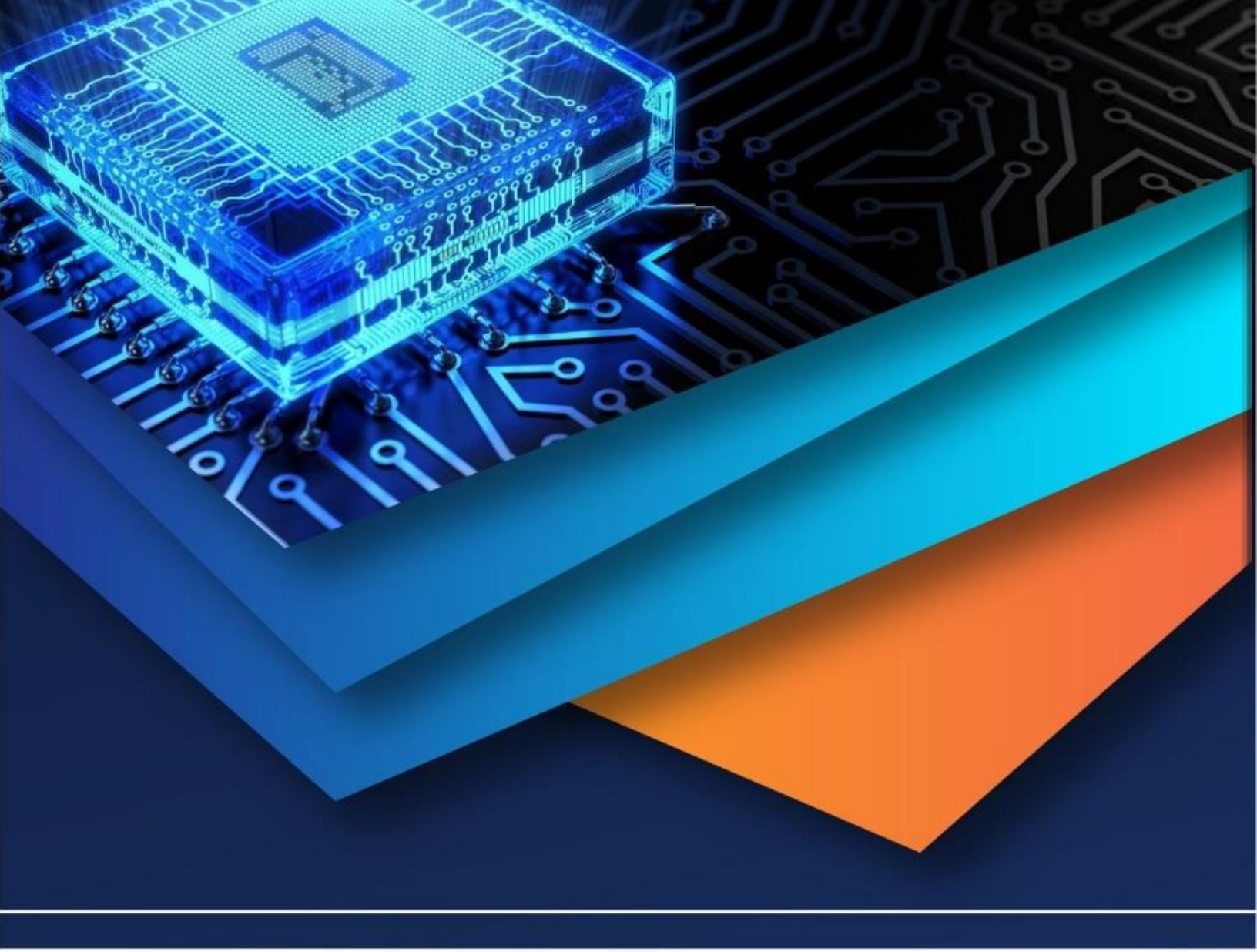
The system can also be enhanced by incorporating real-time streaming data processing technologies to improve scalability and reduce latency in high-volume transaction environments. Additionally, integrating behavioural biometrics such as typing patterns or device interaction behaviour may further strengthen authentication mechanisms.

Another potential improvement includes deploying the system using cloud-based infrastructure to support large-scale digital payment platforms. The integration of explainable artificial intelligence techniques can also be explored to provide transparency in fraud prediction decisions, thereby improving user trust and regulatory compliance.

Future research may also consider adaptive learning mechanisms that continuously update the model based on emerging fraud patterns, ensuring long-term robustness and reliability of the fraud detection system.

REFERENCES

[1] V. J. Hodge and J. Austin, “A survey of outlier detection methodologies,” *Artif. Intell. Rev.*, vol. 22, no. 2, pp. 85–126, 2004.
[2] A. Dal Pozzolo *et al.*, “Learned lessons in credit card fraud detection from a practitioner perspective,” *Expert Syst. Appl.*, vol. 41, no. 10, pp. 4915–4928, 2014.
[3] C. Phua *et al.*, “A comprehensive survey of data mining-based fraud detection research,” arXiv preprint arXiv:1009.6119, 2010.
[4] L. Breiman, “Random forests,” *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, 2001.
[5] J. H. Friedman, “Greedy function approximation: A gradient boosting machine,” *Ann. Stat.*, vol. 29, no. 5, pp. 1189–1232, 2001.
[6] Fawcett, “An introduction to ROC analysis,” *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, 2006.
[7] S. Bhattacharyya *et al.*, “Data mining for credit card fraud: A comparative study,” *Decis. Support Syst.*, vol. 50, no. 3, pp. 602–613, 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY