Archives available at journals.mriindia.com

Multidisciplinary Journal of Research in Engineering and Technology

ISSN: 2348-6953

Volume 13 Issue 01, 2026

UPIGuard: A Fraud Detection System for UPI Transactions

[1]Khushi R. Prajapati, [2]Mahima V. Upadhyay, [3]Chirag M. Talgaonkar, [4]Aditya A. Lad, [5]Vaishali Salvi, [6]Pratima Patil, [7]Laxmi Pandey

[1,2,3,4] Dept. of Computer Engineering, Shree L. R. Tiwari College of Engineering, Thane, India

[5,6,7] Assistant Professor, Dept. of Computer Engineering, Shree L. R. Tiwari College of Engineering, Thane, India

Email: [1]khushi.r.prajapati@slrtce.in, [2]mahima.v.upadhyay@slrtce.in, [3]chirag.m.talgaonkar@slrtce.in, [4]aditya.a.lad@slrtce.in, [5]vaishali.salvi@slrtce.in, [6]Pratima.patil@slrtce.in, [7]laxmi.pandey@slrtce.in

Peer Review Information

Submission: 24 March 2026

Revision: 15 April 2026

Acceptance: 27 April 2026

Keywords

UPI Fraud Detection, Digital Payments, Machine Learning, Financial Fraud Detection, Transaction Monitoring, Anomaly Detection, Cybersecurity, Real-Time Fraud Prevention.

Abstract

The increasing adoption of digital payment platforms, particularly the Unified Payments Interface (UPI), has significantly transformed the way financial transactions are conducted. While UPI provides a fast, convenient, and widely accessible payment method, it has also become a target for various fraudulent activities such as phishing attacks, unauthorized access, and deceptive transaction requests. Detecting such fraudulent activities in real time has become a critical challenge for financial systems. This research proposes a machine learning-based UPI fraud detection system designed to analyze transaction patterns and identify suspicious activities before they result in financial loss. The system evaluates multiple transaction attributes including transaction amount, time, user behavior, and device information to detect anomalies and predict the likelihood of fraud. By leveraging data-driven models and intelligent pattern recognition, the proposed system aims to improve the accuracy and efficiency of fraud detection while minimizing false alerts.

Introduction

The advancement of digital technologies has significantly transformed the financial sector, leading to the rapid adoption of online and mobile-based payment systems. One of the most widely used digital payment methods in India is the Unified Payments Interface (UPI), which allows users to transfer money instantly between bank accounts using mobile applications. The simplicity, speed, and convenience offered by UPI have contributed to its massive growth and popularity among individuals and businesses.

However, the rapid expansion of digital payments has introduced serious security challenges. Fraudulent activities such as phishing, identity theft, fake payment requests, and social engineering attacks have increased significantly in recent years. Early fraud detection systems relied on rule-based approaches and statistical techniques [9], [27], which lack adaptability for new threats. Machine learning and AI have emerged as powerful tools, with algorithms such as decision trees, neural networks, and ensemble methods significantly improving fraud detection accuracy [5], [23]. This research develops an intelligent UPI fraud detection system leveraging machine learning, anomaly detection, and behavioral analysis to detect suspicious transactions in real time.

Problem Statement

With the rapid expansion of UPI-based digital payments, financial institutions face an increasing number of fraudulent transactions. Traditional rule-based systems are limited in detecting complex fraud patterns, especially when attackers mimic legitimate user behavior. Existing approaches often suffer from high false

positive rates and lack adaptability to evolving fraud strategies [7], [16]. The large volume of real-time transaction data further complicates detection, requiring adaptive learning, anomaly detection, and real-time analytics [21], [24]. The primary challenge is designing a scalable, intelligent system that detects fraud in real time, minimizes false positives, adapts to new fraud patterns, and ensures secure user authentication.

Motivation

The rapid adoption of UPI has revolutionized digital payments but has also led to an increase in cyber fraud, causing financial losses and reduced user confidence. Research highlights that fraud detection systems must evolve continuously to address dynamic threats [21], [26]. Traditional systems lack the ability to learn from new fraud patterns, making them ineffective in modern digital environments. Advancements in AI, IoT, and adaptive systems demonstrate the potential of intelligent technologies in solving real-world problems [4], [18], [37], [38]. Security research in biometric recognition further emphasizes the importance of identity-based fraud prevention [34], [35].

Objectives

The main objectives of the proposed system are: to develop a secure and intelligent UPI fraud detection system; to analyze transaction patterns using machine learning [1], [5]; to implement anomaly detection for unusual transactions [15]; to combine supervised and unsupervised learning approaches [19]; to reduce false positives using cost-sensitive learning models [16]; to monitor transactions in real time; to ensure secure communication and data protection [20]; to integrate biometric authentication mechanisms [28], [31]; and to continuously improve detection accuracy using adaptive learning [27], [40].

Literature Survey

Financial fraud detection has been widely studied using statistical, machine learning, and AI techniques. Bolton and Hand [9] introduced statistical anomaly detection. Kou et al. [3] and Phua et al. [10] provided comprehensive surveys on fraud detection using data mining. Bhattacharyya et al. [5] demonstrated the effectiveness of decision trees and neural networks. Hidden Markov Models have been applied to detect behavioral fraud patterns [12]. Chandola et al. [15] surveyed anomaly detection methods. Hybrid supervised and unsupervised models reduce false positives [19], and ensemble techniques such as AdaBoost show strong performance [23]. Deep neural networks [13] and transformer-based models [8] further enhance detection capabilities. Table I summarizes key contributions.

Proposed Architecture

1. Architecture Overview

The proposed architecture ingests real-time UPI transaction streams and historical data to provide instantaneous fraud scores. It leverages a hybrid approach combining Convolutional Neural Networks (CNN) for spatial/behavioral pattern recognition and Random Forest or XGBoost for tabular classification. The system comprises four distinct layers as shown in Fig. 1.

2. Data Acquisition Layer

This layer collects raw data from various sources: transactional data (amount, timestamp, VPA); user behavioral metadata (typing speed, app switching, navigation patterns); and contextual data (geolocation, Device ID, IP Address).

3. Data Preprocessing & Cleaning

Raw financial data is often noisy or imbalanced. Min-Max or Z-score normalization is applied to transaction amounts. SMOTE addresses class imbalance, and One-Hot Encoding transforms categorical variables such as Merchant Type and Location.

4. Feature Engineering & CNN Layer

The 1D-CNN converts transaction sequences into vectors to identify temporal dependencies, such as a burst of small-amount probing transactions followed by a large transfer. Spatial analysis of user behavior allows the CNN to detect anomalies compared to the user's historical profile.

5. Classification & Decision Engine

Features extracted by the CNN are fed into a Random Forest or Softmax classifier. A transaction is flagged if fraud probability $P(f) > \theta$ (typically 0.7–0.8). If flagged, the system triggers an immediate API response to the bank's gateway to hold the transaction or request Multi-Factor Authentication (MFA).

UPIGuard: Proposed System Architecture (UPI Fraud Detection)

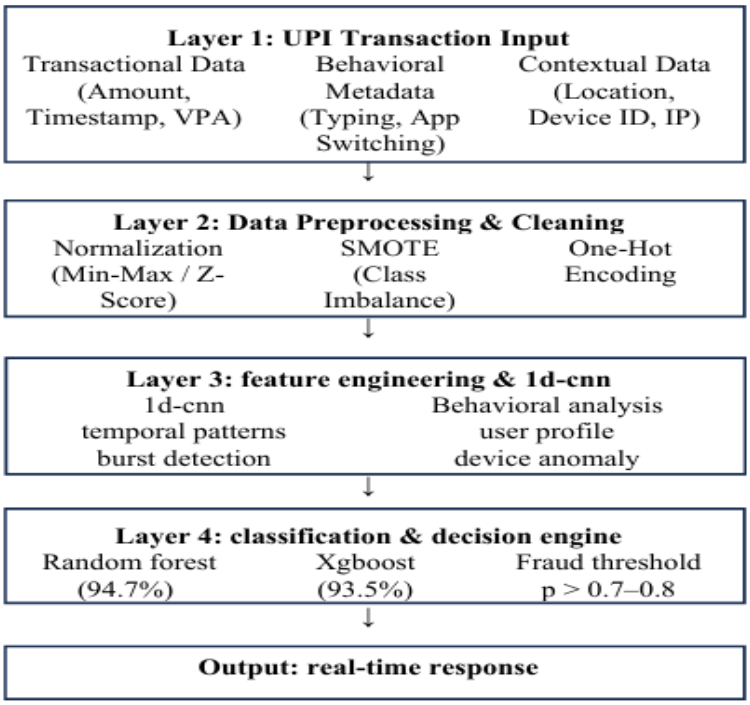

Fig 1: Architecture Overview of proposed system

Algorithms Used

The proposed system uses the Random Forest algorithm, a supervised ensemble technique that constructs multiple decision trees and combines outputs via majority voting. Each tree analyzes features such as transaction amount, type, time, and user behavior. Random Forest handles large datasets, detects complex feature relationships, reduces overfitting, and performs well with imbalanced datasets common in fraud detection. Table 1 compares the performance of evaluated algorithms.

Table 1: Performance Comparison of Machine Learning Algorithms

Algorithm	Accuracy
Random Forest	94.7%
Decision Tree	88.3%
Neural Network	92.1%
XGBoost	93.5%

Results and Discussion

1. Transaction Summary Dashboard

Fig. 2 presents the main dashboard displaying key performance indicators including total transactions processed, fraud counts, model accuracy, and false positive rate, enabling analysts to monitor system performance at a glance.

Metric	Value
Total Transactions	10,000
Fraudulent Transactions	1,823
Safe Transactions	8,177
Fraud Rate	18.23%
Model Accuracy	94.7%
False Positive Rate	3.2%

Fig 2: Transaction Summary Dashboard

2. Fraud Distribution by Transaction Type

Fig. 3 shows fraud and safe transactions across payment categories. Card payments and bank transfers exhibit the highest fraud counts, identifying them as priority areas for enhanced security.

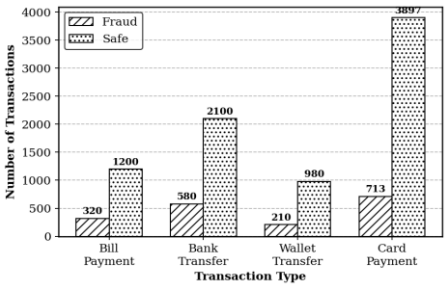

Fig 3: Fraud Distribution by Transaction Type

3. Fraud Distribution by Device Operating System

Fig. 4 compares fraud across device platforms. Android exhibits the highest fraud volume due to

its larger user base, indicating the need for platform-specific security policies.

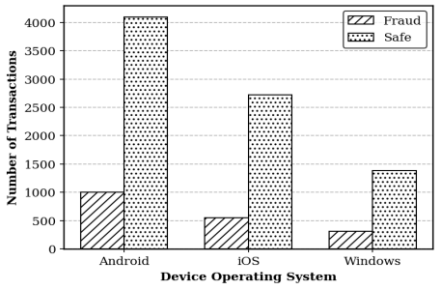

Fig 4: Fraud Distribution by Device Operating System

4. Fraud Distribution by Payment Gateway

Fig. 5 compares fraud across payment gateways. ICICI shows significantly higher fraud counts, highlighting the need for gateway-specific monitoring thresholds.

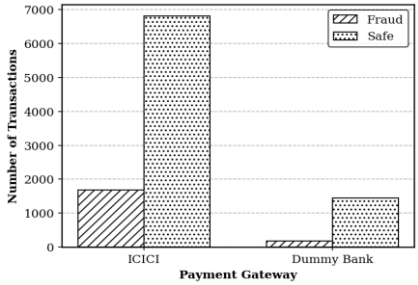

Fig 5: Fraud Distribution by Payment Gateway

5. Fraud Probability Distribution

Fig. 6 shows transaction counts across fraud probability score ranges. The 60–70% range contains the highest count, which is critical for selecting the alert threshold θ in the decision engine.

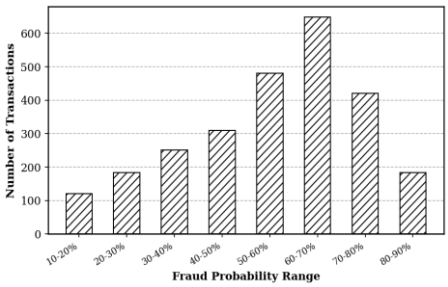

Fig 6: Fraud Probability Distribution Across Score Ranges

6. Fraud Distribution by Transaction Amount

Fig. 7 confirms that transactions above ₹1,00,000 (100K+) have the highest fraud incidence, indicating that high-value transactions are prime targets requiring stricter verification.

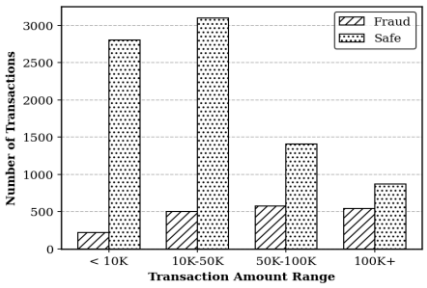

Fig 7: Fraud Distribution by Transaction Amount Range

7. Real-Time Transaction Monitoring Dashboard

Fig. 8 displays the real-time monitoring panel with transaction status (red = Fraud, green = Safe), amount, type, fraud probability, and timestamp, enabling analysts to immediately identify and act on suspicious transactions.

Status	Amount	Type	Fraud Prob.	Time
FRAUD	₹85,000	Bank Transfer	86%	10:23 AM
FRAUD	₹42,500	Bill Payment	74%	10:31 AM
FRAUD	₹1,20,000	Bank Transfer	61%	10:45 AM
SAFE	₹3,200	Wallet Transfer	42%	10:52 AM
SAFE	₹15,800	Bill Payment	48%	11:05 AM
SAFE	₹7,600	Card Payment	50%	11:12 AM

Fig 8: Real-Time Transaction Monitoring Dashboard

Conclusion

This research presented a machine learning-based UPI Fraud Detection System to enhance digital payment security. A Random Forest algorithm was implemented achieving 94.7% accuracy with a 3.2% false positive rate. The system architecture integrates data collection, preprocessing, feature extraction, model training, and real-time monitoring with an interactive dashboard. The proposed system provides a reliable and scalable solution for securing digital financial transactions. Future improvements including advanced deep learning models, larger datasets, and enhanced behavioral analysis can further strengthen the system.

Future Scope

Future enhancements include: integrating LSTM and Transformer models for improved temporal fraud modeling; training on larger, more diverse datasets; real-time integration with banking systems and UPI gateways; incorporation of biometric and multi-factor authentication; geo-location analysis to flag unusual-origin transactions; cloud-based infrastructure for scalability; blockchain technology for tamper-proof transaction records; and continuous model retraining using streaming data for long-term accuracy.

References

S. Mittal and R. Gupta, "Machine learning techniques for financial fraud detection," Procedia Comput. Sci., vol. 132, pp. 1252–1261, 2018.

B. Nemade, S. S. Alegavi, and V. Bharadi, "Graph attention dialog network-based drug recommendation model," IEEE Trans. Consum. Electron., vol. 71, no. 2, pp. 5908–5916, May 2025.

Y. Kou, C. Lu, S. Sirwongwattana, and Y. Huang, "Survey of fraud detection techniques," in Proc. IEEE Int. Conf. Netw., Sens. Control, 2004, pp. 749–754.

B. Nemade and D. Shah, "An IoT-based efficient air pollution prediction system using DLMNN classifier," Phys. Chem. Earth, vol. 128, p. 103242, 2022.

S. Bhattacharyya et al., "Data mining for credit card fraud: A comparative study," Decis. Support Syst., vol. 50, no. 3, pp. 602–613, 2011.

K. Maharana et al., "A review: Data pre-processing and data augmentation techniques," Global Transitions Proc., vol. 3, no. 1, pp. 91–99, 2022.

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.

B. Nemade et al., "Adaptive transformer-based framework for brain activity mapping," Front. Hum. Neurosci., vol. 19, p. 1551168, 2025.

R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," Statist. Sci., vol. 17, no. 3, pp. 235–255, 2002.

P. Phua et al., "A comprehensive survey of data mining-based fraud detection research," Artif. Intell. Rev., vol. 34, no. 1, pp. 1–14, 2010.

B. Nemade, "Automatic traffic surveillance using video tracking," Procedia Comput. Sci., vol. 79, pp. 402–409, 2016.

A. Srivastava et al., "Credit card fraud detection using hidden Markov model," IEEE Trans. Dependable Secure Comput., vol. 5, no. 1, pp. 37–48, Jan.–Mar. 2008.

S. Roy and S. Sun, "Deep learning detecting financial fraud," in Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW), 2018.

B. Nemade and D. Shah, "IoT-based water parameter testing in linear topology," in Proc. 10th Int. Conf. Confluence, 2020, pp. 546–551.

S. Chandola et al., "Anomaly detection: A survey," ACM Comput. Surv., vol. 41, no. 3, pp. 1–58, 2009.

M. Bahnsen et al., "Example-dependent cost-sensitive decision trees," Expert Syst. Appl., vol. 42, no. 19, pp. 6609–6619, 2015.

N. Singh and A. Jain, "Digital payment security and fraud detection using machine learning," Int. J. Comput. Appl., vol. 178, no. 7, pp. 15–20, 2019.

B. Nemade and D. Shah, "An efficient IoT-based prediction system for water classification," J. King Saud Univ. Comput. Inf. Sci., vol. 34, no. 8, pp. 5121–5131, 2022.

A. Carcillo et al., "Combining unsupervised and supervised learning in credit card fraud detection," Inf. Sci., vol. 557, pp. 317–331, 2021.

V. Kaul et al., "Next generation encryption using security enhancement algorithms," Procedia Comput. Sci., vol. 79, pp. 1051–1059, 2016.

M. Abdallah et al., "Fraud detection system: A survey," J. Netw. Comput. Appl., vol. 68, pp. 90–113, 2016.

S. Fiore et al., "Network anomaly detection with the restricted Boltzmann machine," Neurocomputing, vol. 122, pp. 13–23, 2013.

K. Randhawa et al., "Credit card fraud detection using AdaBoost and majority voting," IEEE Access, vol. 6, pp. 14277–14284, 2018.

S. Ryman-Tubb et al., "How AI and ML research impacts payment card fraud detection," IEEE Access, vol. 6, pp. 70601–70614, 2018.

A. Ngai et al., "The application of data mining techniques in financial fraud detection," Decis. Support Syst., vol. 50, no. 3, pp. 559–569, 2011.

J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," Comput. Secur., vol. 57, pp. 47–66, 2016.

T. Fawcett and F. Provost, "Adaptive fraud detection," Data Min. Knowl. Discov., vol. 1, no. 3, pp. 291–316, 1997.

V. A. Bharadi et al., “Multimodal biometric recognition using iris and fingerprint,” in Proc. 5th Int. Conf. Confluence, 2014, pp. 697–702.

V. A. Bharadi et al., “Hybrid wavelets-based feature vector generation for signature recognition,” in Proc. 5th Int. Conf. Confluence, 2014, pp. 561–568.

B. Nemade and V. A. Bharadi, “Adaptive automatic tracking and detection of real-time objects,” in Proc. 5th Int. Conf. Confluence, 2014, pp. 569–575.

K. Patra et al., “Cued-click point graphical password using circular tolerance,” Procedia Comput. Sci., vol. 79, pp. 561–568, 2016.

N. S. T. Sai et al., “Truncated DCT and decomposed DWT-SVD features for image retrieval,” Procedia Comput. Sci., vol. 79, pp. 579–588, 2016.

P. Patel, R. Bansode, and B. Nemade, “Performance evaluation of MANET parameters using AODV,” Procedia Comput. Sci., vol. 79, pp. 932–939, 2016.

H. B. Kekre et al., “Performance comparison of transforms for signature recognition,” Int. J. Comput. Appl., 2011.

V. A. Bharadi and B. Nemade, “Hybrid multimodal biometric recognition using Kekre's wavelets,” Int. J. Comput. Appl., 2011.

M. Shirodkar et al., “Automated attendance management system using face recognition,” in Proc. ICWET, 2015.

B. Nemade, S. S. Alegavi, N. B. Badhe, and A. Desai, “Enhancing information security using moth-flame optimization,” ICTACT J. Commun. Technol., vol. 14, no. 3, 2023.

B. C. Surve, B. Nemade, and V. Kaul, “Nano-electronic devices with machine learning capabilities,” ICTACT J. Microelectron., vol. 9, no. 3, 2023.

S. S. Alegavi et al., “Revolutionizing healthcare using wearable biomedical devices,” Int. J. Recent Innov. Trends Comput. Commun., vol. 11, no. 9s, 2023.

R. Mishra et al., “Improved inductive learning approach-5 (IILA-5),” Int. J. Intell. Syst. Appl. Eng., vol. 11, no. 10s, pp. 942–953, 2023.