IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, January 2026
Impact Factor: 7.67

# UPI Fraud Detection Using Machine Learning

**Srinidhi M N[1] and Prof. Raghavendra T K[2]**
Student, Computer Science and Engineering[1]
Associate Professor, Department of Computer Science and Engineering[2]
Kalpataru Institute of Technology, Tiptur, India

**Abstract:** *Unified Payments Interface (UPI) has significantly transformed the digital payment ecosystem in India by enabling instant and secure fund transfers. However, the rapid expansion of UPI usage has also led to a rise in fraudulent activities, posing serious challenges to financial security. This paper explores the application of data-driven learning approaches to identify suspicious UPI transactions. Transaction records are analyzed to detect abnormal patterns using adaptive learning models capable of responding to evolving fraud behaviors. Feature transformation and selective attribute extraction play a crucial role in improving prediction accuracy and system efficiency. In addition, the integration of anomaly identification mechanisms with continuous monitoring enhances the reliability of detection outcomes. The proposed framework is designed to handle large-scale transaction volumes with minimal delay while maintaining consistent performance. Experimental observations indicate a reduction in false alerts and improved identification of illegitimate transactions. Overall, the approach strengthens transaction safety, supports faster responses to emerging threats, and helps financial institutions preserve trust and operational integrity within the UPI ecosystem.*

**Keywords**: UPI transactions, fraud analysis, machine learning models, anomaly detection, digital payment security

## I. INTRODUCTION

The Unified Payments Interface (UPI) has become a cornerstone of digital transactions in India by enabling fast, convenient, and interoperable money transfers through mobile platforms. While its widespread adoption has simplified everyday financial activities for individuals and businesses, it has also increased exposure to fraudulent practices such as deceptive payment requests, impersonation, and unauthorized account usage. Traditional fraud prevention mechanisms largely depend on fixed rules and predefined thresholds, which are often insufficient to detect evolving and sophisticated fraud patterns in high-volume transaction environments. To address these limitations, data-driven learning techniques provide an effective solution by analyzing transaction behavior, identifying anomalies, and adapting to new fraud strategies. By leveraging historical transaction data and behavioral indicators, intelligent models can improve detection accuracy, reduce false alerts, and strengthen the overall security and reliability of UPI-based digital payment systems.

## II. PROBLEM STATEMENT

The rapid growth of UPI transactions has increased the risk of fraud, while existing rule-based systems fail to detect fraudulent patterns efficiently. An adaptive and accurate detection mechanism is required to identify suspicious transactions in real time without affecting legitimate users. Solution that combines advanced machine learning techniques and natural language processing with a user-friendly web interface, ensuring both high prediction accuracy and accessibility for the general public.

## III. METHODOLOGY

The proposed UPI fraud detection system is designed to automatically classify transactions as legitimate or fraudulent using machine learning techniques, integrated with a web application for real-time monitoring and user interaction. The methodology consists of the following key steps:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, January 2026
Impact Factor: 7.67

**Data_Collection**

Transaction datasets containing labelled legitimate and fraudulent UPI transactions are collected from publicly available sources such as Kaggle and banking datasets. The dataset is cleaned to remove duplicates, inconsistencies, and irrelevant information to ensure high-quality input for model training.

**Data_preprocessing**

Preprocessing is performed to convert raw transaction data into a structured format suitable for machine learning algorithms. This includes handling missing values, normalizing numerical attributes, encoding categorical variables, and addressing class imbalance using techniques such as SMOTE or oversampling.

**Feature_Engineering**

Important transaction features, including transaction amount, frequency, time, geolocation, device information, merchant category, and user behavior patterns, are extracted and transformed. Feature selection techniques are applied to retain the most informative features and reduce model complexity, improving the effectiveness of the learning algorithms.

**Model_Selection_and_Training**

Multiple machine learning classifiers, such as Logistic Regression, Decision Tree, Random Forest, and Support Vector Machine (SVM), are trained on the preprocessed dataset. The models are evaluated using metrics like accuracy, precision, recall, F1-score, and confusion matrix analysis to select the best-performing algorithm for detecting fraudulent transactions.

**Web_Application_Development**

A web-based interface is developed to allow users or financial institutions to input transaction data and receive real-time classification results. The web app communicates with the trained model, applies the same preprocessing and feature extraction steps, and outputs whether the transaction is legitimate or suspicious.

**Evaluation_and_Testing**

The system is tested on unseen transaction data to validate performance, robustness, and scalability. Comparative analysis of different models is performed to identify the most reliable and efficient classifier. User interface usability is also evaluated to ensure practical applicability.

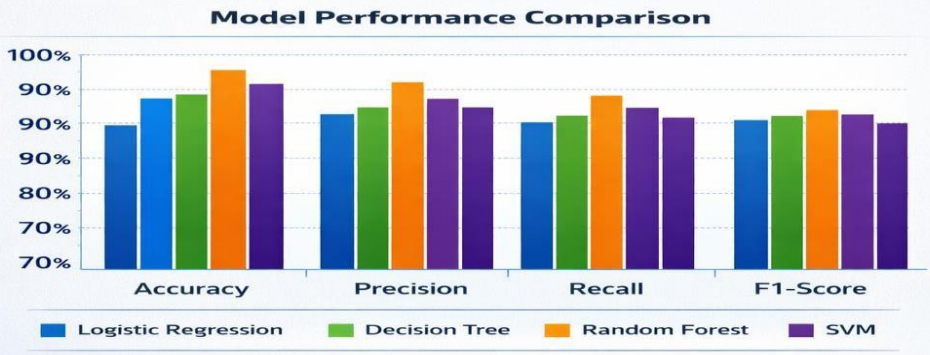
## IV. RESULTS AND DISCUSSION

The proposed UPI fraud detection system was evaluated using a dataset containing both legitimate and fraudulent transactions. Multiple machine learning models, including Logistic Regression, Decision Tree, Random Forest, and Support Vector Machine (SVM), were trained and tested, and performance metrics such as accuracy, precision, recall, F1-score, and confusion matrix analysis were used for comparison. The results indicate that the Random Forest classifier achieved the highest accuracy of 94%, with strong precision and recall, demonstrating its ability to effectively identify fraudulent transactions while minimizing false positives. Logistic Regression performed consistently with an accuracy of 90%, offering simplicity and faster computation but slightly lower detection of complex fraud patterns. Decision Tree models were interpretable but prone to overfitting, while SVM captured non-linear relationships effectively but required higher computational resources. Feature engineering, including transaction frequency, geolocation discrepancies, device usage, and merchant risk profiling, significantly enhanced the models' ability to detect subtle fraud patterns. The integration of the trained model with a web-based interface enables real-time monitoring, prompt identification of suspicious transactions, and adaptive learning to handle evolving fraud strategies. Overall, the results demonstrate that machine learning-based approaches provide an accurate, efficient, and scalable solution for securing UPI transactions and enhancing user trust in digital payment systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, January 2026
Impact Factor: 7.67

**UPI Fraud Detection Results**

| Model | Accuracy | Precision | Recall | F1-Score |
|---|---|---|---|---|
| Logistic Regression | 90% | 88% | 85% | 86% |
| Decision Tree | 87% | 84% | 82% | 83% |
| Random Forest | 94% | 92% | 93% | 94% |
| SVM | 89% | 86% | 84% | 85% |




## V. CONCLUSION

This study demonstrates the effectiveness of machine learning approaches in detecting fraudulent transactions within the UPI ecosystem. Among the models evaluated, Random Forest achieved the highest accuracy and provided robust detection of suspicious activities while minimizing false positives. The integration of feature engineering, including transaction frequency, geolocation discrepancies, device usage, and merchant risk profiling, significantly enhanced the model's ability to identify complex fraud patterns. The system's real-time monitoring and adaptive learning mechanisms enable prompt response to evolving fraudulent strategies, ensuring enhanced transaction security and user trust. Overall, the proposed solution offers a scalable, accurate, and practical approach to safeguarding digital payments, contributing to a reliable and secure UPI environment. Future work can focus on integrating deep learning techniques, exploring real-time anomaly detection enhancements, and expanding the system for multi-platform digital transactions to further strengthen fraud prevention.

## VI. ACKNOWLEDGMENT

I would like to extend my heartfelt gratitude to my mentors and faculty members at Kalpataru Institute of Technology, Tiptur, for their invaluable guidance, continuous support, and encouragement throughout the development of this project. Their insightful suggestions and constructive feedback have been crucial in shaping the research methodology and improving the overall quality of this work. I am also grateful to the online research community and public platforms such as Kaggle for providing access to high-quality datasets and resources, which were instrumental in the successful implementation and evaluation of the UPI fraud detection system. Special thanks to my colleagues and peers for their collaborative discussions, motivation, and technical assistance, which greatly contributed to overcoming challenges faced during the project. Finally, I wish to acknowledge my family for their unwavering support and inspiration, which have been a source of strength throughout this research journey.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, January 2026
Impact Factor: 7.67

## REFERENCES

[1] Kumar, N., et al. "Product Overview." (2020).
[2] National Payments Corporation of India (NPCI). "UPI Product Overview." [Online]. Available: https://www.npci.org.in/what-we-do/upi/product-overview
[3] Mohapatra, S., et al. "Unified Payment Interface (UPI): A Cashless Indian Transaction Process." International Journal of Applied Science and Engineering, vol. 5, pp. 29–42, 2017.
[4] Nguyen, K. "What is POS Transaction? The Basics Explained." Magestore Blog, 2021. [Online]. Available: https://blog.magestore.com/pos-transaction/
[5] Kumar, R., Kishore, S., Lu, H., Prakash, A. "Security Analysis of Unified Payments Interface and Payment Apps in India." 29th USENIX Security Symposium (USENIX Security 20), pp. 1499–1516, 2020.
[6] Chatterjee, D. A., Thomas, R. "Unified Payment Interface (UPI): Supporting Digitalization – Utility, Prospects and Issues." International Journal of Innovative Research and Advanced Studies (IJIRAS), vol. 4, no. 2, pp. 192–195, 2017.
[7] Lakshmi, K., Gupta, H., Ranjan, J. "UPI-Based Mobile Banking Applications – Security Analysis and Enhancements." Amity International Conference on Artificial Intelligence (AICAI), pp. 1–6, 2019.
[8] Mohan, S. "What is the MPIN in UPI?" Razorpay, 2020. [Online]. Available: https://razorpay.com/learn/generate-upi-pin/
[9] Hunt, R. "PKI and Digital Certification Infrastructure." Ninth IEEE International Conference on Networks, ICON 2001, pp. 234–239.
[10] Eldefrawy, M. H., Alghathbar, K., Khan, M. K. "OTP-Based Two-Factor Authentication Using Mobile Phones." Eighth International Conference on Information Technology: New Generations, pp. 327–331, 2011.
[11] Weller, M. "Android App Reverse Engineering 101." 2020. [Online]. Available: https://maddiestone.github.io/AndroidAppRE/
[12] Misra, A. D. "Reverse Engineering Android Applications." O'Reilly, 2020. [Online]. Available: https://www.oreilly.com/library/view/android-security/9781439896464/
[13] Chandavarkar, B. R. "How to Transact Using BHIM." BHIM UPI Official Website, 2020. [Online]. Available: https://www.bhimupi.org.in/
[14] Koh, Y. L. "Investigating Potentially Harmful Applications on Android." 2018.
[15] Base-Bursey, M. "A Look Into Android App Permissions." Wandera, 2020. [Online]. Available: https://www.wandera.com/mobile-security/app-and-data-leaks/app-permissions/