ijamrsd.com
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal | Bi-monthly | Open Access

AI-POWERED UPI FRAUD DETECTION AND ALERT SYSTEM

Ms. Samruddhi Vinayak Mahale[1], Ms. Shubhangi Sopan More[2], Ms. Anam Akhtar Shaikh[3], Ms. Bhairavi Jaykumar Patil[4]

[1,2,3,4] *Department of Computer Engineering, Loknete Gopinathji Munde Institue of Engineering Education and Research Nashik, India.*

Email: mahalesamruddhi09@gmail.com[1], shubhangimore2004@gmail.com[2], anamsk111@gmail.com[3], bhairavijpatil46@gmail.com[4]

Abstract

The AI Powered UPI Fraud Detection and Alert System is a smart mobile application designed to protect users from online financial frauds involving fake brand websites and fraudulent UPI IDs. With the surge in digital payments through Unified Payments Interface (UPI), cybercriminals have begun exploiting user trust by creating fake websites and UPI IDs that mimic genuine businesses or brands. This project provides a real-time fraud detection and alert system that helps users identify suspicious activities before making transactions. The motivation behind this system comes from the growing number of UPI related scams in India, where unsuspecting users are tricked into sending money to fraudulent accounts through fake payment links or cloned websites. Current payment apps lack the ability to verify the authenticity of UPI IDs or detect risky domains. Hence, an intelligent, AI-driven tool is needed to ensure user safety during UPI transactions. The outcome of this project is a fully functional mobile app that verifies UPI IDs. The app is built using Flutter for cross-platform functionality, with Firebase integration for real-time database operations. It uses AI and machine learning models trained to identify patterns in blacklisted UPI IDs, phishing URLs, and risk behaviors. The Firebase collections (blacklisted upi, risk patterns, ml models) help the system store and retrieve fraud data efficiently. The innovation of this project lies in combining AI-based fraud detection, real-time Firebase integration, and a community-driven reporting mechanism, allowing users to contribute to a shared fraud database. Unlike existing payment systems, this application proactively scans and alerts users before transactions occur, significantly reducing the risk of financial scams. The project represents a forward-looking step toward building a secure, intelligent, and trustworthy digital payment ecosystem in India.

Keywords: UPI Fraud Detection, Machine Learning, Random Forest, Cybersecurity, Digital Payments, Firebase, Flutter App, Real-time Alerts, Data Security, AI-based Verification.

► *Corresponding Author: Ms. Samruddhi Vinayak Mahale*

I. Introduction

In recent years, the use of UPI has grown rapidly in India and revolutionized the aspect of digital transactions. While it makes it faster, easier, and quick for millions of users, with this increasing rate comes an important concern: a sudden surge in UPI frauds. Scammers create fake UPI IDs and clone the legitimate payment links of brands to trick users into transferring money. As a result, many people fall victim to such frauds, losing money and personal information.

To meet the challenge, our project introduces an AI-enabled UPI Fraud Detection and Alerting System. Using Machine Learning algorithms, it distinguishes fraudulent UPI IDs through pattern identification, detecting anomalies, and matching with known fraudulent data. When any user enters or scans a UPI ID, the system validates it in real time and generates an alert if it appears suspicious or linked to fraudulent activity.

The system has a Python-based backend with Random Forest as the main classification algorithm. A verified and fraudulent UPI IDs dataset is available for training the model. Flutter is being used for the development of the frontend, which will provide a user-friendly interface on both Android and iOS platforms. Firebase is used to store and manage the data securely with real-time verification and sync.

The main objective of our project is to enhance digital payment security and build user confidence in UPI-based systems. This system aims at preventing fraud before it actually happens, rather than reacting post-loss. Along with the detection, the system supports community reporting through which users can report fake UPI IDs or suspicious links, contributing to a shared fraud-prevention network.

Another significant aspect of the project is brand verification. A number of fraudsters impersonate popular companies by creating fake websites or payment links. Our system helps verify the legitimacy of such brands and ensures users interact only with genuine UPI identifiers. The project is lightweight, free of cost, and highly scalable. It is designed for students, merchants, and daily users who quite often use UPIs to make transactions. The system works on even the most basic smartphones with low internet connectivity.

This project integrates AI, cybersecurity, and mobile development technologies in a model demonstrating how intelligent systems can make online payments safer. It learns

II. Literature Review

A. Limited Real-World Validation While several research papers and systems discuss machine learning-based fraud detection in digital payments, most are evaluated only on static or synthetic datasets. Gap : There is a lack of real-world validation or pilot testing on live UPI transaction data to assess the system's accuracy, response time, and user adoption.

B. Dynamic Nature of Fraudulent Patterns Most of the current systems either use a pre-trained model or rule-based approaches, which become outdated as fraud patterns change rapidly. Gap: The absence of a model that continuously learns from different modalities to cope with newly emerging fraud techniques such as brand impersonation or fake UPI handles.

D. Integration with Existing Payment Infrastructure Much fraud detection research is targeted at banking-level systems, while UPI is inherently a peer-to-peer, open ecosystem. Gap: The solutions are not directly integrated with UPI-based apps or Firebase-backed platforms, which can give instant fraud verification before completing a transaction

E. Data Privacy and Security While fraud detection necessarily involves the analysis of user data, many systems proposed do not discuss how sensitive information is safeguarded. Gap: Well-defined data privacy mechanisms to keep UPI ID, transaction logs, and user reports safe while maintaining regulatory compliances.

F. Brand and Website Verification Most fraud detection in UPI today doesn't catch fraud at the brand level, such as a cloned e-commerce website or a faked payment link. Gap: Missing module for brand authenticity verification, which would confirm if the UPI handle or the website genuinely belongs to a registered business entity.

G. Scalability and Real-Time Processing Most fraud systems based on machine learning work in offline or batch mode. Gap: No real fraud detection system with immediate alerting mechanisms can process a high volume of transactions within a short time using optimized models, including Random Forest.

III. Problem Statement

The surging adoption of UPI in India has also resulted in scams regarding fake web- sites of various brands and fraudulent UPI IDs created by cyber crooks. These rogue websites impersonate genuine businesses and deceive users into transferring money or disclosing personal information. None of the UPI apps are currently able to detect and raise alerts in real time against fraudulent activities. In this respect, the chal- lenge is to design and develop an AI-driven system that can identify suspicious UPI IDs with high accuracy and send instant alerts to users before any transaction takes place. It has to upgrade digital payment security, reduce losses on financial fronts, and help restore user confidence in transacting through UPI.

IV. Objectives

The main objective of this work is to design and implement an AI-powered digital system that can detect fraudulent UPI IDs and fake brand links in real time. The proposed solution ensures secure and trustworthy digital transactions by using machine learning techniques along with real-time alert mechanisms on a mobile-based platform.

Integration with a Firebase-backed mobile interface is also within the scope of this study through Flutter to further enhance user interaction, accessibility, and security. The system enables instant verification of UPI IDs, reporting of suspicious accounts, and real-time fraud alerts for ensuring safety in digital payment through the participation of users on the platform.

Another objective is community-based fraud reporting and maintaining an ever-growing fraud database that increases the accuracy of detection via machine learning model retraining. A system based on algorithms like Random Forest allows for the learning from new patterns and dynamic adaptation to emerging techniques of fraud.

Long-term goals include reducing financial losses, instilling user confidence in UPI-based payment systems, and aligning with government initiatives on increasing digital transactions in India.

A. Prevention of UPI Fraud and User Protection

To design a machine learning-based system that automati-cally detects fraudulent UPI IDs and fake brand payment pages before transactions occur.To protect users from fraud, it pro-vides instant fraud probability scores along with notification alerts. transactions occur.

B. Integration of AI Models with Real-Time Alerting System

To implement a Random Forest algorithm that detects fraud based on transaction behavior, pattern identification in UPI IDs, and historical data.To offer real-time notifications via the mobile application for better decision-making on transactions by the end.

C. Centralized Fraud Detection and Reporting Platform

This objective seeks to unify the platform for users, devel-opers, and authorities on one platform for transparent fraud management. Currently, the reporting of UPI fraud by users is done through fragmented channels, resulting in delayed responses and loss of critical evidence. The proposed system consolidates fraud verification, user alerts, and reporting into a single ecosystem, assuring efficiency and traceability.Verified reports are stored through the Firebase database, while the AI

model continuously updates itself using new fraud entries. This not only improves the detection accuracy but also builds a national-level fraud intelligence network.

D. Accessibility, Security, and Continuous Improvement

This objective stresses the creation of a system that is secure, easy to use, and scalable on mobile devices. The app guarantees data privacy and encryption, coupled with conformity to digital payment standards. It also allows for continuous model retraining on community-reported fraud data to adapt dynamically to new threats. With high scalability assurance, the system supports large user bases by providing fast responses while maintaining high accuracy levels.

V. Methodology

The AI-Powered UPI Fraud Detection and Alerting System follows a structured methodology to ensure accurate detection, with real-time responses through user-friendly interactions. It starts with the requirement analysis, where it studies user behavior, UPI fraud cases, and transaction data for identi-fication of fraudulent activity patterns. Based on such find-ings, the system design phase outlines the architecture by integrating modules on data preprocessing, machine learning-based fraud detection, real-time alerts, and community-based reporting through a secured mobile interface. The technology stack consists of Python for AI model development, Flutter for the frontend mobile app, and Firebase for handling the database and authentication. Machine learning algorithms such as Random Forest enable fraud probability predictions. During the development and integration phase, the AI model, mobile interface, and Firebase backend are aligned and integrated for seamless fraud detection and real-time alerts to users. Rigorous testing ensures accuracy, security, and real-time functionality ahead of deployment on mobile platforms, with further scope for integration on the web. Continuous updates and retraining of the AI model enhance the system's efficiency and adaptability to new fraud patterns.

A. Requirement Analysis

A detailed requirement analysis was performed through the study of common UPI fraud techniques, users' transaction behaviors, and online reports from verified cases of payment fraud. The collected data helped identify critical attributes such as transaction frequency, UPI ID patterns, and fraud reports used for the training of the AI model. This also included the determination of end-user needs, including easy UPI ID verification, alert notifications, and report submission features, which would definitely make sure that the system addresses real-world digital payment security issues.

B. System Design

This includes a number of key components in the archi-tecture of the system: data preprocessing, a machine learn-ing model, a real-time alert generator, and a Firebase-based database. A mobile interface using Flutter allows users to verify UPI IDs and get instant alerts on possibly fraudulent transactions. The backend AI module, implemented in Python, executes data preprocessing, training, and classification of fraud cases. This modular architecture ensures scalability, reliability, and secure data communication between the AI model and the user interface.

C. Technology Stack

The proposed system utilizes a modern and secure technol-ogy stack to ensure seamless development and deployment:

- Frontend: Flutter (for cross-platform mobile application).
- Backend: Firebase (for authentication, cloud storage, and real-time database).
- AI & Model Training: Python, Pandas, NumPy, Scikit-learn, (for fraud detection and classification).

- Integration Tools: Firebase SDKs, REST APIs for real-time model communication

VI. System Architecture

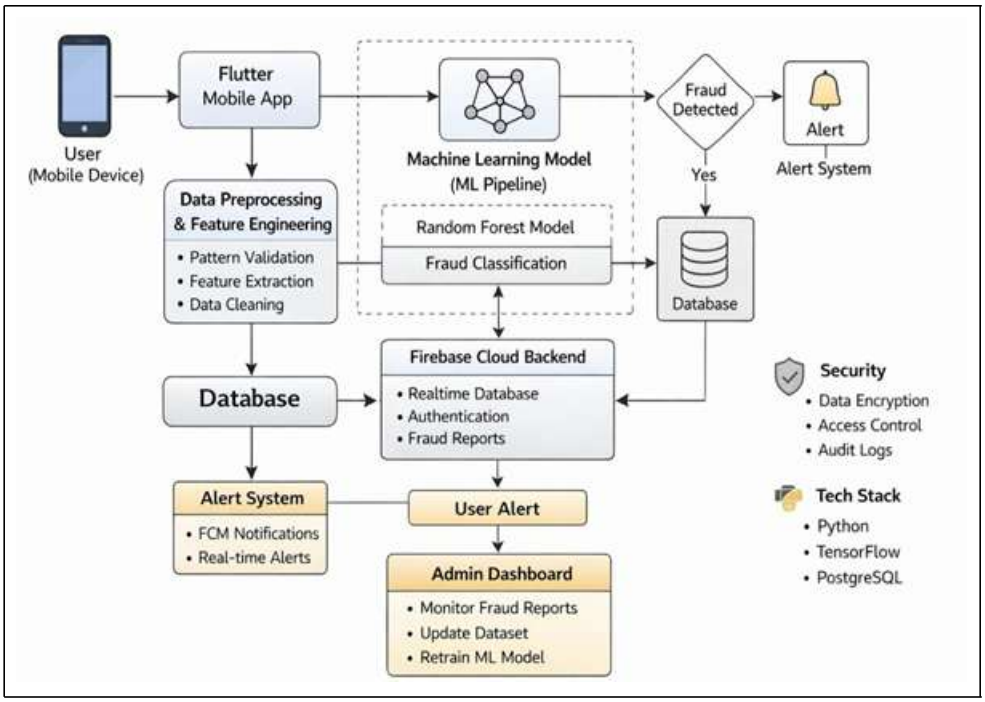

Fig. 1. UPI fraud detection and alert system.

1) User Interface (Flutter App):
The frontend is developed using Flutter, providing a simple and interactive mobile interface. Users can input or scan a UPI ID, view verification results, and receive real-time fraud alerts through push notifications.

2) Data Preprocessing Module:
Once a UPI ID is submitted, the system performs preprocessing tasks such as pattern validation, cleaning of input data, and extraction of key features (e.g., ID frequency, report count, and origin source). This ensures that the data is in a suitable format for model prediction.

3) AI Model (Machine Learning Engine):
The preprocessed data is passed to the AI model built using Random Forest and implemented in Python with Scikit-learn and TensorFlow. The model analyzes the UPI ID's characteristics and classifies it as either Genuine or Fraudulent based on learned patterns.

4) Firebase Integration:
Firebase serves as the cloud backend for storing verified UPI IDs, fraud reports, and user feedback. It enables real-time data synchronization between the app and the machine learning engine and also manages user authentication securely.

5) Alert and Notification Module:
If the AI model detects a potentially fraudulent UPI ID, the system immediately triggers a real-time alert through Firebase Cloud Messaging (FCM). The alert is displayed on the user's device, warning them of possible fraud.

6) Admin Dashboard:
Administrators can view fraud reports, monitor system performance, and update the model dataset. This ensures continuous improvement in accuracy through retraining.

7) Data Storage Layer:
All datasets, trained models, and logs are stored securely in Firebase and local cloud storage. The model peri-odically updates with new data to improve prediction reliability.

VII. Conclusion

This project demonstrates a practical application of AI to reduce UPI financial fraud by monitoring potential fraud before it happens. Using predictive analytics coupled with a user-friendly mobile app, users are warned in real-time against high-risk UPI IDs to prevent monetary loss. Integration of ML models, cloud storage, and a mobile frontend ensures security, efficiency, and real-time fraud detection. The system lays the base for future enhancements such as integrating live transaction systems, adap- tive updating of models, and wider deployment to build trust in UPI transactions.

Acknowledgement

We would like to express our sincere gratitude to Prof. G. V. Barde, Department of Computer Engineering, Loknete Gopinathji Munde Institute of Engineering Education & Re-search, Nashik, for his continuous guidance, encouragement, and valuable feedback throughout the development of this project. His support and insightful suggestions played a vital role in the successful completion of this work.
We also extend our sincere thanks to the Department of Computer Engineering and the institute for providing the nec-essary infrastructure and resources to carry out this research work.
Finally, we express our heartfelt appreciation to all faculty members and peers who contributed through their assistance and constructive discussions during the course of this project titled "AI-Powered UPI Fraud Detection and Alert System."

References

1. N. P. Khopade & S. M. Vitalkar, "UPI Fraud Detection Using Machine Learning," International Journal of Research in Interdisciplinary Studies (IJRIS), Vol. 3, No. 6, pp. 24–26, Jun. 2025.
2. Jallapuram Sindhu & Vijaya Sree Swarupa, "UPI Fraud Detection Using Machine Learning Algorithms," International Journal of Engineering Research and Science & Technology (IJERST), Vol. 20, No. 4, 2024, pp. 57–67.
3. Kothapally Chandini, Akoju Mahender & P. Venkateshwarlu, "UPI Fraud Transaction Detection Using Machine Learning," International Journal of Engineering Research and Science & Technology (IJERST), Vol. 21, No. 4, 2025, pp. 281–285.
4. Renu Chaudhary, Sakshi Singh, Riddhima Singh, Husain Zaidi & Kanishka Jain, "Fraud Detection in UPI Payments Using Tabular Machine Learning Models," IJRASET, 2025-10-31.
5. D. Jaya Kumari, G. Tejaswi, N. Jahnavi Nekkanti, A. Korapati, K. Kotakonda & S. Medapati, "AI-Powered UPI Fraud Detection," International Journal of Innovative Science and Research Technology (IJISRT), Vol. 10, No. 4, 2025, pp. 1208-1213.
6. Akinnagbe O. B. & Akintayo T. A., "The Impact of Machine Learning on Fraud Detection in Digital Payment," Asian Journal of Science, Technology, Engineering, and Art (AJSTEA), Vol. 3, No. 2, 2025, pp. 191-209.
7. Md Zahin Hossain George, Md Khorshed Alam & Md Tarek Hasan, "Machine Learning for Fraud Detection in Digital Banking: A Systematic Literature Review," arXiv preprint, Oct. 2025.
8. Junliang Wang, "Fraud Detection in Digital Payment Technologies Using Machine Learning," Journal of Economic Theory and Business Management, DOI:10.5281/zenodo.10926495.

9. Jakka Venkata Vara Sidhu Naidu, "Machine Learning-Based UPI Fraud Detection System," JETIR, Vol. 12, Issue 3, March 2025.
10. Zong Ke, Shicheng Zhou, Yining Zhou, Chia Hong Chang & Rong Zhang, "Detection of AI Deepfake and Fraud in Online Payments Using GAN-Based Models," arXiv preprint, Jan. 2025.