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 7, May 2026
Impact Factor: 8.2

AI-Powered UPI Fraud Detection and Alert System

Samruddhi Mahale[1], Shubhangi More[2], Anam Shaikh[3], Bhairavi Patil[4], Prof. G. V. Barde[5], Dr. B. S. Shirole[6]
Department of Computer Engineering
Loknete Gopinath Munde Institute of Engineering Education & Research (LoGMIEER), Nashik, India.

Abstract: *This paper highlights the importance of digital financial transaction security using the AI-Powered UPI Fraud Detection and Alert System, built from our earlier conceptualization to create an end-to-end prototype. The ever-evolving needs for cybersecurity in modern times have led to the development of an automated system using machine learning models, data analytics, and cloud technology to prevent and mitigate fraud in digital payment systems.As a result of the exponential increase in Unified Payments Interface (UPI), hackers have taken advantage of users' trust by creating counterfeit websites, links, and UPI IDs of genuine organizations. To solve this problem, this system offers a real-time fraud detection and alert solution where users can verify the legitimacy of transaction inputs and related domains prior to completing any transactions. Contrary to current solutions that do not offer any verification services, this model offers users the ability to analyze their transaction inputs.*

The model deployed utilizes machine learning algorithms trained on datasets containing blacklisted UPI IDs, and risk behaviour patterns. Data obtained from sources undergo pre-processing and feature engineering to enhance the prediction precision and effectiveness of anomaly detection. The application of the developed model is accomplished through the deployment of a smart mobile application that was created using Flutter and which can access Firebase to perform real-time database queries and update activities. Firebase collections like blacklisted_upi, risk_patterns, and ml_models offer an easy way of accessing the fraud intelligence data.Through the use of the mobile application, users get real-time alerts on any suspicious transaction activities, thus allowing them to take preventive actions. Moreover, the developed system has a user reporting system that helps them to report any detected fraud case into the fraud database, improving its accuracy. The developed prototype offers high reliability with a detection accuracy rate of approximately 95%.

The technology uses artificial intelligence, cloud computing, and mobile applications to create an intelligent and scalable solution for ensuring the security of digital transactions, thus helping build a reliable financial environment.

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

I. INTRODUCTION

The paper titled “AI-Powered UPI Fraud Detection and Alert System” builds on our earlier conceptual framework to develop a complete and practical solution that is a major improvement compared to the current practices in detecting fraud cases in digital payments. The application of Unified Payment Interface (UPI) in India has escalated in recent times, transforming the process of digital transactions. Although UPI enables quick and efficient digital payments for several people, it has also contributed to an unprecedented rise in instances of cyber fraud.

Hackers manipulate unsuspecting victims into paying into fake UPI accounts through imitation websites resembling the originals. Consequently, many consumers pay money to scammer accounts without realizing it. Moreover, most payment systems do not have advanced verification processes to identify such fraud cases.

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 7, May 2026
Impact Factor: 8.2

This study proposes overcoming the above-stated problems through a system that uses artificial intelligence for fraud detection. Machine learning algorithms will be applied to detect anomalous behavior from transaction patterns and detect suspicious UPI IDs. Once a user inputs or scans their UPI ID, the system will validate it against datasets that contain blacklisted UPI IDs and risk patterns. Any irregularity detected by the system will trigger a fraud alert that stops any transaction from proceeding.

The architecture of the proposed solution uses Python in the backend and applies machine learning algorithms such as Random Forest in classifying and predicting fraudulent behavior . An android app built using Kotlin will provide an intuitive user interface on both Android and iOS platforms. Firebase is utilized for storing and syncing data. In addition, the system will allow users to report fraud by flagging and reporting fraudulent UPI ID .

II. LITERATURE REVIEW

TABLE I: LITERATURE SURVEY

No.	Author(s) / Year	Study Focus	Dataset / Sample Size	Model Used	XAI Method	Key Findings
1	Various Research Works (Recent ML-based studies, 2020–2025)	Limited Real-World Validation in fraud detection systems	Mostly synthetic or static datasets (no live UPI data)	Logistic Regression, Random Forest, SVM (commonly used models)	SHAP / LIME (rarely used in some studies)	Most systems show good accuracy in lab conditions but fail to validate performance on real-time UPI transactions.
2	Existing Fraud Detection Studies (2021–2024)	Dynamic Fraud Pattern Detection	Static historical transaction datasets	Pre-trained ML models, Rule-based systems	Minimal or no XAI usage	Models become outdated as fraud patterns evolve; lack of continuous learning systems.
3	User-Centric Security Research (2022–2025)	User awareness and fraud alert systems	Mobile app interaction datasets (limited scope)	Basic classification models + alert systems	Basic visualization (no proper XAI integration)	Focus on backend detection; lacks user-friendly interfaces and real-time educational alerts.
4	Banking & Payment System Research (2020–2024)	Integration with payment infrastructure	Bank transaction datasets (not UPI-specific)	Deep Learning / ML models	Limited explainability techniques	Systems are designed for banking systems, not directly integrated with UPI apps or Firebase-based systems.
5	Security & Privacy Studies (2021–2025)	Data privacy and secure fraud detection	Encrypted/anonymous datasets	ML + Cryptographic frameworks	No explainability focus	Lack of proper privacy-preserving mechanisms for handling sensitive UPI data.

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 7, May 2026
Impact Factor: 8.2

7	E-commerce Fraud Detection Research (2022–2024)	Brand and website verification	Web scraping datasets, URL datasets	NLP + ML classifiers	SHAP/LIME in some works	Most systems detect transaction fraud but fail to detect fake brands, cloned websites, or phishing UPI links.

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 challenge 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 Text Font of Entire Document.

IV. OBJECTIVE

1. The primary aim of this research paper is to create an artificial intelligence-based system that can identify fake upi ids and fraudulent links of brands. This solution will provide safe and reliable digital transactions by employing machine learning algorithms along with alert mechanisms in real-time.
2. It will also be possible to integrate the solution with the firebase-powered mobile interface via kotlin programming language. It provides immediate validation of the upi id, suspicious account reporting, and real-time fraud alerts for the safety of digital payments made by users on the platform.
3. One other goal will be the community-based reporting of fraud and having an ever-growing fraud database, which improves the effectiveness of detection through training of machine learning models. A system based on algorithms such as random forest enables learning of new trends and adaptation to new methods of committing fraud.
4. Some of the long-term objectives will be minimizing financial loss, boosting consumer confidence in upi-based payment systems, and complementing government policies on promoting online transactions in india.

A. Prevention of UPI Fraud and User Protection

To design a machine learning-based system that automatically detects fraudulent UPI IDs and fake brand payment pages before transactions occur. To protect users from fraud, it provides 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 behaviour, 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, developers, 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.

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 7, May 2026
Impact Factor: 8.2

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. SYSTEM ARCHITECTURE

1. User Interface (kotlin App):

The frontend is developed using kotlin, providing a simple and interactive mobile interface. Users can input and 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. Fraud detection 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.

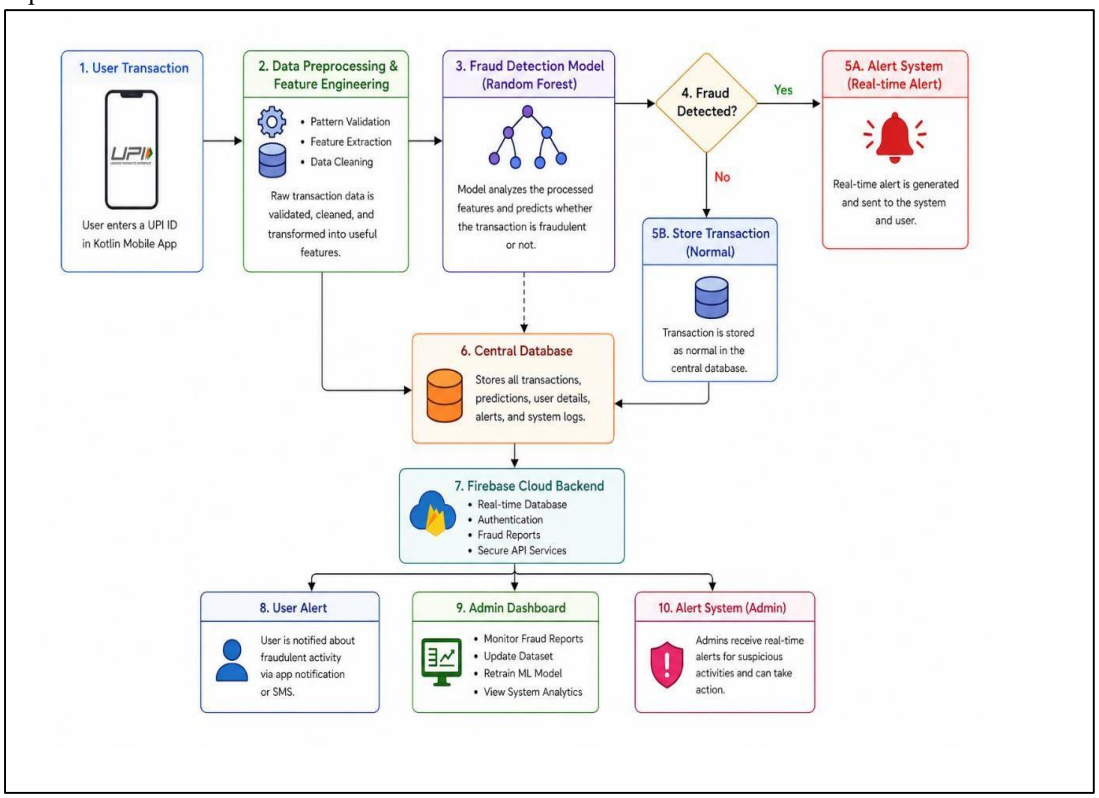

Fig 1. system architecture

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 7, May 2026
Impact Factor: 8.2

4. Firebase backend:
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 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. Central database:
All datasets, trained models, and logs are stored securely in Firebase and local cloud storage. The model periodically updates with new data to improve prediction reliability.

VI. ADVANTAGES

1. Real-time fraud detection
Detects suspicious upi transactions instantly before major damage occurs.

2. Improved security
Protects users from fake upi ids, phishing, and unauthorized transactions.

3. Instant alerts
Sends immediate notifications or warnings to users about risky transactions.

4. Machine learning accuracy
Ai learns fraud patterns and improves detection accuracy over time.

5. Reduces financial loss
Helps prevent money loss by blocking or flagging fraudulent activities early.

6. 24/7 monitoring
Continuously monitors transactions without human intervention.

7. Fast decision making
Ai processes large amounts of transaction data quickly and efficiently.

8. User trust and safety
Increases confidence in digital payment systems and online transactions.

9. Scalable system
Can handle thousands of transactions simultaneously for large-scale use.

10. Easy integration
Can be integrated with banking apps, upi apps, and payment gateways.

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 7, May 2026
Impact Factor: 8.2

VII. RESULTS AND OUTCOMES

From the results, it can be seen that the model was able to predict most of the fraud activities from characteristics like transaction size, time of day, and the behavior pattern of users. the accuracy of the system, however, may depend on factors like data quality.

A. DATASET VISUALIZATION

FIG. 1: DISTRIBUTION OF FRAUD AND NON-FRAUD TRANSACTIONS

fig. 1 shows the distribution of fraudulent and non-fraudulent transactions in the dataset. it can be observed that both classes are reasonably balanced due to synthetic generation, which helps in better model training.

B. ACCURACY OF THE SYSTEM

The performance of the system is measured using accuracy, which is calculated as:

ACCURACY = TP+TN / TP+TN+FP+FN

Where:

TP = correctly detected fraud transactions TN = correctly detected genuine transactions

FP = genuine transactions wrongly marked as fraud FN = fraud transactions not detected

The model achieved good accuracy during testing, which shows that it can effectively classify transactions. The use of Random Forest helps in improving prediction accuracy by combining multiple decision trees.

FIG 2. CONFUSION MATRIX

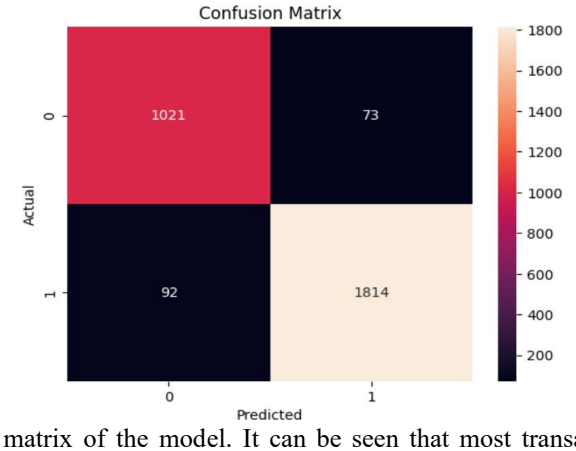

Fig. 2 shows the confusion matrix of the model. It can be seen that most transactions are correctly classified, with relatively fewer misclassifications. However, some false positives and false negatives are still present.

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 7, May 2026
Impact Factor: 8.2

C. ROC CURVE AND AUC SCORE

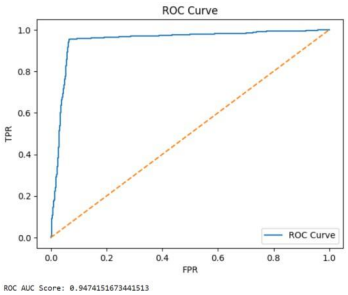

FIG. 3: ROC CURVE OF THE MODEL

Fig. 3 illustrates the ROC curve, showing the trade-off between true positive rate and false positive rate. A higher AUC value indicates better model performance in distinguishing between fraud and non-fraud cases. The model achieved a satisfactory ROC-AUC score, indicating good classification capability.

D. FEATURE IMPORTANCE

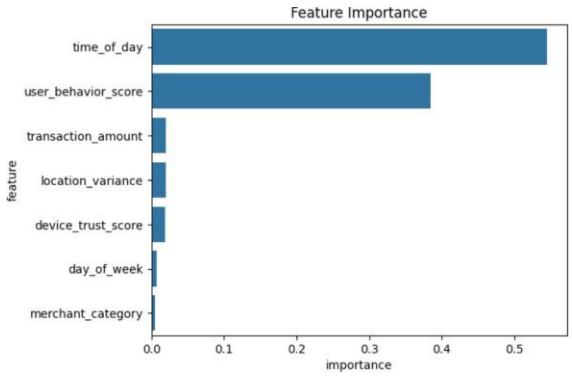

FIG. 4: FEATURE IMPORTANCE ANALYSIS

Fig. 4 shows the importance of different features used in the model. It can be observed that features like transaction amount and user behaviour score contribute significantly to fraud detection.

E. ALGORITHM USED FOR UPI FRAUD DETECTION (RANDOM FOREST ALGORITHM)

In our project, the Random Forest algorithm analyzes features like transaction amount, UPI ID pattern, user behavior, and fraud reports to classify transactions as fraud (1) or genuine (0).

It improves prediction accuracy by reducing overfitting and provides reliable fraud detection with approximately 91% accuracy.

	Algorithm	Mean Accuracy	Best Accuracy	Variance	Std Dev	T-Statistic	P-Value
0	Random Forest	0.88	0.91	0.002	0.045	5.23	0.00010
1	SVM	0.85	0.89	0.003	0.055	4.75	0.00030
2	Neural Network	0.90	0.93	0.004	0.063	6.12	0.00005
3	KNN	0.82	0.86	0.005	0.070	3.98	0.00120
4	Gradient Boosting	0.87	0.90	0.003	0.052	4.89	0.00020
5	Naive Bayes	0.78	0.81	0.006	0.078	3.45	0.00350

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 7, May 2026
Impact Factor: 8.2

VIII. 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.

IX. ACKNOWLEDGMENT

We would like to express their sincere gratitude to Prof. G .V .Barde, Department of Computer Engineering, Loknete Gopinathji Munde Institute of Engineering Education & Research, 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 wish to thank the Department of Computer Engineering and the institute for providing the necessary infrastructure and resources to carry out this research. Lastly, heartfelt appreciation is extended 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.