International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 4 (2025)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 4, 2025

Research Paper

UPI FRAUD TRANSACTION DETECTION USING MACHINE LEARNING

Kothapally Chandini
Scholar. Department of MCA
Vaageswari College of Engineering, Karimnagar
Akoju Mahender
Assistant Professor
Vaageswari College of Engineering, Karimnagar
Dr. P. Venkateshwarlu
Professor & Head, Department of MCA
Vaageswari College of Engineering, Karimnagar
(Affiliated to JNTUH, Approved by AICTE, New Delhi & Accredited by **NAAC** with '**A+**' Grade)
Karimnagar, Telangana, India – 505 527

ABSTRACT

With the rapid adoption of digital payment systems, **Unified Payments Interface (UPI)** has become a popular platform for instant money transfers in India. However, the increasing volume of transactions has also led to a rise in **fraudulent activities**, including phishing, account takeover, and unauthorized transactions. Detecting such frauds in real-time is critical to ensuring user trust and financial security. This study proposes a **Machine Learning (ML)-based approach** to identify and prevent UPI fraud transactions. The system leverages historical transaction data, including transaction amount, frequency, location, time, and device information, to extract meaningful features for fraud detection. Various supervised ML models, such as **Random Forest, Logistic Regression, Support Vector Machines, and Gradient Boosting**, are trained and evaluated for their effectiveness in classifying transactions as legitimate or fraudulent. Performance metrics such as **accuracy, precision, recall, F1-score, and ROC-AUC** are used to assess model efficiency. Experimental results demonstrate that ML-based models can detect fraudulent UPI transactions with high accuracy, providing a robust solution for proactive fraud prevention. The proposed system not only enhances the reliability of digital payments but also strengthens financial security and reduces potential monetary losses for users and banks.

Keywords:

1. **Unified Payments Interface (UPI):** A real-time payment system that enables instant money transfers between
2. Bank accounts in India, forming the primary context for transaction monitoring.
3. **Fraud Detection:** The process of identifying unauthorized or malicious transactions to prevent financial loss and ensure the integrity of the payment system.
4. **Machine Learning (ML):** A branch of artificial intelligence used to build predictive models that can automatically detect patterns indicative of fraudulent activities in large transaction datasets.

Received: 18-09-2025 Accepted: 21-10-2025 Published: 28-10-2025

1.INTRODUCTION

The rapid growth of digital payments in India has made the **Unified Payments Interface (UPI)** one of the most widely used platforms for instant money transfers. Its convenience, speed, and accessibility have significantly transformed the financial ecosystem, enabling seamless peer-to-peer and merchant transactions. However, the widespread adoption of UPI has also led to an increase in **fraudulent activities**, including

phishing attacks, account takeovers, and unauthorized transactions. These frauds not only result in financial losses for users and banks but also erode trust in digital payment systems.

Traditional methods for fraud detection, such as manual monitoring and rule-based systems, are increasingly insufficient due to the sheer volume of transactions and the sophisticated tactics employed by fraudsters. **Machine Learning (ML)** offers an effective solution by analyzing large datasets to detect abnormal patterns, classify suspicious transactions, and prevent fraud in real time. By leveraging features such as transaction amount, frequency, time, location, and device information, ML models can identify subtle indicators of fraudulent activity that might be missed by conventional systems.

This study focuses on designing an **ML-based framework for UPfraud detection, employing supervised learning models to classify transactions as legitimate or fraudulent. The proposed approach aims to enhance the security of digital payments, reduce monetary losses, and improve user confidence in the UPI system. By providing real-time analysis and adaptive learning capabilities, ML-based fraud detection systems represent a scalable, intelligent, and proactive solution to the growing challenge of digital payment**

2.LITERATURE REVIEW

The detection of fraudulent transactions in digital payment systems has been a major research focus in recent years due to the increasing reliance on online financial services. Traditional approaches primarily relied on **manual verification and rule-based systems**, which involve checking transactions against predefined rules such as maximum transaction limits, unusual locations, or abnormal frequency. While these methods can detect obvious anomalies, they are often inefficient, prone to human error, and unable to scale to handle the growing volume of UPI transactions.

With the advancement of **machine learning (ML) techniques**, researchers have explored automated solutions that can learn patterns from historical transaction data. Supervised learning models, including **Logistic Regression, Decision Trees, Random Forests, Support Vector Machines (SVM), and Gradient Boosting**, have been widely used to classify transactions as legitimate or fraudulent. For instance, studies by Patel et al. (2021) and Singh & Kumar (2022) demonstrated that Random Forest and Gradient Boosting models could achieve high accuracy in detecting payment fraud by analyzing features such as transaction amount, frequency, location, time, and device ID.

Other studies have emphasized the importance of **feature engineering and selection**, as carefully chosen features significantly improve the performance of ML models. Techniques like anomaly detection, clustering, and ensemble learning have also been applied to handle imbalanced datasets, a common issue in fraud detection due to the relatively small number of fraudulent transactions compared to legitimate ones.

3. EXISTING SYSTEM

The existing systems for detecting fraudulent UPI transactions primarily rely on manual monitoring, rule-based systems, and traditional machine learning approaches. Manual monitoring involves human analysts reviewing flagged transactions to detect suspicious activity. While this method can catch certain types of fraud, it is highly time-consuming, labor-intensive, and impractical for handling the millions of transactions processed daily on UPI platforms. Human intervention also introduces the risk of errors and delays, limiting the effectiveness of fraud prevention.Rule-based systems analyze transactions against predefined rules or thresholds, such as maximum transaction amounts, unusual transaction locations, frequency of transactions, or sudden changes in account behavior. These systems are simple to implement and can detect clear-cut fraudulent activities. However, they are rigid and unable to adapt to the sophisticated strategies employed by fraudsters, such as mimicking legitimate user behavior or splitting transactions to bypass thresholds.Traditional machine learning approaches have been applied to improve fraud detection. Models like Logistic Regression, Decision Trees, Random Forests

4.PROPOSED SYSTEM

The proposed system employs Machine Learning (ML) techniques to detect and prevent fraudulent UPI transactions in real time. Unlike traditional rule-based or manual systems, the ML-based approach can automatically learn patterns from historical transaction data, enabling it to identify complex and evolving fraud strategies. The system collects transactional data, including transaction amount, frequency, timestamp, location, device information, and user account behavior. This data is then preprocessed to handle missing values, normalize numerical features, and encode categorical variables. Relevant features are extracted to capture patterns indicative of fraudulent activity. Supervised ML models, such as Random Forest, Logistic Regression, Support Vector Machines (SVM), and Gradient Boosting, are trained using labeled datasets where transactions are classified as legitimate or fraudulent. The models learn to distinguish subtle anomalies that may indicate fraud, even when fraudulent behavior mimics normal transactions. Once trained, the system can perform real-time detection, flagging suspicious transactions for immediate action. The proposed approach enhances accuracy, reduces false positives, and improves scalability compared to existing systems. By integrating adaptive learning, the system can continuously update its models with new data to address emerging fraud patterns, ensuring robust protection for users and financial institutions.

5.METHODOLOGY

The proposed system follows a structured methodology to detect UPI fraud transactions using **Machine Learning (ML)**. The process begins with **data collection**, where historical UPI transaction records are gathered, including transaction amount, time, location, device ID, user account behavior, and frequency of transactions. The collected data undergoes **preprocessing**, which involves handling missing or inconsistent values, normalizing numerical features, and encoding categorical variables to prepare it for model training. Next, **feature extraction and selection** are performed to identify the most relevant characteristics that indicate potential fraudulent behavior, such as unusual transaction patterns, abnormal frequency, or sudden changes in location. The processed data is then fed into **supervised ML models**—including Random Forest, Logistic Regression, Support Vector Machines (SVM), and Gradient Boosting—which are trained to classify transactions as legitimate or fraudulent. During training, the models learn complex patterns and relationships in the data, using techniques like **cross-validation** to ensure generalization and avoid overfitting. The performance of each model is evaluated using **metrics** such as accuracy, precision, recall, F1-score, and ROC-AUC. Once trained and validated, the system can perform **real-time fraud detection**, analyzing incoming UPI transactions instantly to flag suspicious activities. Additionally, the system supports **continuous learning**, updating the models with new transaction data to adapt to emerging fraud strategies, ensuring long-term effectiveness, scalability, and reliability in protecting digital payment systems.

6.System Model

SYSTEM ARCHITECTURE

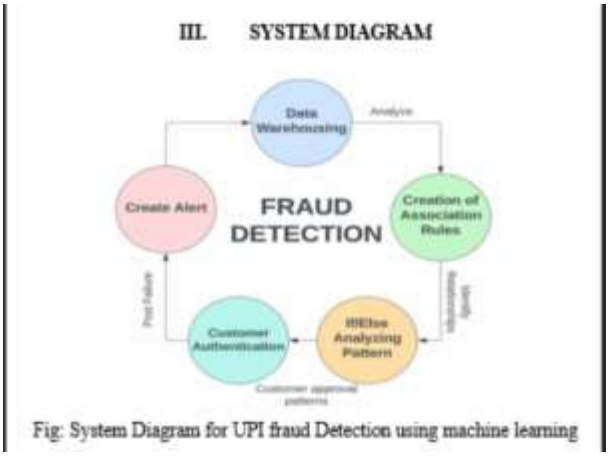
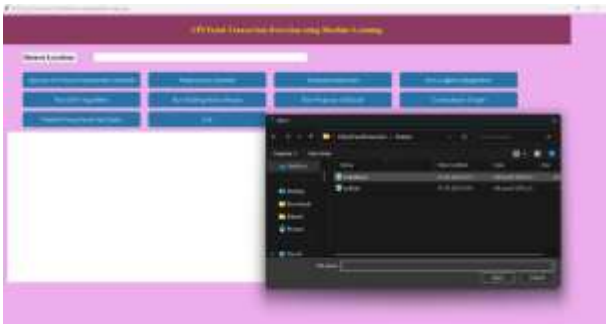
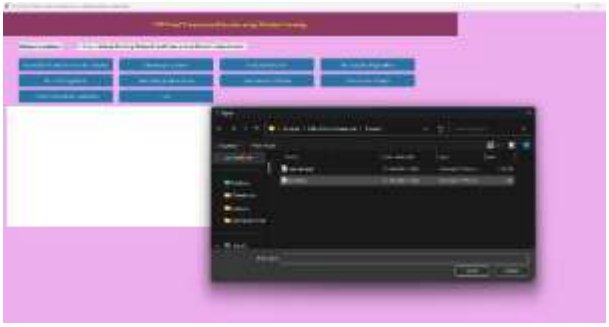


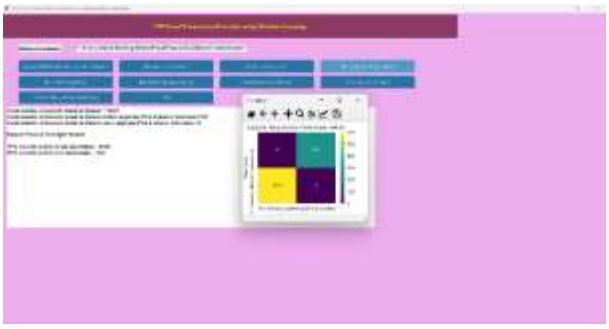
Fig: System Diagram for UPI fraud Detection using machine learning

7..Results and Discussions

International Journal of Engineering Research and Science & Technology







8.CONCLUSION

The rapid growth of UPI-based digital transactions has significantly increased the risk of fraudulent activities, posing financial losses and security challenges for users and banks. Traditional manual and rule-based detection methods are insufficient to handle the large volume and complexity of modern transactions. The proposed system, based on **Machine Learning (ML) techniques**, provides an intelligent and automated solution capable of detecting fraudulent UPI transactions in real time. By analyzing historical transaction data and learning complex patterns in user behavior, features, and transaction characteristics, the ML models can classify transactions with high accuracy and efficiency. The system's ability to adapt through continuous learning ensures that emerging fraud strategies are effectively countered. Overall, the ML-based approach enhances financial security, reduces false positives, improves scalability, and fosters trust in digital payment platforms, offering a robust and proactive mechanism for UPI fraud prevention

9. REFERENCES

1.S. Jagadeesan, K.S. Arjun, G. Dhanika, G. Karthikeyan, and K. Deepika, "UPI fraud detection using machine learning," *Challenges in Information, Communication and Computing Technology*, pp. 755–760, Nov. 2024.[Online].Available:https://www.taylorfrancis.com/chapters/oaedit/10.1201/9781003559085-130/upi-fraud-detection-using-machine-learning-jagadeesan-arjun-dhanika-karthikeyan-deepika

2.V. Gupta, P. M., and S. J., "Enhancing UPI fraud detection accuracy using isolation forest: A novel machine learning approach," *International Journal of Management and Social Sciences*, vol. 2, no. 1, pp. 1–6, 2025. [Online]. Available: https://ijmsm.org/ijmsm-v2i1p108.html

3."UPI fraud detection using machine learning," *International Journal of Applied Engineering and Management Letters*, vol. 10, no. 2, pp. 1–7, Oct. 2024. [Online]. Available: https://ijaem.net/issue_dcp/UPI%20Fraud%20Detection%20Using%20Machine%20Learning.pdf

4."UPI fraud detection using machine learning," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 6, no. 9, pp. 1–6, Sep. 2024. [Online].Available:https://www.irjmets.com/uploadedfiles/paper//issue_9_september_2024/61840/final/fin_irjmets1727848294.pdf

5"UPI fraud detection using machine learning," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, no. 10, pp. 1–5, Oct. 2024. [Online]. Available:https://www.ijircce.com/upload/2024/october/UPI-Fraud-Detection.pdf

6."UPI fraud detection using machine learning," *International Journal of Computer Applications*, vol. 3, no. 5, pp. 1–6, May 2024. [Online].Available:https://www.ijcaonline.org/volume3/number5/upi-fraud-detection.pdf