DADI INSTITUTE OF ENGINEERING & TECHNOLOGY

ONLINE UPI FRAUD DETECTION USING MACHINE LEARNING

A

Proposed Project Power Point Presentation

Submitted in partial fulfilment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING(DATA SCIENCE)

By

B.HEMA DINESH (22U41A4405)

S.LAKSHMAN KUMAR (22U41A4442)

M.JAYANTH KUMAR (22U41A4431)

P.SAI VIGNESH (22U41A4432)

Under the Supervision of

M.KALYANI ,Ass.professor

Dadi Institute of Engineering & Technology

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DADI INSTITUTE OF ENGINEERING & TECHNOLOGY

(AN AUTONOMOUS INSTITUTE)

ANAKAPALLE - 531002, VISAKHAPATNAM, A.P.

MARCH - 2026

Abstract

Unified Payments Interface (UPI) has revolutionized digital payments in India with secure, low-cost, and real-time transfers. However, these advantages have led to increased cyber frauds such as phishing, SIM swap, and social engineering. To address this, a Machine Learning-based framework is proposed to detect fraudulent transactions by analyzing features like amount, timestamp, location, device ID, and user behavior.

The framework applies preprocessing and solves class imbalance using SMOTE. Multiple algorithms including Logistic Regression, Decision Tree, Random Forest, and Gradient Boosting are tested, with ensemble learning providing higher accuracy and reliability. By integrating behavioral analytics, the model generates near real-time alerts, reduces false positives, and prevents financial losses without disturbing genuine transactions.

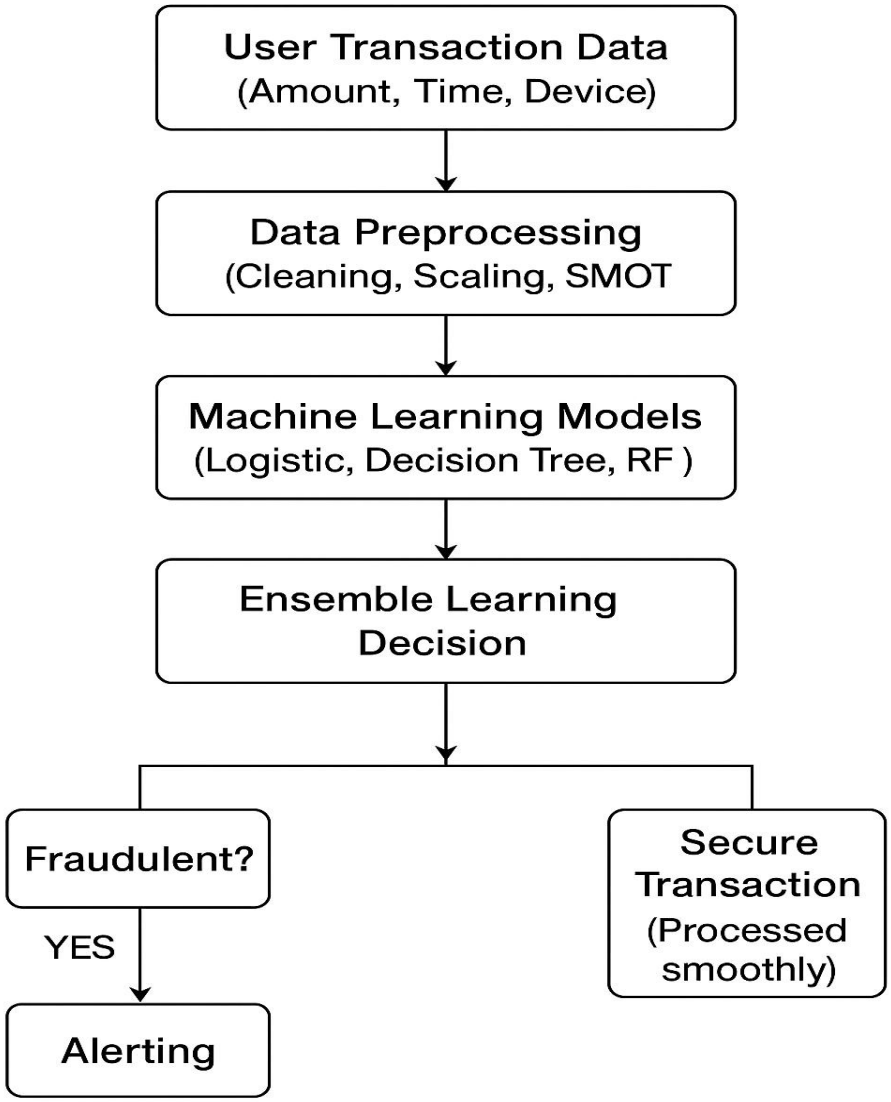
This scalable system can be integrated into payment platforms, adapt to evolving fraud tactics, and strengthen cybersecurity in India's financial ecosystem, ensuring safe digital payments and maintaining public trust.

Keywords: UPI, Fraud Detection, Machine Learning, Ensemble Learning, SMOTE, Cybersecurity, Digital Payments, Behavioral Analytics

INTRODUCTION

- **UPI Transformation**: Unified Payments Interface (UPI) has completely changed the way digital payments work in India by enabling secure, instant, and real-time bank-to-bank transfers through mobile apps.
- **Massive Adoption**: Its speed, interoperability across banks, and low transaction cost have made it the most widely used digital payment method in India, connecting millions of users.
- **Emergence of Cyber Frauds**: With rapid growth, UPI has also attracted cybercriminals. Common frauds include phishing, SIM swap, and social engineering, which are leading to serious financial losses.
- **Impact on Users**: These fraudulent activities not only cause monetary damage but also reduce user confidence and trust in digital financial platforms.
- **Role of Machine Learning**: Advanced Machine Learning techniques can analyze large-scale transaction data, capture hidden patterns, and differentiate between genuine and suspicious activities effectively.
- **Real-Time Fraud Detection**: By leveraging anomaly detection and predictive algorithms, the system can provide real-time alerts to prevent fraudulent transactions before losses occur.
- **Benefits of Proposed Framework**: The approach ensures improved security, adaptability to evolving fraud tactics, scalability for large payment systems, and restoration of public trust in digital payments.

ARCHITECTURE



•**Rule-Based Fraud Detection**
Simple threshold rules like maximum transaction limit or unusual login time.
Effective for basic fraud but fails for new and adaptive fraud patterns.
•**Anomaly Detection Techniques**
Statistical analysis of unusual transaction behavior (amount, frequency, location).
Identifies outliers but may generate false positives.
•**Machine Learning Models**
Logistic Regression, Decision Trees, Random Forests commonly used.
Learn from past data and classify transactions as genuine or fraudulent.
•**Neural Network Approaches**
Deep learning models (RNN, LSTM) analyze sequential transaction data.
Capture hidden fraud patterns in large-scale data.
•**Behavioral Analytics**
User habits like transaction time, device usage, typing/swiping patterns.
Helps in detecting fraud even when credentials are compromised.
•**Hybrid & Ensemble Methods**
Combine multiple algorithms (e.g., Random Forest + Gradient Boosting).
Improve detection accuracy and reduce false alarms.