International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Conference Proceedings: Volume: 05 ACME – 2026 DOI:10.55041/ISJEM.ACME027
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Enhanced Real-Time Detection of UPI Fraud using Advanced Machine Learning Models

M. Ram Kumar [1], T. Anitha [2], P. Harshitha [3], T. Mohan reddy krishna[4], Swayam das [5]

[1,2,3,4,5,6] *Computer Science and Information Technology, Siddharth Institute of Engineering & Technology*

Abstract-Digital payment systems such as the Unified Payments Interface (UPI) have significantly transformed financial transactions by enabling instant, secure, and convenient money transfers. However, the rapid growth of digital transactions has also increased the risk of fraudulent activities. Traditional rule-based fraud detection systems often fail to identify complex and evolving fraud patterns in real time. Therefore, there is a need for intelligent and automated fraud detection systems that can analyze large volumes of transaction data efficiently.This project proposes an advanced fraud detection framework that utilizes machine learning algorithms such as Random Forest, Extra Trees, CatBoost, and LightGBM to detect suspicious UPI transactions. The system analyzes transaction attributes such as transaction type, amount, and account balance details to identify abnormal patterns. A web-based interface developed using Flask allows users to input transaction data and obtain real-time fraud predictions. The proposed model improves fraud detection accuracy and reduces false positives, thereby enhancing the security and reliability of digital payment systems.

Keywords: UPI Fraud Detection, Machine Learning, Random Forest, LightGBM, Digital Payments, Financial Security.

1. INTRODUCTION

Digital payment platforms have become an integral part of modern financial systems. Among them, the Unified Payments Interface (UPI) has gained significant popularity due to its ability to facilitate instant money transfers between bank accounts using mobile devices. With the increasing adoption of digital payments, financial institutions process millions of transactions daily. While these systems provide convenience and efficiency, they also create opportunities for cybercriminals to perform fraudulent activities such as unauthorized transactions, identity theft, and phishing attacks.

Traditional fraud detection methods rely on predefined rules and manual monitoring techniques. These approaches often fail to detect new and sophisticated fraud patterns because fraudsters continuously change their strategies. Machine learning techniques provide an effective solution to this problem by learning patterns from historical transaction data and identifying anomalies automatically. This project aims to develop an intelligent fraud detection system that analyzes transaction details and predicts whether a transaction is fraudulent or legitimate in real time.

2. SYSTEM ANALYSIS

Existing System:

Current fraud detection systems mainly rely on traditional analysis techniques such as:

- **Rule-Based Detection Systems**
- **Manual Monitoring**
- **Statistical Models**
- **BasicMachineLearningModels**

Limitations of Existing Systems

- Limited ability to detect evolving fraud patterns.
- High false positive rate.
- Slow response time for real-time fraud detection.
- Lack of intelligent decision-making mechanisms.
- Inefficient handling of large transaction datasets.

2. PROPOSED SYSTEM

The proposed system introduces an intelligent fraud detection framework that uses advanced machine learning algorithms to analyze UPI transaction data. The system processes historical transaction records and identifies patterns associated with fraudulent behavior. Multiple machine learning models such as Random Forest, Extra Trees, CatBoost, and LightGBM are used to improve prediction accuracy.

3.1 CORE CONCEPT

• **Machine Learning Model:**
The system uses multiple machine learning algorithms to analyze transaction patterns and detect fraudulent activities.
• **Transaction Data:**
Historical UPI transaction data is used for training the machine learning models.
• **Feature Engineering:**
Important transaction attributes such as transaction type, amount, and balance differences are extracted as features.
• **Prediction Engine:**
The trained model evaluates incoming transactions and predicts fraud probability.

3.2 FRAUD DETECTION PROCESS

The system performs the following operations during transaction analysis:

• **Data Input:**
Users provide transaction details through the web interface.
• **Preprocessing:**
The system cleans and normalizes the data before feeding it into the model.
• **Model Prediction:**
The trained machine learning model predicts whether the transaction is fraudulent.
• **Result Display:**
The system displays the prediction result along with confidence score.

3.3 LEARNING PROCESS

The machine learning models are trained using historical transaction data. During training, the system learns patterns associated with fraudulent and non-fraudulent transactions. Through multiple training iterations, the models improve their prediction accuracy and become capable of identifying complex fraud patterns.

3.4 ADVANTAGES OF PROPOSED SYSTEM

●Intelligentautomatedfrauddetection.
● High accuracy in identifying fraudulent transactions.
●Reducedfalsepositiverate.
●Real-timetransactionmonitoring.
● Scalable architecture suitable for large datasets.
● Improved security for digital payment systems.

EXPERIMENTAL RESULTS

The proposed fraud detection system demonstrates significant improvements in fraud prediction accuracy compared to traditional methods. The ensemble machine learning approach enables the system to detect complex fraud patterns more effectively. Experimental results show that the system achieves high prediction accuracy and reduces false positives, thereby improving the reliability of UPI transaction monitoring.

DIAGRAM 1: SYSTEM ARCHITECTURE

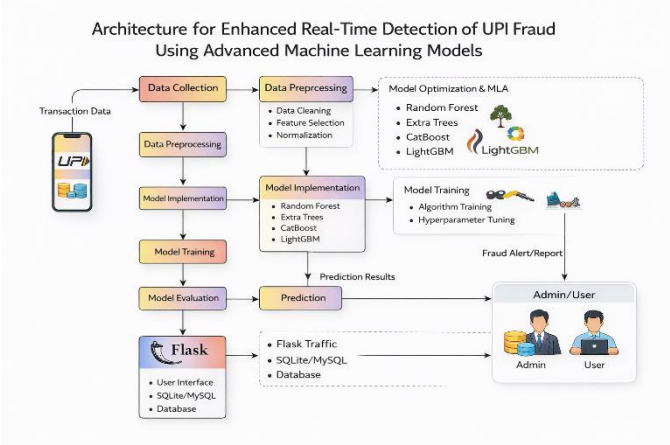

Fig -1: Figure

4. CONCLUSION

This project presents an advanced machine learning-based approach for detecting fraudulent UPI transactions. By integrating multiple machine learning algorithms and real-time prediction mechanisms, the system provides an effective solution for preventing financial fraud in digital payment systems. Overall, the proposed system provides a scalable and intelligent solution for enhancing the security of digital financial transactions and protecting users from fraudulent activities.

FUTURE SCOPE

Future improvements of the proposed system can include the integration of deep learning models for enhanced fraud detection accuracy. Real-time transaction monitoring using streaming data technologies can further improve system responsiveness. The system can also incorporate behavioral analysis and user authentication mechanisms to detect suspicious activities more effectively. In the future, this system can be expanded into a comprehensive financial fraud detection platform capable of monitoring large-scale digital transactions across multiple payment networks.

REFERENCES

- Ashima Narang, Priyanka Vashisht, Shalini Bhaskar Bajaj, "Artificial Intelligence in Banking and Finance," 2024.
- Samrat Ray, "Fraud Detection in E-Commerce Using Machine Learning," 2022.
- Unam Sam et al., "Credit Card Fraud Detection Using Machine Learning Algorithms," 2023.
- Mohd Afjal et al., "Financial Fraud and Credit Risk: Illicit Practices and Their Impact on Banking Stability," 2023.
- Oladimeji Kazeem, "Fraud Detection Using Machine Learning," 2023.

BIOGRAPHY

I, **M.RAM KUMAR**, currently working as an Assistant Professor in the Department of Computer Science and Information Technology at Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India. I am having 3 years of teaching experience in engineering education. I am pursuing my Ph.D. in Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai. My research interests include Machine Learning, Image processing, Artificial Intelligence, Deep learning. I published research papers in reputed journals and conferences. I actively participated in faculty development programs, workshops, and technical seminars. I guided several undergraduate projects and is committed to academic excellence and research innovation.