IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15588

AI-Based UPI Fraud Detection Using Machine Learning and Real-Time Analysis

Atul Shivaji Kamble

Department of Computer Science Engineering, International Center of Excellence In Engineering and Management (ICEEM), Maharashtra, India

Abstract: The rapid adoption of Unified Payments Interface (UPI) has revolutionized digital transactions in India. However, this growth has also led to an increase in fraudulent activities such as phishing, fake payment requests, and unauthorized transactions. Traditional fraud detection systems are often reactive and fail to prevent fraud in real time.

This paper presents an AI-based UPI fraud detection system that uses machine learning techniques to identify suspicious transactions before they are completed. The system analyzes transaction patterns, detects anomalies, and generates real-time alerts for users. A web-based dashboard provides users with insights into their transaction behavior, while Firebase ensures real-time data synchronization and scalability. The proposed system focuses on proactive fraud prevention, improving user trust and enhancing the security of digital payment systems.

Keywords: UPI, Fraud Detection, Machine Learning, Real-Time Analysis, AI, Firebase.

I. INTRODUCTION

The advancement of the digital payment systems has significantly transformed financial transactions, especially in developing countries like India. UPI has become one of the most widely used payment methods due to its simplicity and speed. However, the increase in digital transactions has also resulted in a rise in fraud cases.

Fraudsters exploit user behavior and system vulnerabilities using techniques such as phishing, social engineering, and fake payment links. Most existing systems detect fraud only after the transaction is completed, which results in financial losses.

This research aims to develop a real-time AI-based fraud detection system that can:

- Identify suspicious transactions instantly
- Analyze user behavior patterns
- Alert users before fraud occurs
- Provide a user-friendly monitoring dashboard

The focus is on building a system that is both intelligent and accessible to everyday users.

II. RELATED WORK

Fraud detection has been widely studied in financial systems. Traditional approaches rely on rule-based systems where predefined conditions are used to identify suspicious activities. However, these systems lack adaptability and fail to detect new types of fraud.

Recent studies have explored machine learning approaches such as:

- Decision Trees
- Random Forest
- Logistic Regression
- Neural Networks

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15588

These models improve detection accuracy by learning from transaction data. However, many existing systems lack real-time capabilities and user-friendly interfaces.

The proposed system addresses these gaps by integrating machine learning with real-time processing and a web-based interface.

III. Literature Survey

Several research works highlight the importance of intelligent fraud detection systems:

- Machine learning models are effective in identifying anomalies in transaction data
- Behavioral analysis helps detect unusual user activity
- Real-time monitoring significantly reduces fraud risk
- Cloud platforms enable scalable and efficient data handling
- Web dashboards improve user awareness and system usability

These findings support the development of a system that combines AI, real-time processing, and user interaction.

IV. Proposed System

The proposed system is designed as a complete web-based solution for fraud detection and prevention.

A. System Architecture

The system follows a modular architecture:

- Transaction data is collected through the web application
- The AI module analyzes the data using machine learning algorithms
- The backend (Firebase/Node.js) manages data storage and processing
- The system generates alerts based on risk levels
- The web dashboard displays transaction insights and warnings

Figure 1. Proposed System Architecture

B. Key Features

1) Real-Time Fraud Detection:
The system continuously monitors transactions and identifies suspicious activities before completion.

2) AI-Based Analysis:
Machine learning models analyze:

- Transaction amount
- Frequency
- User behavior patterns

3) Instant Alert System:
Users receive alerts for:

- Suspicious transactions
- High-risk payment requests

4) User Dashboard:
The dashboard provides:

- Transaction history
- Risk indicators

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.15588

- Fraud warnings

5) Secure Authentication:
User data is protected using Firebase Authentication.

6) Admin Panel:
Admin can:

- Monitor system activity
- View fraud reports
- Manage users

Working Flow:

User → Web Interface → Firebase → Fraud Detection System → Transaction Decision

V. Methodology And Validation

The proposed system follows a structured approach to detect fraudulent transactions using machine learning and real-time processing. The methodology focuses on analyzing transaction behavior and identifying anomalies before the transaction is completed.

A. Methodology

The working process of the system is divided into the following steps:

- **Data Collection:**
  Transaction data is collected through the web application, including parameters such as transaction amount, time, frequency, and user behavior.
- **Data Preprocessing:**
  The collected data is cleaned and structured to remove inconsistencies and prepare it for analysis.
- **Feature Extraction:**
  Important features such as transaction patterns, unusual activity frequency, and user behavior trends are identified.
- **Model Application:**
  Machine learning algorithms are applied to classify transactions as normal or suspicious based on learned patterns.
- **Risk Evaluation:**
  Each transaction is assigned a risk level depending on its similarity to known fraud patterns.
- **Alert Generation:**
  If a transaction is identified as suspicious, the system immediately generates an alert to warn the user.

B. Validation

To evaluate the performance of the system, testing was carried out using simulated transaction data representing both normal and fraudulent activities.

- The system was able to correctly identify a majority of suspicious transactions.
- Real-time alerts were generated with minimal delay.
- False positives were reduced by improving feature selection and model tuning.
- The system maintained consistent performance under multiple test scenarios.

The validation results indicate that the proposed system is effective in detecting fraud in real time and can be further improved with larger datasets and advanced models.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15588

VI. RESULTS

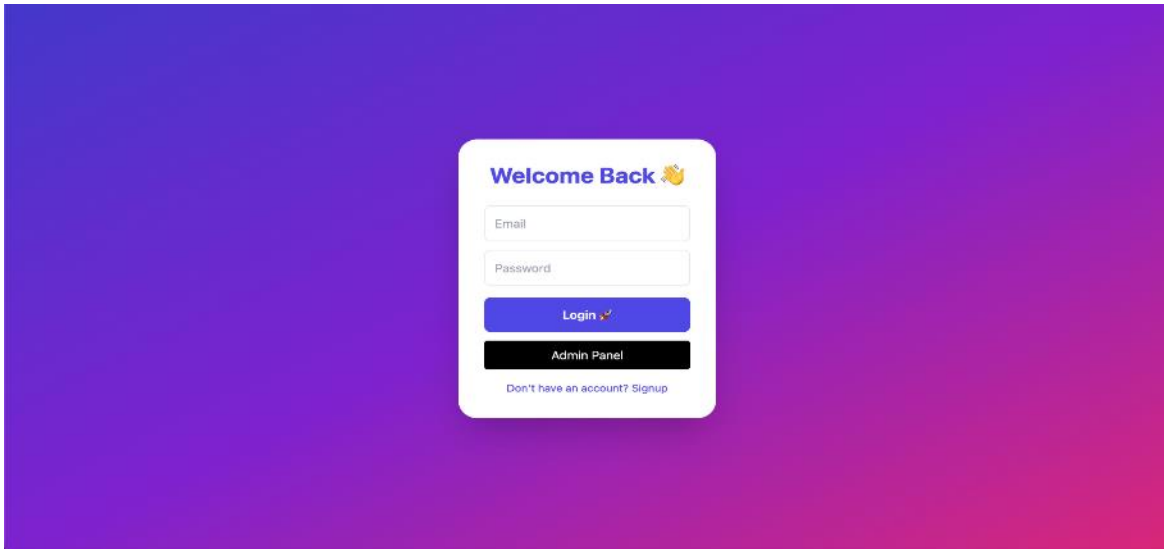
The system was tested using simulated transaction data and different fraud scenarios.

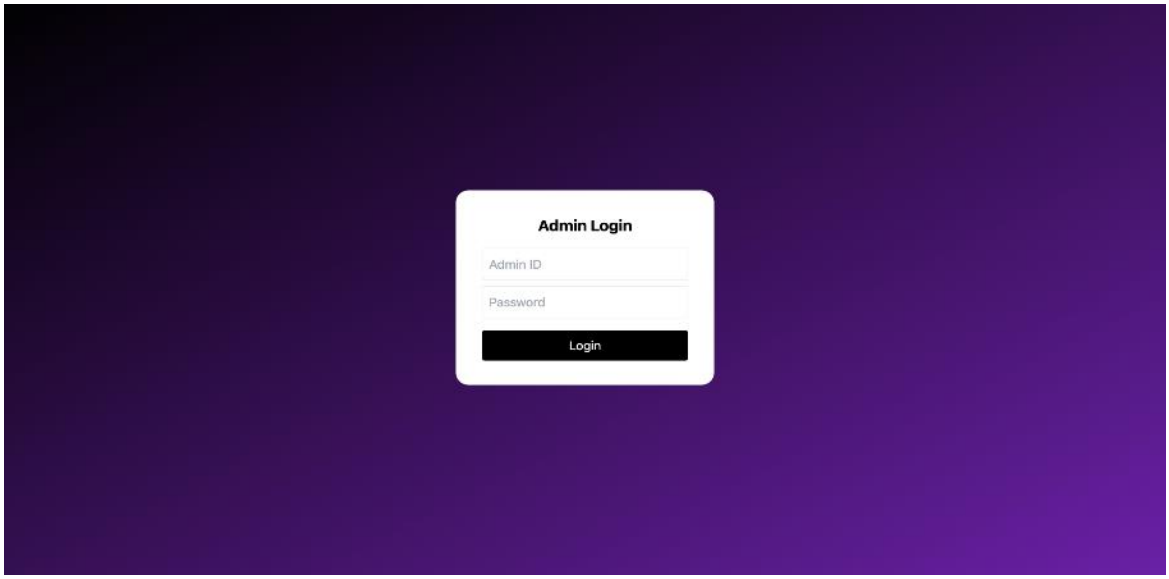
Observations:

- The model successfully identified suspicious transactions
- Real-time alerts helped reduce potential fraud cases
- The dashboard clearly displayed transaction insights
- The system was easy to use and responsive

Compared to traditional systems, the proposed system provides faster and more accurate detection.

USER-LOGIN:





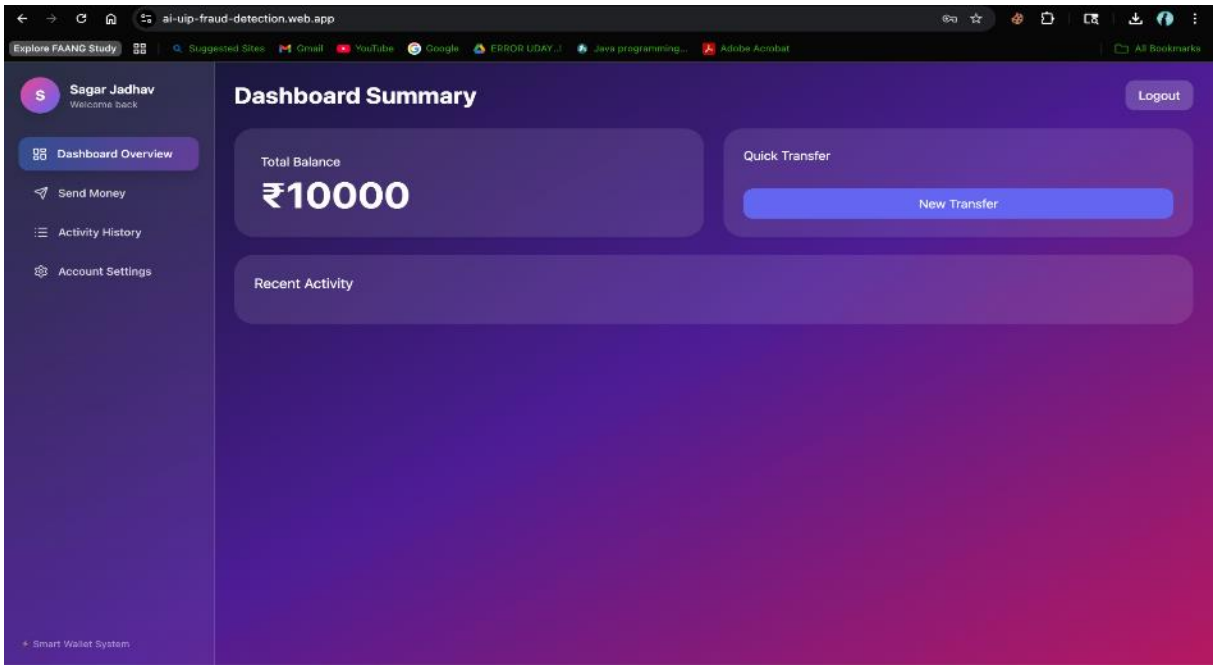
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

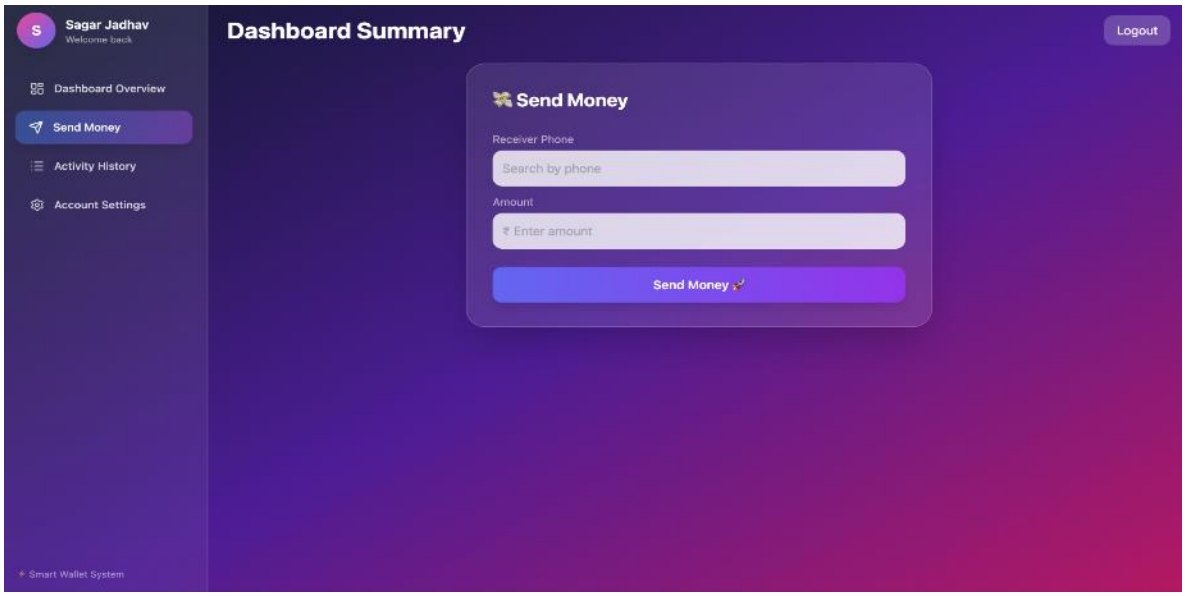
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15588

USER DASHBOARD:



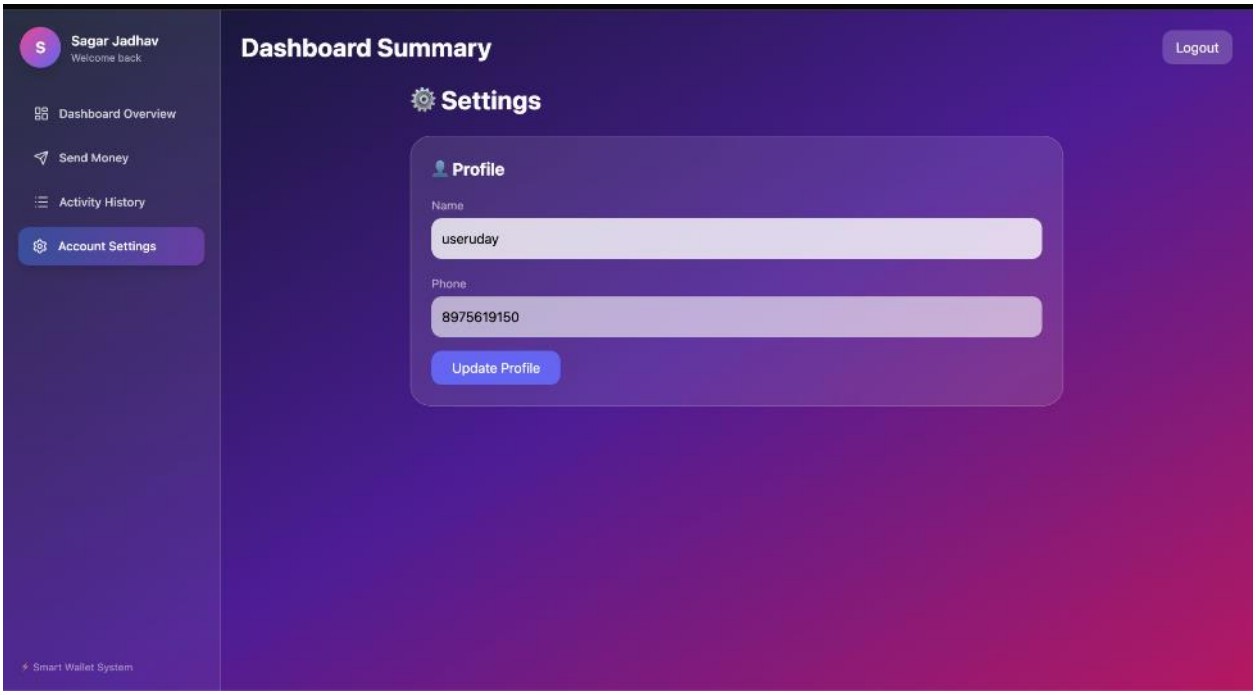


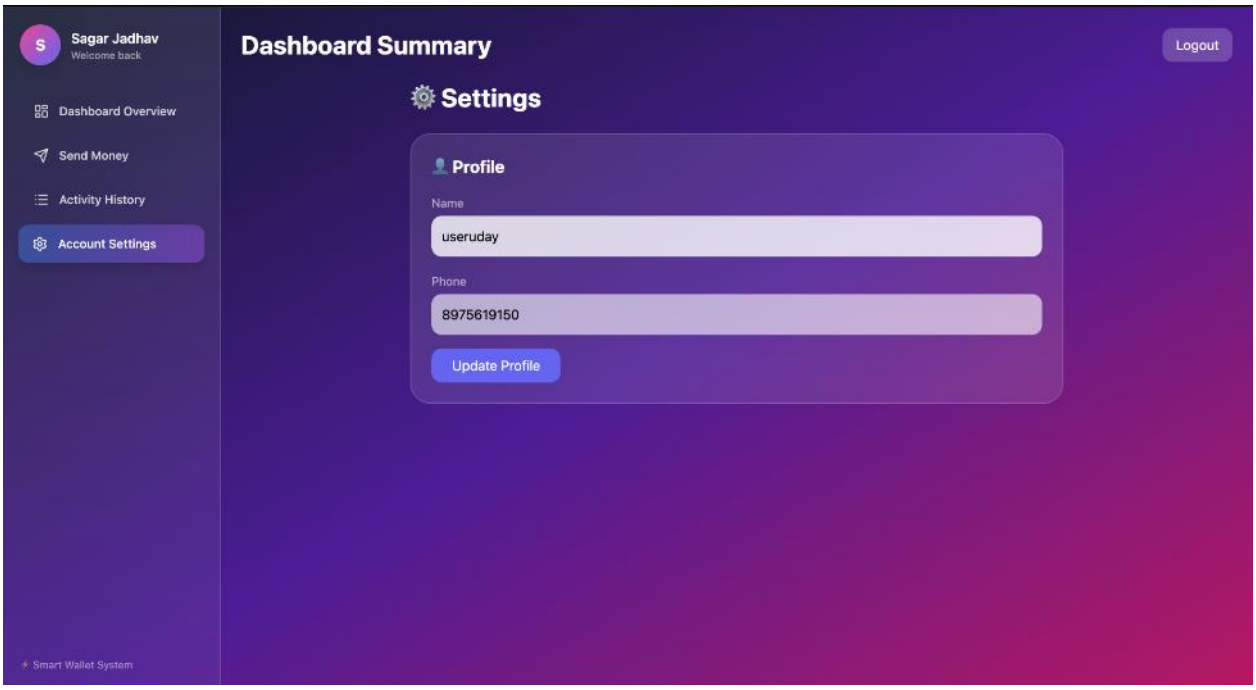
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15588





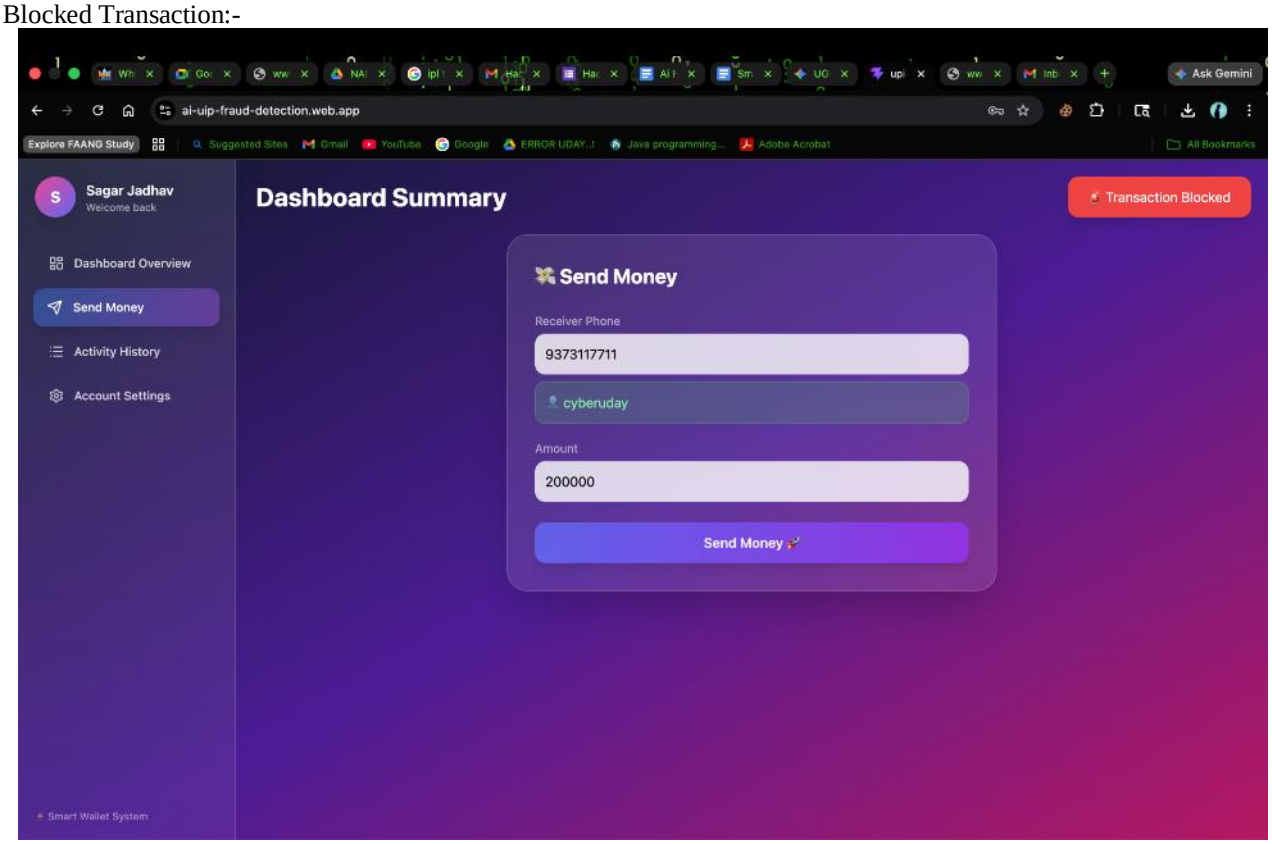
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

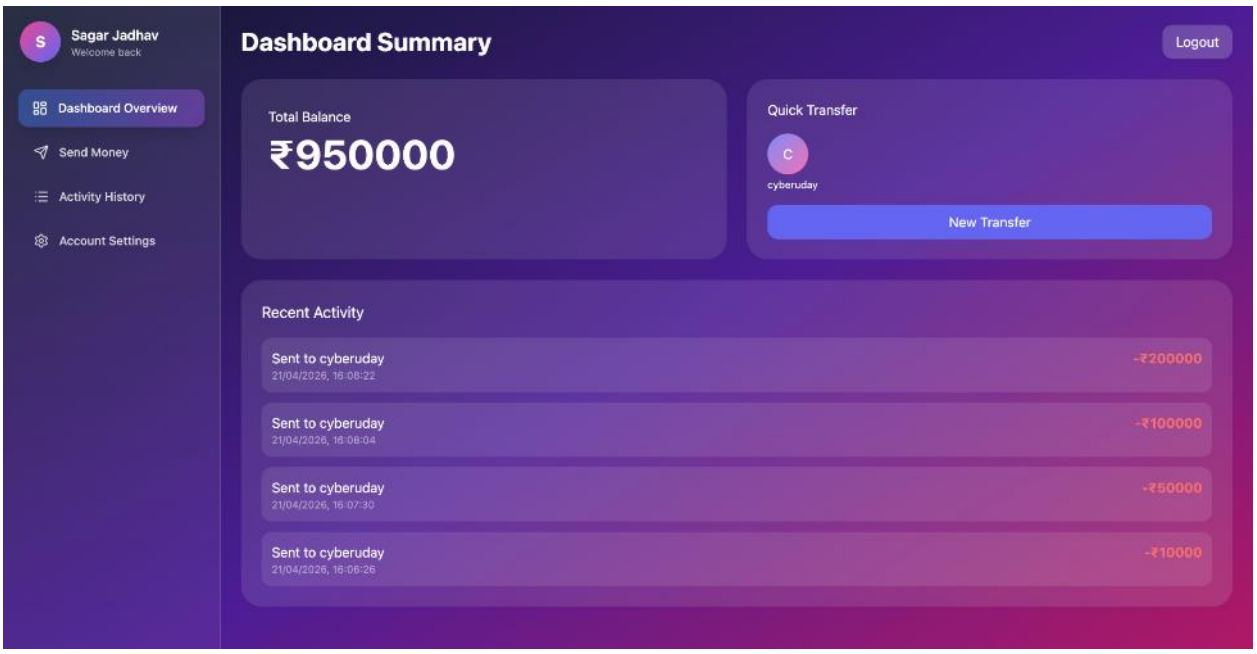
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15588

Blocked Transaction:-



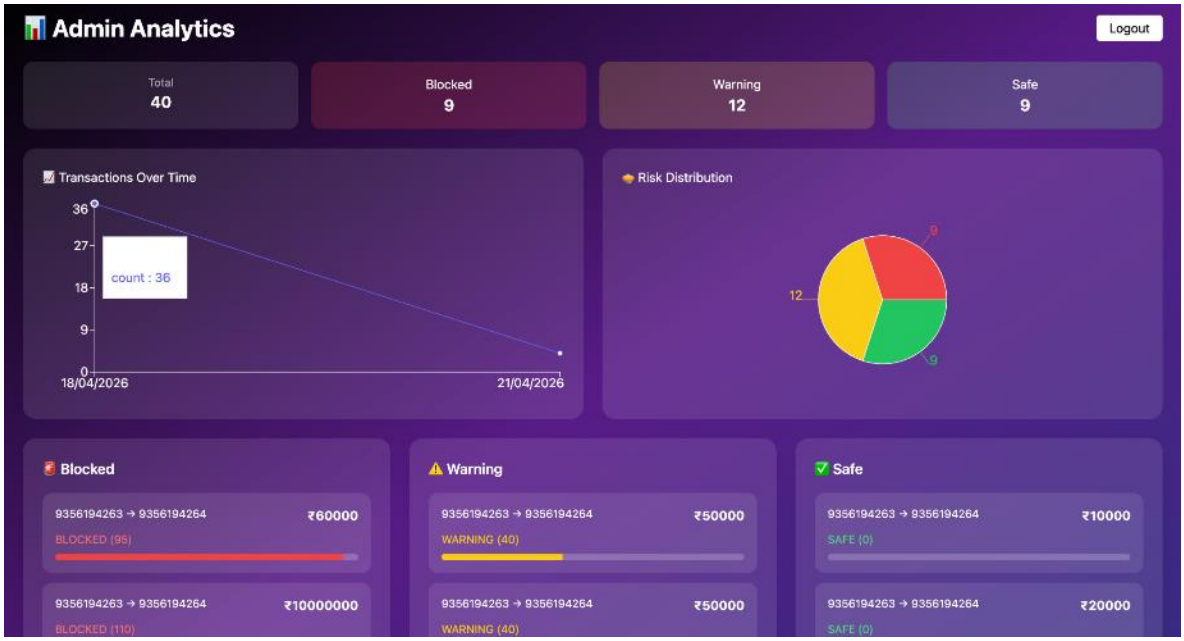


IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

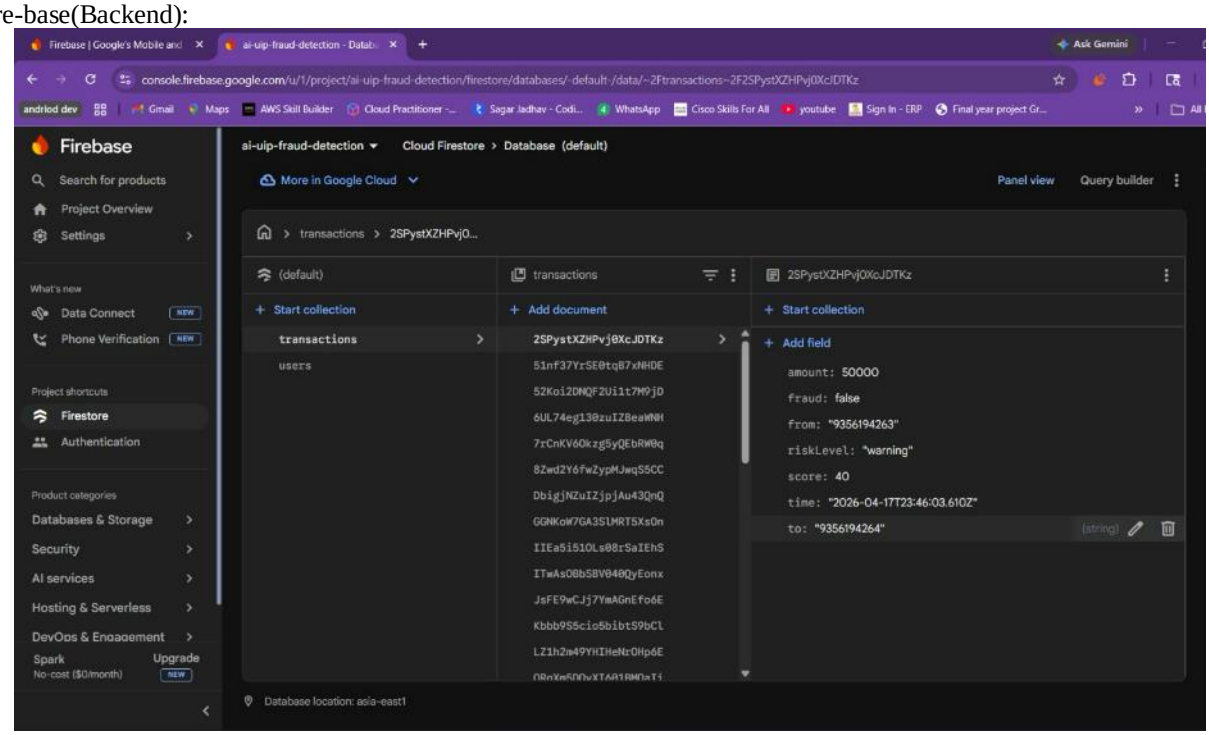
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15588



FIre-base(Backend):



VII. Conclusion and Future Scope

This paper presents an AI-based UPI Fraud Detection Web System that focuses on real-time fraud prevention. By combining machine learning, cloud technology, and web-based interfaces, the system improves the safety of digital transactions.

The system is scalable, efficient, and user-friendly, making it suitable for real-world applications.

Future Scope

The system can be further improved by:

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.15588

- Integrating with banking systems
- Using deep learning for better accuracy
- Developing a mobile application
- Adding voice-based alerts
- Implementing blockchain for secure transactions
- Enhancing behavioral analysis techniques

This project shows how AI can be effectively used to solve real-world financial security problems.

REFERENCES

[1] J. West and M. Bhattacharya, "Intelligent Financial Fraud Detection: A Comprehensive Review," *Computers & Security*, vol. 57, pp. 47–66, 2016.
[2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, 2009.
[3] National Payments Corporation of India (NPCI), "Unified Payments Interface (UPI) Guidelines," Available: https://www.npci.org.in/what-we-do/upi/product-overview
[4] Reserve Bank of India, "Digital Payment Security Controls," Available: https://www.rbi.org.in
[5] Google Firebase Documentation, Available: https://firebase.google.com/docs
[6] React.js Documentation, Available: https://react.dev
[7] Node.js Documentation, Available: https://nodejs.org
[8] S. Jha, M. Guillen, and J. Westland, "Employing Transaction Aggregation Strategy to Detect Credit Card Fraud," *Expert Systems with Applications*, vol. 39, no. 16, pp. 12650–12657, 2012.
[9] A. Srivastava, A. Kundu, S. Sural, and A. Majumdar, "Credit Card Fraud Detection Using Hidden Markov Model," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 1, pp. 37–48, 2008.
[10] K. Randhawa et al., "Credit Card Fraud Detection Using AdaBoost and Majority Voting," *IEEE Access*, vol. 6, pp. 14277–14284, 2018.

