iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** I **Month of publication:** January 2025

DOI: https://doi.org/10.22214/ijraset.2025.66643

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

UPI Fraud Detection Using Machine Learning

Mohammad Yasir[1], N Sudarshan Reddy[2], Niranjan Reddy R[3], Nithin A[4], Professor Madhuri Akki[5]
Ballari Institute of Technology & Management, India

Abstract: ***Digital transactions have been growing rapidly, leading to a parallel increase in online payment fraud. According to the Reserve Bank of India, digital payments saw a 216% rise in volume and a 10% increase in value between March 2019 and March 2022. As more people embrace digital payment methods, security challenges and a lack of awareness about online payments persist. A few years ago, online payments were rare, but now UPI payment QR codes can be found at nearly every doorstep. This has opened the door for scammers and fraudsters to exploit these systems, deceiving people and carrying out fraudulent transactions. However, online transactions are monitored, which allows for the application of advanced tools to analyze them. This system aims to develop a machine learning model to detect fraudulent activities within transaction datasets.***

I. INTRODUCTION

Mobile payments have become a widely adopted payment method, leading to a surge in transaction volumes on online platforms. However, this increased usage has also drawn the attention of fraudsters who exploit the complexities of network systems to carry out fraudulent activities. Such fraud not only impacts consumers but also hinders the sustainable development of the digital economy. As a result, effective fraud detection in transactions is crucial for combating these issues. Traditional fraud detection methods often rely on statistical analysis and multi-dimensional techniques. While these methods can verify certain aspects of transactions, they often fail to identify deeper patterns within transaction data, limiting their overall effectiveness. In contrast, advancements in big data and machine learning provide more robust solutions for detecting fraudulent activities. Machine learning algorithms, especially when applied to extensive datasets, can capture critical features that traditional statistical techniques might overlook. By applying suitable machine learning methods, models can be created to analyze transaction data and identify fraudulent behavior, thereby reducing financial losses.

II. LITERATURE REVIEW

A. UPI Fraud Detection using Machine Learning

This study explores the application of machine learning techniques for detecting fraudulent transactions in UPI systems. The authors implement supervised learning models such as decision trees and logistic regression to classify transactions based on suspicious behavior. The paper highlights the importance of feature engineering in identifying key patterns indicative of fraud. The findings show that machine learning-based approaches.

B. Fraud Detection in UPI Transactions Using Machine Learning

This research investigates the use of advanced machine learning models for detecting fraud in UPI payment systems. The study integrates algorithms like Random Forest and Gradient Boosting for supervised classification, while also employing anomaly detection through unsupervised techniques. Key findings suggest that combining supervised and unsupervised models enhances fraud detection rates while maintaining a low incidence.

C. A Review on UPI Fraud Detection using Machine Learning and Deep Learning

This study consolidates the advancements in machine learning and deep learning techniques for detecting fraud in UPI transactions. The authors survey methods such as Convolutional Neural Networks (CNN), Autoencoders, and Decision Trees, evaluating their effectiveness in identifying fraudulent activities. The review concludes that deep learning methods, particularly CNN, are highly effective in capturing complex fraud patterns.

D. UPI Fraud Detection Using Convolutional Neural Networks (CNN)

This study delves into the use of Convolutional Neural Networks (CNN) for detecting fraud in UPI transactions. The study demonstrates how CNNs can efficiently analyze large volumes of transactional data to identify patterns indicative of fraudulent activities. The results indicate that CNN models outperform traditional machine learning algorithms in terms of accuracy and processing speed.

©IJRASET: All Rights are Reserved

E. UPI Fraud Detection Using Machine Learning

This study examines the application of machine learning algorithms, particularly Random Forest and Support Vector Machines, for UPI fraud detection. The authors highlight the role of ensemble methods in improving classification accuracy and reducing false-positive rates. Preprocessing techniques are emphasized as a critical step in enhancing the overall performance of the models.

III. PROBLEM DEFINITION

The rapid adoption of digital payment systems, particularly UPI, has led to a surge in online transactions. However, this growth has also increased the risk of fraudulent activities, jeopardizing user trust and financial security. Existing fraud detection methods often struggle to address key challenges, such as handling highly imbalanced datasets, integrating labeled and unlabeled data, and processing large transaction volumes efficiently. These limitations hinder the ability to detect and prevent fraud in real-time effectively

IV. METHODOLOGY

To analyze cardholder behavior and detect fraudulent transactions, we first utilize a clustering technique to group cardholders into distinct categories—high, medium, and low—based on their transaction amounts using range partitioning. Following this, the Sliding Window method is applied to consolidate transactions within each group and extract relevant features that reflect behavioural patterns. These features include the highest and lowest transaction amounts, the average transaction value within the window, and the time elapsed.

A. Algorithm 1: Sliding Window-Based Transaction Aggregation and Feature Extraction Input:

1) Cardholder ID
2) Sequence of transactions (t)
3) Window size (w) Output:
4) Aggregated transaction details
5) Cardholder behavioral features

Steps:

a) Create an empty list for aggregated transaction details.
b) Create an empty list for cardholder features.
c) Set start_idx to 0 and end_idx to w.
d) While end_idx is within the length of transactions:

- Extract transactions from start_idx to end_idx.
- Calculate metrics such as maximum, minimum, average transaction amounts, and elapsed time.
- Derive behavioral features from the window.
- Append aggregated metrics and features to respective lists.
- Slide the window forward by 1.

e) Return aggregated metrics and feature

B. Algorithm 2: Classifier Accuracy Rating Update Input:

Output: Steps:

- Cardholder ID
- Previous and current transactions
- Classifier's updated accuracy rating

1) Initialize the classifier's accuracy rating to 0.
2) For each incoming transaction:

- Update the classifier with previous and current transactions.
- Compare the classifier’s prediction to the actual label.
- Adjust the rating—increment for correct predictions and decrement for incorrect ones.
- Update the previous transaction for the next iteration.

3) Return the updated rating score.

IV. RESULTS AND EVALUATION

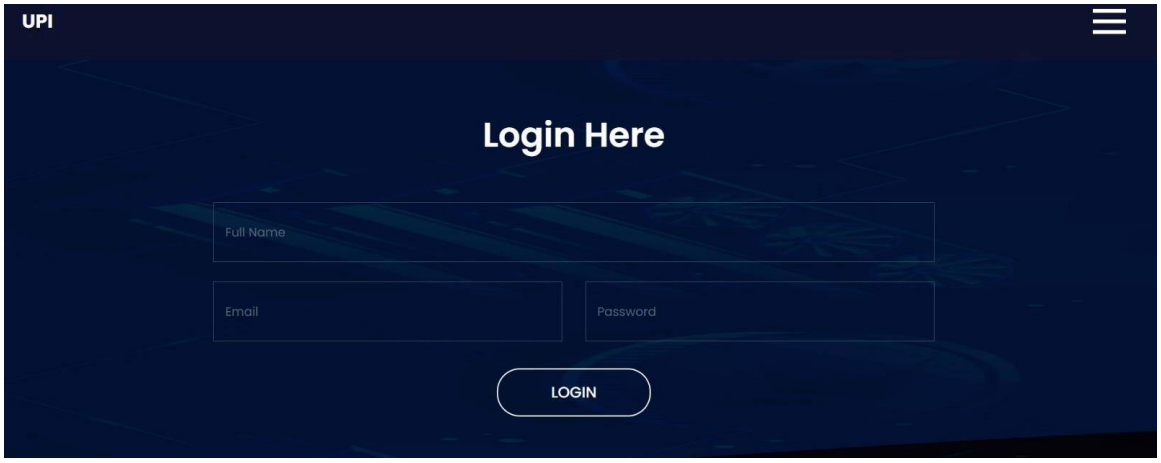


Fig1: login page

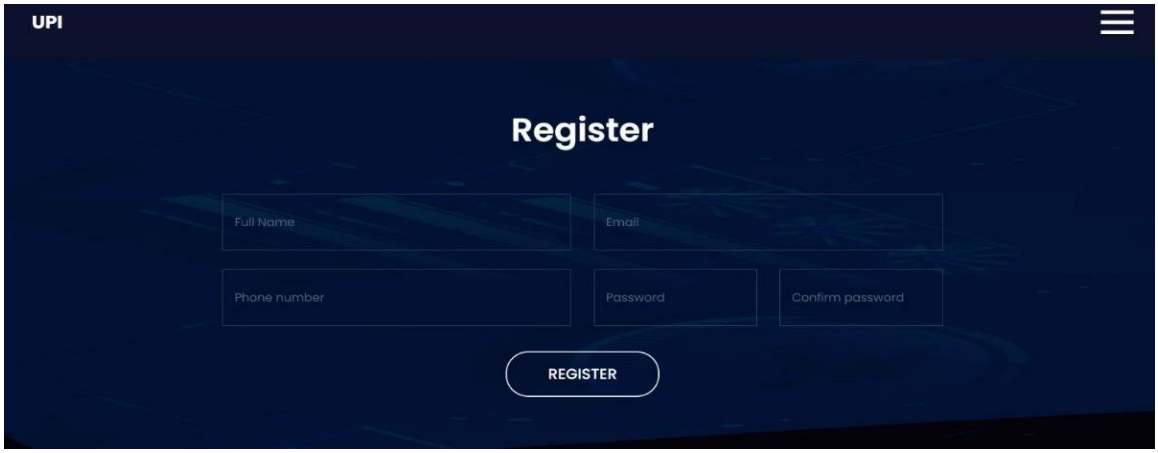


Fig2: user registration page

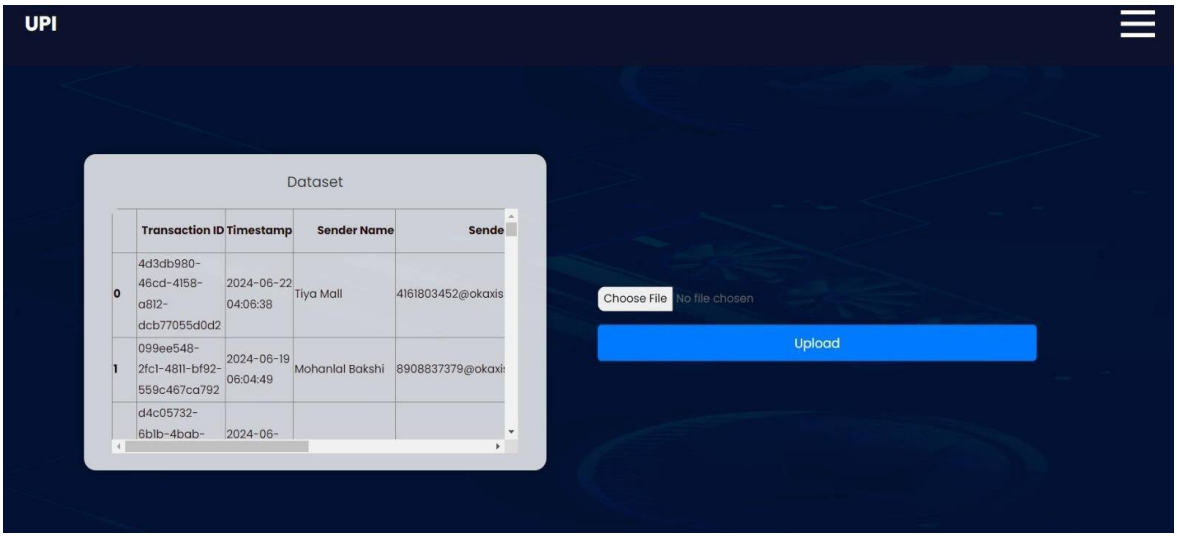


Fig3: Upload Dataset

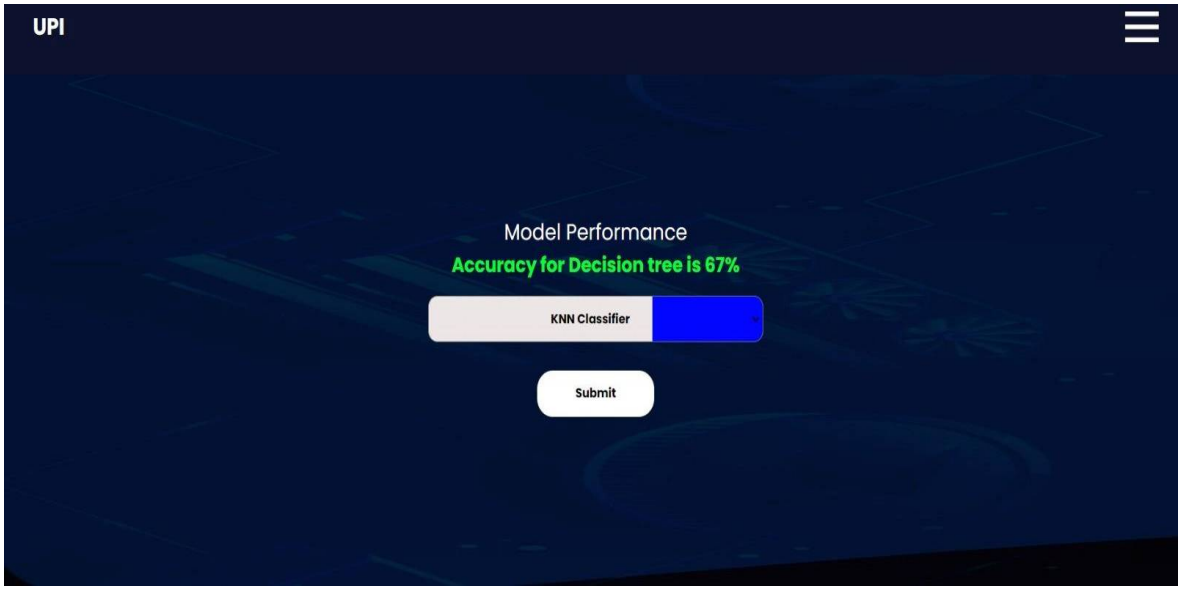


Fig4: Model Performance

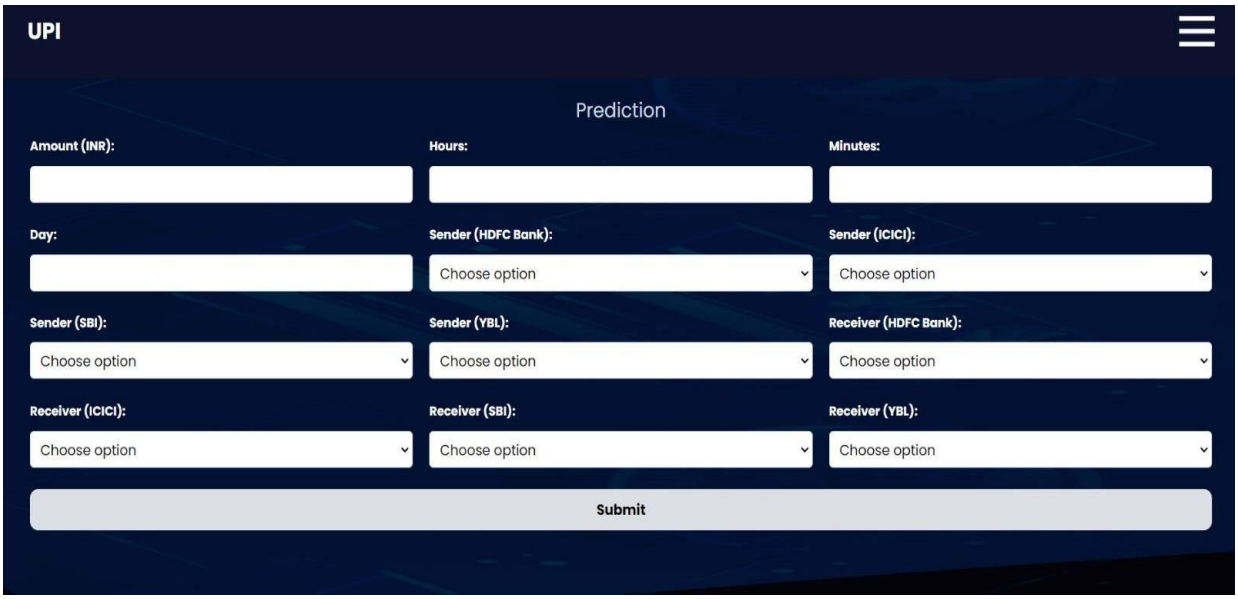


Fig5: Prediction

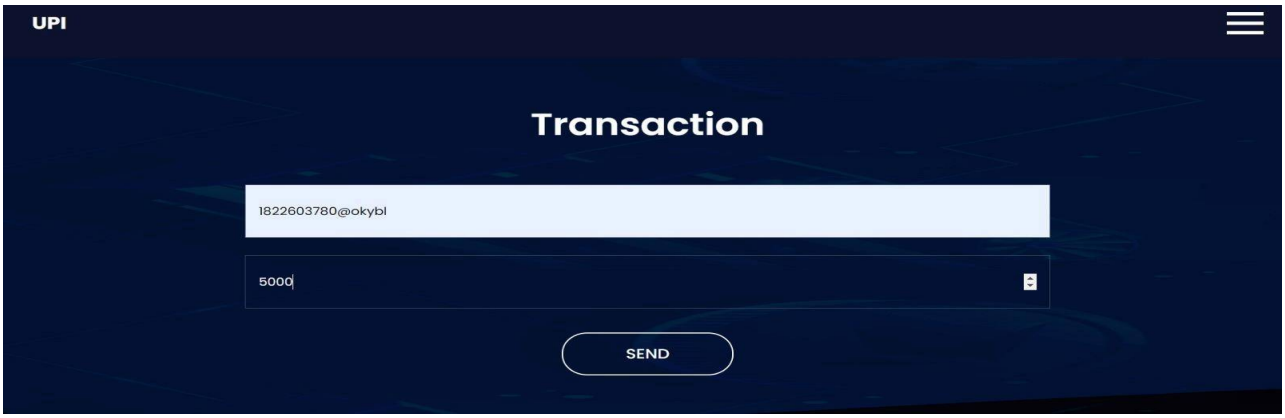


Fig6: Quiz Analysis page

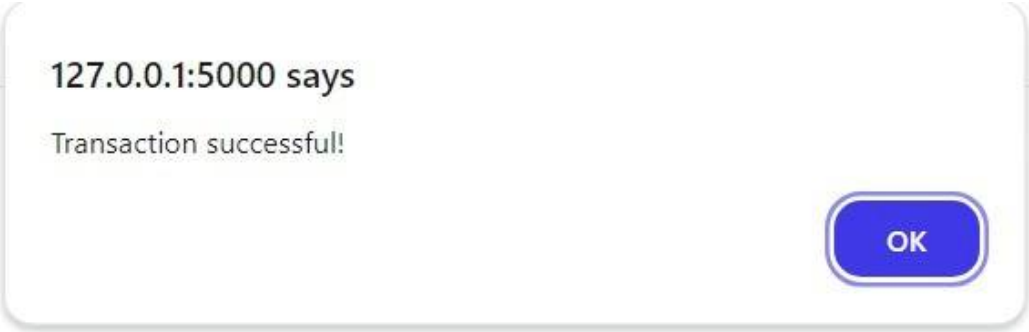


Fig7: Transaction

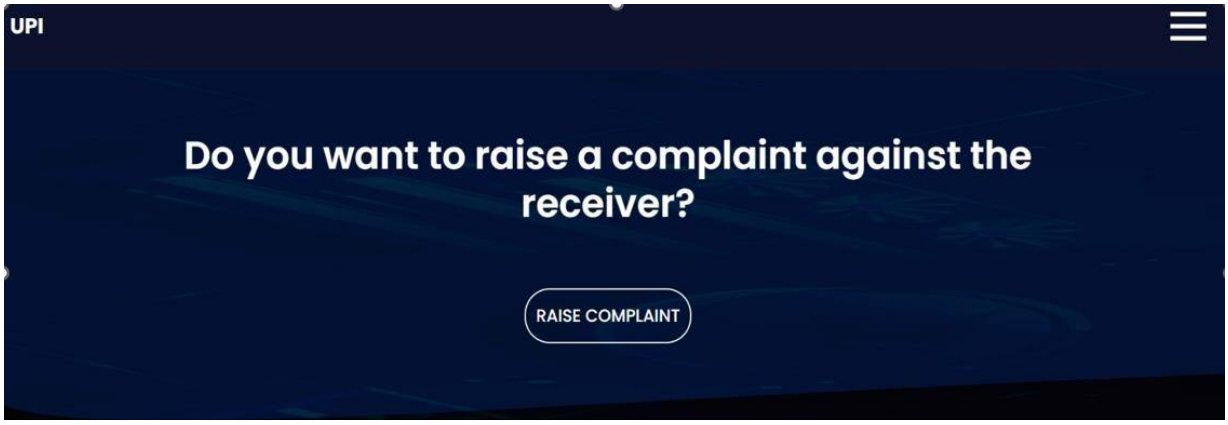


Fig8: Raise Complaint

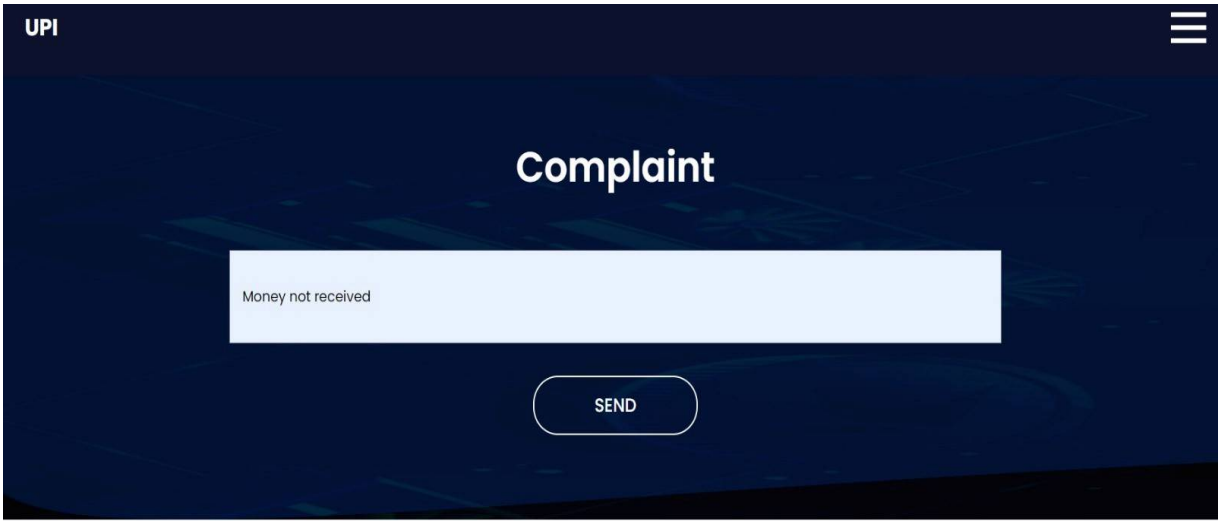


Fig9: Description of Complaint

V. CONCLUSION

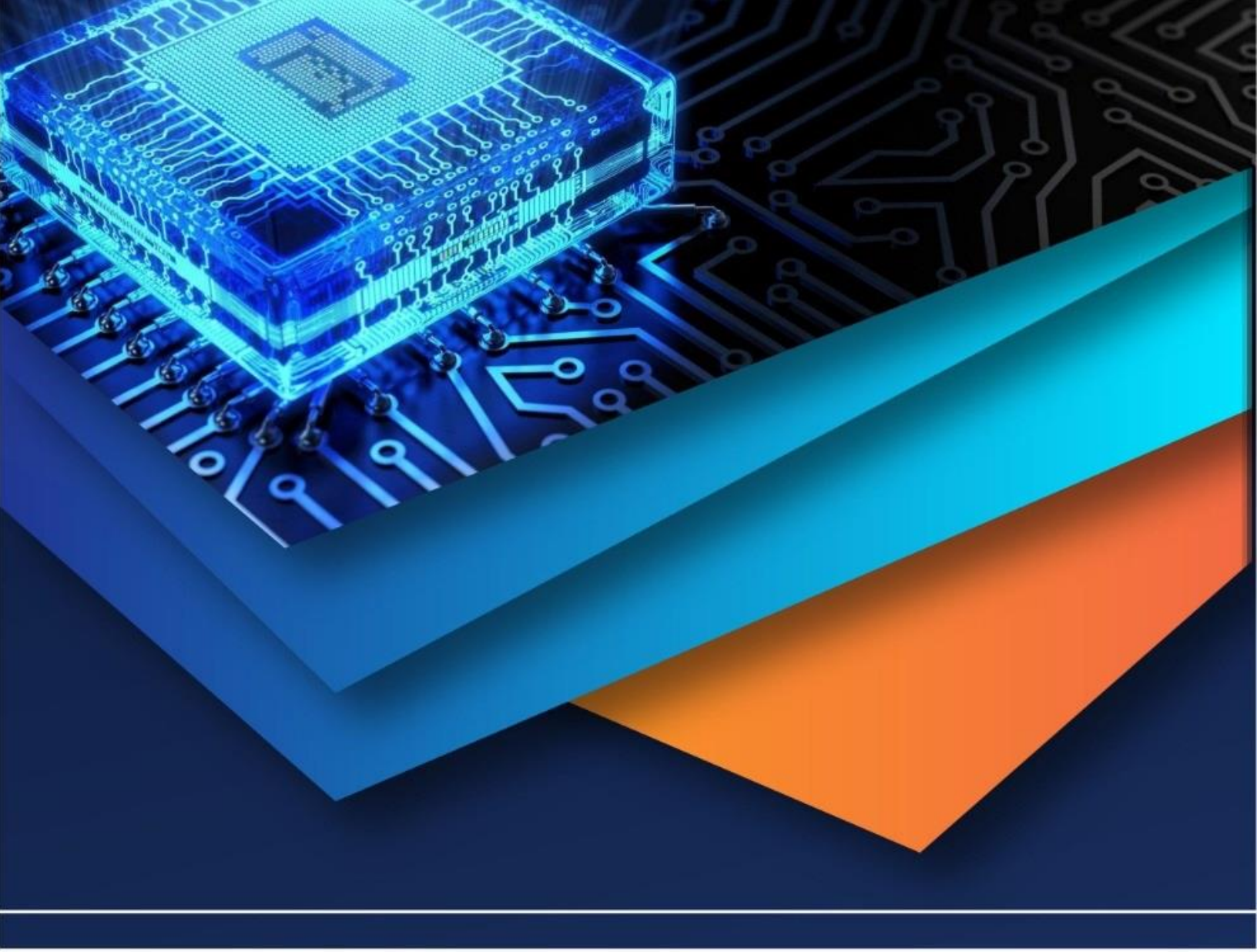
UPI transactions become more prevalent, robust fraud detection is essential for user protection. Our multi- algorithm approach, combining Random Forest, K-Nearest Neighbours (KNN), and Decision Trees, effectively identifies fraudulent transactions while ensuring legitimate ones are processed smoothly. The proposed model enhances accuracy, resilience, and interpretability, helping financial institutions improve security and user confidence. This research contributes to mitigating fraud in digital payments, ensuring the integrity and reliability of UPI as a trusted payment method.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

REFERENCES

[1] Sayalee S. Bodade, Prof. P.P. Pawade, "UPI Fraud Detection using Machine Learning," Journal of Emerging Technologies and Innovative Research (JETIR), ISSN: 2349-5162, Volume 11, Issue 4, April 2024.
[2] J. Kavitha, G. Indira, A. Anil Kumar, A. Shrinita, D. Bappan, "Fraud Detection in UPI Transactions Using Machine Learning," International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), ISSN: 2582-5208, Volume 6, Issue 9, September 2024.
[3] Mrs. Sridevi N, Ayush Singh, Ashish G, Gulsan Gupta, Gaurav Shandil, "A Review on UPI Fraud Detection using Machine Learning and Deep Learning," International Journal for Research in Applied Science and Engineering Technology (IJRASET), ISSN: 2321-9653, Volume 12, Issue 12, December 2024.
[4] Akash Sharma, Veena Raj, "UPI Fraud Detection Using Convolutional Neural Networks (CNN)," ResearchGate, December 2024.
[5] Ankit Gupta, Nisha Mehta, "UPI Fraud Detection Using Machine Learning," International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), ISSN: 2320-9801, Volume 12, Issue 4, April 2024.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)