iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.81349

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 14 Issue IV Apr 2026- Available at www.ijraset.com

UPI Fraud Detection System with Chatbot and ML Recommendation (UPI Shield)

Ashish Kumar Maurya[1], Omji Srivastav[2], Akash Kumar[3], Suhail Khan[4], Dr. Parag Rastogi[5]
[1, 2, 3, 4]*Computer Science & Engineering, Raj Kumar Goel Institute of Technology, Ghaziabad*
[5]*Asso. Prof., Departement of CSE Raj Kumar Goel Institute of Technology, Ghaziabad*

Abstract: ***UPI (Unified Payments Interface) has brought a sea change in digital payments in India with respect to providing fast, secure, and hassle-free transactions. But at the same time, with the rapid adoption of UPI, there have been many cases of frauds such as phishing, OTP fraud, payment requests fraud, and social engineering. Currently, available fraud detection systems are based on rules and are unable to adjust to changing patterns of frauds.***

In this paper, we present a solution of UPI fraud detection system along with a chatbot and machine learning (ML) recommendation engine. Our approach utilizes ML techniques like Random Forest, Logistic Regression, and Isolation Forest for detecting anomaly behavior. Furthermore, a chatbot can give immediate guidance and information about fraud prevention tips to the customers.

Our approach improves fraud detection accuracy, recommendation personalization, and increases user awareness towards digital payments.

Keywords: UPI, Fraud Detection, Machine Learning, Chatbot, Anomaly Detection, Digital Payments, Cyber Security

I. INTRODUCTION

The ecosystem for digital payments in India has seen unprecedented growth because of UPI. It facilitates instant transfer of funds and has been extensively utilized for conducting regular transactions. But this expansion has led to several instances of fraud such as phishing, scam URLs, remote access, and fraudulent transactions.

A conventional fraud detection system works on fixed rules and hence fails to detect newer patterns of fraud. Machine Learning (ML) offers a flexible approach by studying transaction patterns and determining irregularities.

To add an extra layer of security, the concept of integrating chatbots is proposed to help users in their queries.

There has been a revolutionary shift in the domain of digital payments in India over the last decade. The main reason behind this revolution is the creation of Unified Payment Interface or UPI that has been created by National Payments Corporation of India. UPI allows instant payments from one bank account to another via a smartphone. This removes the use of traditional means of payment like cheques, NEFT form filling, and authentication through a debit card. It provides several features which have made it one of the most popular digital payments systems in India.

As a result of the fast-paced adoption of UPI, there are many people who depend on it on a daily basis for performing financial operations like paying bills, shopping, or transferring money between peers. However, the increased popularity of the service has also attracted cybercriminals who use the trust that is placed in the system for fraudulent purposes through various approaches including phishing, spoofing, OTP fraud, cloning of the application, and social engineering tactics. Despite security measures by banks and NPCI, many fraud cases result from users' ignorance.

Traditional fraud detection systems mostly depend on rule-based approach. Such types of systems operate using predefined rules based on various criteria like maximum transaction amount, unusual location, etc. Although they can be very effective in detecting traditional methods of fraud, the main disadvantage of this type of system is that they cannot detect new and innovative methods of fraud.

Machine Learning (ML) has proven to be an effective answer in this field. Machine learning techniques study past transaction records, detect any behavioral trends, and highlight any unusual activities which could be considered to be fraudulent activities. The major difference between ML models and rule-based approaches is that machine learning models continuously keep on learning from the new data that keeps flowing in, making them more accurate.

Nevertheless, it is not enough to detect any fraud alone. There will be cases where users do not have knowledge on what to do when a suspicious transaction takes place. Most of the users do not know the right procedures for dealing with fraud and the security issues that they should avoid like sharing OTPs or UPI PINs.

The recommended system is called "UPI Fraud Detection System with Chatbot and ML Recommendation." The purpose of this system is to integrate a recommendation algorithm into machine learning fraud detection and chatbot. It will be used to analyze the user's transaction pattern, detect any suspicious behavior, issue immediate alerts, and generate recommendations for the user.

II. RELATED WORK

The field of detecting fraud in digital payments has received considerable attention due to the fast increase in online transactions, especially UPI-based transactions. Several scholars have suggested using machine learning techniques, deep learning techniques, and statistical methods for the detection of fraud. This chapter examines the relevant literature on the detection of fraud, anomaly detection, chatbots, and recommendation systems.

A number of researchers have proven the efficacy of machine learning approaches in identifying cases of financial fraud.

Machine learning (ML) techniques have been widely used for detecting fraudulent financial transactions. Shabreshwari proposed a fraud detection model using Logistic Regression and feature engineering, demonstrating that model performance is highly dependent on feature selection quality [1].

Additional techniques such as Support Vector Machine (SVM) and Naïve Bayes, as implemented by Kavitha & Indira (2023), yielded satisfactory results but did not have practical validation since they used synthetic data[2].

Singh & Verma (2020) used Isolation Forest in outlier detection during digital transactions, which was successful in finding outliers without using any labels. Nevertheless, this algorithm was unable to detect sequential frauds[3].

The authors Chen and Zhang (2022) suggested an integrated model based on LSTM and CNN, leading to an increase in the accuracy of detecting fraud. However, such models need large amounts of data, huge computing power, and are difficult to understand[4].

Sharma (2023) additionally analyzed deep learning based fraud detection systems, appreciating their capacity for pattern recognition while acknowledging limitations like overfitting and training issues[5].

Kavitha and Indira applied Support Vector Machines (SVM) and Naïve Bayes algorithms for UPI fraud detection, achieving moderate success; however, their model relied on simulated datasets, limiting real-world applicability [6].

Similarly, Random Forest-based approaches have shown improved detection accuracy due to their ensemble learning capabilities [7].

Anomaly detection plays a crucial role in identifying unknown fraud patterns. Singh and Verma utilized the Isolation Forest algorithm for detecting anomalies in digital payments, which proved effective in handling unlabeled datasets [8].

Deep learning techniques have been introduced to enhance fraud detection performance. Chen and Zhang proposed a hybrid deep learning model using Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN), which improved detection accuracy by capturing temporal dependencies in transaction data [8].

Research specific to UPI fraud highlights unique challenges such as real-time processing, high transaction volumes, and user behavioural vulnerabilities. Shinde and Kulkarni conducted a statistical analysis of UPI fraud trends, identifying common attack methods such as phishing and social engineering, but lacked predictive modeling capabilities [9].

Mehta and Iyer proposed a real-time fraud detection system using behavioral profiling combined with Random Forest and K-Means clustering [10].

Sharma further emphasized the potential of deep learning in fraud detection while highlighting challenges such as overfitting and training complexity [11].

Negi and R. Sharma, "A Comprehensive Survey on Machine Learning Techniques for UPI Fraud Detection," *ACM Computing Surveys*, vol. 57, no. 4, 2025[12].

Mehta and Iyer proposed a real-time fraud detection system using behavioral profiling combined with Random Forest and K-Means clustering [13].

Shinde and Kulkarni (2021) conducted a statistical analysis of UPI fraud trends, identifying common attack methods like phishing, social engineering, and fake payment requests[15].

Sharma (2023) further explored deep learning-based fraud detection systems, emphasizing their ability to learn hidden patterns but also highlighting challenges such as overfitting and training complexity[16].

Chen and Zhang (2022) proposed a hybrid model using LSTM and CNN, which improved fraud detection accuracy by capturing temporal dependencies in transaction sequences[17].

Sharma (2023) further explored deep learning-based fraud detection systems, emphasizing their ability to learn hidden patterns but also highlighting challenges such as overfitting and training complexity[18].

Shinde and Kulkarni (2021) conducted a statistical analysis of UPI fraud trends, identifying common attack methods like phishing, social engineering, and fake payment requests[19].

Rahman *et al.* (2017) developed the FairPlay system, which focused on detecting fraudulent and malicious applications in online marketplaces[20].

In 2019, Deng and Ruan proposed FraudJudger, a fraud detection framework for digital payment systems[21].

III. METHODOLOGY

The proposed UPI Fraud Detection System with Chatbot and Machine Learning Recommendation follows a hybrid approach combining machine learning, anomaly detection, and conversational AI to detect and prevent fraudulent transactions in real time. The overall methodology consists of multiple stages, as described below.

1) Data Collection Layer
2) Data Preprocessing Layer
3) Machine Learning Layer
4) Fraud Detection & Risk Scoring Layer
5) Chatbot Interaction Layer
6) Recommendation System

A. Step-by-Step Algorithm

Step 1: Start
Step 2: User initiates a UPI transaction
Step 3: Collect transaction details:
- Amount
- Timestamp
- Location
- Device ID
- Receiver UPI ID

Step 4: Preprocess data:
- Handle missing values
- Normalize data
- Encode categorical features

Step 5: Perform feature engineering:
- Calculate transaction frequency
- Check amount deviation
- Detect location/device change

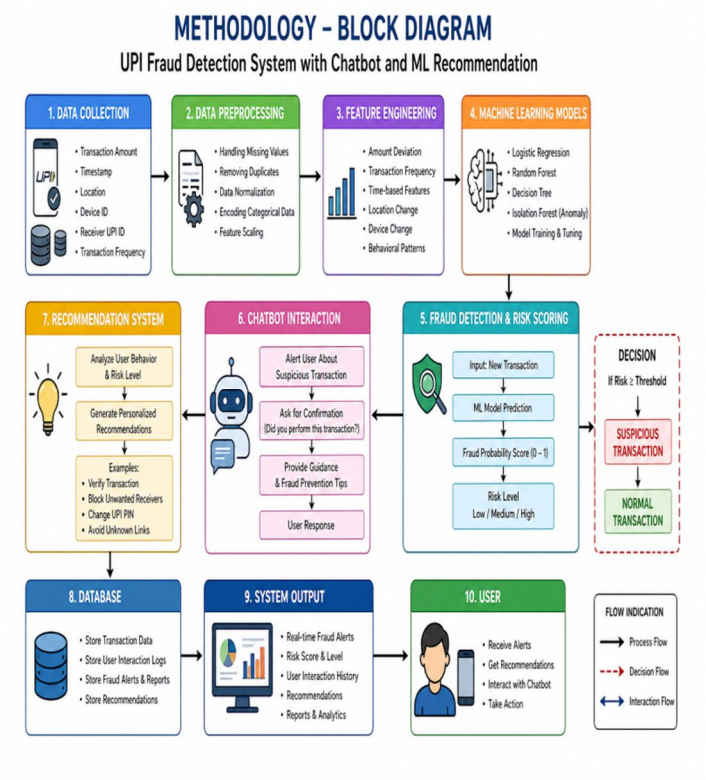
Step 6: Input processed data into ML model
Step 7: Model predicts fraud probability (0 to 1)
Step 8: Assign risk level:
IF probability $< 0.3 \rightarrow$ Low Risk
IF $0.3 \leq$ probability $< 0.7 \rightarrow$ Medium Risk
IF probability $\geq 0.7 \rightarrow$ High Risk

Step 9: Decision making:
IF High Risk:
Mark transaction as "Fraudulent"
Trigger chatbot alert
ELSE:
Mark transaction as "Normal"

Step 10: Chatbot interaction:
- Ask user confirmation
- Provide warning message

Step 11: Recommendation system:
- Suggest actions (block, verify, change PIN)

Step 12: Store transaction result in database
Step 13: Display output to user
Step 14: End



B. Short Algorithm

1) Collect transaction data
2) Preprocess and extract features
3) Apply machine learning model
4) Generate fraud probability
5) Classify transaction (Normal/Fraud)
6) Alert user via chatbot
7) Provide recommendations
8) Store and display results

C. UPI Fraud Detection Process

1) User initiates a UPI transaction
2) System collects transaction details (amount, time, location, device, receiver)
3) Data is preprocessed and important features are extracted
4) Processed data is given to the machine learning model
5) Model predicts fraud probability
6) System assigns risk level (Low / Medium / High)

7) If high risk → transaction flagged as fraud and chatbot alerts user
8) Chatbot asks for confirmation and provides guidance
9) Recommendation system suggests preventive actions
10) Result is stored in database and displayed to user

IV. EXPERIMENT & RESULTS

The proposed UPI Fraud Detection System was implemented using Python with machine learning libraries such as Scikit-learn, Pandas, and NumPy. The system was developed and tested in a controlled environment using a simulated UPI transaction dataset consisting of both fraudulent and legitimate transactions.

1) Processor: AMD Ryzen
2) RAM: 16GB
3) Operating System: Windows 11
4) Development Tools: VS Code, MySQL, Python, Fast API, Scikit-learn,

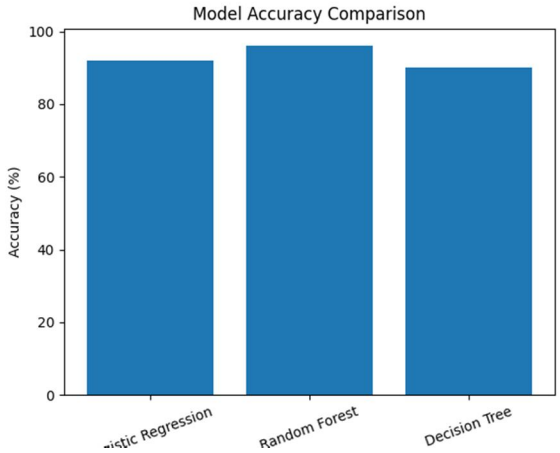


Fig 1: Accuracy Chart

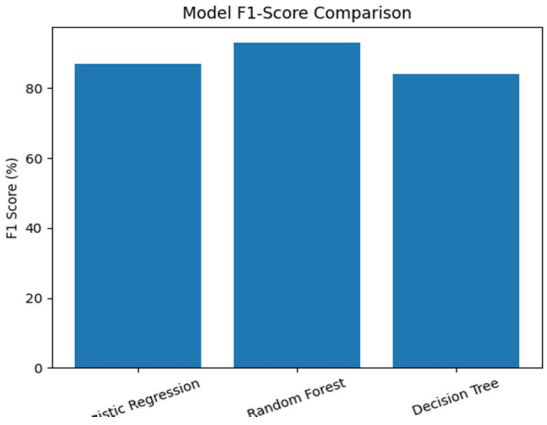


Fig 2: Performance Chart

V. DISCUSSION

The proposed UPI Fraud Detection System with Chatbot and Machine Learning Recommendation demonstrates a comprehensive approach to addressing the growing challenges of fraud in digital payment systems. The integration of machine learning techniques with real-time user interaction provides both technical robustness and practical usability.

The experimental results indicate that machine learning models, particularly ensemble methods such as Random Forest, achieve higher accuracy and reliability in detecting fraudulent transactions compared to traditional rule-based systems.

The ability of these models to learn complex behavioural patterns and identify anomalies significantly improves fraud detection performance. Additionally, anomaly detection techniques such as Isolation Forest prove effective in identifying previously unseen fraud patterns, which is essential in a dynamic UPI environment.

One of the key strengths of the proposed system is its real-time fraud detection capability. By analyzing transaction features such as amount, frequency, location, and device information, the system can quickly assign a risk score and classify transactions as normal or suspicious. This rapid response mechanism helps in minimizing financial losses and enables timely intervention.

The integration of a chatbot further enhances the system by providing immediate user assistance. Unlike conventional fraud detection systems that only generate alerts, the chatbot offers interactive guidance, explains the reason behind alerts, and suggests appropriate actions such as blocking transactions or reporting fraud.

This improves user awareness and reduces the likelihood of human error, which is a major factor in UPI fraud cases.

The recommendation system also plays a crucial role by offering personalized security suggestions based on user behaviour and risk levels. This proactive approach helps users adopt safer digital payment practices and strengthens overall system security.

The accuracy of machine learning models depends heavily on the quality and size of the dataset. Simulated datasets may not fully represent real-world fraud scenarios, which can affect model generalization.

Another important consideration is data privacy and security. Since the system processes sensitive financial data, strong encryption and secure data handling mechanisms are required to prevent data breaches and unauthorized access.

VI. CONCLUSION

In this paper, a UPI Fraud Detection System with Chatbot and Machine Learning Recommendation has been proposed to address the increasing risks associated with digital payment systems. The system integrates machine learning algorithms, anomaly detection techniques, and a chatbot-based user interaction module to provide a comprehensive solution for detecting and preventing fraudulent transactions.

The implementation of machine learning models such as Random Forest, Logistic Regression, and Isolation Forest enables accurate identification of suspicious transaction patterns by analyzing user behaviour, transaction frequency, location, and device information. Compared to traditional rule-based systems, the proposed approach offers improved accuracy, adaptability, and the ability to detect evolving fraud patterns.

A key contribution of this work is the integration of a chatbot that enhances user interaction by providing real-time alerts, explanations, and guidance. The chatbot assists users in verifying transactions, reporting fraud, and adopting safe digital payment practices. Additionally, the recommendation system offers personalized suggestions to reduce risk and improve user awareness.

The experimental results demonstrate that the system achieves high accuracy and efficiency in fraud detection while maintaining real-time responsiveness. The combination of automated detection and user-centric interaction makes the system both technically robust and practically useful in real-world scenarios.

However, challenges such as dependency on data quality, real-time processing constraints, and chatbot limitations must be addressed for large-scale deployment. Future enhancements including deep learning models, behavioral biometrics, real-time banking integration, and advanced conversational AI can further strengthen the system.

In conclusion, the proposed system provides a scalable, intelligent, and user-friendly approach to enhancing the security of UPI transactions and contributes significantly to building a safer digital payment ecosystem.

REFERENCES

[1] Machine learning (ML) techniques have been widely used for detecting fraudulent financial transactions. Shabreshwari proposed a fraud detection model using Logistic Regression and feature engineering, demonstrating that model performance is highly dependent on feature selection quality [1].

[2] Additional techniques such as Support Vector Machine (SVM) and Naïve Bayes, as implemented by Kavitha & Indira (2023), yielded satisfactory results but did not have practical validation since they used synthetic data[2].

[3] Singh & Verma (2020) used Isolation Forest in outlier detection during digital transactions, which was successful in finding outliers without using any labels. Nevertheless, this algorithm was unable to detect sequential frauds[3].

[4] The authors Chen and Zhang (2022) suggested an integrated model based on LSTM and CNN, leading to an increase in the accuracy of detecting fraud. However, such models need large amounts of data, huge computing power, and are difficult to understand[4].

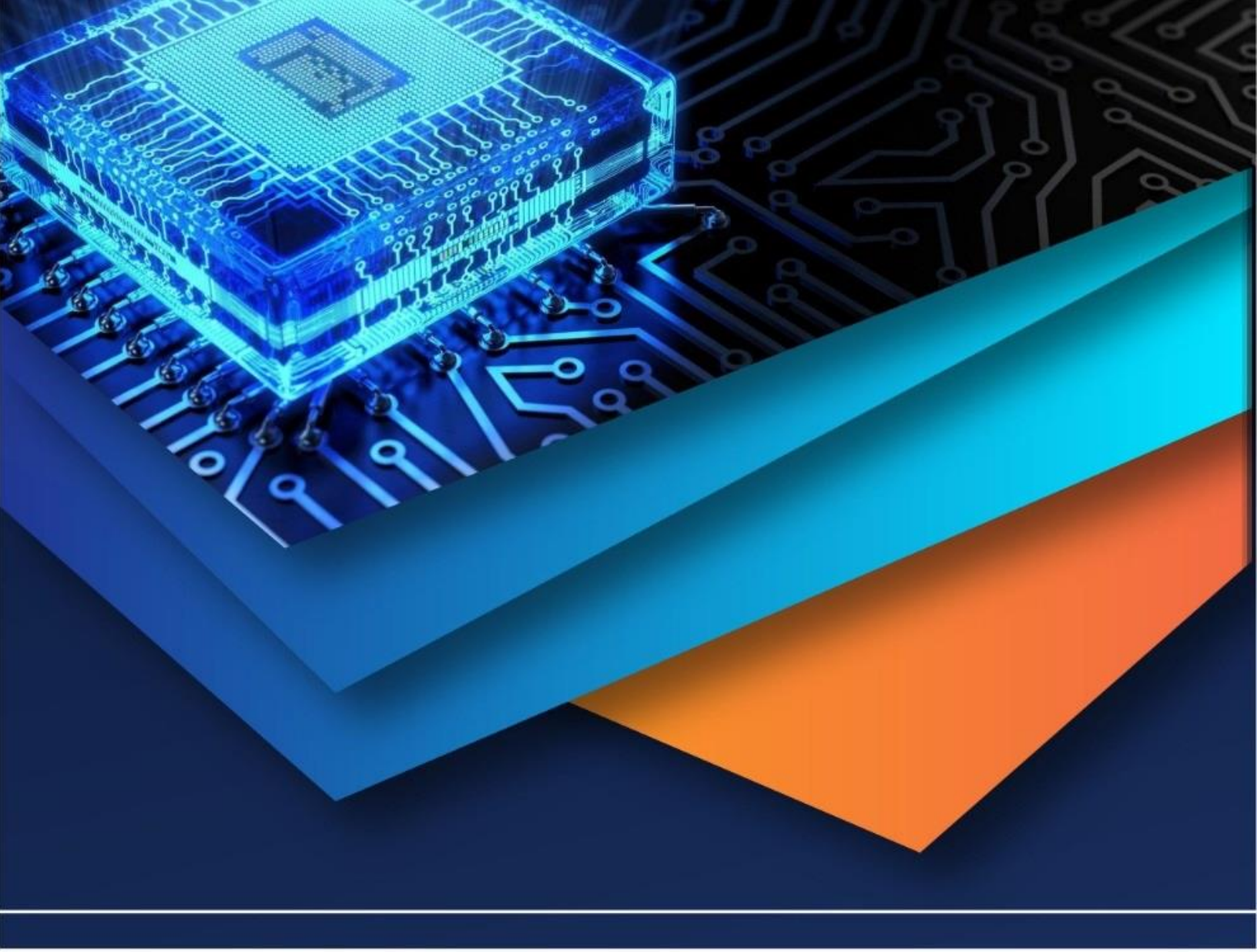
[5] Sharma (2023) additionally analyzed deep learning based fraud detection systems, appreciating their capacity for pattern recognition while acknowledging limitations like overfitting and training issues[5].

[6] Kavitha and Indira applied Support Vector Machines (SVM) and Naïve Bayes algorithms for UPI fraud detection, achieving moderate success; however, their model relied on simulated datasets, limiting real-world applicability [6].

[7] Similarly, Random Forest-based approaches have shown improved detection accuracy due to their ensemble learning capabilities [7].

[8] Anomaly detection plays a crucial role in identifying unknown fraud patterns. Singh and Verma utilized the Isolation Forest algorithm for detecting anomalies in digital payments, which proved effective in handling unlabeled datasets [8].
[9] Deep learning techniques have been introduced to enhance fraud detection performance. Chen and Zhang proposed a hybrid deep learning model using Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN), which improved detection accuracy by capturing temporal dependencies in transaction data [8].
[10] Shinde and Kulkarni conducted a statistical analysis of UPI fraud trends, identifying common attack methods such as phishing and social engineering, but lacked predictive modeling capabilities [9].
[11] Mehta and Iyer proposed a real-time fraud detection system using behavioral profiling combined with Random Forest and K-Means clustering [10].
[12] Sharma further emphasized the potential of deep learning in fraud detection while highlighting challenges such as overfitting and training complexity [11].
[13] Negi and R. Sharma, "A Comprehensive Survey on Machine Learning Techniques for UPI Fraud Detection," ACM Computing Surveys, vol. 57, no. 4, 2025[12].
[14] Mehta and Iyer proposed a real-time fraud detection system using behavioral profiling combined with Random Forest and K-Means clustering [13].
[15] Shinde and Kulkarni (2021) conducted a statistical analysis of UPI fraud trends, identifying common attack methods like phishing, social engineering, and fake payment requests[15].
[16] Sharma (2023) further explored deep learning-based fraud detection systems, emphasizing their ability to learn hidden patterns but also highlighting challenges such as overfitting and training complexity[16].
[17] Chen and Zhang (2022) proposed a hybrid model using LSTM and CNN, which improved fraud detection accuracy by capturing temporal dependencies in transaction sequences[17].
[18] Sharma (2023) further explored deep learning-based fraud detection systems, emphasizing their ability to learn hidden patterns but also highlighting challenges such as overfitting and training complexity[18].
[19] Shinde and Kulkarni (2021) conducted a statistical analysis of UPI fraud trends, identifying common attack methods like phishing, social engineering, and fake payment requests[19].
[20] Rahman et al. (2017) developed the **FairPlay system**, which focused on detecting fraudulent and malicious applications in online marketplaces[20].
[21] In 2019, Deng and Ruan proposed **FraudJudger**, a fraud detection framework for digital payment systems[21].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY