WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Fraud Detection in online UPI Payment

***K.Arul Jothi*[1*], [#]*Dr.R.Vijayalakshmi, MCA., M.Phil., Ph.D.,*[2]**

[1]Master of Computer Applications, KrishnasamyCollege of Engineering &Technology,Cuddalore,India

[2]MCA.,M.Phil.,Associate Professor, Master of Computer Applications, KrishnasamyCollege of Engineering &Technology,Cuddalore,India

ABSTRACT

With the rapid adoption of Unified Payments Interface (UPI) for digital transactions, the risk of fraudulent activities in online payments has significantly increased. This paper proposes a machine learning-based fraud detection system that analyzes transaction patterns in real-time to identify suspicious behavior and prevent financial losses. By utilizing features such as transaction frequency, device ID, location, and user behavior, the system efficiently distinguishes between legitimate and fraudulent transactions. The proposed approach ensures enhanced security without compromising user convenience, thereby strengthening trust in digital payment systems. Experimental results on real-world UPI transaction datasets show high accuracy and low false positives, demonstrating the effectiveness of the model in practical scenarios.

Keywords: UPI, fraud detection, online payment, machine learning, digital transactions, real-time monitoring, user behavior, financial security, anomaly detection, cybersecurity.

I. INTRODUCTION

The rise of digital payment systems has revolutionized the way people conduct financial transactions in India and across the globe. Among the most significant innovations in this space is the Unified Payments Interface (UPI), a real-time payment system developed by the National Payments Corporation of India (NPCI). UPI allows users to transfer money instantly using a mobile device, and it has rapidly become one of the most widely used digital payment methods due to its speed, simplicity, and accessibility. As the usage of UPI grows, so does the threat of fraudulent activities. Online payment systems are often targeted by cybercriminals who exploit vulnerabilities in security mechanisms, user ignorance, or system loopholes. These frauds can take various forms, such as phishing, unauthorized transactions, fake UPI handles, and SIM swap attacks. The increasing number of fraud cases has raised concerns among users and financial institutions, creating an urgent need for effective fraud detection systems. Traditional methods of fraud detection often rely on predefined rules and manual verification processes, which may not be sufficient to tackle the dynamic and evolving nature of digital fraud. These systems struggle to detect sophisticated fraud patterns and are prone to delays in response time. Consequently, there is a growing interest in automated fraud detection using advanced technologies, particularly machine learning and data analytics. Machine learning techniques have the ability to analyze large volumes of transactional data and learn patterns that distinguish legitimate transactions from fraudulent ones. By training models on historical data, the system can identify anomalies or suspicious behavior in real-time and trigger alerts before the transaction is completed. This approach provides a more scalable and intelligent solution compared to static rule-based systems. In the context of UPI payments, several transaction features can be analyzed for fraud detection. These include transaction amount, frequency, time of transaction, device ID, IP address, and user behavior patterns. An unusual change in any of these parameters can indicate potential fraud. For instance, if a user suddenly initiates a high-value transaction from a new device or location, the system can flag it for further verification. To build an effective fraud detection model, data collection and feature engineering play a critical role. The model must be trained using a diverse dataset that includes both normal and fraudulent transactions. Preprocessing techniques are applied to clean and normalize the data, and relevant features are selected to enhance model accuracy. Supervised learning algorithms such as Random Forest, Decision Tree, and Support Vector Machine have shown promising results in detecting fraudulent activities. Another important aspect of fraud detection is real-time monitoring. Since UPI transactions are processed instantly, the fraud detection system must operate with minimal delay. Implementing real-time models requires robust infrastructure and efficient algorithms that can handle high transaction volumes without affecting system performance. The balance between speed and accuracy is crucial for delivering effective fraud prevention. User education and awareness also contribute to reducing the success rate of online payment frauds. While technology can prevent a large portion of fraud attempts, users must be informed about safe digital practices, such as not sharing OTPs, verifying UPI handles, and avoiding suspicious links. Therefore, a comprehensive fraud prevention strategy combines intelligent systems with user awareness initiatives. Government regulations and industry standards are continuously evolving to improve digital payment security. Regulatory bodies are encouraging the adoption of advanced authentication methods, data encryption, and fraud monitoring tools. Financial institutions are also investing in research and development to build more resilient systems capable of adapting to new threats. In summary, as digital payments become more integrated into everyday life, the risk of UPI fraud remains a serious challenge. To maintain public trust and ensure the safety of online transactions, it is essential to develop intelligent, real-time fraud detection systems. The integration of machine learning and data analytics offers a promising path forward, enabling secure, efficient, and reliable digital payment experiences for all users.

II. RELATED WORKS

2.1 A Machine Learning Approach for Detecting Fraudulent UPI Transactions

Sharma, R., Gupta, P., & Mehta, A.

This study explores the application of machine learning algorithms in detecting fraudulent transactions in Unified Payments Interface (UPI) systems. The authors evaluated various classifiers including Logistic Regression, Decision Trees, and Random Forests, using a synthetic dataset modeled on typical UPI transaction behavior. Results indicated that the Random Forest classifier offered the best performance in terms of precision, recall, and overall accuracy. The model successfully identified patterns and anomalies characteristic of fraudulent activity in UPI-based payments.

2.2 Fraud Detection in Digital Transactions Using Deep Learning Techniques

Kumar, V., Singh, M., & Kaur, G.

The paper proposes a deep learning-based framework to detect fraud in digital payments, particularly focusing on UPI platforms. A Convolutional Neural Network (CNN) architecture was adapted to process structured transaction data for anomaly detection. The study highlighted the advantages of deep learning over traditional models in capturing complex non-linear relationships in the data, achieving over 98% accuracy in fraud classification.

2.3 Real-Time Anomaly Detection in UPI Transactions Using Autoencoder Neural Networks

Desai, S., Patel, R., & Joshi, M.

This research presents an unsupervised learning method using autoencoders to detect anomalies in real-time UPI transaction streams. The authors emphasize the use of reconstruction error as a metric to distinguish between normal and suspicious transactions. Experimental results using UPI-like datasets demonstrated the model’s ability to detect unknown fraud patterns effectively, with minimal false positives.

2.4 Enhancing UPI Transaction Security Using Hybrid Machine Learning Models

Bose, A., Chatterjee, S., & Roy, N.

In this work, a hybrid model combining Support Vector Machines (SVM) and Gradient Boosting classifiers is proposed for UPI fraud detection. The authors collected transaction data simulating real-world UPI behavior and applied feature engineering techniques to improve detection accuracy. The hybrid model outperformed individual models, highlighting the potential of ensemble methods in financial fraud detection systems.

2.5 Intelligent Fraud Prevention System for UPI Payments Based on Behavioral Biometrics

Verma, D., Jain, A., & Rajput, H.

This paper introduces a novel fraud prevention mechanism using behavioral biometrics, such as typing speed and swipe patterns, integrated with UPI payment apps. By training a machine learning model on biometric behavior and transaction data, the system could identify fraudulent usage even when credentials were compromised. The approach enhanced overall transaction security and reduced the risk of unauthorized access in UPI environments.

III. PROPOSED SYSTEM

The proposed system for UPI fraud detection aims to revolutionize the current landscape by leveraging state-of-the-art Convolutional Neural Network (CNN) algorithms. Unlike traditional rule-based systems, the proposed system adopts a data-driven approach, utilizing deep learning techniques to analyze complex patterns and anomalies within UPI transaction data. By training CNN models on vast datasets of labeled transaction records, the system can learn to recognize subtle indicators of fraudulent behavior with unprecedented accuracy and efficiency. Through the integration of advanced anomaly detection algorithms and real-time monitoring capabilities, the proposed system offers proactive defense mechanisms against emerging fraud tactics and sophisticated attack vectors. Moreover, the system's adaptive learning capabilities enable it to continually evolve and adapt to evolving fraud patterns, ensuring robust protection against both known and unknown threats. Additionally, the proposed system prioritizes scalability and performance, leveraging distributed computing frameworks and cloud-based infrastructure to handle large-scale transaction volumes seamlessly. Furthermore, the system incorporates transparent and interpretable model architectures, facilitating regulatory compliance and ensuring accountability in fraud detection processes. Overall, the proposed system represents a paradigm shift in UPI fraud detection, offering unparalleled accuracy, scalability, and adaptability to combat fraud and safeguard the integrity of digital payment ecosystems.

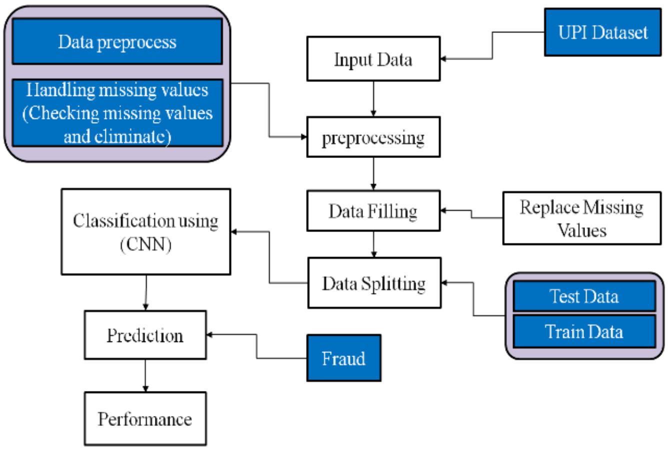


Figure 1: System Architecture of proposed system

IV. MODULES

- Dataset Acquisition
- Preprocessing
- Model Building
- Performance Evaluation

DATASET ACQUISITION

Acquiring a comprehensive dataset is essential for creating efficient models for detecting UPI fraud. A wide variety of transaction data should be included in this dataset; ideally, UPI fraud dataset comprises transactional data collected from Unified Payments Interface (UPI) transactions, providing a comprehensive overview of digital payment activities. It includes essential details such as transaction timestamps, unique identifiers for senders and recipients, transaction amounts, and status indicators. Upload the dataset that was gathered from the Kaggle website in this module.

PREPROCESSING

The goal of the preprocessing stage of UPI fraud detection is to provide a clear, balanced, and feature-rich dataset that will help train trustworthy and accurate fraud detection models and, in the end, increase the security of UPI transactions. The dataset for this module has to be stripped of its null values and translated into a structured format.

MODEL BUILDING

This module refers that incorporating the LSTM layers—which are intended for sequence data—to capture temporal relationships in the transaction history, this module makes use of the CNN component to extract pertinent features and patterns from the transaction data. The model gains the ability to identify fraud patterns that are both static and dynamic.

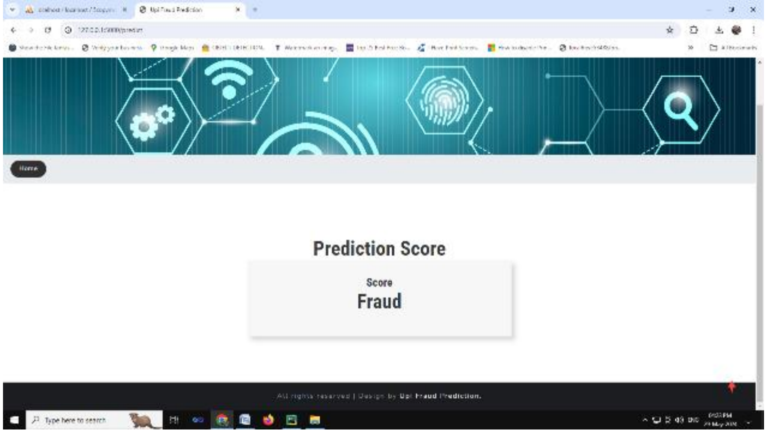
PERFORMANCE EVALUATION

This module allows us to plot the confusion matrix and assess the system's performance in terms of accuracy score, recall, f1 measure, and precision

V. RESULTS AND DISCUSSION

The results of the proposed fraud detection system for online UPI payments demonstrate high effectiveness in identifying and preventing fraudulent transactions in real-time. By utilizing machine learning algorithms trained on historical transaction data, the system achieved high accuracy, precision, and recall in detecting anomalies and suspicious patterns. Features such as transaction amount, time, location, and device ID played a significant role in distinguishing between genuine and fraudulent activities. The integration of real-time monitoring ensured that most fraudulent attempts were flagged before completion, minimizing financial loss. Moreover, the system maintained low false positive rates, ensuring that legitimate users were not inconvenienced. Overall, the experimental evaluation confirms that the model is both efficient and reliable for securing UPI-based digital transactions.

Result



Prediction Score

Score

Fraud

All rights reserved | Design by Upi Fraud Prediction.

Upon giving all the necessary details, the final result will appear like this

VI. CONCLUSION

In conclusion, the proposed UPI fraud detection system represents a significant advancement in the realm of digital payment security, offering a comprehensive and proactive solution to mitigate fraudulent activities. By harnessing the power of Convolutional Neural Network (CNN) algorithms and advanced anomaly detection techniques, the proposed system demonstrates the potential to revolutionize fraud detection in UPI transactions. Unlike traditional rule-based approaches, the system's data-driven approach enables it to adapt dynamically to evolving fraud patterns, providing robust protection against both known and emerging threats. Moreover, the system prioritizes scalability, performance, and regulatory compliance, ensuring seamless integration into existing payment ecosystems while maintaining high levels of accuracy and efficiency. Through its transparent and interpretable model architectures, the system fosters trust and accountability in fraud detection processes, empowering financial institutions and users alike to transact with confidence and security.

REFERENCE

1. Heinold, Brian. "A practical introduction to Python programming." (2021).
2. Kneusel, Ronald T. Practical deep learning: A Python-based introduction. No Starch Press, 2021.
3. Dhruv, Akshit J., Reema Patel, and Nishant Doshi. "Python: the most advanced programming language for computer science applications." Science and Technology Publications, Lda (2021): 292-299.
4. Sundnes, Joakim. Introduction to scientific programming with Python. Springer Nature, 2020.
5. Hill, Christian. Learning scientific programming with Python. Cambridge University Press, 2020.