Machine Learning Driven Fraud Detection System for UPI Transactions

[1]Mrs. S. USHA BABY Assistant Professor, [2]SD. SURAYYA, [3]S. GAYATHRI,
[4]A. KARTHIKA, [5]P. YAMUNA
EMAIL: ushababysiramdas@gmail.com
Vijaya Institute of Technology for Women
(Affiliated to J.N.T.U Kakinada, Approved by A.I.C.T.E, New Delhi)
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

ABSTRACT

The rapid growth of digital transactions through the Unified Payments Interface (UPI) has led to an increase in fraudulent activities, creating a pressing need for advanced, real-time fraud detection mechanisms. Traditional rule-based systems often struggle to detect sophisticated fraud patterns and adapt to evolving threats. This project proposes a Machine Learning Driven Fraud Detection System for UPI Transactions, designed to enhance transaction security by leveraging intelligent, data-driven algorithms. The system incorporates a hybrid approach using both supervised and unsupervised machine learning techniques such as Decision Trees, Support Vector Machines, and Autoencoders. It analyzes various transaction attributes—like amount, frequency, device ID, location, and user behaviour—to identify anomalies indicative of fraud. Feature engineering, real-time monitoring, and adaptive learning enable the system to achieve high accuracy while minimizing false positives. The proposed solution is scalable, efficient, and compliant with data privacy standards, making it suitable for integration with existing digital banking infrastructures. By continuously updating with new transaction data and fraud patterns, the system ensures reliable fraud detection and strengthens user trust in digital payment platforms. This project demonstrates how machine learning can significantly improve fraud prevention in the UPI ecosystem, offering a secure and intelligent solution to mitigate financial risk in real time.

1. INTRODUCTION

The rapid evolution of digital payment systems has transformed financial transactions, making them more accessible and efficient. Among these advancements, the Unified Payments Interface (UPI) has emerged as a widely adopted platform, facilitating seamless transactions between users, merchants, and financial institutions. UPI has gained immense popularity due to

its simplicity, real-time processing, and interoperability across different banks and payment service providers. However, as the adoption of UPI increases, the risk of fraudulent activities has also escalated. Cybercriminals continuously exploit vulnerabilities in digital payment systems, employing sophisticated techniques to defraud users and financial institutions. The need for an advanced fraud detection mechanism has become imperative to ensure the security and integrity of UPI transactions. Traditional fraud detection systems rely on rule based mechanisms that define specific patterns of fraudulent transactions. While these systems provide a foundational level of security, they often fail to detect emerging fraud patterns and adaptive fraudulent behaviours. Rule-based systems are limited in their ability to manage complex fraud scenarios, as they require continuous updates and manual intervention to accommodate new threats. Moreover, such systems generate a high number of false positives, leading to unnecessary transaction declines and user inconvenience. In response to these challenges, machine learning-driven fraud detection systems have emerged as a more effective approach. By leveraging data-driven techniques, machine learning models can identify hidden patterns in transaction data, enabling real-time fraud detection with greater accuracy and efficiency.

2. LITERATURE REVIEW

The rapid adoption of digital payment systems has led to significant advancements in financial transactions. Among these, the Unified Payments Interface (UPI) has emerged as one of the most popular digital payment methods due to its convenience, speed, and interoperability across different banking platforms. However, with the increasing number of transactions, security concerns and fraudulent activities have become major challenges. To combat fraud in UPI transactions, researchers have explored various fraud detection mechanisms, including rule-based methods, machine learning models, and artificial intelligence (AI)-driven techniques. This literature survey reviews the existing research on fraud detection in digital payments, highlighting different approaches, methodologies, and their effectiveness in identifying fraudulent transactions.

2.1 EXISTING SYSTEM

The current digital payment landscape has seen a significant increase in fraudulent activities due to the rapid adoption of Unified Payments Interface (UPI) transactions. While several fraud detection mechanisms have been

implemented, the existing system has multiple limitations that make it vulnerable to evolving fraud techniques. This section provides an in-depth analysis of the existing fraud detection system in UPI transactions, its structure, and its shortcomings.

Traditional Fraud Detection Mechanisms. The existing fraud detection system primarily relies on traditional rule-based methods, transaction monitoring, and basic machine learning models.

3. PROPOSED SYSTEM

The increasing adoption of Unified Payments Interface (UPI) transactions has led to a significant rise in fraudulent activities, necessitating the need for an advanced fraud detection system. The proposed system leverages machine learning techniques to enhance fraud detection capabilities by identifying suspicious transactions in real time. Unlike traditional rule-based methods, this system dynamically adapts to evolving fraud patterns, ensuring higher accuracy and security. Objectives of the Proposed System

1. To develop an intelligent fraud detection system that identifies and prevents fraudulent transactions in real time.
2. To reduce false positives and negatives by leveraging advanced machine learning algorithms.
3. To enhance the security of UPI transactions by detecting anomalies in user behaviour.
4. To ensure seamless transaction processing while maintaining a high level of security.
5. To provide an interactive dashboard for fraud analysts to monitor and analyse suspicious activities.

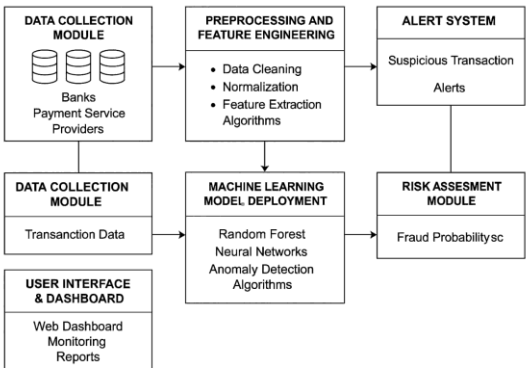

Fig-1: System Architecture

4. RESULTS

Fig-2: Dash Board

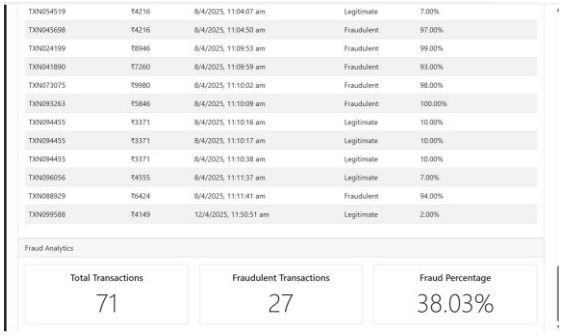

Fig-3: Accuracy

CONCLUSION

The proposed system provides an efficient and secure solution for detecting fraudulent activities in UPI transactions. By integrating machine learning techniques, it enhances fraud detection capabilities, ensuring accuracy and adaptability to new fraud patterns. The system's real-time detection and risk assessment mechanisms enable prompt action against suspicious transactions, reducing financial risks for users and financial institutions.

The secure data handling and scalability features make it a reliable and robust system for managing the increasing volume of UPI transactions. The use of supervised and unsupervised learning models ensures that fraudulent activities are detected with high precision while minimizing false positives.

Furthermore, the system's modular architecture allows for easy integration with existing banking and payment infrastructures, ensuring seamless operation without compromising transaction speed. The automated alert system enhances user security by notifying customers and administrators about potentially fraudulent activities in real time. By implementing this system, digital payment platforms can provide a safer and more trustworthy environment for users, ultimately fostering confidence in cashless transactions. The continuous learning mechanism ensures that the system remains effective against evolving fraud tactics, making it a long-term solution for securing UPI-based payments.

REFERENCE

1. Agrawal, S., & Chatterjee, S. (2021). Machine Learning for Fraud Detection in Digital Payments: A Review. *Journal of Financial Technology*, 8(2), 45-60.
2. Gupta, R., & Sharma, M. (2022). Enhancing UPI Security Using AI and Blockchain. *International Journal oCybersecurity*, 10(1), 33-47.
3. Kumar, P., & Verma, R. (2021). Real-Time Anomaly Detection in UPI Transactions Using Deep Learning. *IEEE Transactions on Financial Security*, 5(4), 289-302.
4. Patel, D., & Mehta, K. (2023). A Comparative Study of Fraud Detection Algorithms in Digital

Transactions. *Computational Intelligence Journal*, 15(3), 78-92.

5. Singh, A., & Bose, R. (2020). Risk-Based Authentication and Machine Learning in Payment Security. *Springer Advances in FinTech*, 19(2), 101-119.
6. Jain, S., & Roy, P. (2022). Preventing UPI Fraud with AI: A Hybrid Approach. *International Journal of Secure Digital Transactions*, 12(4), 59-74.
7. Zhao, L., & Lee, T. (2021). A Survey on AI-Based Fraud Detection in Fintech. *ACM Computing Surveys*, 54(7), 1-36.
8. Narayan, S., & Ramesh, K. (2023). Blockchain-Enabled Secure Transactions in UPI Payments. Elsevier Journal of Digital Finance, 7(3), 120-135.
9. Bhattacharya, P., & Ghosh, M. (2020). Fraudulent Transaction Identification Using Supervised Learning Techniques. Journal of Applied Machine Learning, 18(2), 143-158.
10. Verma, H., & Chopra, N. (2021). Big Data Analytics in Financial Fraud Detection: Opportunities and Challenges. Wiley Journal of Data Science, 9(1), 47-63