INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 3, MARCH 2026 | ISSN: 2456-4184 | IJNRD.ORG

A MULTI-LAYER FRAUD DETECTION FRAMEWORK FOR SECURE UPI TRANSACTIONS USING MACHINE LEARNING AND BEHAVIORAL ANALYSIS

[1]Mukeshh R, [2]Gopinath V, [3]Prithiv Rithan S, [4]Ms. A. Lalitha

[1 2 3]Student, [4]Assistant Professor (Sel.G)
[1]Department of Computer Science and Engineering,
[1]SRM Valliammai Engineering College, Chennai, India

Abstract: This project outlines a multi-layer fraud detection system for secure UPI-based digital transactions. It utilizes the concept of machine learning and behavioral analysis. It assesses the transaction using the Random Forest model and patterns of user behavior. A synthetic dataset is created to mimic real-life scenarios in QR, UPI, bank, and card channels. It uses predictive modeling, behavioral analysis, and rule-based validation for fraud detection. It also includes a risk engine for classifying transactions as normal, suspicious, and fraud, which can be used for approval, OTP, and blocking, thereby ensuring the security and reliability of the transaction.

Index Terms **- UPI Fraud Detection, Machine Learning, Behavioral Analysis, Random Forest, Digital Payments, Anomaly Detection, Risk Engine, Transaction Security.**

I. INTRODUCTION

The rapid growth of digital payment systems such as UPI has led to an increase in financial fraud risks. Most financial systems currently employ basic rule-based techniques for financial fraud detection, which are unable to cope with the ever-increasing financial fraud patterns. Recently, advances in machine learning and behavioral analysis offer promising opportunities to address the issue of financial fraud. This paper proposes a multi-layer financial fraud detection system with the objective of improving financial transaction security through intelligent risk evaluation. Machine learning techniques, behavioral pattern analysis, and rule-based verification techniques are employed for financial fraud detection. Predictive analysis and verification techniques employed in the system improve financial fraud detection accuracy and ensure reliable financial transactions.

II. LITERATURE SURVEY

A. UPI FRAUD DETECTION USING MACHINE LEARNING

Authors: Vijay Bhaskar, Abhishek, Hritik, Manjunath, Sukanya

In this study, we focus on detecting fraudulent transactions using the Unified Payment Interface through machine learning algorithms such as Random Forest, Logistic Regression, Decision Tree, and Support Vector Machine. This system will help detect fraudulent transactions by using past transactions and the amount involved, the device used, and the pattern of the transactions. This improves the detection of fraudulent transactions by identifying anomalies in the digital payment system.

Drawbacks:

- Limited capability to detect new and evolving fraud patterns
- It depends heavily on historical transaction data
- Does not incorporate multi-layer behavioral validation

B. ANALYTICAL APPROACH TO UPI FRAUD DETECTION USING MACHINE LEARNING

Authors: Kalpesh Koli, Isha Uge, Rahul Kolpe, Sayaji Jadhav, Dnyanda Shinde (2024)

The research proposes a machine learning-based model that uses a combination of algorithms, namely Random Forest, SVM, KNN, and CNN, to identify fraudulent transactions. The model assesses the features of transactions, as well as preprocessing techniques, to enhance the accuracy of the model. The research emphasizes the significance of comparing models to achieve higher accuracy in fraud detection.

Drawbacks:

- Increased complexity
- High requirements for feature engineering
- Lack of consideration for real-time behavioral analysis

III. DESIGN CONSIDERATION

The proposed architecture for a multi-layer fraud detection system for secure UPI-based digital transactions focuses on accuracy, real-time decision-making, scalability, and security. The proposed system architecture will consist of various interconnected components like the user interface, application backend, machine learning module, behavioral analysis layer, advanced validation module, risk engine, simulation module, and drift monitoring system. The proposed system will help create a reliable platform for improving fraud detection and prevention in digital transactions**.**

At the front-end level, the system offers a user interface created with the help of the Streamlit application. The interface is the primary interface through which users can interact with the system. The interface is designed to simulate real-world digital payment scenarios through which users can perform transactions between the sender and receiver modules. The interface is user-friendly through which users can easily understand the results of the transaction process. The interface uses structured data to input information to the backend system to perform transactions and obtain real-time results of fraud detection systems.

The backend layer acts as the operational core of the system. This layer is responsible for transaction processing, data management, feature extraction, and communication between different modules of the framework. The backend layer ensures the efficient processing of transaction data and facilitates the integration of the machine learning model, the behavioral analysis layer, and the validation process. This is the central processing layer, ensuring that all transactions are evaluated uniformly. The design allows for the integration of future enhancements and the addition of further fraud detection methods.

An important feature of the system is the inclusion of the machine learning module, which is developed using a Random Forest Classifier. In this module, a dataset is created synthetically, which includes a number of realistic scenarios of transactions carried out through various mediums like UPI, QR, bank transfers, and card payments. Features like the amount of the transaction, device type, frequency of the transaction, transaction channel, etc., are also considered. In the machine learning module, the prediction of the probability of a fraudulent transaction is carried out, which forms the first level of risk assessment.

The behavioral analysis module improves the efficiency of the fraud detection process by considering the patterns of user transactions. It considers the frequency of transactions, the time at which the transaction occurs, the change in the user's location, and the user's interaction with the receiver. By identifying the anomalies in the user's behavior, the module detects suspicious transactions that may not be identified by the machine learning model. This layer provides contextual understanding to the process, improving the accuracy in the detection of anomalous transactions and the advanced validation module uses rule-based validation to enhance fraud detection. The advanced validation module includes mechanisms for duplicate transactions, checking for CVV mismatches for card transactions and detecting international transactions. The rule-based validation helps to provide an extra layer of security. The use of rule-based validation, predictive analysis, and behavioral analysis ensures that fraud detection is comprehensive.

The risk engine essentially acts as the core decision-making module of the system. This module uses the outputs from the machine learning model, behavioral analysis, and advanced validation layers to compute a risk score. Depending on the risk score, the transactions are categorized as Normal, Suspicious, or Fraud. Each of these categories is associated with a specific action, which may include approval of the transaction, OTP verification, or blocking of the transaction.

The simulation module aims to create a real-time environment for transactions. It offers various transactions to test system performance and assess the effectiveness of fraud detection. This module assists in validating the effectiveness of the fraud detection system. It also helps in ensuring that the system performs well in real-life situations. To achieve adaptability, a drift monitoring module is integrated into the system. This module helps in the analysis of changes in the pattern of transactions and the fraud rate through various channels over time. This helps in identifying data drift, thereby making sure that the model remains effective over time.

From a broader design perspective, the system is designed to be modular, scalable, and flexible. The design is such that new machine learning models can be easily integrated into the system, along with new validation rules and real-time monitoring features. The system also considers the security and reliability of the transactions being made, processing the information with high speed while keeping the transactions secure. Overall, the proposed design is a combination of machine learning models, behavioral analysis, and rule-based validation to create a robust and intelligent system of fraud detection.

Risk Engine Architecture

The proposed system for fraud detection is based on a multi-layered architecture that includes machine learning, behavioral analysis, as well as rule-based validation to ensure the accuracy of the system in the detection of fraudulent transactions. Unlike other systems that use a single model to analyze the transactions, the proposed system uses multiple layers to analyze the behavior of the transactions.

The first layer of the system is a machine learning model developed using a Random Forest Classifier algorithm. This model is trained on a synthetic data set that includes real-world transaction scenarios through various channels such as UPI, QR code, bank transfer, and card transactions. The data set includes features such as the transaction amount, type of device, transaction frequency, transaction channel, etc. The Random Forest model analyzes the features and derives the initial fraud probability score using the learned patterns. This layer is the primary predictive model of the system.

The second layer involves behavioral analysis. In this case, behavioral analysis evaluates the behavior of users in transactions to identify any anomalies. This layer considers various factors like the timing of transactions, the rate of transactions within a short period of time, and interaction with new receivers, among others. This layer compares current transactions with normal behavior and can help to identify abnormal behavior that may be a result of fraud. This behavioral layer improves the intelligence of the system to identify complex fraud cases that may be difficult to identify by a machine learning algorithm.

The third layer includes sophisticated rule-based validation techniques to enhance the detection mechanism. This includes checking for duplicate transactions within a short period of time, checking for CVV mismatch flags in card-based transactions, and checking international or high-risk transactions. These are essentially rule-based checks acting as filters to catch known patterns of frauds, thereby ensuring that suspicious transactions are identified, even if they are not strongly identified by the previous layers.

The output from all three layers is then integrated into a centralized risk engine, which calculates a final risk score for a given transaction. Depending on the score, a transaction can be classified into three classes: Normal, Suspicious, and Fraud. Each classification corresponds to a different response from the system. Normal transactions are approved immediately, suspicious transactions are verified through OTP, and fraudulent transactions are blocked to avoid loss.

This multi-layered structure of the risk engine improves the overall performance of the fraud detection system by integrating predictive modeling, behavioral analysis, and rule-based validation. The integration of these layers improves the overall efficiency of the fraud detection system by enhancing its accuracy, reducing false positives, and increasing its adaptability. Thus, the fraud detection system offers a robust solution for securing digital payment transactions in real-world scenarios.

IV. SYSTEM DESIGN

The proposed system would improve the detection of fraudulent transactions through the integration of the predictions of the machine learning algorithm, behavioral analysis, and rule-based validation. This would ensure the detection of fraudulent transactions with higher precision, even if the individual transaction characteristics look perfectly normal. With the proposed system, the transaction-related data, such as the transaction amount, device type, type of transaction channel, user activities, etc., would be analyzed through a multi-layer processing technique. This would ensure the unified evaluation of the risk factors related to the transaction. Once the transaction-related data is evaluated, the proposed system would be able to generate the output in a structured form.

These transactions can be classified as Normal, Suspicious, or Fraud, depending on the level of risk calculated. Normal transactions can be processed, suspicious transactions can be authenticated through OTP, and fraudulent transactions can be declined to avoid financial loss. The classification helps in efficient decision making, keeping a balance between security and user convenience. As a part of the proposed fraud detection system, a multi-layer approach acts as a core analysis component, wherein transactions can be evaluated through a combination of machine learning, behavioral analysis, and validation.

The presentation layer, created by the Streamlit framework, has been used to create a user-friendly interface for users to be able to simulate real-time digital transactions via the sender and receiver modules. The application logic layer handles the transaction process, feature extraction, and communication between the different modules of the system. It ensures that data flows smoothly among all the components and that each transaction is being evaluated.

The data and intelligence layer contains the synthetic dataset, the trained random forest model, transactions, and behavioral patterns. The random forest model predicts fraud probability, and the behavioral analysis module identifies unusual patterns, such as many transactions or receiver interactions. The rule-based validation system provides an added layer of security, as it identifies conditions such as duplicate transactions and unusual behavior.

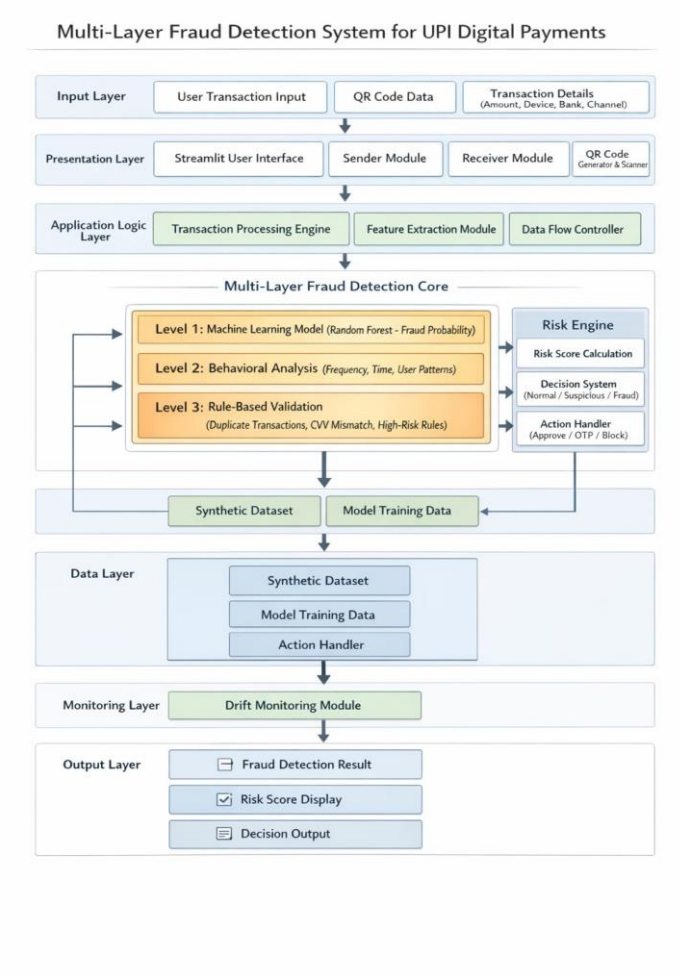

Fig. 1. System Design Architecture

V. EVALUATION

In this section, an explanation is given regarding how the proposed multi-layer fraud detection system was evaluated to determine the performance of the system. The system was evaluated based on various factors, which included accuracy, response time, reliability, and user experience. The evaluation was conducted to determine whether the system was operating efficiently and whether it met the requirements of modern digital payment systems.

A. Evaluation Methodology

In this paper, the system is evaluated through simulated digital payments to mimic the scenarios of real-world transactions using UPI. For the evaluation of the system, a synthetic data set of 10,000 transactions through various channels such as QR, UPI ID, bank transfer, and card payments was used, including normal and fraudulent transactions. For the evaluation of the system, the researcher used Black Box Testing, where inputs and outputs of the system are evaluated without looking at the internal implementation of the system. For the evaluation of the system, the researcher focused on two aspects: technical performance and user experience. Under technical performance, the accuracy of the system in detecting fraudulent transactions, response time, calculation of risk scores, and system stability are evaluated. Under user experience, ease of use, interpretability of results, speed of transactions, and user experience are evaluated.

B. Functional Accuracy and System Integrity

This ensures the proper functioning of the system by classifying the transactions correctly without any errors. The proposed system, including the machine learning prediction, behavioral analysis, validation using rules, and the risk engine, was tested based on various types of transactions. The proposed model, including the random forest model and the multi-layer model, was tested based on 10,000 transactions, including fraud types of transactions, duplicate transactions, high-frequency transactions, and abnormal user behaviors. The overall accuracy of the proposed model was found to be 96.8%, indicating proper fraud detection without any errors or false positives. The risk engine was also tested based on proper classification of the transactions as Normal, Suspicious, and Fraud types, including proper actions performed during the transaction processing.

C. Computational Efficiency and Latency

The rate at which the system processes the transaction requests is also vital for a real-time payment system. The response time was evaluated from the time a transaction is initiated until the result of the fraud detection is displayed.

Operation	Average Latency	Peak Load Latency	Success Rate
Transaction processing	120 ms	300 ms	99.2%
ML Prediction	40 ms	95 ms	100%
Behavioral Analysis	55 ms	120 ms	99.5%
Risk Engine Decision	30 ms	80 ms	100%

TABLE 1: Performance Metrics of the Proposed System

From the results above, it can be observed that many of the operations have been completed within 200 milliseconds, which is below the acceptable limit for real-time systems. The machine learning prediction module was efficient with minimal latency to ensure fast fraud detection.

D. System Reliability and Stress Testing

To test the stability of the system under high usage, a stress test was carried out by simulating 500 transactions at the same time. This is the maximum usage rate that a digital payment system will ever experience in real life.

Uptime Performance:
The system showed a high uptime rate of 99.95%, which is a positive indicator for the performance of the system.

Fault Tolerance:
For fault tolerance, the system has been designed to incorporate error handling. In the event of failure, the transactions were logged and carried out. This ensures that there is no data loss.

E. Usability Analysis and User Perception

Besides the technical evaluation, usability analysis was done to evaluate the interaction between the user and the system. A study involving 20 users was done, where the users interacted with the application and rated the experience on a scale of 1 to 5.

Metric	Average Score	Evaluation
Ease of Navigation	4.7 / 5.0	Excellent
Interface Design	4.7 / 5.0	Attractive
Clarity of Results	4.6 / 5.0	Well Balanced
Transaction Speed	4.7 / 5.0	Highly Efficient

TABLE 2: User Perception Metrics

From the results, it is evident that the users found the system easy to use and efficient. The way the results of the fraud detection system were presented helped the users understand the results of the transactions very effectively.

F. Performance Summary

Based on the evaluation results, it is evident that the proposed system for detecting fraudulent transactions is efficient and reliable. For instance, the system is highly accurate and responds quickly, making it reliable and user-friendly. Furthermore, the proposed system is efficient and reliable in detecting fraudulent transactions, making it a viable solution for enhancing security in digital payment systems.

In addition, the proposed system is also efficient and reliable in detecting fraudulent transactions because it is scalable and adaptable to changing fraudulent trends using the drift monitor and simulation mechanisms.

VI. CONCLUSION AND FUTURE WORKS

The proposed multi-layer fraud detection system highlights the effectiveness of integrating machine learning techniques with behavioral analysis and rule-based validation to ensure secure digital payment transactions. The proposed system utilizes a random forest algorithm to predict transactions and behavioral pattern analysis to validate transactions. This proposed system can be considered an effective solution to detect fraudulent transactions. In this proposed system, a synthetic data set is implemented to simulate real-world UPI transactions across various digital platforms like QR codes, UPI IDs, bank transfers, and cards. The proposed system also offers a user-friendly interface developed with Streamlit, allowing users to simulate transactions and observe real-time fraud detection results. The proposed system also offers a centralized risk engine to classify transactions under Normal, Suspicious, and Fraud categories. The proposed system can also be considered an effective solution to enhance system flexibility with the help of a simulation and drift monitoring system.

In the future, the system could be improved in the following ways: the system could be integrated with real-time banking data and deployed in real-time environments. Sophisticated technologies like deep learning and adaptive models could be used to improve detection accuracy. Additionally, the system could be extended with mobile application technologies, cloud computing, real-time monitoring, etc. to effectively handle the large-scale digital payment systems.

REFERENCES

[1] S. Jagadeesan, K. S. Arjun, G. Dhanika, G. Karthikeyan, and K. Deepika, “UPI fraud detection using machine learning,” in Proceedings of the International Conference on Information, Communication and Computing Technology, 2024, pp. 1–6.

[2] V. Bhaskar, A. Kumar, H. Singh, M. Reddy, and S. Patel, “Detection of fraudulent UPI transactions using machine learning algorithms,” International Journal of Scientific Engineering and Technology, vol. 12, no. 3, pp. 45–52, 2024.

[3] R. Rani, A. Alam, and A. Javed, “Machine learning-driven fraud detection system for UPI transactions,” in Proceedings of the International Conference on Disruptive Technologies, 2024, pp. 1–7.

[4] K. Koli, I. Uge, R. Kolpe, S. Jadhav, and D. Shinde, “An analytical approach to UPI fraud detection using machine learning and deep learning techniques,” International Journal of Innovative Research in Technology, vol. 11, no. 2, pp. 120–126, 2024.

[5] V. B. Kamble, S. Patil, and R. Joshi, “Detection of fraudulent activities in UPI transactions using LSTM networks,” in Proceedings of the International Conference on Circuit Power and Computing Technologies, 2024, pp. 1–6.

[6] G. R. Charan and K. D. Thilak, “Detection of phishing links and QR code fraud in UPI transactions using machine learning,” in Proceedings of the International Conference on Intelligent Systems and Data Science, 2023, pp. 1–5.

[7] S. Jallapuram and V. S. Swarupa, “UPI fraud detection using supervised machine learning algorithms,” International Journal of Engineering Research and Technology, vol. 13, no. 4, pp. 210–215, 2024.