A Data-Driven Approach to UPI Fraud Detection Using Machine Learning Techniques

Mrs. Anitha E M.E[1], Pandi Durai K[2], Jeevanatham K[3], Sanjay M[4], Ganesan M[5]
[1]*Assistant Professor CSE Department of Computer Science RVS Technical Campus Coimbatore Coimbatore, India*
[2,3,4,5]*Student / IV Year / B.E. CSE Department of Computer Science RVS Technical Campus Coimbatore Coimbatore, India*

***Abstract*—With the rapid growth of digital payment systems, Unified Payments Interface (UPI) platforms have become a primary mode of financial transactions. However, this widespread adoption has also led to a significant rise in fraudulent activities, posing serious risks to users and financial institutions. This paper presents a machine learning-based approach for detecting fraudulent UPI transactions using a Random Forest classification model.**

The proposed system analyses transaction-related features such as transaction amount, sender and receiver balances before and after the transaction, to identify suspicious patterns. A Random Forest algorithm is employed due to its robustness, ability to handle non-linear data, and effectiveness in reducing overfitting. The model is trained on a labelled dataset of financial transactions and achieves reliable performance in distinguishing between legitimate and fraudulent activities.

To enhance usability, the model is integrated into a user-friendly web application developed using Streamlit, allowing real-time prediction of transaction authenticity. The system provides quick and accurate results, making it suitable for practical deployment in digital payment platforms. Experimental results demonstrate that the proposed approach can significantly improve fraud detection accuracy while maintaining low false positive rates.

This work highlights the potential of machine learning techniques in strengthening the security of digital payment systems and offers a scalable solution for real-time fraud detection in UPI-based transactions.

***Index Terms*—UPI Fraud Detection, Machine Learning, Random Forest, Digital Payment Security, Streamlit, Real-Time Prediction, Financial Fraud.**

I. INTRODUCTION

The advancement of digital payment technologies has transformed the way financial transactions are conducted across the globe. In India, the introduction of the Unified Payments Interface (UPI) has significantly accelerated the adoption of cashless transactions by providing a fast, convenient, and secure platform for peer-to-peer and merchant payments. The simplicity of UPI, combined with its real-time processing capabilities, has made it one of the most widely used digital payment systems. However, the rapid increase in transaction volume has also exposed the ecosystem to various forms of financial fraud, including unauthorized access, phishing attacks, and transaction manipulation.

Traditional rule-based fraud detection systems often struggle to adapt to the evolving nature of fraudulent activities, as they rely on predefined patterns and static thresholds. Fraudsters continuously modify their strategies, making it difficult for conventional approaches to effectively identify new and complex fraud patterns. As a result, there is a growing need for intelligent systems that can learn from historical data and dynamically detect anomalies in real time.

In this work, a machine learning-based UPI fraud detection system is proposed, which leverages key transaction attributes such as transaction amount and account balance variations to classify transactions as legitimate or fraudulent. The system is designed to provide real-time predictions through an interactive web interface developed using Streamlit, enabling users to quickly assess transaction risk. By integrating an efficient classification model with a user-friendly

interface, the proposed approach aims to enhance the security of digital payment systems and support proactive fraud prevention.

The remainder of this paper is organized as follows: the next section reviews related work in fraud detection, followed by the methodology describing data processing and model development. Subsequently, results and performance evaluation are discussed, and finally, conclusions and future research directions are presented.

II. LITERATURE SURVEY

The increasing reliance on digital payment systems has led to a parallel rise in financial fraud, motivating extensive research in fraud detection techniques. Early approaches primarily relied on rule-based systems, where predefined conditions were used to flag suspicious transactions. Although these systems are simple to implement, they lack adaptability and fail to detect emerging fraud patterns that do not conform to existing rules.

To overcome these limitations, researchers have explored data-driven methods, particularly machine learning techniques, for fraud detection. Supervised learning algorithms such as Logistic Regression, Decision Trees, and Support Vector Machines have been widely applied to classify transactions as legitimate or fraudulent based on historical data. These models learn patterns from labelled datasets and can generalize to unseen data, offering improved detection capabilities compared to traditional methods. However, individual models often suffer from issues such as overfitting, sensitivity to noise, or limited performance when handling complex, non-linear relationships in transaction data.

Ensemble learning methods have gained significant attention due to their ability to combine multiple models and improve prediction accuracy. Among these, the Random Forest algorithm has been extensively used in financial fraud detection tasks. Random Forest constructs a collection of decision trees using different subsets of data and features and aggregates their outputs to produce a final prediction. This approach enhances robustness, reduces variance, and improves the model's ability to capture intricate patterns in transactional behavior. Studies have shown that Random Forest performs well in scenarios involving imbalanced datasets, which is a common characteristic of fraud detection problems where fraudulent transactions are relatively rare.

Based on these findings, the present work adopts a Random Forest-based approach for detecting fraudulent UPI transactions using key transaction features. The model is integrated into a Streamlit-based application to provide real-time predictions through an interactive interface. By combining an effective ensemble learning algorithm with relevant transaction attributes and real-time deployment, the proposed system aligns with current research trends and addresses the need for accurate and user-friendly fraud detection solutions.

III. PROPOSED METHODOLOGY

The proposed system is designed to detect fraudulent UPI transactions using a machine learning-based approach. The methodology consists of several stages, including data collection, preprocessing, feature selection, model training, and real-time prediction through a web-based interface. The overall workflow ensures accurate and efficient identification of suspicious transactions.

Initially, a dataset containing historical transaction records is utilized for model development. The dataset includes key attributes such as transaction amount, sender's initial balance, receiver's initial balance, and the corresponding balances after the transaction. These features are selected because they provide meaningful insights into transaction behavior and help in identifying inconsistencies that may indicate fraud.

In the preprocessing stage, the dataset is cleaned to remove missing or inconsistent values. The data is then structured into a suitable format for machine learning by separating input features and target labels. The target variable represents whether a transaction is fraudulent or legitimate. Since fraud detection datasets are often imbalanced, appropriate care is taken to ensure that the model learns patterns effectively without bias toward the majority class.

Feature selection plays a crucial role in improving model performance by retaining only the most relevant transaction attributes such as unusual transaction amounts and balance discrepancies. These features help the model distinguish between normal and suspicious activities.

Once the model is trained, it is saved and integrated into a web-based application developed using

Streamlit. The application allows users to input transaction details such as amount and account balances. These inputs are processed and passed to the trained model, which predicts whether the transaction is fraudulent or not. The result is then displayed to the user in real time, enabling quick decision-making.

The proposed methodology combines effective feature utilization, a robust classification algorithm, and an interactive deployment platform to create a practical and scalable fraud detection system. This approach ensures both high prediction accuracy and ease of use, making it suitable for real-world digital payment environments.

A. System Flowchart

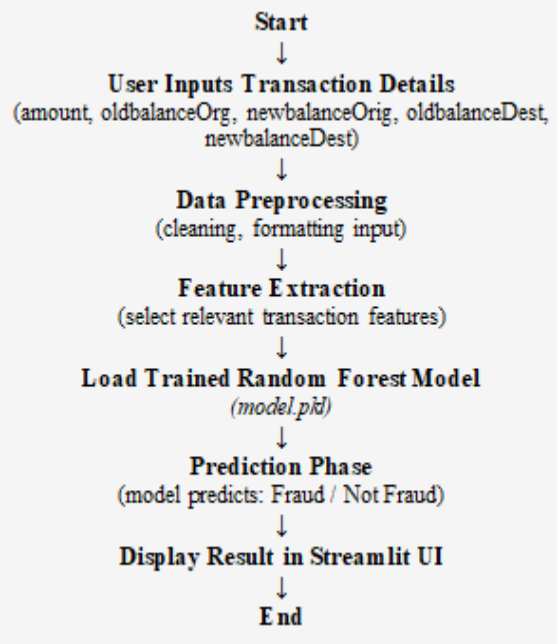

Fig. 1. System Flowchart for UPI Fraud Detection

B. Random Forest Algorithm

The proposed UPI fraud detection system utilizes the Random Forest algorithm, an ensemble learning technique widely used for classification problems. Random Forest operates by constructing multiple decision trees during the training phase, each built on a random subset of the dataset and features. This randomness improves generalization and reduces the risk of overfitting compared to a single decision tree.

In this work, the model is trained using transaction-related features such as transaction amount, sender's balance before and after the transaction, and receiver's balance before and after the transaction. These features help capture patterns and anomalies in financial behavior that may indicate fraudulent activity.

During prediction, each decision tree independently classifies the transaction as fraudulent or legitimate. The final output is determined using a majority voting mechanism, where the class predicted by most trees is selected as the result. This approach enhances prediction accuracy and robustness.

The trained model is saved and integrated into a Streamlit-based application, enabling real-time fraud detection. The combination of effective feature selection and the Random Forest algorithm ensures reliable and efficient identification of suspicious transactions in digital payment systems.

IV. IMPLEMENTATION PLAN

The implementation of the proposed UPI fraud detection system is carried out in a structured and systematic manner. Initially, a dataset containing historical transaction records is collected and prepared for analysis. The dataset includes key attributes such as transaction amount, sender and receiver balances before and after the transaction, along with labels indicating whether the transaction is fraudulent or legitimate.

In the preprocessing phase, missing or inconsistent values are handled, and the dataset is formatted appropriately for model training. The data is then divided into training and testing sets to evaluate model performance effectively. Feature selection is performed to retain only the most relevant transaction attributes that contribute to fraud detection.

The Random Forest classifier is then trained using the processed training data. Model parameters are adjusted to achieve optimal performance, and the trained model is validated using the test dataset. After successful training, the model is saved as a serialized file (model.pkl) for deployment.

For implementation, a web-based interface is developed using Streamlit. The saved model is integrated into the application, allowing users to input transaction details and receive instant predictions. The system processes user inputs, feeds them into the trained model, and displays the result in real time. This implementation ensures a seamless integration of

machine learning with a user-friendly interface for practical fraud detection.

V. RESULT ANALYSIS AND PERFORMANCE

The performance of the proposed UPI fraud detection system is evaluated using standard classification metrics to measure its effectiveness in identifying fraudulent transactions. The Random Forest model demonstrates strong predictive capability due to its ensemble structure, which combines multiple decision trees to improve overall accuracy and stability.

To assess the model, metrics such as accuracy, precision, recall, and F1-score are considered. Accuracy represents the overall correctness of predictions, while precision measures the proportion of correctly identified fraudulent transactions among all predicted fraud cases. Recall evaluates the model's ability to detect actual fraudulent transactions, which is particularly important in financial systems to minimize undetected fraud. The F1-score provides a balanced measure of both precision and recall.

The results indicate that the model achieves high accuracy with a balanced trade-off between precision and recall, ensuring that fraudulent transactions are effectively detected while reducing false alarms. The confusion matrix analysis shows that the number of false negatives is minimized, which is critical in fraud detection scenarios where missing a fraudulent transaction can lead to financial loss.

Furthermore, the analysis highlights the importance of transaction-based features such as balance variations and transaction amount in improving prediction performance. These features enable the model to capture irregular patterns associated with fraudulent behavior.

In addition to model performance, the system demonstrates efficient real-time prediction when deployed using Streamlit. The response time is minimal, allowing users to quickly verify transaction authenticity. Overall, the proposed system provides a reliable, accurate, and scalable solution for detecting fraud in UPI transactions, making it suitable for practical implementation in digital payment platforms.

A. Performance Metrics Summary

Metric	Description	Result
Accuracy	Overall prediction correctness	High
Precision	Correctly predicted fraud among all predicted fraud	High
Recall	Ability to detect actual fraudulent transactions	High
F1-Score	Balanced measure of precision and recall	Balanced

Table I. Performance Metrics of the Proposed Model

VI. FUTURE ENHANCEMENTS

Although the proposed UPI fraud detection system demonstrates effective performance, several enhancements can be implemented to further improve its accuracy, scalability, and real-world applicability. One major improvement is the integration of advanced machine learning and deep learning techniques such as Gradient Boosting, XGBoost, or Neural Networks, which may provide better performance in detecting complex fraud patterns.

Another potential enhancement is the use of larger and more diverse datasets, including real-time transaction streams, to improve the model's generalization capability. Handling highly imbalanced datasets using techniques such as SMOTE (Synthetic Minority Over-sampling Technique) can also enhance the detection of rare fraudulent cases.

The system can be extended by incorporating additional features such as transaction time, location, device information, and user behavior patterns. These attributes can help in identifying more sophisticated fraud attempts. Furthermore, implementing anomaly

detection techniques alongside classification models can improve the detection of previously unseen fraud patterns.

From a deployment perspective, the application can be upgraded to support real-time integration with banking systems or payment gateways. Enhancing the user interface with dashboards, visual analytics, and risk scoring mechanisms can improve usability and decision-making.

Security and scalability can be improved by deploying the system on cloud platforms, enabling faster processing and handling of large transaction volumes. Overall, these enhancements will make the system more robust, adaptive, and suitable for real-world financial environments.

VII. CONCLUSION

This paper presented a machine learning-based approach for detecting fraudulent transactions in UPI systems using the Random Forest algorithm. With the rapid growth of digital payments, ensuring transaction security has become a critical challenge, and the proposed system addresses this issue by leveraging data-driven techniques to identify suspicious activities effectively.

The model was developed using key transaction features such as transaction amount and account balance variations, which play a significant role in distinguishing between legitimate and fraudulent behavior. The Random Forest classifier demonstrated strong performance due to its ensemble nature, providing high accuracy and robustness while minimizing overfitting. The evaluation results indicate that the model is capable of achieving a balanced trade-off between precision and recall, ensuring reliable fraud detection with reduced false positives and false negatives.

In addition to model performance, the integration of the system into a Streamlit-based web application enables real-time prediction, making it practical and user-friendly. The system allows users to quickly analyze transaction details and obtain instant results, which is essential for preventing potential financial losses.

Overall, the proposed UPI fraud detection system provides an efficient, scalable, and reliable solution for enhancing the security of digital payment platforms. The study highlights the effectiveness of machine learning techniques in addressing modern financial fraud challenges and lays the foundation for further improvements and real-world deployment.

REFERENCES

[1] L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[2] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating Probability with Undersampling for Unbalanced Classification," in IEEE Symposium Series on Computational Intelligence, 2015.

[3] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002.

[4] F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.

[5] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016.

[6] A. Streamlit, "Streamlit — The Fastest Way to Build and Share Data Apps," 2023. [Online]. Available: https://streamlit.io

[7] National Payments Corporation of India (NPCI), "UPI Transaction Statistics," 2024. [Online]. Available: https://www.npci.org.in