

UPI Online Transaction Fraud Detection

Ms. Anusha P M² Nikitha K V¹

²Assistant Professor, Department of MCA, BIET, Davanagere

¹Student, 4th Semester MCA, Department of MCA, BIET, Davanagere

ABSTRACT

The proliferation of Unified Payments Interface (UPI) transactions has transformed the landscape of digital payments in India, offering unparalleled convenience and efficiency for instant money transfers. However, this surge in adoption has been accompanied by a significant rise in fraudulent activities, posing critical security challenges to users and financial institutions. This paper presents an intelligent fraud detection framework leveraging machine learning methods for detecting and topping fraudulent UPI transactions in real time. By analyzing key transaction features such as transaction type, amount, and account balances, a Decision Tree Classifier is trained to distinguish between legitimate and suspicious activities. The proposed system is implemented as a web-based platform, providing distinct functionalities for both users and administrators, including secure user registration, real-time fraud assessment, FAQ management, and feedback mechanisms. Results from experiments show how well the machine learning model works to identify fraudulent transactions, improving the security and dependability of UPI-based financial systems. This approach offers a scalable and automated solution to safeguard digital payment ecosystems against evolving fraud threats, fostering greater trust and adoption among users.

Keywords: *Unified Payments Interface (UPI), Fraud Detection, Machine Learning, Decision Tree Classifier, Digital Payments, Real-time Detection, Financial Fraud.*

I.INTRODUCTION

The rapid digitization of financial services has significantly transformed the way individuals and businesses conduct monetary transactions, with the Unified Payments Interface (UPI) emerging as one of the most popular and widely adopted payment platforms in India. UPI enables instant, seamless, and interoperable fund transfers across multiple banks through mobile devices, revolutionizing the digital payment ecosystem by offering convenience, speed, and accessibility. Since its

inception, UPI has witnessed exponential growth, processing billions of transactions monthly and becoming a critical component of India's push towards a cashless economy. However, this surge in usage has also garnered more interest from fraudsters who exploit vulnerabilities in the system to carry out unauthorized and malicious transactions. The resulting fraudulent activities pose significant risks, including financial losses for users, erosion of trust in digital payment platforms, and potential regulatory challenges for financial institutions.

Traditional fraud detection mechanisms, which often rely on static rule-based systems, are increasingly inadequate in addressing the sophisticated and evolving nature of fraudulent schemes targeting UPI transactions. These conventional methods typically depend on predefined thresholds and heuristics that may fail to capture

complex patterns or adapt quickly to new fraud tactics. Consequently, there is an urgent need for more intelligent, adaptive, and automated approaches capable of analyzing real-time analysis of massive amounts of transaction data to identify irregularities and stop fraud effectively. Machine learning (ML) offers a promising solution in this regard, as it enables systems to learn from historical data, identify subtle patterns indicative of fraud, and continuously improve detection accuracy through retraining. By leveraging features such as transaction type, amount, frequency, account balances, and user behavior, ML models are more accurate than conventional techniques at differentiating between transactions that are suspicious and those that are legitimate.

This paper focuses on the development of a machine learning-based fraud detection system specifically tailored for UPI transactions. The core of the proposed solution is a Decision Tree Classifier trained on transaction data to predict the likelihood of fraud. The model utilizes a set of carefully selected features that capture the transactional and contextual characteristics relevant to fraud detection. Beyond the predictive model, the system is designed as a web-based

platform that caters to both end-users and administrators. Users can securely register and log in to the platform, input transaction details, and receive real-time assessments regarding the legitimacy of their transactions. The platform also includes a comprehensive FAQ section to assist users and a feedback mechanism that allows users to communicate issues or suggestions to administrators. On the administrative side, the platform provides features for user account management, updating FAQs, and monitoring user feedback, thereby ensuring smooth operation and continuous improvement.

The significance of this research lies in addressing the critical challenge of securing digital payment systems against fraud while maintaining user convenience and trust. By integrating machine learning techniques with a user-friendly web interface, the proposed system offers a scalable and practical solution that enhances the security posture of UPI transactions. The automated nature of the fraud detection process enables real-time monitoring and prompt intervention, which are essential for minimizing financial losses and safeguarding user confidence.

II. RELATED WORK

Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions, Authors: Rupa Rani, Adnan Alam, Abdul Javed. This paper presents robust fraud Detection system for UPI(Unified Payments Interface) transactions using the XGBoost machine learning algorithm. By leveraging transaction features like amount, frequency, and location, the model is trained on a labeled dataset to identify fraudulent patterns with

high accuracy (98.2%). The system integrates real-time monitoring and alert mechanisms to enhance financial security, making it a significant step toward combating digital payment fraud. The study highlights the effectiveness of machine learning in strengthening the safety of rapidly growing digital financial platforms.[1]

UPI Based Deep Learning for the Identification of Financial Fraud Approach, Authors: Vaishali Gupta, Sahil Sharma, Suhani Nimkar, Suhani Pathak.

This paper presents a novel approach to detecting financial fraud in UPI transactions using a Recurrent Neural Network (RNN), moving beyond traditional machine learning techniques. By applying RNN on UPI transaction data, The technology successfully differentiates between genuine and fraudulent activities. The model's performance, evaluated through a confusion matrix, demonstrates a True Positive Rate (TPR) of 87.5% and a False Positive Rate (FPR) of 13.4%. The study emphasizes the growing need for intelligent fraud detection systems in the evolving digital payment landscape.[2]

Machine Learning-Based Recognition of Fraud in the Unifying Payments Interface - LSTM Networks, Authors: M. Naga Raju, Yarramreddy Chandrasena Reddy, Polavarapu Nagendra Babu, Venkata Sai Pavan Ravipati, Velpula Chaitanya.

This paper presents an advanced fraud detection model for UPI transactions using Long Short- One kind of recurrent neural network is called a Term Memory (LSTM) network. optimized for sequential data analysis. By leveraging LSTM's ability to detect intricate temporal patterns, the model effectively identifies anomalies in UPI

transaction sequences that may indicate fraudulent behavior. Evaluated on real-world data, the system demonstrates high accuracy in detecting fraud with minimal errors, offering a promising direction for enhancing digital payment security through deep learning.[3]

LLM-Powered UPI Transaction Monitoring and Fraud Detection, Authors: Anupriya K., Avinash K., Hariharan S., Bhavesh R., Rengith Kumaran R.

This paper introduces a novel approach Detecting UPI fraud using Large model of languages (LLMs), highlighting their ability to analyze user behavior, transaction data, and even social media interactions in real time. Unlike traditional machine learning and rule-based systems, LLMs bring contextual understanding and adaptability, enabling the detection of emerging fraud patterns and deceptive narratives. The study demonstrates how LLMs can significantly enhance transaction monitoring systems by addressing the limitations of static, inflexible fraud detection techniques.[4]

UPI Based Mobile Banking Applications – Security Analysis and Enhancements, Authors: K. Krithiga Lakshmi, Himanshu Gupta, Jayanthi Ranjan.

This paper examines the growing use of UPI-based mobile banking applications in India's digital payment landscape, emphasizing their simplicity, certification by NPCI, and relative security. It provides an in-depth analysis of the architecture, features, and transaction processes of UPI apps, while identifying security vulnerabilities. The authors propose enhanced authentication and authorization mechanisms to

further safeguard these apps against cyber threats and fraudulent activities. The study underscores the importance of continuous technological evolution to ensure secure mobile banking experiences.[5]

A Robust UPI Fraud Identification Scheme over Digital Money Transactions using Learning Powered Classification Principles, Authors: Ragavee. U, M. Prithive Raj, Janav. N. Mithra, Sudharshan Balaji S, Ajay Narayanan L, Jacob Mahimai Dass Y.

This paper introduces a robust fraud detection system tailored for Unified Payments Interface (UPI) transactions, leveraging a modified Deep Belief Network (M-DBN) model. The system incorporates a two-phase verification mechanism—cloud-based third-party validation of sender information and real-time scam scoring using hierarchical learning through Restricted Boltzmann Machines. The model dynamically adjusts fraud thresholds based on transaction history and user credibility, achieving an impressive 98.4% accuracy. This advanced method shows strong potential in enhancing security and trust in digital financial systems by effectively identifying QR and UPI-ID based scams.[6]

UPI Fraud Detection Using Machine Learning, Authors: Shabreshwari R M, Shafiya Mehrooz, Sidra Fatima, Tanmai R B, Prof. Ganesh Manasali. This paper presents a machine learning-based approach to detect UPI fraud by analyzing transaction patterns and anomalies. Leveraging a heterogeneous dataset of genuine and fraudulent transactions, the authors applied feature engineering and trained a classification model

using key indicators like transaction amount, timestamp, user location, and device information. The model was integrated into the UPI system for real-time fraud monitoring, with alert mechanisms designed to trigger instant responses. This proactive approach aims to enhance the security and reliability of UPI-based digital payment platforms.[7]

UPI Fraud Detection using Machine Learning, Authors: Kavya K R, Usha Sree R.

This paper explores the application of Several machine learning methods, such as logistic regression, decision trees, random forests, and neural networks—for detecting fraud in UPI transactions. As UPI adoption grows, so does the threat of digital fraud, challenging traditional detection systems. The authors collected a large dataset of transaction data, performed preprocessing, and trained multiple models. Their comparative analysis shows that deep learning and ensemble models yield higher fraud detection accuracy, offering a scalable solution for enhancing the safety and trustworthiness of UPI-based digital payments.[8]

Online Transactions and UPI Fraud Detection, Authors: Mrs. K Komali, Ms. Likitha P, Mr. D D S Rambabu, Mr. G Vinay, Mr. B Dileep.

This research presents a machine learning-based approach for detecting fraud in UPI transactions, addressing the limitations of traditional rule-based systems. By leveraging the Random Forest algorithm, the model identifies anomalous patterns in real-time and reduces both false positives and negatives. An automated alert mechanism ensures quick stakeholder notifications upon detecting

suspicious activity. The system is deployed via a Flask web interface for real-time monitoring, offering a robust and scalable solution for enhancing security in digital payments. Future enhancements may incorporate deep learning and behavioral analytics to further refine fraud detection.[9]

UPI Fraud Detection Using Machine Learning,
Authors: Mohammad Yasir, N Sudarshan Reddy,
Niranjan Reddy R, Nithin A, Professor Madhuri Akki.

This paper addresses the rising challenge of fraud in UPI-based digital transactions by proposing a machine learning-based detection model. As mobile and digital payments become increasingly ubiquitous in India, so do the risks of fraudulent activities exploiting QR codes and online payment channels. The proposed system analyzes transaction datasets using advanced machine learning algorithms to identify patterns associated with fraudulent behavior. By leveraging large-scale transaction data, the model aims to improve detection accuracy compared to traditional statistical methods, offering a more reliable defense against online payment fraud and enhancing digital transaction security.[10]

III. METHODOLOGY

The methodology for UPI fraud detection using machine learning begins with collecting a labeled dataset of UPI transactions, which includes both legitimate and fraudulent cases. The data undergoes preprocessing to address missing values, normalize numerical features, and encode categorical

variables, ensuring consistency and readiness for modeling. Feature selection techniques are then applied to identify the most informative attributes—such as transaction amount, type, account balances, and behavioral patterns—that help distinguish fraudulent transactions from genuine ones. With the refined dataset, a Decision Tree Classifier is trained to learn the patterns associated with fraud, using supervised learning on historical transaction data. The trained model is evaluated using metrics like accuracy, precision, and recall to ensure its effectiveness in detecting fraudulent activities. Once validated, the model is integrated into a web-based platform, enabling real-time prediction and risk assessment for new transactions, while also providing user and admin functionalities for seamless management and feedback.

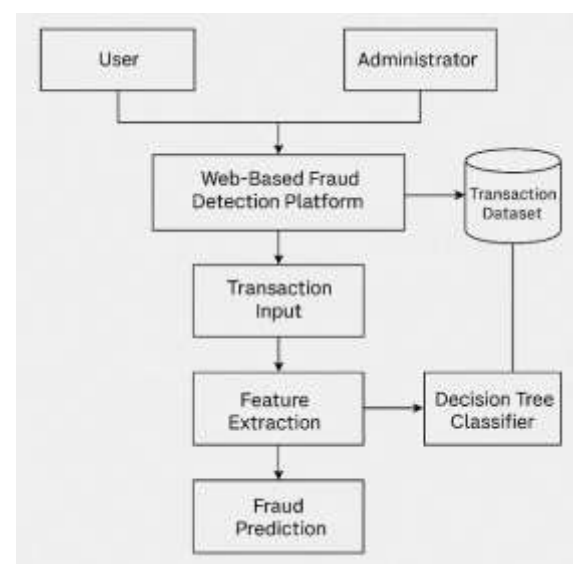


Fig 3.1. Proposed Methodology

1. Dataset Collection: A labeled dataset containing UPI transaction records, each marked as either fraudulent or genuine, is gathered. This dataset serves as the foundation for training and evaluating the machine learning model.

2.Data Preprocessing: The collected data is cleaned and prepared by handling missing values, normalizing numerical data, and encoding categorical variables. This step ensures that the data is consistent and suitable for analysis and modeling.

3.Feature Selection: Relevant features that contribute most to distinguishing fraudulent transactions are identified using statistical and algorithmic methods. Effective feature selection improves model accuracy and reduces computational complexity.

4.Model Training: as A Decision Tree Classifier is trained on the processed and feature-selected dataset. The model learns to associate specific patterns and attributes with fraudulent or legitimate transactions using supervised learning techniques.

5.Model Evaluation: The trained model is rigorously evaluated using metrics such as accuracy, precision, recall, and F1- score to assess its ability to correctly identify fraudulent activities while minimizing false positives and negatives.

6.Deployment and Real-Time Prediction: After validation, the model is deployed within a web-based application. This platform allows users to input transaction details and receive instant fraud risk assessments, while administrators can manage users, FAQs, and feedback, ensuring a secure and user-friendly experience.

IV. TECHNOLOGIES USED

The UPI fraud detection system leverages a combination of modern technologies spanning machine learning, web development, and data engineering to provide accurate, identification and

real-time fraud a seamless user experience. The core technologies used include:

Machine Learning Algorithms: The system employs advanced algorithms such as Decision Trees, Random Forest, Logistic Regression, Neural Networks, and ensemble methods to analyze transaction data and detect fraudulent patterns. Deep learning techniques like Convolutional Neural Networks (CNNs) are also utilized for feature extraction and improved anomaly detection.

Python Programming Language: Python is the primary language for implementing data preprocessing, feature engineering, model training, and evaluation, due to its rich ecosystem of machine learning libraries.

Machine Learning Libraries: Key libraries include Scikit-learn for classical ML models, TensorFlow or PyTorch for deep learning, and Pandas/Numpy for data manipulation and analysis.

Data Analytics Tools: Data analytics and visualization tools are used to explore transaction trends, user behaviors, and model performance, ensuring robust feature selection and engineering.

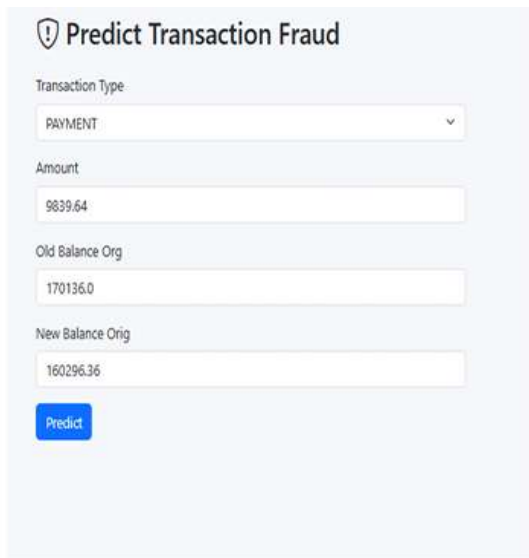
Web Technologies: The front-end of the platform is built using HTML, CSS, and JavaScript to provide a user-friendly interface, while the back-end is often developed with frameworks like Flask or Django for seamless integration with the ML model and database.

Database Systems: Relational databases such as MySQL or SQLite are used to store transaction records, user details, FAQs, and feedback, ensuring data integrity and efficient retrieval.

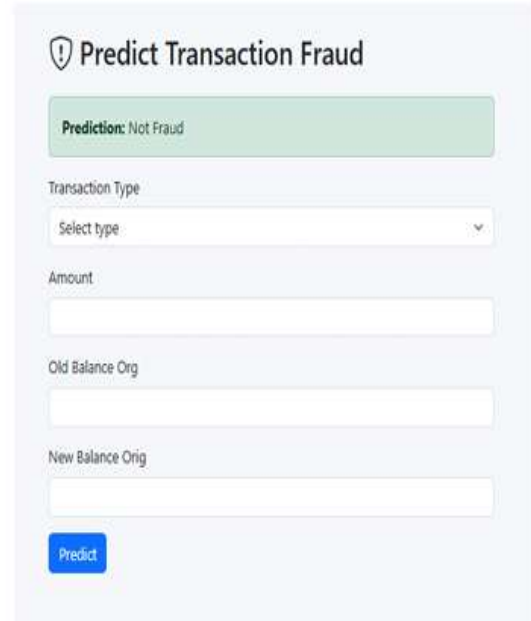
Real-Time Monitoring and Alerting: The system is designed for real-time processing, enabling immediate fraud detection and alerting for suspicious transactions.

Data Balancing Techniques: To address class imbalance in transaction data, techniques like SMOTE (Synthetic Minority Oversampling Technique) are applied during model training. These technologies collectively enable a robust, adaptive, and scalable UPI fraud detection system capable of safeguarding digital payment transactions against evolving threats.

V. Result



Here user is feeding parameters to detect fraud or not.



It is result page.it is showing fraud or not.

VI. CONCLUSION

In conclusion, the proposed the growing threat of fraudulent transactions in digital payments can be effectively and adaptably countered by a machine learning-based UPI fraud detection system platforms. By utilizing a Decision Tree Classifier trained on key transaction features and integrating it within a secure, user-friendly web platform, the system enables real-time identification of suspicious activities with high accuracy. This not only helps in minimizing financial losses but also enhances user trust and confidence in UPI transactions. The inclusion of administrative tools for user and content management further strengthens the platform's robustness and usability. Overall, this solution demonstrates the machine learning's vital role in improving the dependability and security of digital payment ecosystems and creating the framework for future improvements to address evolving fraud patterns.

REFERENCES

- [1]. Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions, Authors: Rupa Rani, Adnan Alam, Abdul Javed, DOI: 10.1109/ICDT61202.2024.10489682, Publisher: IEEE, Conference: 2024 2nd International Conference on Disruptive Technologies (ICDT), Greater Noida, India [2]. UPI Based Financial Fraud Detection Using Deep Learning Approach, Authors: Vaishali Gupta, Sahil Sharma, Suhani Nimkar, Suhani Pathak, DOI: 10.1109/ACROSET62108.2024.10743663, Publisher: IEEE, Conference: 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), Indore, India
- [3]. Detection of Fraudulent Activities in Unified Payments Interface using Machine Learning - LSTM Networks, Authors: M. Naga Raju, Yarramreddy Chandrasena Reddy, Polavarapu Nagendra Babu, Venkata Sai Pavan Ravipati, Velpula Chaitanya, DOI:10.1109/ICCPCT61902.2024.10672890, Publisher: IEEE, Conference: 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT), Kollam, India
- [4]. LLM-Powered UPI Transaction Monitoring and Fraud Detection, Authors: Anupriya K., Avinash K., Hariharan S., Bhavesh R., Rengith Kumaran R., DOI: 10.1109/ICSCAN62807.2024.10894012, Publisher: IEEE, Conference : 2024 International Conference on System, Computation, Automation and Networking (ICSCAN), Puducherry, India
- [5]. UPI Based Mobile Banking Applications – Security Analysis and Enhancements, Authors: K. Krithiga Lakshmi, Himanshu Gupta, Jayanthi Ranjan, DOI:10.1109/AICAI.2019.8701396, Publisher: IEEE, Conference: 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates
- [6]. A Robust UPI Fraud Identification Scheme over Digital Money Transactions using Learning Powered Classification Principles, Authors: Ragavee. U, M. Prithive Raj, Janav. N. Mithra, Sudharshan Balaji S, Ajay Narayanan L, Jacob Mahimai DassY, DOI:10.1109/ICEARS64219.2025.10941576, Publisher: IEEE, Conference: 2025 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India
- [7]. UPI Fraud Detection Using Machine Learning, Authors: Shabreshwari R M, Shafiya Mehrooz, Sidra Fatima, Tanmai R B, Prof. Ganesh Manasali, DOI:10.35629/5252-060698100, 2395-5252, Publisher: International ISSN: Journal Advances in Engineering Management of and (IAEM), Volume/Issue: Volume 6, Issue 06, June 2024
- [8]. UPI Fraud Detection using Machine Learning, Authors: Kavya K R, Usha Sree R, DOI: 10.48175/IJARSCT-22521, ISSN: Not explicitly mentioned (journal listed as online, multidisciplinary with impact factor: 7.53), Publisher: International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume/Issue: Volume 4, Issue 6, November 2024
- [9]. Online Transactions and UPI Fraud Detection, Authors: Mrs. K Komali, Ms. Likitha P, Mr. D D S

Rambabu, Mr. G Vinay, Mr. B Dileep, ISSN/DOI:

Not explicitly mentioned, Publisher: Not specified
(likely institutional or conference publication via
Raghu Engineering College)

[10]. UPI Fraud Detection Using Machine Learning,

Authors: Mohammad Yasir, N Sudarshan Reddy,
Niranjan Reddy R, Nithin A, Professor Madhuri
Akki, DOI:

<https://doi.org/10.22214/ijraset.2025.6664> 3, ISSN:
2321-9653, Publisher: International Journal for
Research in Applied Science and Technology
(IJRASET) Engineering