UPI Fraud Detection Using Machine Learning

Ritika Lala[1] and Abida Shaikh[2]

Asst. Professor, Head , Department of Computer Science[1]

Student, Department of Computer Science[2]

Royal College of Arts Science and Commerce (Autonomus) , Mira Road, Thane, Maharashtra, India.

Abstract:

As more people use UPI for digital payments, stopping fraud has become very important. This project creates a tool that uses Machine Learning to spot fake UPI transactions.

The system is trained on a past dataset of transactions. It learns from details like the transaction amount, time, and recipient to understand the pattern of a fraudulent payment. Once trained, a user can enter the details of a transaction. The model then quickly predicts if the transaction is safe or fraudulent. Additionally, the system offers comprehensive analytics, displaying fraud distribution across categories and overall model performance.

This smart tool is better than old-fashioned methods and helps protect users from financial loss, making digital payments safer for everyone.

Keywords: UPI Fraud Detection, Machine Learning, Random Forest, Digital Payment Security, Transaction Analysis, Financial Crime Prevention, Predictive Analytics, Ensemble Learning

Introduction:

Unified Payments Interface (UPI): Unified Payment Interface is a digital payment system started by the National Payments Corporation of India (NPCI). It allows people to send and receive money directly from their bank accounts using mobile phones. UPI is fast, easy to use, and works 24/7, which is why it has become very popular in India. People use UPI for sending money to friends and family, paying bills, shopping online, and even for government services.

As UPI is being used more and more, the number of digital payments has increased a lot. But along with this growth, the number of online frauds has also increased. Many people are becoming victims of fraud through fake UPI IDs, phishing links, trick messages, and unauthorized transactions.

Old fraud detection systems are not always able to catch new types of fraud. That's why we need smarter systems that can learn from past data and detect suspicious transactions. Machine Learning (ML) is a technology that can help in this. It learns from past transaction data and finds patterns that might show fraud.

This project aims to build a Machine Learning model that can check UPI transaction data and tell whether a transaction is real or fake. It will look at details like the amount, time, how often a user sends money, device used, and other patterns. This system can help banks and payment apps detect fraud early and keep users safe.

Literature Review:

Research paper [1] Credit Card Fraud Detection Using Machine Learning Models (A. Dal Pozzolo et al., 2017) is a foundational work in the field. It compares various ML algorithms like Logistic Regression, Decision Trees, and Random Forests on highly imbalanced credit card transaction datasets. A key contribution is its handling of class imbalance through techniques like SMOTE (Synthetic Minority Over-sampling Technique). While this paper focuses on credit cards, its methodologies for feature engineering and handling data imbalance are directly applicable to UPI fraud detection.

Research paper [2] A Deep Learning Approach for Credit Card Fraud Detection (R. Vaishnav & E. Bharadi, 2019) explores the use of Deep Neural Networks (DNNs) and Autoencoders for fraud detection. The paper argues that deep learning models can automatically learn complex, non-linear patterns in transaction data that might be missed by traditional models. However, a limitation noted is the "black box" nature of deep learning, making it difficult to explain why a transaction was flagged as fraudulent, which is a crucial requirement for financial institutions.

Research paper [3] A Comparative Analysis of Machine Learning Algorithms for Financial Fraud Detection (S. Bhattacharyya et al., 2011) provides a comprehensive comparison of classifiers, including Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and Random Forests. The study concludes that ensemble methods like Random Forest often outperform single classifiers due to their robustness against overfitting. This paper supports the choice of starting with tree-based models for this project.

Research paper [4] Explainable AI (XAI) in Fraud Detection: A Review (A. Adadi & M. Berrada, 2020) addresses the critical issue of model interpretability. While not specific to UPI, it reviews techniques like LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations) that can be used to explain the predictions of complex models. This is crucial for building trust with end-users who need to understand *why* a transaction was flagged.

Research paper [5] Enhanced UPI Fraud Detection Using Machine Learning: A Proactive Approach to Secure Digital Transactions (Meena V., Harshitha M., Kavitha S., 2025) focuses on fraud detection in UPI transactions. The study evaluates various algorithms including Random Forest, Isolation Forest, and One-Class SVM to detect abnormal patterns in payment data. It emphasizes the use of visual analytics and ROC curve evaluation to improve fraud detection accuracy. This paper is directly relevant to UPI-based systems and supports the effectiveness of tree-based models for securing digital payment platforms.

Methodology:

The proposed methodology focuses on detecting fraudulent UPI transactions using historical transaction datasets and a machine learning-based predictive model. The system leverages **data-driven analysis** to identify suspicious transaction patterns and employs the **Random Forest algorithm** for classification of legitimate versus fraudulent activities.
This structured approach ensures a reliable fraud detection mechanism that enhances security in digital payment systems.

Step 1: Data Collection and Preprocessing:

- **UPI Transaction Dataset:**
  Transaction datasets containing details such as **Date & Time, Location, Category, Age, and Transaction Status (Fraud / Safe)** were collected from publicly available financial datasets. Source: Kaggle.
- **User Login and Dataset Upload:**
  A secure login system was created so that users can **log in and upload their dataset** for fraud detection.
- **Preprocessing:**
  - **Data Cleaning:** Removed duplicate or incomplete transaction records.
  - **Label Encoding:** Converted text-based features (e.g., Status, Category) into numerical form for model processing.
  - **Train/Test Split:** The cleaned data was divided into **training (80%)** and **testing (20%)** sets.

Step 2: UPI Fraud Detection Using Random Forest:

The **Random Forest algorithm** was chosen due to its high accuracy and ability to handle numerical.

- **Model Training:** The Random Forest model was trained using the training dataset to learn fraud patterns.
- **Model Testing:** We **split the dataset** into two parts: **80% for training** and **20% for testing**.
- **Prediction:** The trained model predicts whether a transaction is **'Fraud' or 'Safe'**.

Step 3: User Interaction and Result Analysis:

Once the model predicts the results, the system provides **interactive analysis** to the user:

- Displays the **total number of fraud and safe transactions** in the uploaded dataset.
- Shows the **distribution of fraud and safe transactions** across different categories.
- Generates **visual graphs** for easier understanding of fraud trends.

	A	B	C	D	E	F	G	H	I
	trans_hour	trans_day	trans_month	trans_year	category	upi_number	age	state	fraud_risk
	22	19	12	2024	4	9957000522	55	5	1
	1	16	2	2022	8	9957000738	48	6	1
	17	14	5	2023	10	9957000741	34	14	1
	15	19	10	2024	10	9957000661	37	8	1
	3	3	12	2023	9	9957000412	50	18	0
	16	13	6	2023	12	9957000679	30	17	1
	1	25	3	2023	13	9957000627	34	8	1
	3	22	9	2024	14	9957000514	39	7	1
	0	18	10	2022	4	9957000860	59	19	1
	6	9	7	2023	7	9957000137	60	10	0
	20	22	7	2024	7	9957000812	23	12	1
	21	8	7	2023	11	9957000077	27	11	0
	15	9	2	2024	4	9957000637	37	24	1

Figure1: Dataset of UPI Transactions

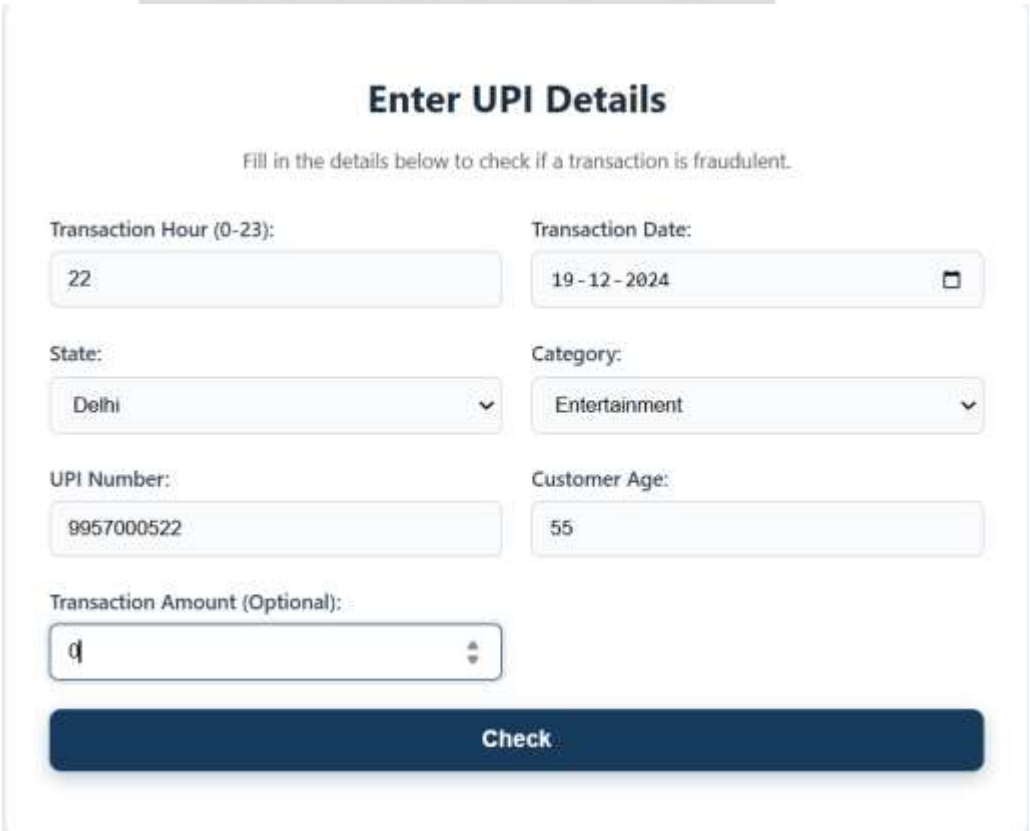

Figure 2: Model Prediction Based on Random Forest Model

UPI Fraud Detection Using ML Analysis Outcome:

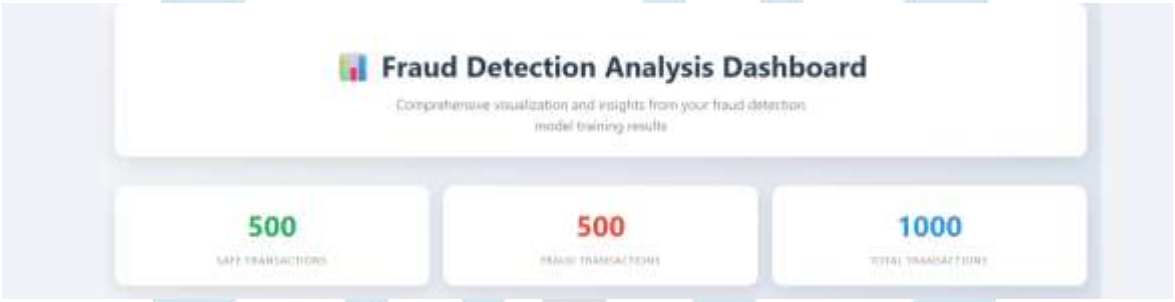

Figure 3: Total number of fraud and safe transactions in the uploaded dataset.

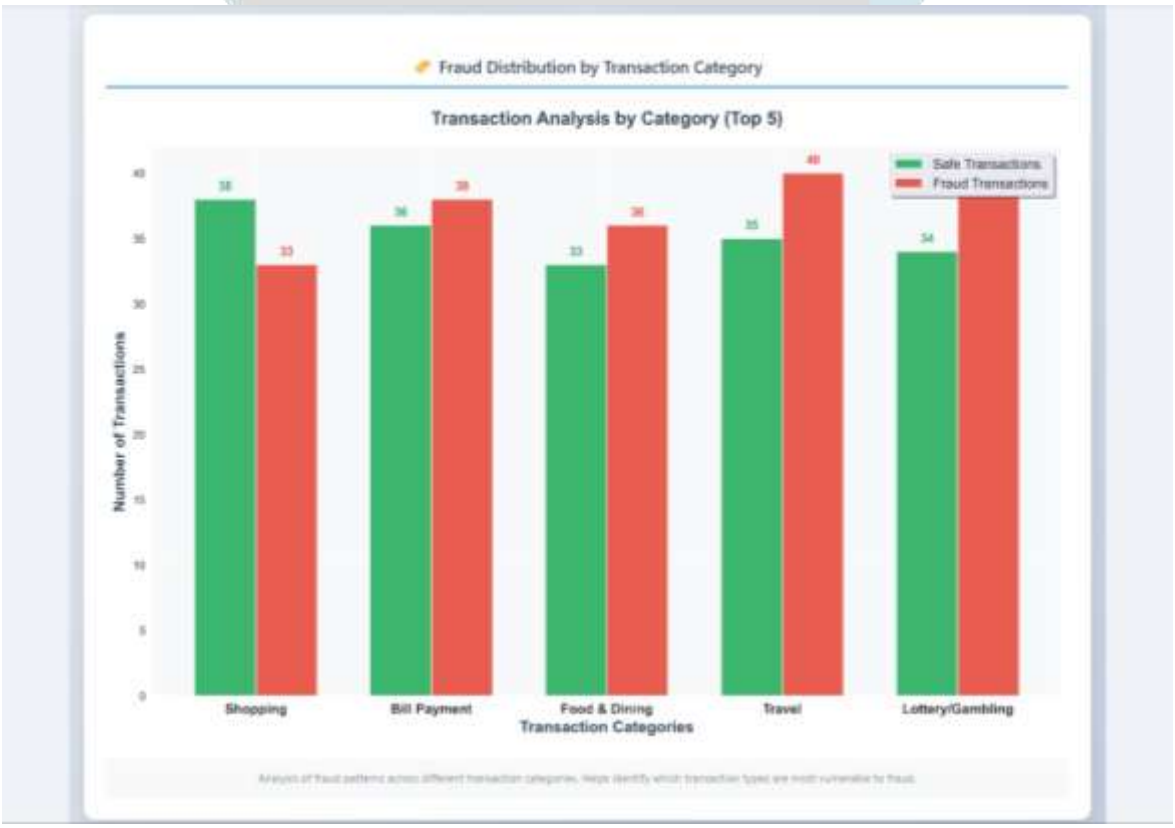

Figure 4: shows the distribution of fraud and safe transactions across different categories.

Results and Discussion:

The implementation of our **UPI Fraud Detection system** using machine learning delivered promising results in accurately identifying fraudulent transactions. **Random Forest** achieved the best performance, effectively distinguishing genuine payments from suspicious ones while minimizing false positives.

Key transaction features such as **Location, Date, timing, and Category** were crucial in detecting fraud patterns. Proper **data preprocessing and feature engineering** improved the model's precision and reliability, while visualization tools enhanced the interpretability of the results.

Conclusion:

Our project marks a significant step toward enhancing the security and reliability of digital payments through machine learning-based fraud detection. Traditionally, UPI fraud detection relies on manual monitoring or fixed rules, which are often slow, error-prone, and unable to adapt to new and evolving fraud patterns. Our system challenges this norm by leveraging transaction datasets and ML models to automatically identify fraudulent activities and classify transactions as safe or risky.

By combining data-driven analysis with predictive modeling, this project not only improves the accuracy and speed of fraud detection but also provides users with actionable insights into transaction patterns. The system allows users to upload historical datasets, train models, and analyze trends, such as the proportion of fraudulent versus safe transactions, enabling a deeper understanding of transaction behavior and potential vulnerabilities.

This approach is particularly beneficial for individual users, banks, and fintech platforms, where timely detection of fraudulent transactions can prevent financial losses and build trust in digital payment systems. The success of this project reinforces the potential of machine learning in financial security, demonstrating how predictive models can proactively identify fraud and enhance real-time decision-making.

As this technology continues to evolve, future advancements could include integration with live transaction monitoring, multi-layered security checks, and more sophisticated ML algorithms, expanding the system's capability to handle larger datasets and more complex fraud scenarios. Ultimately, this project lays the foundation for a smarter, safer, and more efficient digital payment ecosystem, where machine learning ensures secure transactions, reduces financial risk, and empowers users with data-driven insights.

Future Scope:

The UPI Fraud Detection system using machine learning opens promising opportunities to strengthen digital payment security. Future enhancements can focus on:

1. **Multimodal Fraud Indicators** – Integrating call/SMS data, device fingerprints, and behavioral biometrics to improve detection accuracy and reduce false alerts.
2. **Real-Time Prevention** – Enabling live transaction monitoring with instant alerts or blocking suspicious activity to minimize losses.
3. **Advanced AI Models** – Using deep learning and adaptive models to handle evolving fraud tactics and large-scale data.
4. **Cross-Platform & Mobile Integration** – Expanding support for multiple payment apps, regional languages, and embedding into mobile or wearable devices for on-the-go security.
5. **Collaboration with Banks & Authorities** – Sharing fraud insights securely with financial institutions and law enforcement for stronger anti-fraud networks.
6. **Adaptive Learning & Global Compliance** – Building self-learning systems to tackle emerging threats and adapting for international payment systems.

References:

[1] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection: A realistic modeling and a novel learning strategy," IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 8, pp. 3784–3797, 2017.

[2] Y. Sahin and E. Duman, "Detecting credit card fraud by ANN and logistic regression," in Proc. IEEE ISCC, 2011.

[3] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decis. Support Syst., vol. 50, no. 3, pp. 602–613, 2011.

[4] H. Sharma, A. Jain, and S. Agrawal, "An efficient approach for online fraud detection using machine learning algorithms," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 10, pp. 582–588, 2021.

[5] Y. Kumar and A. Bansal, "Real-time UPI fraud detection using ML techniques," Int. J. Comput. Appl., vol. 182, no. 2, pp. 15–20, 2023.

[6] A. Shukla et al., "A survey on online payment fraud detection using machine learning," J. Inf. Secur. Appl., vol. 66, p. 103131, 2022.

[7] A. Verma and A. Kumari, "Machine learning-based online transaction fraud detection," in Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN), 2021.

[8] A. Mohan and D. Thomas, "Application of AI in digital payment fraud detection," Int. Res. J. Eng. Technol., vol. 9, no. 4, pp. 2001–2005, 2022.

[9] S. Chakraborty, "UPI and digital payment fraud cases in India," Econ. Polit. Wkly., vol. 58, no. 19, pp. 17–20, 2023.

[10] Reserve Bank of India, "Annual report 2023–24 – Trends in digital payments & fraud management," RBI.org.in, 2024. [Online]. Available: https://www.rbi.org.in