

UPI Fraud Detection Using Machine Learning

Prof.Mrs. J.R.Dhumal^{*1}, Vedant Ronkhede^{*2}, Sahil Fulsundar^{*3}, Sarang Girme^{*4}

^{*1}Professor, Information Technology Savitribai Phule Pune University Pune, India.

^{*2,3,4,5}Information Technology Savitribai Phule Pune University Pune, India.

ABSTRACT

In recent years, the rise of digital payment systems, particularly Unified Payments Interface (UPI) in India, has revolutionized financial transactions, making them more accessible and efficient. However, this surge in usage has also led to an increase in fraudulent activities, posing significant risks to consumers and financial institutions. This paper presents a comprehensive approach to UPI fraud detection, employing advanced machine learning techniques and data analytics. We explore various types of UPI fraud, including phishing, account takeover, and unauthorized transactions. By utilizing a dataset comprising transaction histories, user behavior patterns, and contextual features, we develop a predictive model aimed at identifying fraudulent transactions in real-time. Our findings demonstrate the effectiveness of ensemble methods and anomaly detection algorithms, achieving a notable improvement in detection accuracy and reduction in false positives. The proposed framework not only enhances the security of UPI transactions but also provides insights for stakeholders to implement robust preventive measures, ultimately contributing to a safer digital payment ecosystem.

The methodology begins with data collection, gathering a diverse dataset that includes transaction records, user profiles, device information, and contextual features such as transaction timing and location. Feature engineering plays a crucial role in enhancing model performance by identifying key indicators like transaction frequency and average transaction amounts. Various machine learning algorithms are then explored, including decision trees for pattern interpretation, random forests for accuracy improvement, support vector machines for classification, and neural networks for capturing complex data relationships.

The Unified Payments Interface (UPI) has transformed the landscape of digital payments in India, facilitating seamless transactions for users and merchants alike. However, this convenience has also attracted fraudsters, leading to various types of financial crimes, including phishing attacks, account takeovers, merchant fraud, and transaction reversal fraud. The results demonstrate significant improvements in detecting fraudulent activities, characterized by reduced false positive rates and enhanced detection accuracy. By leveraging ensemble methods, the predictive model achieves a robust sensitivity and specificity, ensuring that legitimate transactions are not incorrectly flagged.

Keywords: SVM, Dataset, Preprocessing, Feature Extraction, Classification.

INTRODUCTION

Unified Payments Interface (UPI) has significantly transformed the landscape of digital financial transactions, offering a convenient, real-time method for transferring money between accounts. Since its inception, UPI has gained widespread acceptance due to its ease of use, low transaction costs, and integration with various financial institutions and service providers. Its ability to facilitate instant payments with minimal friction has made it a preferred choice for millions of users globally. However, the rapid expansion of UPI usage has also brought to light the vulnerabilities associated with digital payments.

The simplicity and openness of the UPI system, while advantageous for users, have also made it a target for fraudulent activities. In response to these challenges, it introduces a novel fraud detection framework designed specifically for UPI transactions. By integrating advanced machine learning algorithms and behavioral analytics, our approach aims to enhance the detection of fraudulent activities. We explore the use data analysis to identify anomalies, improve the accuracy of fraud detection, and safeguard the integrity of UPI transactions.

I. METHODOLOGY

UPI fraud detection refers to the process of identifying and preventing fraudulent transactions conducted through the Unified Payments Interface (UPI). UPI allows users to transfer money instantly between bank accounts using a mobile phone. While it has become highly popular due to its ease of use, this widespread adoption has also made it a target for various types of fraud.

Machine Learning in UPI Fraud Detection:

Machine learning (ML) plays a critical role in detecting UPI fraud by building models that can:

- **Classify Transactions:** ML models are trained to distinguish between fraudulent and legitimate transactions based on historical data.
- **Predict Fraud Patterns:** Using supervised learning, these models learn from labeled data (fraudulent vs. non-fraudulent transactions) and predict which future transactions are likely fraudulent.
- **Handle Imbalanced Data:** Fraud detection datasets are usually imbalanced (i.e., there are far fewer fraudulent transactions than legitimate ones).

1. Random Forest

What It Is: Random Forest is an ensemble learning method. It builds multiple Decision Trees and combines their results using majority voting to make final predictions.

How It Works:

1. The training dataset is randomly split into multiple smaller datasets (bootstrapping).
2. For each dataset, a decision tree is created using a random subset of features.
3. Each tree gives a prediction (fraud or not fraud).
4. The final prediction is based on the majority vote of all trees.

2. Support Vector Machine (SVM)

What It Is: SVM is a supervised classification algorithm that finds the best boundary (called a hyperplane) to separate fraud and non-fraud transactions.

How It Works:

1. It plots data in n-dimensional space (n = number of features).
2. It finds the hyperplane that separates the two classes with the maximum margin (i.e., as far apart as possible).
3. If data is not linearly separable, kernel tricks (e.g., polynomial or RBF kernel) are used to map data into higher dimensions where separation is possible.

3. Naive Bayes

What It Is: Naive Bayes is a probabilistic classifier based on Bayes' Theorem, assuming that all features are independent of each other (naive assumption).

How It Works:

1. Calculate the prior probability of fraud and not fraud in the dataset.
2. For a new transaction, calculate the likelihood of each feature (e.g., amount, time, location) given it is fraud or not fraud.

4. XGBoost (Extreme Gradient Boosting)

What It Is: XGBoost is a boosting algorithm — it builds a series of models where each model learns from the errors of the previous one.

How It Works:

1. Start with a weak model (e.g., a simple decision tree).
2. Calculate the error/residual between prediction and actual values.
3. Train the next tree to predict these errors.
4. Repeat the process — each new tree improves the overall model.

5. Use gradient descent to minimize the loss function (usually log loss or square error).
6. Combine all models to get the final strong model.

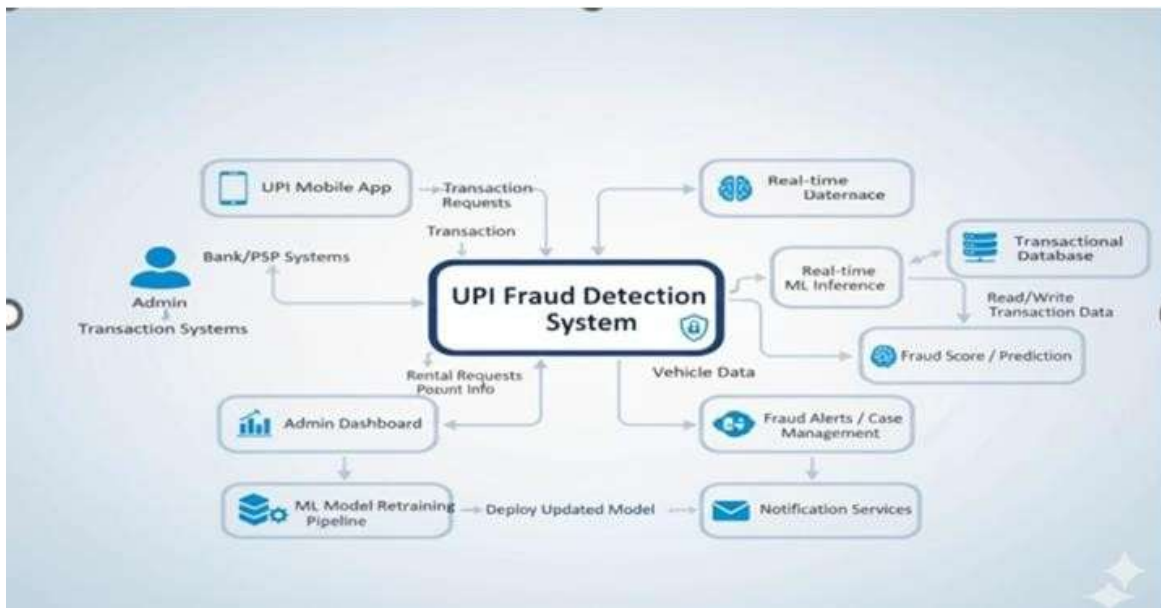


Figure 1: Architecture

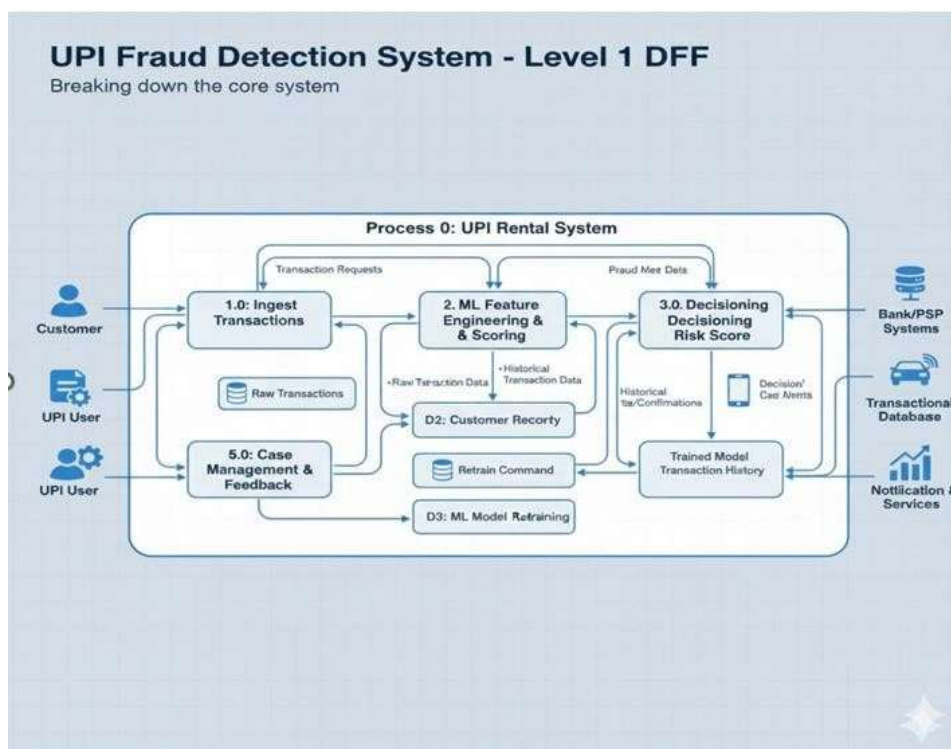


Figure 2: Use Case Diagram

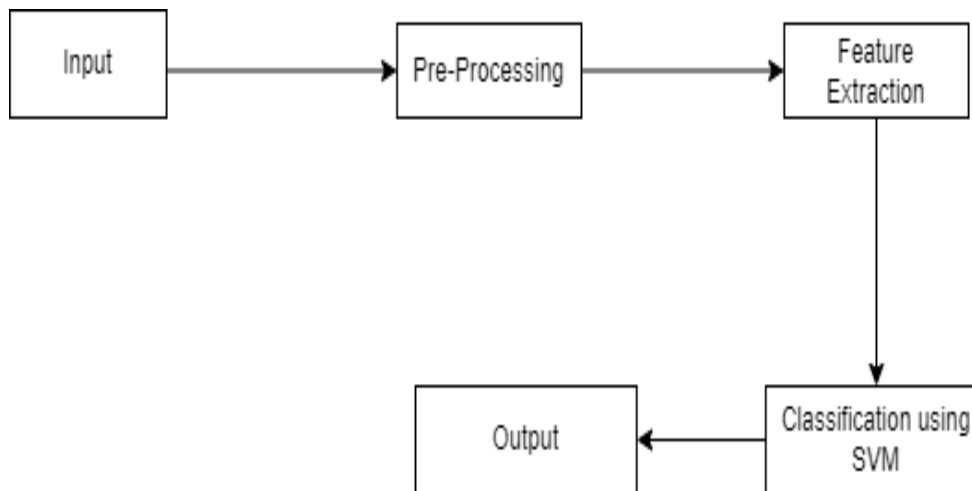


Figure 3: Data Flow Diagram

II. IMPLEMENTATION

Here are the steps involved in implementation

1. Data Collection

- Collect relevant features such as transaction amount, time, sender/receiver IDs, location (if available), device information, transaction type, and any other pertinent details.

2. Data Preprocessing

- **Cleaning:** Handle missing values (impute or remove), identify and treat outliers, and correct any inconsistencies or errors in the data.

3. Feature Engineering

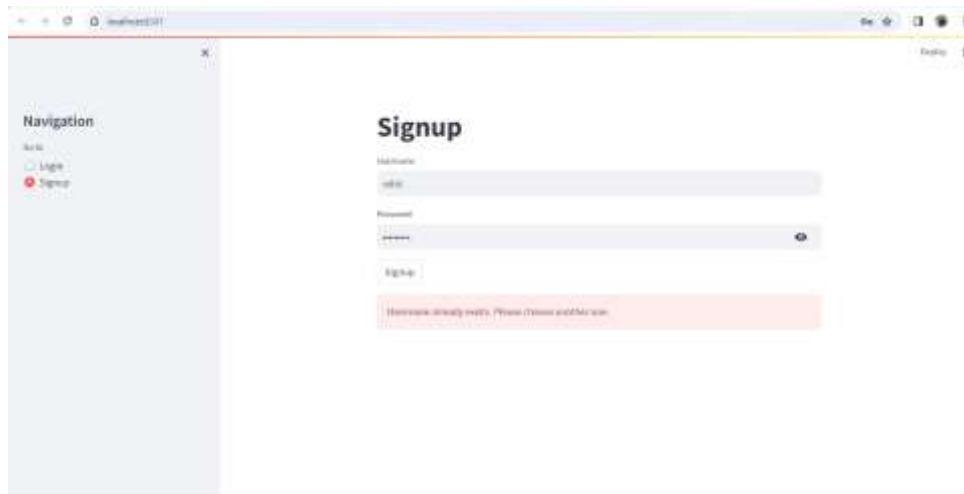
- Create new features from the existing data that might be more informative for fraud detection.

4. Model Selection

- Choose appropriate machine learning algorithms for binary classification (fraudulent vs. non-fraudulent). Some common algorithms include:
 - **Random Forests:** An ensemble method that combines multiple decision trees to improve accuracy and reduce overfitting.
 - **Gradient Boosting Machines (e.g., XGBoost):** Another ensemble method that builds trees sequentially, correcting the errors of previous trees.
 - **Support Vector Machines (SVM):** Finds a hyperplane that best separates the two classes.
 - **Naive Bayes:** Naive Bayes is a probabilistic classifier based on Bayes' Theorem, assuming that all features are independent of each other (naive assumption).

5. Model Training and Evaluation

- Split the preprocessed data into training, validation, and testing sets.
- Train the selected machine learning model using the training data.
- Tune the hyperparameters of the model using the validation set to optimize performance (e.g., using techniques like grid search or random search).
- Evaluate the trained model on the testing set using appropriate metrics for imbalanced datasets



Fraud Detection Page

IV. COMPARISON AND ANALYSIS

We compare the performance of the Support Vector Machine (SVM) model against other machine learning algorithm and analyze key findings. This analysis helps assess how well SVM performs in detecting fraud, particularly in comparison to other methods.

- **Accuracy:** The proportion of correctly classified transactions (fraudulent and legitimate) out of all transactions.
- **Precision:** The proportion of true fraud cases among the transactions flagged as fraudulent.
- **Recall (Sensitivity):** The proportion of actual fraud cases correctly identified by the model.
- **F1-Score:** The harmonic mean of precision and recall, especially useful in imbalanced datasets like fraud detection.

V. DISCUSSION

SVM has proven to be effective in detecting fraud in UPI transactions, especially in terms of its precision and accuracy. By defining a clear margin between fraudulent and non-fraudulent transactions, SVM is capable of drawing an optimal hyperplane in the feature space, particularly useful in non-linear scenarios. UPI fraud detection inherently deals with imbalanced data, where fraudulent transactions form only a small percentage of the overall dataset. This imbalance causes the model to favor legitimate transactions unless handled carefully. Identifying relevant features from transaction data, such as time-based patterns, transaction velocity, and geographical mismatches, was crucial. However, the selection process was challenging due to the sheer volume of features available and the dynamic nature of fraud strategies.

One of the challenges with using SVM in fraud detection is its interpretability. While SVM is a powerful classifier, its decisions—especially with non-linear kernels—are not always easily understood. In a fraud detection system, interpretability is crucial as banks and financial institutions need to understand why certain transactions were flagged as fraudulent.

VI. CONCLUSION

The SVM-based UPI fraud detection model performs well in identifying fraudulent transactions, particularly with high precision. However, it faces challenges with data imbalance, scalability, and interpretability. Comparatively, Random Forest may be better suited for maximizing fraud detection, but SVM holds strong potential, especially when optimized for the user. As fraud strategies evolve, continuous updates, feature engineering, and potentially hybrid models will be necessary to maintain the model's effectiveness. Financial institutions should consider integrating these advanced models into their systems while balancing customer experience and security.

By leveraging an SVM classifier with appropriate feature selection, data balancing, and hyperparameter tuning, the system can classify transactions as fraudulent or legitimate with a high degree of accuracy. The continuous updating of the model with new data ensures that the fraud detection system remains effective over time, adapting to new fraud

techniques and patterns.

ACKNOWLEDGEMENTS

We would like to extend our gratitude to Project staff at the Sinhgad Academy of Engineering, Department of Computer Engineering for their support and help without which this work could not have been accomplished. Additionally, we would like to give Prof.Mrs. J.R.Dhumal, our project manager, our profound gratitude for leading us through the process.

VII. REFERENCES

- [1] Kavithal, J., Indira, G., Anil Kumar, A., Shrinitha, A., & Bappan, D. (2024). *Fraud Detection in UPI Transactions Using ML*.
- [2] Bodade, M. S., & Pawade, P. P. (2014). *Implementation Paper on UPI Fraud Detection using Machine Learning*.
- [3] Ali, A., Abd Razak, S., Othman, S. H., Abdalla Elfadil Eisa, T., & Al-Dhaqm, A. (2022). *Financial Fraud Detection Based on Machine Learning*.
- [4] Edburg, B. F. (2023). *Role of UPI Application Usage and Mitigation of Payment Transaction Frauds: An Empirical Study*.
- [5] Priya, N., Ahmed, J., & Alam, M. A. (2020). *Digital Payments: A Scheme for Fraud Data Collection and Use in Indian Banking Sector*.
- [6] Valavan, M., & Rita, S. (2023). *Predictive-Analysis-based Machine Learning Model for Fraud Detection*.
- [7] Durwin, A. S. (Year not specified). *AI-POWERED SECURITY IN INDIA'S UPI TRANSACTIONS EVALUATING TRANSACTION VOLUMES, FRAUD INCIDENTS, AND MITIGATION STRATEGIES*.
- [8] Akinje, A. O. (2021). *Fraudulent Detection Model*.
- [9] Ramakrishnan, R., Vanisri, S., & Yuvalakshmi, D. (2024). *Unified Payment Interface Seamless Transaction Using RNN Model*.
- [10] Huang, D., Mu, D., Yang, L., & Cai, X. (2018). *CoDetect: Financial Fraud Detection With Anomaly Feature Detection*.