International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

UPI Fraud Detection Using AI & ML

Dasani Ravikiran Babu[1], Perkari Srichandana[2], Kashetti Maduri[3], Nagula Anil[4], Thallapelly Bhanuteja[5]

[1]*Electronics & communication , Jyothishmathi institute of technology and science*
[2]*Electronics & communication , Jyothishmathi institute of technology and science*
[3]*Electronics & communication , Jyothishmathi institute of technology and science*
[4]*Electronics & communication , Jyothishmathi institute of technology and science*
[5]*Electronics & communication , Jyothishmathi institute of technology and science*

ABSTRACT - The Unified Payments Interface (UPI) has made digital payments fast and convenient.However, the increase in UPI usage has also led to a rise in fraud cases. This project focuses on detecting fraudulent UPI transactions using AI and Machine Learning. The system analyzes transaction details such as amount, time, location, and behavior. Machine learning algorithms are used to identify suspicious patterns. The model learns from past transaction data to predict fraud in new transactions. Data preprocessing and feature selection improve the system's accuracy. Performance is evaluated using metrics like accuracy, precision, and recall. The goal is to reduce financial losses and improve transaction security. This AI-based approach helps make digital payment systems safer and more reliable..

Key Words: AI, ML, VScode, Pandas, Numpy Seaborn, XGBoost

1. INTRODUCTION

The Unified Payments Interface (UPI) has revolutionized digital payments by enabling fast, secure, and real-time money transfers. However, its widespread adoption has also led to a rise in fraud activities such as phishing, fake payment requests, and identity theft. Traditional rule-based fraud detection methods are often ineffective against evolving fraud patterns. Artificial Intelligence (AI) and Machine Learning (ML) provide advanced solutions for detecting suspicious transactions in real time. These technologies analyze large volumes of transaction data to identify hidden patterns and anomalies. ML models learn from historical user behavior and continuously adapt to new fraud strategies. Parameters like transaction frequency, location, device details, and spending habits help distinguish genuine users from fraudsters. AI-driven systems improve detection accuracy while reducing false alarms. Implementing AI and ML enhances security, builds user trust, and minimizes financial losses. Thus, AI- and MLbased UPI fraud detection plays a crucial role in ensuring safe and reliable digital payment ecosystems.

2. PROBLEM STATEMENT:

User security and confidence are seriously in danger due to the sharp increase in fraudulent transactions brought on by the quick implementation of the Unified Payments Interface (UPI). It is challenging for standard technologies to identify sophisticated fraud schemes due to the large volume of transactions and changing fraud patterns. The objective of this project is to detect and stop fraudulent activity in UPI transactions in order to improve the security and dependability of the digital payment ecosystem. In order to do this, an efficient fraud detection system will be created using cutting-edge machine learning techniques.

3. EXISTING SYSTEM:

The existing system for fraud detection in digital payment platforms, including UPI, primarily relies on traditional rule-based and manual monitoring approaches. These systems use predefined rules such as transaction limits, unusual transaction frequency, or blacklist verification to identify suspicious activities. When a transaction exceeds a set threshold or violates a rule, it is flagged as potentially fraudulent. Although this approach provides a basic level of security, it lacks the flexibility to adapt to new and sophisticated fraud patterns. Fraudsters continuously modify their techniques, making static rule-based systems less effective over time. Additionally, these systems often generate a high number of false positives, where legitimate transactions are incorrectly flagged as fraud, causing inconvenience to users and additional verification overhead for financial institutions.

Another limitation of the existing system is its dependency on manual intervention and retrospective analysis. Fraud detection often occurs after the transaction is completed, which means financial losses may already have occurred before preventive action is taken. The absence of real-time monitoring capabilities restricts the ability of these systems to respond promptly to suspicious activities. Furthermore, traditional systems do not effectively analyze user behavioral patterns such as spending habits, device usage, and location consistency, which are critical indicators of fraudulent activity. The lack of advanced data analytics and intelligent pattern recognition reduces the overall detection accuracy. These systems also struggle to handle the massive volume of digital transactions generated by UPI platforms, leading to scalability challenges and delayed processing

4. PROPOSED SYSTEM:

The proposed system for UPI fraud detection leverages Artificial Intelligence (AI) and Machine Learning (ML) techniques to provide an intelligent, adaptive, and real-time fraud prevention framework. Unlike traditional rule-based systems, the proposed model focuses on analyzing transaction data and user behavior patterns to accurately identify suspicious activities. The system begins with collecting historical and real-time transaction data, including features such as transaction amount, time, location, device details, transaction frequency, and user spending habits. This data is then preprocessed through cleaning, normalization, and handling missing values to ensure high-quality input for model training. Feature engineering is performed to extract meaningful behavioral indicators, such as unusual transaction spikes, sudden location changes, or deviations from normal spending patterns

Once the dataset is prepared, machine learning algorithms such as Logistic Regression, Decision Trees, Random Forest, Support Vector Machines, and Neural Networks are applied to develop predictive fraud detection models. These models are trained on labeled datasets containing both genuine and fraudulent transactions, enabling them to learn distinguishing characteristics of fraud. To address class imbalance, techniques such as oversampling or SMOTE are used to improve model sensitivity toward fraudulent cases. After training, the models are evaluated using performance metrics like accuracy, precision, recall, and F1-score to select the most effective algorithm. Hyperparameter tuning and cross-validation further optimize the model and prevent overfitting.

The validated model is then integrated into a real-time monitoring system capable of analyzing incoming UPI transactions instantly. When suspicious activity is detected, the system generates alerts and may trigger additional authentication measures such as OTP verification or transaction blocking to prevent financial loss. The proposed system also includes a user-friendly dashboard that provides visualization of fraud trends, transaction analysis, and risk assessment for financial institutions. Continuous learning and periodic model retraining ensure that the system remains adaptive to evolving fraud strategies. Additionally, the framework is designed to be scalable, enabling it to handle large transaction volumes efficient.

5. SOFTWARE REQUREMENTS:

i. Pyhton 3.x
ii. Jupyter Notebook

LIBRARIES:

1. Pandas
2. Numpy
3. Scikit-learn
4. Imbalanced-learn
5. Matplotlib
6. Seaborn
7. XGBoost
8. LightGBM
9. Tensor flow

6. SIGNIFICANCE OF THE WORK

The significance of this work lies in addressing the growing security challenges associated with digital payment systems, particularly the Unified Payments Interface (UPI). With the rapid increase in online transactions, fraudsters are continuously developing sophisticated techniques to exploit vulnerabilities, making traditional security measures insufficient. This project contributes to enhancing financial security by integrating Artificial Intelligence (AI) and Machine Learning (ML) for proactive fraud detection. The proposed system enables real-time monitoring of transactions, helping financial institutions and payment platforms detect suspicious activities before financial damage occurs. By analyzing user behavior patterns, the system improves the accuracy of fraud detection and

reduces false positives, ensuring a seamless experience for genuine users

7. BLOCK DIAGRAM:

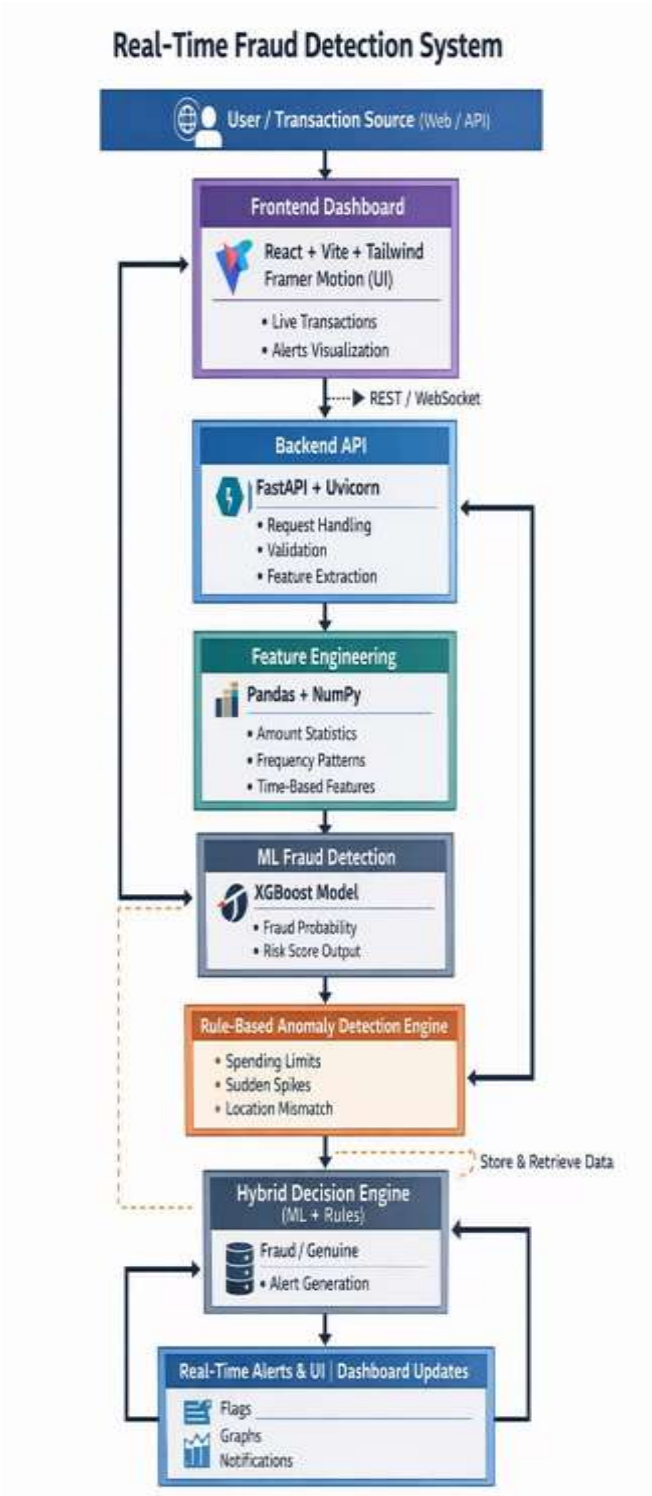

Fig: proposed block diagram

8. SCOPE OF THE PROJECT:

To build on the current project, several enhancements and future works can be considered to expand its functionality and effectiveness:

1. Integration of Real-time Transaction Monitoring
2. Implementation of Advanced Deep Learning Models
3. Cloud-based Fraud Detection System
4. User Behavior and Device Fingerprint Analysis
5. Multi-platform Digital Payment Support
6. Enhanced Security and Encryption Mechanisms
7. Mobile Application Integration for Alerts and Monitoring

9. CONCLUSION:

The UPI Fraud Detection system was successfully developed using Python and machine learning techniques to identify fraudulent transactions. Data preprocessing and SMOTE helped handle class imbalance and improve fraud detection capability. Multiple models such as Random Forest, XGBoost, and LightGBM were implemented, with boosting algorithms showing better performance. The system achieved reliable results based on accuracy, precision, recall, and F1-score evaluation metrics. Overall, the project demonstrates the effective use of AI/ML in enhancing digital payment security and preventing financial fraud.

The project achieved key objectives, such as:

1. **Fraud Detection System Development:** The project successfully developed a machine learning-based UPI fraud detection system capable of classifying transactions as fraudulent or genuine. The implemented solution addressed the primary goal of improving transaction security. This demonstrates the effectiveness of AI techniques in financial fraud prevention.
2. **Data Preprocessing:** Transaction data was cleaned, transformed, and prepared using Pandas and NumPy to remove inconsistencies and missing values. Proper preprocessing improved dataset quality and ensured better model learning. This step played a crucial role in enhancing prediction accuracy.
3. **Handling Class Imbalance:** SMOTE was applied to balance the dataset by increasing minority fraud samples. This helped the model learn fraud patterns more effectively and reduced bias toward legitimate transactions. As a result, fraud detection performance improved significantly.

4. **Feature Importance Identification:** Important transaction features influencing fraud prediction were analyzed using model-based techniques. Feature importance improved interpretability and understanding of decision-making processes. This contributed to building a transparent fraud detection system.

10. RESULT:

The UPI Fraud Detection system was developed using Python and machine learning techniques. Data preprocessing and visualization were performed using Pandas, NumPy, Matplotlib, and Seaborn. Imbalanced-learn was used to balance the dataset and improve fraud detection performance. Machine learning models such as Random Forest, XGBoost, and LightGBM were trained and evaluated using accuracy and recall metrics.

Fig. Dashboard

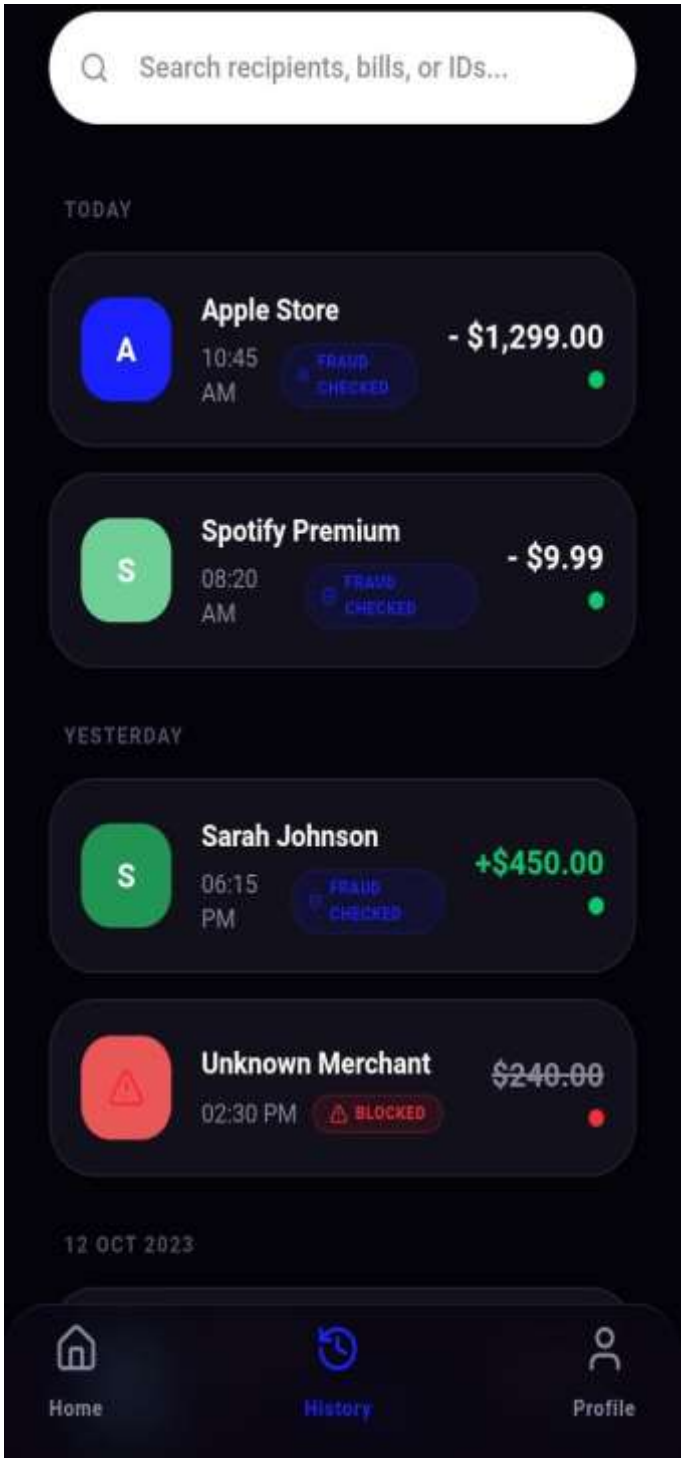

Fig: Transaction History

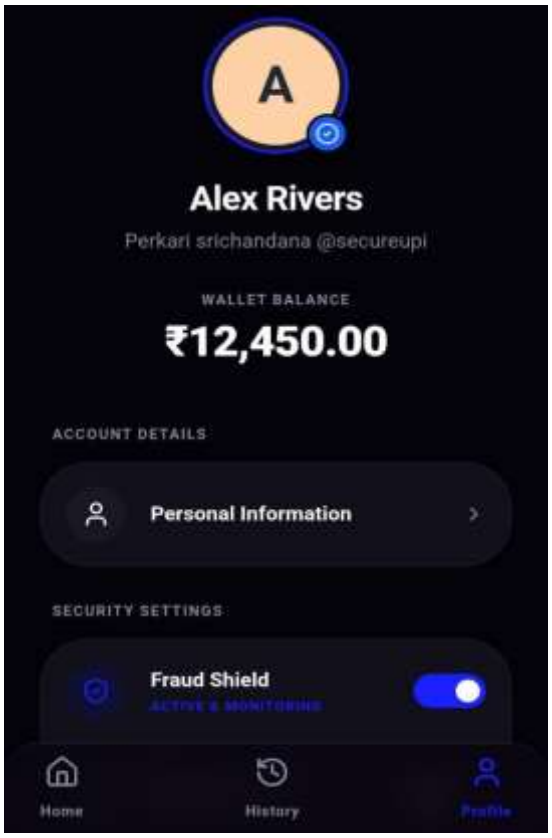

Fig: Profile

11. REFERENCES:

1. Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015). Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. IEEE Transactions on Neural Networks and Learning Systems.

2. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A Comprehensive Survey of Data Mining-based Fraud Detection Research. Artificial Intelligence Review, 34(1), 1– 14.

3. Whitrow, C., Hand, D., Juszczak, P., Weston, D., & Adams, N. (2009). Transaction Aggregation as a Strategy for Credit Card Fraud Detection. Data Mining and Knowledge Discovery, 18(1), 30–55.

4. Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2018). Scarff:

5. A Scalable Framework for Streaming Credit Card Fraud Detection with Spark. Information Fusion, 41, 182–194. Pedregosa, F., Varoquaux, G., Gramfort, A., et al. (2011). Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research, 12, 2825–2830. Lemaître, G., Nogueira, F., & Aridas, C. K. (2017).

6. Imbalanced-learn: A Python Toolbox to Tackle the Curse of Imbalanced Datasets in Machine Learning. Journal of Machine Learning Research, 18(17), 1–5.

7. Chen, T., & Guestrin, C. (2016). XGBoost: A Scalable Tree Boosting System. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.

8, Ke, G., Meng, Q., Finley, T., et al. (2017). LightGBM: A Highly Efficient Gradient Boosting Decision Tree. Advances in Neural Information Processing Systems (NeurIPS).

9, Abadi, M., Agarwal, A., Barham, P., et al. (2016). TensorFlow: Large-scale Machine Learning on Heterogeneous Distributed Systems. arXiv preprint arXiv:1603.04467.