Machine Learning-Driven UPI Fraud Detection

Sameeksha K S[1], Prof. Suma N R[2]

[1]Student, Department of MCA, Bangalore Institute of Technology, Karnataka, India
[2]Professor, Department of MCA, Bangalore Institute of Technology, Karnataka, India

---

Abstract - Financial transactions have been transformed by the emergence of digital payment platforms such as the Unified Payments Interface (UPI), which offer quick and easy services. But this ease of use has also raised the possibility of fraud, which presents serious problems for both consumers and financial institutions. This project offers a machine learning-based method for efficiently identifying fraudulent UPI transactions. To improve model accuracy, a wide range of data was gathered and preprocessed, including transaction frequency, amount, location, device information, and user behavior. Missing value handling, class imbalance correction, and feature selection using Lasso regression were among the preprocessing steps. To find important patterns connected to fraud, correlation and graphical analyses were performed. After several machine learning models were trained and assessed, the top-performing model was incorporated into an HTML, CSS, and Flask web application. The backend uses the trained model to instantly classify transactions as either legitimate or fraudulent after users safely enter transaction details. The findings show how machine learning can improve the security of UPI transactions by providing a scalable, effective, and user-friendly fraud detection solution that supports the development of digital financial systems.

Key Words: UPI, Amount, Transactions, Analysis, Fraud, Security, Digital payment

1. INTRODUCTION

The quick uptake of online payment methods in the digital age has completely changed how financial transactions are carried out. In many nations, especially India, the Unified Payments Interface (UPI) has become a well-liked and practical way to send money instantly. But as the use of UPI grows, so does the risk of fraudulent transactions, which can cause large losses for both financial institutions and individuals [1].

This project suggests a strong machine learning-based approach for identifying fraudulent UPI transactions in order to address this issue. The project entails gathering and examining a large dataset that includes attributes like transaction volume, frequency, location, device details, and user behaviour. The project intends to develop an efficient fraud detection model by preprocessing the data to handle null values, address class imbalance, and choose the most pertinent features using methods like Lasso regression [2].

In order to comprehend the connections between various variables and how they affect fraud detection, the method also incorporates comprehensive graphical and correlation-based analyses. To guarantee the highest level of prediction accuracy, a number of machine learning models will be created and assessed [3].

Additionally, the project will use HTML, CSS, and Flask to create a user-friendly web application. Users can safely enter transaction information, including the amount, credit card number, and CVV, using this application. After retrieving the required transaction information, the backend system will use the machine learning model that has been trained to decide whether to approve the transaction or mark it as possibly fraudulent [4].

By using cutting-edge machine learning techniques, this project seeks to improve the security of UPI transactions while also advancing the field of fraud detection.

2. LITERATURE SURVEY

With the introduction of mobile-based banking and payment systems, the digital revolution has drastically changed India's financial scene. The National Payments Corporation of India (NPCI) unveiled the Unified Payments Interface (UPI) in 2016, which is one of the most groundbreaking innovations. Through mobile applications, UPI facilitates smooth, real-time money transfers between bank accounts, speeding up, simplifying, and increasing accessibility for the general public. UPI has experienced rapid growth in recent years and is now the preferred payment method for millions of people and businesses due to its convenience, interoperability, and round-the-clock availability. [1]

The use of digital payments is growing, and with it, so are the security risks. Fraudulent activities have increased in tandem with the growth in UPI transactions. These include, among other things, social engineering techniques, phony merchant handles, phishing scams, and fraudulent UPI links. In addition to causing users to suffer immediate financial losses, these scams also help to erode public confidence in digital payment systems. The intricacy and sophistication of contemporary fraud schemes are too great for the conventional methods of fraud detection, which are usually based on static, rule-based systems. These systems frequently result in either missed frauds or high false-positive rates because they are inflexible, unadaptable, and unable to identify previously unseen fraudulent patterns. [2]

Machine Learning (ML) is a strong and clever solution in this situation. Large volumes of transaction data can be analyzed by ML algorithms, which can also identify subtle patterns and adjust to changing fraud tactics. Machine learning models, in contrast to conventional techniques, have the capacity to continuously learn from fresh data and enhance their detection skills over time. Because of this, they are very successful at detecting fraud in real time in dynamic settings like UPI.

Classification and anomaly detection are the core functions of machine learning in fraud detection. Supervised learning algorithms can accurately classify future transactions by training on transaction data from the past that has been classified as either legitimate or fraudulent. As an alternative, unsupervised learning techniques can spot data anomalies or outliers that might point to fraud, even in the absence of examples with labels. Machine learning can take into account a variety of factors in the case of UPI, including transaction amount, transaction time, frequency, device information, geolocation, and user behavior patterns. [3]

A substantial amount of research has been done in the last ten years to investigate the potential of machine learning methods for identifying financial fraud, including that which takes place via digital payment systems like UPI. These studies cover a wide range of topics, from traditional supervised learning models to more sophisticated deep learning and hybrid techniques.

One of the first reviews of data mining methods for fraud detection was given by Phua et al. (2010). Their thorough analysis examined the effectiveness of supervised, unsupervised, and hybrid models in a range of financial domains and emphasized the need for real-time detection systems. The study set the stage for further investigation into scalable and dynamic approaches to managing transaction data with high velocity. [4], [5]

In the context of credit card fraud, Bhattacharyya et al. (2011) compared various machine learning models, including Random Forests, Neural Networks, Decision Trees, and Logistic Regression. Although the work focuses on credit card transactions, there are significant similarities to UPI fraud scenarios, particularly when it comes to class imbalance and the need for real-time detection.

Sahin et al. (2013) suggested cost-sensitive learning strategies to address class imbalance, a significant issue in fraud detection. Their research demonstrated that model precision could be greatly increased without negatively affecting recall by appropriately weighting the minority fraud class. This is especially important for UPI fraud detection, where fraudulent transactions are uncommon but crucial. [6]

Sharma and Kalra's (2021) more recent study focused on UPI fraud detection. Using Random Forest and SVM algorithms, they created a predictive model that showed that device consistency, transaction velocity, and time-based features (like odd transaction hours) were important predictors of fraud. Their model's high recall shows how useful behavioral features are in UPI situations.

Singh and Saha (2022) made another significant contribution by using Long Short-Term Memory (LSTM) networks to model UPI transactions sequentially. Their method successfully identified anomalies that might not be visible in static feature sets and captured the temporal dependencies in user behavior. The significance of comprehending user-specific transaction sequences was emphasized by this deep learning-based approach. [7], [8]

Ahmed et al. (2016) investigated unsupervised anomaly detection methods like autoencoders, DBSCAN, and isolation forests. These models were particularly helpful when there was a lack of labeled data or when fraud trends were continuously changing. Their results lend credence to the use of anomaly-based models in a rapidly expanding transaction ecosystem such as UPI.

Jurgovsky et al. (2018) investigated a hybrid strategy that combined supervised and unsupervised learning, utilizing feature-based ensemble methods in conjunction with recurrent neural networks. Their hybrid system showed that a more reliable fraud detection pipeline was created by fusing feature classification and temporal modeling. More and more people believe that fraud detection systems will go in this dual-strategy direction in the future. [9]

Additionally, a study by Dwivedi and Varshney (2020) investigated how SMOTE and GANs (Generative Adversarial Networks) can be used to generate synthetic data in order to address the lack of fraud samples. Their findings showed higher detection rates and models that were more broadly applicable to a variety of fraud situations.

When taken as a whole, this literature review shows that machine learning provides supervised, unsupervised, and hybrid approaches for developing intelligent and flexible fraud detection systems. The knowledge gathered from these investigations emphasizes how crucial feature engineering, class balancing, real-time processing, and sequential modeling are to improving UPI fraud detection models. [10], [11]

3. EXISTING SYSTEM

To detect fraudulent activity, the current UPI transaction systems mainly rely on manual intervention and rule-based detection methods. These systems keep an eye on suspicious transactions using pre-established rules, like transaction limits, frequency thresholds, or flagged geographic areas. Transactions coming from unidentified locations or surpassing a specific threshold, for example, might be marked for review. Although this method provides a fundamental level of fraud detection, it is unadaptable and inflexible when dealing with quickly changing fraud patterns [6], [8]

Additionally, traditional systems mainly rely on user-reported complaints and manual audits, which can delay the detection and response to fraudulent activity. This reactive strategy frequently permits fraudulent transactions to remain undetected until serious harm has been done. Furthermore, it is difficult to identify complex fraudulent behaviour that involves several subtle indicators rather than just one anomaly due to a lack of intelligent data analysis [9].

The high rate of false positives and false negatives is another significant drawback of the current systems. While sophisticated fraudulent activities may go unnoticed because the system is unable to analyse the relationships between different transaction parameters, many legitimate transactions are flagged as suspicious, which inconveniences users. These rule-based approaches fall short of offering a scalable, real-

time, and flexible way to adequately safeguard the expanding digital payment ecosystem as the volume of UPI transactions keeps growing at an exponential rate [12].

4. PROPOSED SYSTEM

This project, "UPI Fraud Detection using Machine Learning," offers a thorough method for identifying fraudulent transactions through the use of cutting-edge machine learning techniques. Python is the primary programming language used in the solution's construction, and SQLite3 is used to safely manage and store user information. In order to improve model efficiency, data preprocessing included handling missing values, correcting class imbalances, and selecting features using techniques like Lasso regression. Based on characteristics like transaction frequency, amount, location, device details, and user behaviour, the potent gradient boosting algorithm XGBoost was trained and refined to provide high predictive accuracy.

With the help of an HTML and CSS web interface, the trained model was easily integrated into a Flask-based backend, giving users a straightforward and safe way to enter transaction information like the amount, credit card number, payment method, CVV, expiration date, etc. After submission, the backend system applies the machine learning model, extracts the necessary features, and decides whether to approve the transaction or mark it as suspicious. This project provides a scalable and real-time fraud detection system that helps make digital financial transactions safer by showcasing the useful application of machine learning to improve UPI security.

The project's outcomes show how machine learning can improve UPI transaction security by offering a scalable and efficient fraud detection solution. The ongoing efforts to safeguard users from fraudulent activity and secure digital financial systems are aided by this work.

5. IMPLEMENTATION

Creating a real-time web application that incorporates machine learning techniques is necessary to implement the UPI Fraud Detection system in order to accurately and efficiently identify fraudulent transactions. The following elements and procedures are used in the system's implementation:

1. Environment and Programming Language

- Python is the main language used for data processing, backend integration, and model development.
- Models are trained, tested, and evaluated using Jupyter Notebook.
- The backend framework for managing requests and answers is Flask.

2. Gathering and Preparing Data

- Payment method, transaction amount, credit card number, CVV, and transaction metadata are among the features that are gathered from past transactions.
- The purpose of data cleaning is to eliminate anomalies, duplicates, and missing values.
- Encoding categorical variables, scaling numerical features, and, if necessary, managing unbalanced datasets with methods like SMOTE are all part of feature engineering.

3. Development of Machine Learning Models

- Extreme Gradient Boosting, or XGBoost, is chosen for classification tasks due to its high accuracy and effectiveness.
- Training and testing sets are separated from the dataset (e.g., 80:20).
- To determine whether a transaction is fraudulent or legitimate, the model is trained using pertinent features.
- Metrics like accuracy, precision, recall, F1-score, and confusion matrix are used to assess performance.

4. Integration of Databases

- Prediction logs, transaction records, and user information are all stored in SQLite3.
- To safely preserve user credentials, transaction history, and fraud detection results, a structured schema is used.

5. Development of Web Applications

- Frontend: a straightforward and easy-to-use interface created with HTML and CSS.
- User requests like login, registration, transaction submission, and fraud check requests are handled by the backend (Flask).
- Paths:
  - ✓ To register as a user, use /register.
  - ✓ For authentication, use /login.
  - ✓ To submit transaction details, use /transaction.
  - ✓ To predict fraud, use /predict.

6. Workflow for Fraud Detection

- After logging in, the user enters the transaction information (card number, CVV, amount, and payment method).
- Data is retrieved and verified by Flask.
- The trained XGBoost model receives the data.

- The transaction is predicted by the model to be either legitimate or fraudulent.
- The system either approves the transaction or marks it for additional examination based on the prediction.
- For the purposes of monitoring and retraining, prediction results are recorded in the database.

7. Safety Procedures

- Before being stored or processed, sensitive information such as CVV and credit card numbers is encrypted.
- To stop unwanted access, authentication procedures are in place.

8. Implementation

- The Flask application is set up on either a cloud platform or a local server.
- For real-time predictions, the web application incorporates the machine learning model, which is saved using joblib/pickle.

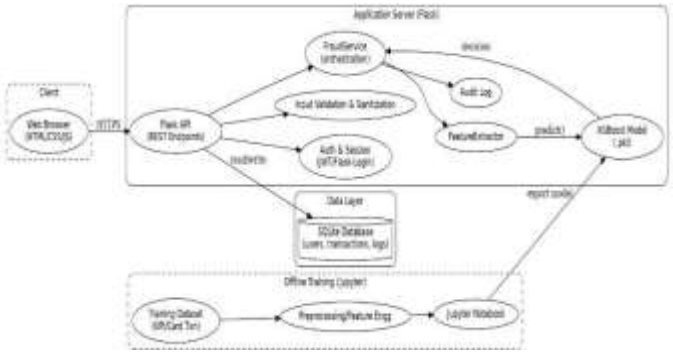

Fig. 1 System Architecture

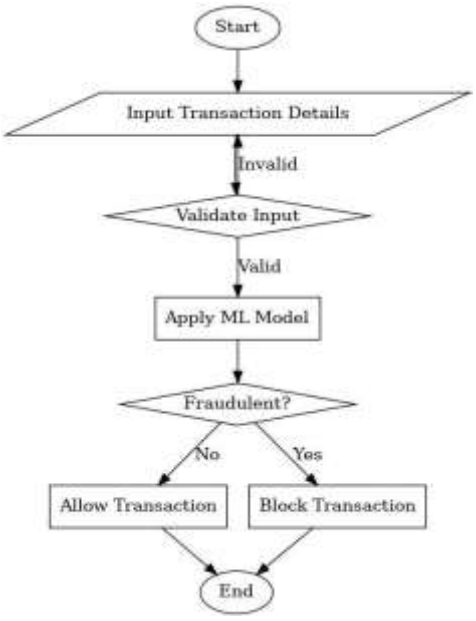

Fig. 2 Flow Chart

6. CONCLUSION

The "UPI Fraud Detection using Machine Learning" project offers a thorough and efficient method for locating and stopping fraudulent transactions in Unified Payments Interface (UPI) systems. Through the use of sophisticated machine learning algorithms like XGBoost, the system detects anomalies with high accuracy and delivers real-time fraud alerts via an easy-to-use web application interface.

Promising developments in identifying and stopping UPI fraud are provided by machine learning. Financial institutions can greatly improve the security and reliability of digital payment systems by employing a variety of algorithms and continuously improving the models based on transaction data. However, issues like real-time scalability, model accuracy, and data privacy continue to be crucial factors for realistic implementation.

To provide a trustworthy fraud detection mechanism, this methodology combines strong data preprocessing techniques, effective Flask backend processing, and secure SQLite3 database integration. The development of adaptive systems that can learn and get better over time is crucial to guaranteeing the security of UPI transactions and shielding users from financial risks as fraud tactics continue to change.

By encouraging safer digital payment methods and assisting users and financial institutions in staying ahead of new fraud threats, this project ultimately helps to create a more secure and reliable digital economy.

7. FUTURE ENHANCEMENTS

1. Combining Deep Learning Models

In order to better analyse sequential transaction data, future iterations of this project can integrate deep learning techniques like Gated Recurrent Units (GRU) or Long Short-Term Memory (LSTM) networks. Traditional machine learning models may miss intricate and non-linear fraud patterns, but these models are able to capture them. This will improve the fraud detection system's precision and flexibility in quickly changing fraud situations.

2. Processing Large Data in Real Time

Large-scale UPI systems can manage high transaction volumes by integrating real-time big data processing frameworks like Spark Streaming or Apache Kafka. This would ensure quicker fraud detection and lower the latency between transaction initiation and fraud alert generation by enabling the system to process and analyse massive data streams instantly.

3. Mechanism of Adaptive Learning

Patterns of fraud are dynamic and evolve over time. The system will be able to learn continuously from new data without needing to be completely retrained by incorporating online or adaptive learning techniques. This guarantees that the model

maintains high detection accuracy and stays current with new fraud trends.

4. Authentication with multiple factors (MFA)

System security can be improved by implementing MFA for transactions that are flagged or considered high-risk. To confirm the validity of a transaction before processing, this may entail incorporating One-Time Passwords (OTP), biometric authentication (facial recognition or fingerprint), or device fingerprinting.

5. Implementation of Explainable AI (XAI)

Explainable AI techniques can be used to provide an explanation for a transaction's fraudulent flag, increasing transparency and user trust. This feature would ensure accountability and lower false dispute claims by assisting end users, auditors, and financial institutions in understanding the model's decision-making process.

6. Integration of Cross-Bank and Multi-Payment Platforms

The system can be extended to include more digital payment platforms and banks. This would improve the security of digital payments across the country by establishing a single fraud detection ecosystem that can keep an eye on a variety of transaction channels.

7. Profiling User Behaviour

Building dynamic user profiles based on variables like transaction frequency, geolocation, device usage, and spending patterns is possible with the use of advanced behavioural analytics. Early fraud warnings may be triggered by any notable departure from these pre-established profiles.

8. Development of Mobile Applications

A specialized mobile application can be created to improve accessibility and monitoring convenience. Administrators and users would be able to view transaction history, handle flagged transactions, and get real-time fraud alerts all from their smartphones.

8. REFERENCES

[1] Nakra, V., Pandian, P. K. G., Paripati, L., Choppadandi, A., & Chanchela, P. (2024). “Leveraging machine learning algorithms for real-time fraud detection in digital payment systems”. International Journal of Multidisciplinary Innovation and Research Methodology.

[2] Kavitha, J., Indira, G., Kumar, A. A., Shrinita, A., & Bappan, D. (2024). “Fraud detection in UPI transactions using ML”. EPRA International Journal of Research & Development.

[3] S. Jagadeesan, K. S. Arjun, G. Dhanika, G. Karthikeyan, and K. Deepika, "UPI fraud detection using machine learning," in Challenges in Information, Communication and Computing Technology, V. Sharmila et al., Eds. London: Taylor and Francis, 2025. https://www.taylorandfrancis.com.

[4] Y. Gupta, N. Saxena, and K. Kumar, "UPI fraud detection using machine learning," International Journal of Advances in Engineering and Management (IJAEM), Oct. 2024. https://www.ijaem.net.

[5] Navaneetha Talari, M. Geetha, Bellamkonda Nuthana, and Remalli Rohan, "Real-Time Fraud Detection in Online Payments: A Comprehensive Review of Machine Learning Techniques," International Journal of Progressive Research in Engineering Management and Science (IJPREMS), Dec. 2024. https://www.doi.org/10.58257/IJPREMS37828.

[6] S. Sharma and M. Kalra, “Fraud detection in UPI transactions using supervised machine learning techniques,” in Proc. Int. Conf. Mach. Learn. Data Sci. (ICMLDS), Springer, 2021.

[7] Sridevi N., A. Singh, A. G., G. Gupta, and G. Shandil, "A Review on UPI Fraud Detection using Machine Learning and Deep Learning," International Journal for Research in Applied Science and Engineering Technology (IJRASET), Dec. 2024.

[8] J. Sindhu and V. S. Swarupa, "UPI Fraud Detection Using Machine Learning Algorithms," International Journal of Engineering Research and Science & Technology (IJERST), Oct. 2024. https://ijerst.org/index.php/ijerst/article/view/446.

[9] B. Liu, X. Chen, and K. Yu, "Online Transaction Fraud Detection System Based on Machine Learning," Journal of Physics: Conference Series, 2021. https://iopscience.iop.org/article/10.1088/1742-6596/2023/1/012054.

[10] M. Nazmoddin, M. Swetha, G. Yashwanthi, and Y. Divyasree, "UPI Fraud Detection Using Machine Learning," Journal of Computational Analysis and Applications (JoCAAA),Sep.2024. https://eudoxuspress.com/index.php/pub/article/view/1875.

[11] M. Yasir, N. S. Reddy, N. R. Reddy, A. Nithin, and M. Akki, "Review on UPI Fraud Detection using Machine Learning," International Journal for Research in Applied Science and Engineering Technology (IJRASET), Dec. 2024. https://www.ijraset.com/research-paper/review-on-upi-fraud-detection-using-machine-learning.

[12] R. K. Inampudi, T. Pichaimani, and Y. Surampudi, "AI-Enhanced Fraud Detection in Real-Time Payment Systems: Leveraging Machine Learning and Anomaly Detection to Secure Digital Transactions," Australian Journal of Machine Learning Research & Applications, vol. 2, Mar. 2022. https://sydneyacademics.com/index.php/ajmlra/article/view/189.

[13] J. Arjun, D. Karthikeyan, and D. Deepika, "UPI Fraud Detection Using Machine Learning," in Challenges in Information Security, 1st ed., CRC Press, pp. 1301–1308, Jan. 2025.

https://www.taylorfrancis.com/chapters/oaedit/10.1201/9781003559085-130/upi-fraud-detection-using-machine-learning-jagadeesan-arjun-dhanika-karthikeyan-deepika.

[14] Bindela, A., Lakshminath Reddy, C., Bhavana, P., Anitha, C., & Jayasimha Raju, B. (2025). UPI Fraud Detection using Machine Learning. International Journal of Multidisciplinary Research (Vol. 7, Issue 2, March–April 2025).

[15] R. Rani, A. Alam, and A. Javed, "Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions," in Proceedings of the 2024 2nd International Conference on Disruptive Technologies (ICDT), Mar. 2024. https://www.researchgate.net/publication/379775058_Secure_UPI_Machine_Learning-Driven_Fraud_Detection_System_for_UPI_Transactions.

[16] Sakshith A. R., & Shashidhar Kini K. (2025). UPI Fraud Detection Using Machine Learning: A Predictive Model with Random Forest, XGBoost, and LSTM. Journal of Emerging Technologies and Innovative Research (JETIR), Vol. 12, Issue 7, July 2025.

[17] Aishwarya Murkute, Deepali Jadhav, & Yuvaraj Patil. (2025). UPI Fraud Detection Using Machine Learning: Voting Classifiers Combining RF, LR, DT, and SVM. International Journal of Creative Research Thoughts (IJCRT), Vol. 13, Issue 4, April 2025.

[18] Agrawal, P., Garg, S., & Gupta, S. (2025). Fraud Detection in UPI Transactions. International Journal for Multidisciplinary Research (IJFMR), Vol. 7, Issue 2, March–April 2025. This study explores supervised, unsupervised, and semi-supervised learning techniques (including anomaly detection algorithms) combined with effective feature selection to detect unusual patterns in UPI transaction data, enhancing real-time fraud monitoring and adaptive learning strategies.

[19] Vitthal B. Kamble, Krushna Pisal, Pranav Vaidya, & Sahil Gaikwad. (2025). Enhancing UPI Fraud Detection: A Machine Learning Approach Using Stacked Generalization. International Journal of Multidisciplinary on Science and Management, Vol. 2, No. 1, pp. 69–83.

[20] Aishwarya Murkute, Deepali Jadhav, & Yuvaraj Patil. (2025). UPI Fraud Detection Using Machine Learning. International Journal of Creative Research Thoughts (IJCRT), Vol. 13, Issue 4, April 2025.