UPI Fraud Detection Using ML

N. Jayamma[1], Ballatigi Anvitha[2], Uppara Suma Harikha[3], Dhotray Kalyani[4], B. Devi[5]
[1]*Professor, Dept. of Computer Science and Engineering (Artificial Intelligence), St. Johns College of Engineering and Technology, Yemmiganur 518301, India*
[2,3,4,5]*Dept. of Computer Science and Engineering (Artificial Intelligence), St. Johns College of Engineering and Technology, Yemmiganur 518301, India*

***Abstract*—Rapid growth in Unified Payment Interface (UPI) systems made digital payments much more convenient, but this growth also brought with it cases of fraudulent activity in digital transactions. Conventional rule-based techniques to handle fraudulent activity are often found to be ineffective in detecting subtle changes in fraudulent activity, often resulting in misleading results. In this regard, this present research proposes that machine learning-based techniques be used to generate a fraudulent activity detector system for digital transactions made through Unified Payment Interface systems, which accurately identifies fraudulent activity by employing machine learning algorithms that analyze transaction activity. Unlike conventional techniques, which often fail to produce accurate results, machine learning techniques can accurately distinguish between fraudulent activity undertaken in Unified Payment Interface digital transactions. For this purpose, this present research proposes that Logistic Regression, Random Forest, and XGBoost machine learning techniques be employed to produce accurate results, as these machine learning techniques are quite accurate in detecting subtle changes in fraudulent activity, which makes this proposed model much superior to conventional techniques for detecting fraudulent activity in Unified Payment Interface digital transactions.**

***Index Terms*—UPI Fraud Detection, Machine Learning, Digital Payment Security, Financial Fraud Analysis, Transaction Monitoring, Supervised Learning, Anomaly Detection**

I. INTRODUCTION

This revolution in adopting digital payment systems has completely changed the financial environment, where the unified payment interface has turned out to be one of the popular systems in executing real-time transactions. This digital payment method facilitates instant, secure, and convenient transactions, which are considered to be the major advantages for the users who choose to transfer funds using the UPI platform. However, the growing number of transactions conducted using the UPI platform has led to the execution of fraudulent activities like unauthorized access, phishing attacks, identity theft, and transaction tampering. These have turned out to be major risks for the users and financial institutions, causing them to suffer financial losses and lack of trust in online transactions systems.

To counter these challenges, machine learning methods have shown potential in resolving issues through automatically learning patterns from past transactional records. Using complex relationships in characteristics like transaction value, frequency, location, and time, machine learning approaches can effectively identify fraudulent transactions. Supervised learning algorithms enable fraud detection systems to learn and improve continuously based on fresh data.

The main aim of this project is to develop a machine learning-based UPI fraud detection system, which improves accuracy and reduces false alarm occurrences. The proposed project, therefore, seeks to offer real-time fraud identification, enhance security for UPI, and assist financial organizations in preventing fraud effectively. The intelligent data-driven technology, offered by this project, helps in creating a safe and reliable digital payment platform.

II. SYSTEM ARCHITECTURE

The system architecture for the UPI Fraud Detection project is implemented for efficient processing of transactions and detection of fraudulent activities

using machine learning algorithms. The architecture for this project includes UPI transactions collected from users or financial systems, where attributes such as transaction amount, date and time, and frequency of transactions are included. This collected information is then used as an input to a data preprocessing module for processing transactions where missing values are handled and noise is removed. The pre-processed information is then used as an input for machine learning model training. In this module, a model is trained for detecting fraud transactions. The trained model then classifies transactions as genuine or fraudulent. The outcome of this classification will then indicate whether an alarm is raised for such transactions. The idea is to provide alerts for suspicious transactions.

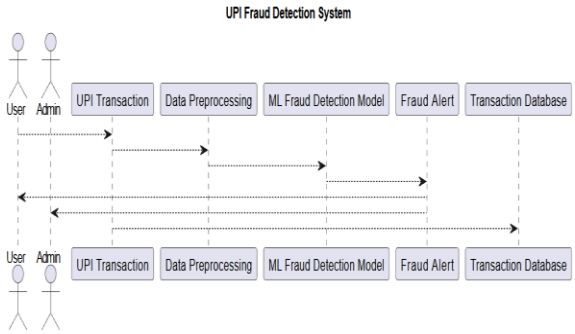

Fig: System Architecture of the UPI Fraud Detection

III. METHODOLOGY

A. Data Collection and Preprocessing

The methodology will start with collecting UPI transaction data from reliable sources, such as simulated banking datasets or real-world anonymized transaction records. Attributes to be considered within the dataset consist of, but are not limited to, transaction amount, transaction time, sender and receiver identifiers, transaction frequency, and the transaction status. Data preprocessing improves data quality to ensure model accuracy. This consists of handling missing values, removal of duplicate or inconsistent records, and numerical feature normalization. The categorical attributes are encoded using appropriate encoding techniques, such as label encoding or one-hot encoding. Detection and treatment of outliers and noisy data are identified to avoid model bias. Feature selection will be carried out in terms of retaining only those attributes relevant to the fraud detection mechanism. Pre-processed data will then be divided into training and testing datasets to provide for an effective model evaluation. Proper data preprocessing ensures that machine learning algorithms learn meaningful patterns and improves the overall system performance.

B. Machine Learning Model Development

At this stage, the fraud detection model is built using supervised machine learning algorithms. Some of the common algorithms used are Logistic Regression, Random Forest, and XGBoost. These algorithms are trained on the pre-processed dataset with labelled transaction outcomes. The models learn patterns from the transaction behaviour that distinguish fraudulent transactions from legitimate ones. Next, hyperparameter tuning is done for optimizing model performance and reducing overfitting of models. Then, models are evaluated for their performance by metrics such as accuracy, precision, recall, F1-score, and ROC-AUC. Among the different trained models, the best performing model is selected for deployment. To handle one of the major challenges in fraud detection-class imbalance-resampling or class weighting techniques can be used. This stage will definitely ensure a robust and reliable fraud detection model which can adapt to different evolving fraud patterns.

C. Fraud Detection and System Deployment

Following the process of model development, validation, and tuning, the selected machine learning model is implemented and integrated within the fraud detection system. Consequently, the machine learning model receives the UPI transactions for real-time analysis and detection. These transactions undergo the same stages within the machine learning pipeline before the model classifies a fraud detection outcome within a short period. If the machine learning model gives a fraud outcome for the processed transactions, the system generates an alert and informs the user or bank administrator about the transactions for further acknowledgment and validation. Further, all the transactions and the fraud detection outcome are maintained within a database for proper monitoring

and improvement of the machine learning model for further effectiveness and accuracy. Nevertheless, the proposed strategy creates an efficient and sound means for fraud detection purposes within the digital payment systems and UPI transactions.

D. Model Evaluation and Performance Analysis

Model evaluation is an essential step where the evaluation results are obtained to assess the effectiveness of the proposed UPI fraud detection system. After the trained machine learning model is developed, the effectiveness of the machine learning model is tested with different transaction data to assess the generalization capability of the machine learning model. For the machine learning model to assess the effectiveness, different metrics or methods are adopted to assess the accuracy of the machine learning model. In the context of UPI transaction fraud detection, the accuracy metrics considered are accuracy, precision, recall, F1-score, and confusion matrix analysis. In the context of machine learning or fraud detection, the accuracy metrics considered are receiver operating characteristics curves and the area under the curve analysis. Additionally, a comparative analysis is carried out to assess the different machine learning algorithm effectiveness in the context of the proposed UPI transaction fraud detection system. The effectiveness results are obtained from the machine learning algorithm to assess the different metrics related to the machine learning algorithm effectiveness, i.e., accuracy, precision, recall, etc. After the effectiveness analysis, the machine learning model parameters are updated to assess the accuracy results for the proposed UPI transaction fraud detection.

Component	Technology Used
Frontend	HTML5, CSS3, JavaScript
Backend	Python, Flask (REST APIs)
Database	SQLite
Machine Learning	Random Forest Classifier
Data Processing	Pandas, NumPy
Feature Engineering	Label Encoding, Normalization
Email Alerts	SMTP

IV. IMPLEMENTATION

The proposed UPI system for fraud detection is built in such a modular fashion that it can be easily upgraded, modified, and in case of failures, it can be handled effectively. The system comprises varied individual modules that work in conjunction to provide efficient fraud detection in real-time. The backend of the proposed system is built using Python with support from the Flask platform, as it allows RESTful APIs to be created, and communication between various modules of the system works effectively through these APIs.

The system, which makes up the backend, has different functional blocks. There is one block that caters to the validation and authentication of transactions for the user, which can be carried out with the help of the UPI system. Another block processes the UPI transaction data, which comprises specific parameters such as the amount, time, and pattern associated with the UPI transactions the user undertakes. The machine learning block uses the features and values associated with the transaction, which can help design the system for fraudulent predictions with the help of historical data associated with the transactions that are carried out.

SQLite is used as the database to store transaction records, user information, or prediction results in a secure manner. SQLite is used as the database in this system, as it provides much simpler configuration to set up with minimal requirements to run as a separate server. All kinds of transaction logs or fraudulent activity notifications are stored in the database, which can be used as future training material for the machine learning models. In this proposed system, HTML5, CSS3, JavaScript, etc., are used to develop the frontend of the system, which makes this system much simpler for users to interact with. In this proposed system, data visualization techniques, including charts or graphs, are used to represent or display fraudulent statistics or trends, which helps to give insights to end users or system administrators regarding how this system works or how it can be used to avoid fraudulent situations or acts. Email notifications or alerts are sent

to keep track of fraudulent activities or situations while transactions take place.

V. RESULTS AND DISCUSSION

On the proposed UPI fraud detection system, the experiment has been performed for the considered transactions gathered from different users at different time intervals. For further understanding, the proposed system performed well in the detection and differentiation between fraudulent and valid transactions. In addition to that, the proposed Random Forest classifier has shown accurate detection and low false detection rates for the transactions. Moreover, the proposed systems have successfully inspected the different characteristics associated with the transactions, and the experiment has proved the detection mechanisms for the fraudulent behaviour patterns.

Based on the above-mentioned outcomes, it has been declared that the developed model meets its objectives for providing security in terms of transaction and minimizing fraud risks for UPI-based payment systems. The practical implementation has significantly justified how machine learning is helpful in increasing accuracy for fraud detection purposes, contemplating its applications in rule-based systems. The model has further scope for enhancement for its practical uses in banking scenarios.

VI. ADVANTAGES AND APPLICATIONS

Advantages

Early Fraud Risk Identification:

The proposed UPI fraud detection system facilitates the early detection of suspicious and potentially fraudulent transactions. In this context, the system keeps a tab on the patterns of the transaction, such as the amount, number of times the same amount of money is being transferred, time of the transaction, and other factors. These factors enable the detection of any suspicious activity at an early stage. This assumes significance because any fraudulent individual can undertake several transactions within a small-time frame. In this respect, the proposed fraud detection system for UPI essentially assumes the role of a protective layer for the users.

Risk Score Classification:

The system assigns a fraud risk score to each transaction, making it easy to understand the severity of risk involved.

Readiness Score Range	Category
0 – 40	High Risk
40 – 70	Medium Risk
70 – 100	High Ready

This scoring mechanism helps banks and users decide whether a transaction should be allowed, flagged, or blocked.

Explainable Machine Learning Predictions:

The system supports UPI transactions via real-time processing. The moment a transaction occurs, it is analyzed using machine learning, and thus, the result comes up instantaneously. The dashboards are also up-to-date at any moment as new data from transactions comes up.

Reduced Manual Monitoring Effort:

Automation in the detection of fraud reduces the necessity for monitoring transactions carried out by individuals in the course of work at a bank. This reduces human error and saves time for the personnel to handle suspicious transactions only.

Improved Security and User Trust:

By preventing unauthorized transactions and providing instant alerts, the system increases user confidence in UPI platforms. Strong security leads to higher adoption of digital payment systems.

Applications

UPI Transaction Fraud Detection:

The system has the potential for use in detecting fraudulent UPI transactions by both banks and payment service providers.

Banking and Financial Institutions:

Moreover, the banking industry can utilize the system for monitoring transactions and checking losses, thus enhancing strategies for fraud control.

Customer Alert and Protection Systems:

The system is capable of notifying the users in real time to take prompt action against suspicious transactions through alerts. Regulatory and Compliance Support: Information stored on transaction logs and reports of fraud can enable a financial institution to comply with regulations and perform audits. Predictive Fraud Prevention: With data analysis, historical data helps organizations and

institutions anticipate fraud patterns and improve security measures in the future.

VII. CONCLUSION

The purpose and description of this project are based on providing a Machine Learning-based UPI Fraud Detection System. The main purpose of providing this type of system and model is to increase the level of security for users. Due to increased usage and popularity, fraud has become a significant issue for users and organizations who allow Unified Payments to function. The proposed model is capable of analysing and detecting fraud through supervised machine learning techniques, specifically by applying Random Forest.

The system supports real-time monitoring, explainable predictions, and alerting. Thus, it is an efficient tool for contemporary online payments. It minimizes dependencies on conventional rule-based approaches, increases detection accuracies, and reduces false alert issues. The system application proves that ML processes will further support fraud detection and defence processes. In conclusion, this application will further assist UPI operations for reliable online deals, trust UPI users, and better manage fraud risks for financial institutions. With further development and enhancement of this system, it will be applicable for use in online banking.

ACKNOWLEDGMENT

I would like to extend my sincere gratitude towards my project guide for their continuous guidance, valuable suggestions, and encouragement throughout the completion of this project. I am also thankful to all the faculty members of the department for their support and technical assistance during the project development.

I would like to thank my institution immensely for providing the right infrastructure, resources, and learning environment needed to pursue this work successfully. Lastly, I would like to thank my family and friends for continuous motivation, patience, and support without which it was not possible to remain focused and successfully complete this venture.

REFERENCES

[1] Dal Pozzolo, A., Bontempi, G., Snoeck, M., & Snoeck, C., "Adversarial drift detection for fraud detection," IEEE International Conference on Data Mining, 2015.

[2] Bahnsen, A. C., Aouada, D., & Ottersten, B., "Costsensitive decision trees for fraud detection," Expert Systems with Applications, vol. 39, no. 5, 2012.

[3] Carcillo, F., Dal Pozzolo, A., Snoeck, M., Bontempi, G., & Snoeck, C., "Scarff: A scalable framework for streaming credit card fraud detection," Information Fusion, 2021.

[4] Phua, C., Lee, V., Smith, K., & Gayler, R., "A comprehensive survey of data mining-based fraud detection research," arXiv preprint arXiv:1009.6119, 2010.

[5] Dal Pozzolo, A., Boracchi, G., Bontempi, G., & Snoeck, C., "Credit card fraud detection: A realistic modeling and new public dataset," IEEE Intelligent Systems, 2015.

[6] Breiman, L., "Random forests," Machine Learning, vol. 45, no. 1, 2001.

[7] Chandola, V., Banerjee, A., & Kumar, V., "Anomaly detection: A survey," ACM Computing Surveys, vol. 41, no. 3, 2009.

[8] Kaggle, "Credit Card Fraud Detection Dataset," Available: Kaggle Repository, 2018.

[9] Goodfellow, I., Bengio, Y., & Courville, A., Deep Learning, MIT Press, 2016.

[10] Reserve Bank of India (RBI), "Guidelines on Digital Payment Security Controls," RBI Publications, India.

[11] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C., "Data mining for credit card fraud: A comparative study," Decision Support Systems, 2011.

[12] UPI NPCI, "Unified Payments Interface – Product Overview," National Payments Corporation of India, 2023.

[13] Zanin, M., et al., "Machine learning approaches for fraud detection in financial transactions," IEEE Access, 2018.

[14] Friedman, J., Hastie, T., & Tibshirani, R., The Elements of Statistical Learning, Springer, 2009.

[15] Scikit-learn Developers, "Machine Learning in Python," Journal of Machine Learning Research, vol. 12, 2011.