International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Fraud Detection in UPI Transcations

Mohanapriya J [1], Dr.B.Leelavathi[2]

[1] Undergraduate Student [2] Professor Department Of computer Technology, Dr.N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India

https://doi.org/10.55041/ijsmt.v2i3.065

Cite this Article: J, M. (2026). Fraud Detection in UPI Transcations. International Journal of Science, Strategic Management and Technology, *02*(03). https://doi.org/10.55041/ijsmt.v2i3.065

Abstract

The digital payment landscape in India has undergone a paradigm shift with the advent and widespread adoption of the Unified Payments Interface (UPI). While UPI has democratized access to cashless financial services, its exponential growth has been accompanied by a surge in sophisticated fraudulent activities, ranging from high-value transaction manipulation to unauthorized device usage. Traditional rule-based detection mechanisms often fail to adapt to these evolving threat vectors, resulting in high rates of false negatives. This paper proposes a robust machine learning framework leveraging the XGBoost classification algorithm to detect fraudulent UPI transactions in real time. The system integrates diverse attributes, including transaction velocity, device novelty, and merchant risk profiles, and utilizes Scikit-learn's Standard Scaler for feature normalization. Deployed via a Flask-based web application, the model provides instantaneous fraud probability scores. Theoretical analysis and methodological design suggest that this approach offers a scalable, high-confidence solution for securing the modern digital payment ecosystem against dynamic financial threats.

Keywords: UPI Fraud Detection, Machine Learning, XGBoost, Digital Payments, Financial Security, Transaction Monitoring

INTRODUCTION

The rapid expansion of digital payment technologies has fundamentally transformed the financial ecosystem in India, positioning the country as a global leader in real-time cashless transactions. The Unified Payments Interface (UPI) serves as the backbone of this revolution, enabling instant, peer-to-peer, and peer-to-merchant transfers with unprecedented ease. However, the increasing reliance on these digital platforms has introduced significant security challenges. As transaction volumes soar, so too does the incidence of fraudulent activities, including phishing attacks, remote screen mirroring scams, and unauthorized account access. The dynamic nature of these threats renders static security measures insufficient, creating an urgent need for intelligent defense mechanisms that can analyze behavioral patterns and transactional anomalies in real time.

Existing fraud detection systems largely rely on rule-based logic, such as static limits on transaction amounts or blacklisting known suspicious IP addresses. While these methods are easy to implement, they suffer from critical limitations. First, they are reactive rather than proactive; they can only detect fraud after a specific pattern has been identified and hard-coded, often leaving a window of vulnerability for new types of attacks. Second, they struggle to distinguish between legitimate high-frequency usage and actual fraud, leading to friction for genuine users. This inadequacy parallels challenges in other domains where identifying rare but critical events is essential. For instance, in astrophysics, standard methods often fail to find rare

metal-poor stars without advanced classification algorithms . Similarly, in the context of UPI, the subtle behavioral shifts indicating fraud require a non-linear, adaptive approach that traditional heuristics cannot provide.

To address these gaps, this paper presents a machine learning-based framework for real-time UPI fraud detection using the XGBoost classification algorithm. Our contributions are threefold:

1. We propose a comprehensive feature engineering strategy that combines transactional data (amount, time) with behavioral contexts (device novelty, transaction velocity, foreign transaction indicators).

2. We implement a robust preprocessing pipeline using Scikit-learn for feature normalization to ensure model stability across varied transaction magnitudes.

3. We present a deployment architecture using Flask that enables the model to function as a real-time web service, bridging the gap between offline model training and live transaction monitoring.

LITERATURE REVIEW

At a time when digital payments are evolving rapidly, fraud detection has become more important than ever in Fintech, as can be seen with UPI (Unified Payments Interface) enabling immediate Bank-to-Bank payments through Mobile Phones. UPI transactions are exploding and therefore the number of fraudulent UPI transactions is rising. And this should provide evidence of the need for a sophisticated fraud detection system to identify suspicious behaviour throughout the financial transaction process.

Research conducted recently on this subject has included many works using machine learning algorithms to find fraudulent uses of UPI. Khopade & Vitalkar [1] developed a model based on machine learning to detect fraud within UPI transactions through analysis of transaction attributes like: the amount of the transaction, time of transaction, behaviour of the user engaging in the transaction. This showed that machine learning can accurately detect when there are abnormal patterns within UPI transactions and subsequently lead to an increase in the ability for these types of systems to operate reliably for digital payments.

Sadaf & Manivannan [2] used the same methodology but with a different algorithm (Gradient Boosting) in order to enhance their fraud detection model. Data collected after using this method resulted in an improved ability to predict outcomes related to fraud by learning complex patterns in a dataset of transactions; and therefore improve the outcome of the classification based on this data than any of the traditional classification methods used prior to their study.

More research was done on multiple ML models used to detect fraudulent transactions. For example, a research paper by Sindhu & Swarupa [3] analyzed multiple Methods including Random Forests, Decision Trees, and Logistic Regression for detecting fraudulent transactions using UPI. The paper concludes that using ensemble learning algorithms increased the ability of the algorithm to identify fraudulent activities from financial datasets. Another study on detecting fraudulent UPI transactions [4] applied classification methods from machine learning to analyze transaction data in an effort to identify suspicious activities as they occur.

A number of researchers have also explored how tabular machine learning models can be used to detect financial fraud. Chaudhary et al. [5] looked at how machine learning-based models such as Random Forest and Gradient Boosting could be applied to structured datasets of transaction data. They found that these models are able to accurately identify fraudulent transactions based on a combination of transaction attributes, and they can do so with relatively high levels of accuracy. Additionally, Bhaskar et al. [6] designed a fraud detection system that uses machine learning algorithms to analyze transaction patterns, with the goal of finding (and thus preventing) fraudulent transactions in UPI payment systems.

Kavitha et al. [7] conducted a different study that showed the need to implement machine learning models to improve the security of digital payment systems. The results of the study found that fraud detection systems could significantly reduce financial loss through the early detection of questionable transactions through machine learning techniques. Additionally, Dahiphale et al. [8] presented a new method to improve the trust and safety of digital payment systems using large language models (LLMs). Their study found that AI methods could be effective in detecting fraud by studying complex financial patterns and user behaviour.

In addition to research specific to UPI, previous research on ways to identify potential fraud through financial means have played a key role in enhancing detection systems today. A comparative analysis of data mining methods used to identify credit card fraud was performed by Bhattacharyya et al. [9]. In this evaluation, the researchers demonstrated that machine learning models can effectively help identify fraudulent financial transactions. Additionally, Carcillo et al. [10] created a scalable method for real-time detection of fraud using large amounts of data and distributed computing systems. They noted that it is crucial to have a scalable framework in order to manage large amounts of data from financial transactions. . Additionally, B Leelavathi et al. [11] proposed a system for detecting network worms by analysing multiple, distinct features of executables to identify malicious behaviour, aiming for a high detection rate with low false positives.

METHODOLOGY

The overall research methodology creates a framework for developing machine learning-based UPI fraud detection system by combining a literature review, design the system, develop a model and validate through experiments. The main goal of this methodology is to create an intelligible fraud detection model that is technically dependably built and can be practically applied in real-world digital payment environments. Phase one consists of reviewing the current research on fraud detection in digital payment systems, credit cards, anomaly detection and financial cybersecurity. In reviewing the previous research completed between 2015 and 2024, various studies, IEEE conference and journal publications and FinTech reports were evaluated to determine how fraud detection systems are created and used.

The review included analysis on the types of machine learning algorithms commonly used, methods for managing an imbalanced dataset, developing feature engineering methods, and methods of evaluation. The primary purpose of this phase was to establish research gaps, as well as identify the need for a more efficient and interpretable fraud detection model that is specifically designed for UPI transactions.

In this project, we developed an initial theory or concept upon which to build the development of the application. After developing this concept, we followed a stepwise process using Software Development Life Cycle (SDLC) methodology to create the application.

We started with determining what was needed to develop the application based on functional requirements (e.g., transactions to be monitored; fraud prediction to occur, generation of alerts regarding high-risk transactions) and non-functional requirements (e.g., the application's performance, scalability, security-related items, and real-time response times).

With the above functional and non-functional requirements established, based upon our earlier understanding of what was required, a three-tier architecture was developed for the application as follows: The first tier (Presentation Layer) will provide an interface for the user to monitor their transactions, and for them to view the results of the fraud predictions; the second tier (Application Layer) will contain the machine learning model and all the data processing functions; and the third tier (Data Layer) will store historical transaction records and keep them secure.

Fraud detection datasets can be extremely large and imbalanced, meaning they often have a far greater number of legitimate than fraudulent transactions so there is special care taken during processing to handle issues relating to class imbalance. Various techniques such as over-sampling, under-sampling and cleaning are used in processing both legitimate and fraudulent transactions to ensure models have adequate training data available during the training process.

Cleaning the data ensures there are no inconsistencies (duplicate records) or any missing records in the data set. Numerical variables will need to be scaled before they can be processed by machine learning algorithms, and categorical variables will need to be encoded to make them compatible with machine learning algorithms

The importance of feature engineering in detecting fraudulent transactions is that it can improve detection performance. Besides basic transaction details like time and amount alone, there are also behavioral indicators that have significant effect on transaction fraud detection.

The different behavioral indicators consist of things like abnormal spending patterns, frequency of transactions and the timing of transactions not being normal. They provide the model with additional features

to help separate normal activity of the user and suspicious activity.

We used four different supervised machine learning algorithms to help figure out if transactions were fraud: logistic regression, decision trees, random forests and support vector machines.

When we got done with implementation of our models we evaluated them and divided our data into training and testing in order to find out how the model performed against transactions it had never seen before.

We evaluated each of these models on performance indicators such as accuracy, precision, recall, and f1-score. Recall is particularly important since not identifying a fraudulent transaction correctly could result in extreme financial loss.

In addition to this portion of the fraud detection system, we also added a risk scoring model which allows the model to generate a probability score for each transaction indicating whether or not it has potential to be "fraud." If the probability score exceeds a set threshold, that transaction will be flagged for either manual verification or automatically blocked. This greatly enhances the usability of the fraud detection system and supports decision-making in real-time.

After we're finished developing the system, we'll use test transactions on the system to check how accurate it is at predicting, how quickly it processes, and how reliable it is. We'll then analyze the results of those tests to ensure the system meets its intended objectives and is consistent.

Overall, this project uses a combination of theory, structured development of the system, and experimentation to develop a fraud detection system for UPI transactions using machine learning and a more structured development method.

The result will be a fraud detection system that is efficient, scalable, and secure for detecting fraud in digital transactions.

WORKFLOW

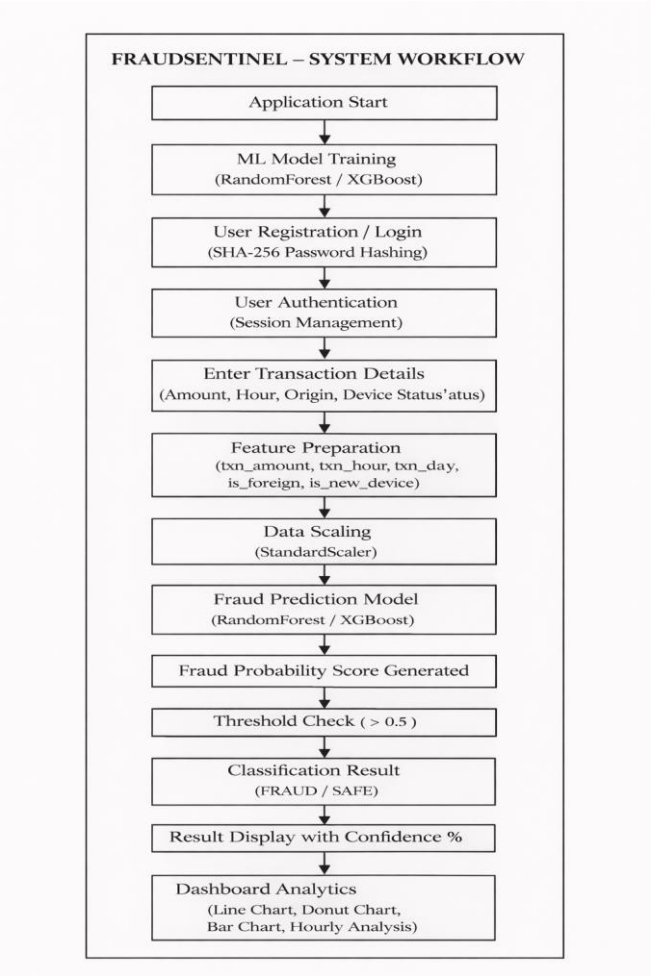

Figure1: *Workflow of Proposed Methodology*

CONCLUSION

In the digital age, we now rely on UPI transactions more than ever before because they provide a speedy and easy way to manage everyday transactions. However, along with these technological advances come increased opportunities for fraudulent activities.

To combat this increase in fraud, we at the FraudSentinel have created a system that combines secure authentication processes with machine-learning methods to detect fraud by identifying unusual transaction details (e.g., transaction amount, time, location, device information).

By using Random Forest and XGBoost techniques, we can determine whether each transaction is likely safe or fraudulent, resulting in a probability score to help facilitate your decision-making process. The FraudSentinel helps detect fraud in a more accurate manner than traditional rule-based systems throughout the transaction detection process.

The dashboard allows users and managers alike to view their transaction patterns and fraud data through visual charts and summary reports. This not only enhances overall accountability within the system but also aids in better tracking of finances and making decisions about what actions to take.

In general, FraudSentinel has shown that machine learning can be an effective tool to enhance security of digital payments. The FraudSentinel project is a practical, highly useable, and easily scalable project with potential applications in the "real" world. Future enhancements could include real-time connectivity with banks, more sophisticated anomalous behaviour detection algorithms, and expanding the size of the data set thereby increasing accuracy and efficiency.

Overall, this project has significantly improved the security and planning for digital payment systems.

REFERENCES

[1] N.P. Khopade & S.M. Vitalkar, "UPI Fraud Detection Using Machine Learning," International Journal of Research in Interdisciplinary Studies, 2025; vol. 3 (6): 24-26.

[2] R. Sadaf & R. Manivannan, "Enhanced Detection of Fraud in Unified Payments Interface (UPI) Transactions Using Gradient Boosting Method," International Journal of Interpreting Enigma Engineers, 2025

[3] J. Sindhu & V.S. Swarupa, "UPI Fraud Detection Using Machine Learning Algorithms," International Journal of Engineers Research and Science & Technology, 2024; vol. 20 (4): 57-67.

[4] "UPI Fraud Transaction Detection Using Machine Learning," International Journal of Engineers Research and Science & Technology, 2025; vol. 21 (4): 281-285.

[5] R. Chaudhary, S. Singh, R. Singh, H. Zaidi & K. Jain, "Fraud Detection in UPI Payments Using Tabular Machine Learning Models," International Journal for Research in Applied Science & Engineering Technology, 2025.

[6] V. Bhaskar, Abhishek, Hritik, Manjunath, and Sukanya, (2026) "UPI Fraud Detection Using Machine Learning" in International Journal of Science, Engineering and Technology.

[7] J. Kavitha, G. Indira, A. Anil Kumar, A. Shrinita, and D. Bappan, (2024) "Fraud Detection in UPI Transactions Using Machine Learning" in EPRA International Journal of Research and Development, Vol. 9, No. 4.

[8]D. Dahiphale et al. (2024) "Enhancing Trust and Safety in Digital Payments: An LLM-Powered Approach" on arXiV.

[9] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, (2011) "Data Mining for Credit Card Fraud: A Comparative Study" in Decision Support Systems, Vol. 50, No. 3, 602-613.

[10] F. Carcillo, A. Dal Pozzolo, Y. Le Borgne, O. Caelen, and G. Bontempi, (2017) "SCARFF: A Scalable Framework for Streaming Credit Card Fraud Detection with Spark" in IEEE Big Data Research.

[11] B. Leelavathi, "An Efficient Worm Detection System Using Multi Feature Analysis and Classification Techniques," *Springer Nature Link,* vol. pp 1054–1064, 2019.