International Journal of Research in Interdisciplinary Studies
Volume 3, Issue 6, June 2025
https://www.ijris.com | ISSN (Online): 2584-1017

UPI Fraud Detection Using Machine Learning

Nilam Prakash Khopade[1*], Shubhangi M. Vitalkar[2]
[1]Student, Department of MCA, Trinity Academy of Engineering, Pune, India
[2]Professor, Department of MCA, Trinity Academy of Engineering, Pune, India

Abstract—In recent years, digital transactions have surged, driven by convenience and accessibility, but this growth has also led to a rise in online payment fraud. According to the Reserve Bank of India, digital payment volumes and values increased by 216% and 10%, respectively, from March 2019 to March 2022. While consumers increasingly embrace digital payments, security concerns and a lack of awareness about safe online practices persist. Just a few years ago, online payments were rare, but today, UPI QR codes are commonplace, even at doorsteps. This widespread adoption has attracted fraudsters who exploit vulnerabilities to deceive users and siphon funds. Fortunately, digital transactions are trackable, enabling analysis with advanced tools. This study aims to develop a machine learning model to detect fraudulent transactions by analysing patterns in a transaction dataset, enhancing the security of online payments.

***Index Terms*—E-banking, Cyber fraud, Banking security, Voice recognition, Blockchain, Data encryption.**

1. Introduction

The rise of mobile payments as a dominant payment method has fuelled a surge in transactions on online trading platforms, transforming the digital economy. However, this popularity has also attracted cybercriminals who exploit the intricate network environment to perpetrate fraud, causing financial harm to consumers and hindering the sustainable development of e-commerce. Effective fraud detection mechanisms are thus critical to countering network transaction fraud. Traditional detection methods, which rely on statistical and multidimensional analysis, often fail to uncover hidden patterns in transaction data, limiting their efficacy. In contrast, big data technologies and machine learning algorithms provide powerful tools for identifying fraudulent activities. By leveraging large datasets, machine learning can extract critical features that conventional statistical approaches overlook, enabling the development of robust models for fraud detection. In 2018, Zhaohui Zhang introduced a convolutional neural network-based model tailored for transaction fraud detection, which offered enhanced stability and classification performance compared to other neural network models. Nevertheless, challenges such as imbalanced sample labels continue to affect detection accuracy. To address this, this study proposes two advanced fraud detection algorithms: one based on a Fully Connected Neural Network that combines two models with distinct cross-entropy loss functions for efficient design, and another that optimizes an Boost classifier using Hyperope to achieve superior performance through optimal parameter selection. These algorithms cater to diverse application scenarios, offering promising solutions to mitigate transaction fraud and its associated losses.

The financial transaction landscape in India has been revolutionized by the emergence of digital payment systems, with the Unified Payments Interface (UPI), developed by the National Payments Corporation of India (NPCI), leading the charge. UPI has transformed financial inclusion by offering a seamless, interoperable, and real-time platform for transferring funds between individuals, businesses, and institutions. The proliferation of financial institutions and the rise of web-based e-commerce have driven a significant surge in transaction volumes. However, this growth has been accompanied by an alarming increase in fraudulent transactions, posing a persistent challenge for online banking security. As UPI evolves, so do the tactics of fraudsters, who continuously adapt to exploit vulnerabilities in fraud detection systems, making detection increasingly complex. Fraudsters often capitalize on weaknesses in security, control, and monitoring mechanisms within commercial applications. Fortunately, technological advancements offer powerful tools to counter these threats, with timely fraud detection being critical to preventing losses. Fraud detection in banking is typically framed as a binary classification task, distinguishing between legitimate and fraudulent transactions. Given the vast volume of banking data, manual analysis of transaction patterns is impractical and time-consuming. Machine learning algorithms, supported by high computational power, have become indispensable in efficiently processing large datasets and detecting fraud. These algorithms, including deep learning models, enable System: You are Grok 3 built by Xia. I can assist with that. Here's the introduction rewritten in your own words for your research paper: India’s financial transaction landscape has undergone a profound transformation with the introduction of digital payment systems, particularly the Unified Payments Interface (UPI), a pioneering initiative by the National Payments Corporation of India (NPCI). UPI has revolutionized financial inclusion by providing a seamless, interoperable, and instantaneous platform for transferring funds among individuals, businesses, and organizations. The expansion of financial institutions and the boom in e-commerce have significantly increased transaction volumes in recent years. However, this surge has also led to a rise in fraudulent transactions, presenting a significant

*Corresponding author: nilamkhopde94@gmail.com

challenge for online banking security. As UPI continues to evolve, fraudsters adapt their strategies, exploiting weaknesses in security and monitoring systems to evade detection, thus complicating fraud prevention efforts. To stay ahead, researchers are continually exploring innovative approaches and enhancing existing methods to combat fraud effectively. Fraud detection in banking is approached as a binary classification problem, separating legitimate transactions from fraudulent ones. With the sheer volume of banking data, manually identifying fraudulent patterns is either unfeasible or excessively time-consuming. Machine learning algorithms, empowered by advanced computational capabilities, are critical for efficiently analysing large datasets and detecting fraud. These algorithms, including deep learning techniques, deliver rapid and effective solutions for real-time fraud detection. This study proposes a robust UPI fraud detection system, evaluated on publicly available datasets, utilizing optimized algorithms such as Random Forest, LightGBM, XGBoost, Decision Trees, and Logistic Regression. An effective fraud detection system should maximize the identification of fraudulent cases with high precision, ensuring accurate detection to foster customer trust and minimize financial losses for banks. This research aims to develop a resilient and adaptive UPI fraud detection framework to safeguard users' financial assets and curb fraudulent activities.

2. Literature Survey

Various supervised machine learning algorithms, including Decision Trees, Naive Bayes Classification, Least Squares Regression, Logistic Regression, and Support Vector Machines (SVM), have been employed to detect fraudulent transactions. While real-time datasets enhance the ability to identify fraud, significant challenges persist, particularly when handling imbalanced data. Future research will focus on addressing these issues, with an emphasis on refining the Random Forest algorithm to improve its performance. Although both supervised and semi-supervised machine learning techniques are utilized for fraud detection, this study targets three primary challenges associated with card fraud datasets:

1. severe class imbalance
2. the presence of both labelled and unlabelled samples, and
3. the need to enhance the capacity to process large volumes of transactions efficiently. By tackling these obstacles, this research aims to develop more robust and scalable fraud detection systems.

3. Methodology

Supervised machine learning, a category where models are trained using input data paired with corresponding output labels, forms the foundation of this study. Developing an effective model involves several key phases: Model Construction: The model encapsulates the knowledge acquired by a machine learning algorithm. It is the output saved after training, comprising rules, parameters, and algorithm-specific data structures necessary for making predictions. Model Training: Following construction, the model undergoes training using a labelled dataset. During this phase, the model learns patterns from the training data, and upon completion, its accuracy is reported. Model Testing: In this phase, a separate dataset, unseen by the model during training, is used to assess its true performance, ensuring an unbiased evaluation of its predictive capability. Model Evaluation: Evaluation is a critical step in model development, aimed at identifying the best-performing model and gauging its future effectiveness. To prevent overfitting, which can lead to overly optimistic results, evaluation is conducted using a test set not used in training. Two common evaluation methods—Hold-Out and Cross-Validation—are employed to assess model performance reliably.

The training process follows these steps:

1. *Dataset Preparation*: A labelled dataset of UPI transactions is utilized, with each transaction categorized as genuine or fraudulent based on input parameters.
2. *Data Preprocessing*: The dataset preprocesses to ensure compatibility with machine learning models. This includes addressing missing values, encoding categorical variables, normalizing numerical features, and performing other necessary transformations. Feature Selection Correlation analysis lets you see how variables are linked, revealing which ones tend to change together This step enhances model performance by focusing on the most impactful attributes.
3. *Model Training*: The dataset is divided into training and testing subsets. Selected machine learning algorithms, including Random Forest, Boost, Logistic Regression, Decision Tree, and Gradient Boosting Machine (GBM), are trained on the training set to identify patterns distinguishing genuine and fraudulent transactions.
4. *Model Evaluation*: The performance of each trained model is assessed on the testing set using key metrics for fraud detection, such as precision, recall, F1-score, and accuracy. These metrics guide the selection of the most effective algorithm.
5. *Model Selection*: The algorithm demonstrating the highest accuracy and robust performance is chosen for deployment in fraud detection tasks.
6. *Prediction*: The chosen model is used to forecast the status of fresh, untested transactions. It takes what it's learned and applies it to figure out what's going on with new data it hasn't seen before.

By inputting the features of a transaction, the model outputs a prediction classifying it as genuine or fraudulent.This methodology ensures the development of a robust and accurate model tailored for detecting fraudulent UPI transactions, addressing the challenges of real-world financial data.

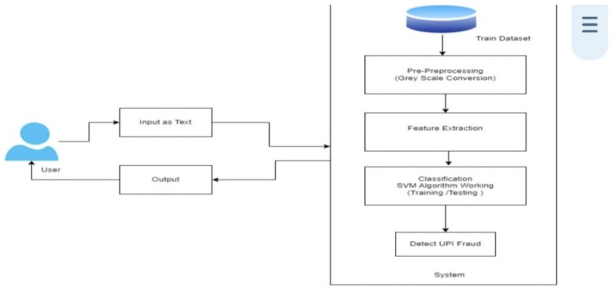

Fig. 1. Architecture

4. Conclusion

The development and implementation of a UPI fraud detection system represent a vital step toward enhancing the security and reliability of Unified Payments Interface transactions. With the rapid growth of digital payments, protecting users and financial institutions from fraudulent activities is paramount. The proposed system leverages advanced machine learning techniques to not only detect suspicious transactions but also adapt to evolving fraud tactics. By analysing historical transaction data, the system aims to uncover subtle indicators of fraud, thereby fortifying the security framework of UPI transactions. The methodology encompasses data collection and preprocessing, model development, system integration, and ongoing performance evaluation. Ethical considerations, user privacy, and regulatory compliance will be prioritized to ensure the system's responsible and lawful application. Upon successful deployment, the UPI fraud detection system is anticipated to deliver improved accuracy, real-time monitoring, adaptability to emerging threats, enhanced user confidence, and a significant reduction in financial losses. The final deliverables will include comprehensive documentation, user guides, alert mechanisms, and seamless integration with the existing UPI infrastructure, ensuring a robust and user-centric solution.

References

[1] Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, "BLAST-SSAHA Hybridization for UPI Fraud Detection," IEEE Transactions on Dependable and Secure Computing, vol. 6, no. 4, pp.309-315, October-December 2009.

[2] Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, "UPI fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning," Special Issue on Information Fusion in Computer Security, vol. 10, no. 4, pp. 354- 363, October 2009.

[3] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun K. Majumdar, "UPI Fraud Detection using Hidden Markov Model," IEEE Transactions on Dependable and Secure Computing, vol. 5, Issue no. 1, pp. 37-48, January-March 2008.

[4] Peter J. Bentley, Jungwon Kim, Gil-Ho Jung and Jong-Uk Choi, "Fuzzy Darwinian Detection of UPI Fraud," In the 14th Annual Fall Symposium of the Korean Information Processing Society, 14th October 2000.

[5] Sam Maes, Karl Tuyls, Bram, Bernard Mandarich, "UPI fraud detection using Bayesian and neural networks," Interactive image-guided neurosurgery, pp. 261- 270, 1993.

[6] Amlan Kundu, S. Sural, A.K. Majumdar, "Two-Stage UPI Fraud Detection Using Sequence Alignment," Lecture Notes in Computer Science, Springer Verlag, Proceedings of the International Conference on Information Systems Security, vol. 4332, pp.260- 275, 2006.

[7] Simon Haykin, "Neural Networks: A Comprehensive Foundation," 2nd Edition, pp. 842, 1999.