International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-5

Secure UPI Machine Learning-Driven Fraud Detection System for UPI Transactions

[1]M. Prasanna Kuamr, [2]M.Sivaparvathi, [3]D. Sravya
[1]Assoc. Prof, Department of CSE, MAM Women's Engineering College, Narasaraopet, Palnadu, A.P., India.
[2,3]Asst. Prof., Department of CSE, MAM Women's Engineering College, Narasaraopet, Palnadu, A.P., India.

***Abstract* – The UPI's ascent to prominence has been nothing short of spectacular, and it has completely altered the landscape of online payment systems by facilitating simple, fast, and secure money transactions. Since the quantity of UPI transactions has grown in tandem with illegal activity, effective fraud detection is critical for maintaining user trust and ensuring the security of these transactions. This paper proposes a machine learning-based solution for real-time detection of fraudulent UPI transactions. The proposed system makes heavy use of data preparation techniques such exploratory data analysis (EDA), feature selection, data cleaning, and missing value management to improve data quality and model performance. The procedure involves the training and evaluation of several machine learning algorithms, such as XGBoost, Naïve Bayes, K-Nearest Neighbours (KNN), Decision Tree, Support Vector Machine (SVM), and Logistic Regression. Ensemble learning methods, such as Stacking Classifier and Voting Classifier, are used to bolster the prediction accuracy and resilience even more. A Flask-based web app with SQLite authentication incorporates the trained model to provide secure, real-time fraud prediction. It turns out that the Stacking Classifier achieves the highest detection accuracy of 99.4% of all the machine learning models according to the trial results. With its scalability, efficiency, and reliability, the proposed technique can detect fraudulent UPI transactions, which contributes to the improvement of digital payment system security.**

***Keywords* – UPI Fraud Detection, Machine Learning, XGBoost, Ensemble Learning, Stacking Classifier, Voting Classifier, Flask, SQLite, Exploratory Data Analysis (EDA), Digital Payments..**

I. INTRODUCTION

The banking business has seen a dramatic shift due to the widespread availability of secure, fast, and user-friendly online payment options. The Unified Payments Interface (UPI) has risen to prominence as a leading real-time payment platform among these systems, thanks to its user-friendliness, compatibility, and ease of use. Unfortunately, the increase in fraudulent activities such as phishing attacks, identity theft, unauthorised transactions, and social engineering schemes has occurred at the same time as UPI's expanding popularity, posing substantial challenges for both consumers and financial institutions [1].

In order to identify suspicious financial transactions, classic fraud detection systems rely on manually defined criteria and predetermined thresholds. Although these techniques are effective at identifying long-term patterns of fraud, they struggle to keep up with hackers' dynamic attack strategies. Because of this, sophisticated fraud detection systems with the ability to understand intricate transaction patterns have become more important [2, 3].

Machine learning has become a promising tool for detecting financial fraud because of its capacity to automatically learn patterns from data on past transactions and accurately distinguish between legitimate and fraudulent ones. Supervised learning techniques such as Decision Tree, Logistic Regression, Support Vector Machine (SVM), K-Nearest Neighbours (KNN), Naïve Bayes, and ensemble learning methods have accomplished a remarkable job of detecting fraudulent financial transactions [4, 5].

The ability to recognise complex behavioural and temporal patterns in financial data may be further improved with the use of deep learning models, recurrent neural networks, and hybrid AI techniques, according to new study. These approaches are very effective in identifying digital payment system fraud in real-time [6, 7].

When training fraud detection systems, it is crucial to utilise accurate and comprehensive data. The model's performance may be enhanced with the help of data preparation procedures. Missing value handling, duplication removal, feature selection, data normalisation, and Exploratory Data Analysis (EDA) are all part of these methods. Effective preprocessing has the potential to improve prediction accuracy, computational cost, and model bias [8, 9].

Great advances have also been made in fraud detection via the use of ensemble learning techniques. These approaches combine the predictions of many ML models to achieve better accuracy and generalisability than individual classifiers. When faced with highly imbalanced fraud datasets, voting and stacking classifiers have shown superior performance by reducing false positives and enhancing overall detection capabilities [10], [11].

In view of these developments, this research introduces a Machine Learning-Powered System for Detecting Fraud in UPI Transactions. The proposed technique trains several machine learning models, such as XGBoost, Decision Tree, Logistic Regression, K-Nearest Neighbours (KNN), Naïve Bayes, and Support Vector Machine (SVM). Voting Classifier and Stacking Classifier are two examples of ensemble learning methods used to further improve the accuracy of fraud detection. Building a web app using Flask and connecting it to SQLite authentication allows us to securely forecast fraud in real-time for UPI transactions. The proposed system can identify fraudulent transactions with a high degree of reliability, accuracy, and scalability, according to experimental results [12], [13].

International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-5

II. RELATED WORK

One of the most effective ways to spot fraudulent financial transactions is by using machine learning, which is very accurate at learning complex transaction patterns and recognising suspicious behaviours. To improve the efficacy of fraud detection, several articles have proposed various supervised learning algorithms, ensemble learning methodologies, and data pretreatment methods.

In order to identify instances of credit card fraud, Bhattacharyya et al. [14] examined data mining techniques. Proper feature engineering and preprocessing significantly improved the performance of machine learning models, according to the findings. Their study proved that dealing with imbalanced datasets and selecting important transaction characteristics are crucial for fraud classification accuracy.

Compared to traditional machine learning methods, Branco et al.'s [15] RNN architecture with interleaved sequences more accurately represents the behaviour of sequential transactions, making it a superior choice for fraud detection. Their findings suggest that by deciphering the temporal connections within transaction sequences, deep learning methods could improve the precision of fraud detection for complex financial datasets.

With the IRIC framework for binary imbalanced classification, which Zhu et al. [16] introduced, fraud detection may finally address the imbalance between actual and phoney transactions. Using appropriate evaluation metrics and balancing procedures, their research demonstrated that classification models significantly outperform on highly skewed datasets.

Although prior research shown the efficacy of individual ML and deep learning models, many existing systems either do not provide real-time deployment or use an inadequate number of classifiers. Differently, the proposed work integrates many machine learning algorithms, including XGBoost, Decision Tree, Logistic Regression, Support Vector Machine (SVM), K-Nearest Neighbours (KNN), Naïve Bayes, and ensemble learning techniques like Voting and Stacking Classifiers. The recommended approach combines feature engineering, comprehensive data preparation, and a SQLite-authenticated Flask web app with real-time UPI fraud detection.

III. MATERIALS AND METHODS

1. Proposed System Architecture

The suggested UPI fraud detection system can detect fraudulent transactions instantly by using machine learning techniques. The overall design of the system is shown in Figure 1. Data cleaning, duplication removal, missing value handling, feature scaling, and exploratory data analysis (EDA) are some of the first procedures performed on the dataset to get it ready for UPI transaction data. Afterwards, you need to divide the dataset into two parts: a training set and a testing set. The procedure involves the training and evaluation of several machine learning algorithms, such as XGBoost, Naïve Bayes, K-Nearest Neighbours (KNN), Decision Tree, Support Vector Machine (SVM), and Logistic Regression. To improve the accuracy of predictions, ensemble learning methods are used. Two examples of these methods are Stacking Classifier and Voting Classifier. Finally, a web app built using Flask and integrating SQLite authentication is used to implement the best model. With this program, UPI transaction fraud may be safely predicted in real time.

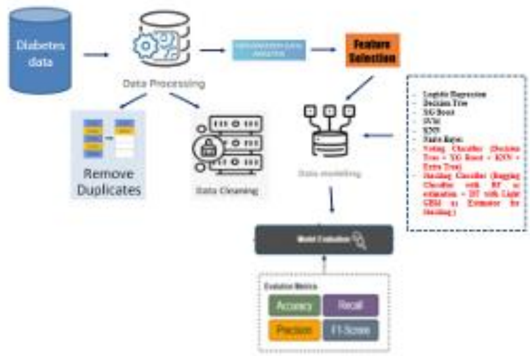

Fig. 1. Proposed Architecture of the Machine Learning-Based UPI Fraud Detection System

2. Dataset Collection

Records of UPI transactions that are available to the public make up the dataset used for this study. Items such as amount, type, time, merchant category, payment method, device, user demographics, location, and fraud status are included in each entry. Just by glancing at the label, you can determine whether a transaction is real or fraudulent. The dataset is highly biased since fraudulent transactions are far less common than legitimate ones. That is why appropriate methods for preprocessing and balancing are used before the machine learning models are trained.

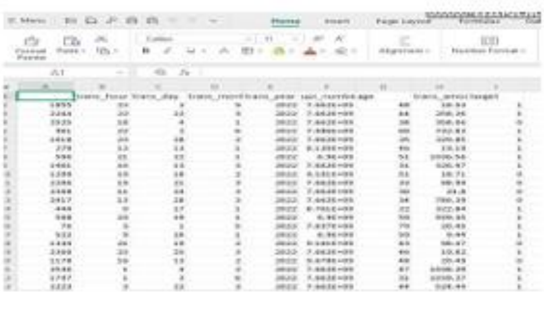

Fig. 2. Sample UPI Transaction Dataset

3. Data Preprocessing

If you want your transaction data to be as good as possible before you train your model, data preparation is a must. The following methods are used for preprocessing:

One, Eliminating Duplicates

The goal is to enhance data consistency by identifying and removing duplicate transaction records.

International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-5

Insufficient Value Processing
The mode is used to fill in categorical variables, whereas statistical imputation techniques like the median and mean are used to replace missing numerical values.

Thirdly, Cleaning Data
To enhance the overall quality of the dataset, transaction records that are irrelevant, inconsistent, or noisy are deleted.

Sizing Up Features
When training a model, it is important to normalise or standardise numerical features so that they all contribute equally.

Data Analysis for Exploration (EDA)
Using graphical and statistical methods, EDA examines feature correlations, outliers, fraud distributions, and transaction patterns.

Sixthly, Selecting Features
Reducing computational complexity and boosting model accuracy are achieved by selecting relevant characteristics depending on their contribution to fraud detection.

4. Model Training and Validation
The processed dataset is used to construct training and testing sets. Machine learning models are built using the training dataset, whereas unobserved transactions are tested using the testing dataset. Training and evaluating classification systems often makes use of evaluation metrics such as Accuracy, Precision, Recall, F1-Score, and ROC-AUC. We also employ ensemble learning approaches to improve forecast accuracy and minimise classification errors.

IV. RESULTS & DISCUSSION

Taken at face value. To find out whether the test is accurate, you have to figure out how many cases had valid findings compared to how many did not. In principle, it seems to be OK:

$$"Accuracy = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} (1)"$$

The preciseness of a detection is defined as the percentage of occurrences or samples that satisfy the epithetical criteria when detected affirmatively. We used the following formula to get this number:

$$\text{“}Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} (2)\text{”}$$

To evaluate the model's performance in finding all relevant class samples, Metric Machine Learning is used. The ratio of true positives to properly predicted positive instances is one metric for evaluating the model's performance in capturing the class instance.

$$"Recall = \frac{\text{TP}}{\text{TP} + \text{FN}} (3)"$$

Using the F1-score is one approach to assess the efficacy of theoretical ML models. The combined ratings for accuracy and download are calculated. When applied to different datasets, this statistic shows how effectively the model generalises.

$$"F1\ Score = 2 * \frac{Recall \text{ X } Precision}{Recall + Precision} * 100(4)"$$

Precision, accuracy, recall, and score F1 (1) are some of the criteria used to compare the algorithms in the table. On a regular basis, the Voting Classifier beats all of its rivals. Additionally, the tables provide a comparison of the metrics for the alternative methodologies.

Table.1 Measures for Assessing Extra Tree FS's Performance

Model	Accuracy	Precision	Recall	F1-Score
XG Boost	0.934	0.936	0.934	0.935
Decision Tree	0.906	0.907	0.906	0.907
Navie Bayes	0.588	1.000	0.588	0.741
Logistic Regression	0.588	1.000	0.588	0.741
SVM	0.588	1.000	0.588	0.741
KNN	0.843	0.847	0.843	0.844
Voting Classifier	**0.921**	**0.922**	**0.921**	**0.922**
Stacking Classifier	**0.994**	**0.994**	**0.994**	**0.994**

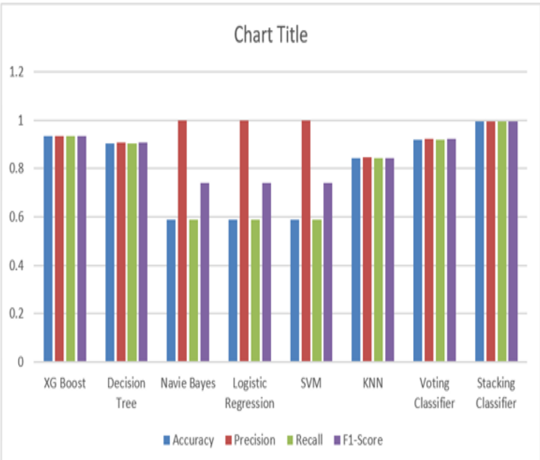

Fig. 3. Performance Comparison of Machine Learning Models

Graphs illustrate the following: F1-Score in light yellow, recall in grey, accuracy in light blue, and precision in orange (1). When it comes to performance and outcomes, the Voting Classifier is unrivalled. In the graphs up above, you can see these results represented graphically. The first stage

V. CONCLUSION

Finally, the UPI fraud detection system that relies on machine learning greatly improves the security of online banking. The system achieves a high level of accuracy in detecting fraud by using a number of classification models, stacking classifiers, decision-making trees, xgboost, svm, KNN, and naive Bayes. Additionally, it makes use of file approaches like voting. Digital transactions are protected in a strong and scalable manner thanks to the system's integration with a Flask-based frontend and SQLite-based user authentication. The findings show that the Stacking Classifier successfully boosts XGBoost's accuracy to 99.4 percent. This guarantees the possibility of real-time fraud detection. In this study, we highlight how ML and EL may improve the security, efficiency, and reliability of systems that identify fraudulent online payments.The future of this fraud detection system is filled with numerous exciting plans, such as exploring deep learning techniques like neural networks to improve performance, adding more features to the model to make it more generalisable, and expanding the dataset to incorporate more varied transaction patterns. The system's accuracy and adaptability may be greatly enhanced with the addition of real-time anomaly detection together with continuous model updates. The system may be enhanced in terms of security, scalability, and flexibility for a wider variety of financial applications by integrating with other payment systems and using new encryption techniques.

REFERENCES

1. M. Adekunle and P. Ozoh, "Fraud detection model for illegitimate transactions", Kabale University Interdisciplinary Research Journal, vol. 2, no. 2, pp. 21-37, 2023.
2. P. Boulieris, J. Pavlopoulos, A. Xenos and V. Vassalos, "Fraud detection with natural language processing", Machine Learning, vol. 1, pp. 22, 2023.
3. B. Mytnyk, O. Tkachyk, N. Shakhovska, S. Fedushko and Y. Syerov, "Application of Artificial Intelligence for Fraudulent Banking Operations Recognition", Big Data and Cognitive-Computing, vol. 7, no. 2, pp. 93, 2023.
4. R. Ridwan, S. Abdullah and F. Yusmita, "IMPLEMENTATION OF CASHLESS POLICY STRATEGIES TO MINIMIZE FRAUD IN THE GOVERNMENTSECTOR: SYSTEMIC REVIEW", JurnalAkuntansi, vol. 12, no. 3, pp. 181 201, 2022.
5. V. Chang, A. Di Stefano, Z. Sun and G. Fortino, "Digital payment fraud detection methods in digital ages and Industry 4.0", Computers and Electrical Engineering, vol. 100, pp. 107734, 2022.
6. S. K. Bandyopadhyay and S. Dutta, "Detection of fraud transactions using recurrent neural network during COVID-19: fraud transaction during COVID-19", Journal of Advanced Research in Medical Science & Technology, vol. 7, no. 3, pp. 16-21, 2020, ISSN 2394-6539.
7. S. Manocha, R. Kejriwal and D. A. Upadhyaya, "The impact of demonetization on ISSN:0377-9254 digital payment transactions: a statistical study", Proceedings of International Conference on Advancements in Computing & Management (ICACM), September 2019.
8. Diadiushkin, K. Sandkuhl and A. Maiatin, "Fraud detection in payments transactions: Overview of existing approaches and usage for instant payments", Complex Systems Informatics and Modeling Quarterly, no. 20, pp. 72-88, 2019.
9. B. Baesens, S. Höppner and T. Verdonck, "Data engineering for fraud detection", Decision Support Systems, vol. 150, pp. 113492, 2021.
10. M. Carminati, A. Baggio, F. Maggi, U. Spagnolini and S. Zanero, FraudBuster: temporal analysis and detection of advanced financial frauds. In Detection of Intrusions and Malware and Vulnerability Assessment: 15th International Conference DIMVA 2018 Saclay France June 28 29 2018 Proceedings 15, pp. 211-233, 2018.
11. S. Rastogi, A. Sharma, C. Panse and V. M. Bhimavarapu, "Unified Payment Interface (UPI): A digital innovation and its impact on financial inclusion and economic development", Universal Journal of Accounting and Finance, vol. 9, no. 3, pp. 518-530, 2021.
12. P. Gupta, A. Varshney, M. R. Khan, R. Ahmed, M. Shuaib and S. Alam, "Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques", Procedia Computer-Science, vol. 218, pp. 2575-2584, 2023.
13. J. Hariharakrishnan, S. Mohanavalli and K. S. Kumar, "Survey of pre-processing techniques for mining big data", 2017 international conference on computer communication and signal processing (ICCCSP), pp. 1-5, January 2017.
14. S. Bhattacharyya, S. Jha, K. Tharakunnel and J. C. Westland, "Data mining for credit card fraud: A comparative study", Decision support systems, vol. 50, no. 3, pp. 602-613, 2011.
15. B. Branco, P. Abreu, A. S. Gomes, M. S. Almeida, J. T. Ascensão and P. Bizarro, "Interleaved sequence rnns for fraud detection", Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery & data mining, pp. 3101-3109, August 2020.

16. B. Zhu, Z. Gao, J. Zhao and S. K. Vanden Broucke, "IRIC: An R library for binary imbalanced classification", -SoftwareX, vol. 10, pp. 100341, 2019.