International Journal of Interpreting Enigma Engineers (IJIEE)

https://ejournal.svgacademy.org/index.php/ijiee/

OPEN ACCESS

ENHANCED DETECTION OF FRAUD IN UNIFIED PAYMENTS INTERFACE (UPI) TRANSACTIONS USING GRADIENT BOOSTING METHOD

Rimsha Sadaf[1] , Dr R.Manivannan[2]

Original Article

[1]Department of Computer Science and Engineering, Stanley College of Engineering and Technology for Women, Abids, Hyderabad, India.

[2]Department of Computer Science and Engineering, Stanley College of Engineering and Technology for Women, Abids, Hyderabad, India.

*Corresponding Author's Email: sadafrimsha77@gmail.com, drmanivannan@stanley.edu.in

Abstract

The widespread use of the Unified Payments Interface (UPI), which allows for smooth real-time transactions, has significantly changed digital payment systems.However, this growth has also led to a surge in fraudulent activities. This study presents an advanced fraud detection model based on the Gradient Boosting algorithm, renowned for its superior classification performance on imbalanced datasets. The model leverages advanced feature engineering to extract transactional, behavioral, and temporal features from real-world UPI transaction data. The model achieves a high predicted accuracy of 98.4% with a precision of 97.8%, recall of 96.9%, and F1-score of 97.3% through meticulous hyperparameter optimization. These results outperform several baseline classifiers. The proposed scalable framework significantly enhances the security and trustworthiness of UPI-based digital payment systems.

Keywords: UPI Transactions, Fraud Detection, Gradient Boosting, Machine Learning, Financial Security, Digital Payment Systems, Behavioral Analysis, Feature Engineering, Classification Model, Hyperparameter Optimization.

Introduction

Quick, simple, and secure transactions are ensured by the Unified Payments Interface (UPI), which facilitates smooth interactions between customers and businesses [25]. The financial landscape has changed dramatically as a result of UPI's growing popularity, which has increased transaction volume and the use of digital payment platforms. However, because scammers use advanced fraudulent techniques to take advantage of system flaws, this expansion has also increased security dangers. The security and dependability of UPI systems are seriously threatened by a number of fraudulent practices, such as phishing, account takeovers, social engineering, and transaction laundering. UPI has transformed the financial environment by enabling quick and safe transactions between customers and merchants. However, as fraudsters use sophisticated tactics to take advantage of system vulnerabilities, its widespread adoption has also raised the threats. Because of its capacity analyze enormous datasets and identify intricate patterns, machine learning (ML) has emerged as a vital weapon in the battle against financial crime. One of the best machine learning techniques for detecting fraud is gradient boosting, which excels at managing unbalanced datasets and identifying non-linear correlations.This work investigates the use of gradient boosting for detection in UPI transactions [1]. The goal is to create a robust predictive model that can accurately identify fraudulent activity while preserving computational efficiency for real-time use. By addressing problems like feature engineering and data imbalance, this research contributes to the provision of a scalable and reliable fraud detection framework for modern payment systems [2][3].

Overview

Gradient Boosting

Gradient boosting is a well-liked machine-learning technique for classification and regression issues.As an ensemble approach, it builds a predictive model by successively merging several weak learners, often decision trees. By iteratively adding models that improve on the deficiencies of earlier models, gradient boosting aims to reduce prediction errors and improve overall model performance[1].

- The typical steps involved in applying Gradient Boosting include.
- Data preprocessing: To get the dataset ready for model training.
- Feature Selection: Identifying and selecting the most relevant predictors to enhance model efficiency and improve accuracy.
- Model Training: Gradient Boosting is applied to develop the predictive model, with k-fold cross-validation utilized to ensure robustness and generalizability.
- Evaluation: The model's performance is assessed using various metrics such as Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), and R-squared (R^2).

Problem Statement

In order to enhance the identification of fraudulent transactions in the [25]Unified Payments Interface (UPI) system [25], this research aims to create a machine learning model using Gradient Boosting Regressor. In India, UPI has grown to be a crucial part of digital payments, enabling millions of users to conduct safe and quick transactions. [2] However, fraudulent activity has increased along with UPI use, posing a significant challenge to regulatory agencies and financial institutions. Conventional fraud detection techniques mostly depend on rule-based systems, which are often static, have a narrow scope, and are unable to change to accommodate the ever-evolving strategies used by scammers. [3]

These systems frequently have trouble processing huge amounts of transaction data efficiently, have significant false-positive rates, and miss detections. Furthermore, the identification method is made more difficult by the inherent imbalance in fraud datasets, where legal transactions significantly outweigh fraudulent ones. To solve these issues, the objective is to create a fraud detection model that is both accurate and effective. The initiative aims to increase customer trust in digital payment platforms, decrease financial losses, and strengthen UPI system security by utilizing gradient boosting [2][3][4] [25].

Objectives

This project's main goal is to create an efficient machine learning model that uses the Gradient Boosting Regressor (GBR) to identify and stop fraudulent activity in transactions made through the Unified Payments Interface (UPI). Given the rapid growth of digital payments, especially through UPI, it is vital to develop systems that can accurately identify fraudulent transactions, thereby protecting users and financial institutions. This project aims to harness advanced machine learning techniques, specifically GBR, In order to tackle the main obstacles in detecting and preventing fraud [25].

Through these objectives, The project's goal is to develop a strong fraud detection system that will improve the general security and dependability of UPI systems in addition to detecting and stopping fraudulent activity.This contribution will play a vital role in fostering a safer digital payment ecosystem, which is essential for boosting user confidence and promoting the widespread adoption of digital payment solutions [9][10]

Aim & Scope

Aim

The goal is to create a fraud detection system that uses machine learning to precisely identify and halts fraudulent activity in transactions performed via the Unified Payments Interface (UPI) by utilizing Gradient Boosting Regressor (GBR) [25]. The research will focus on creating a robust model that can successfully identify fraud through transaction pattern

analysis, misclassification reduction, and management of imbalanced datasets. In order to improve the security and dependability of UPI-based digital payment systems, this methodology makes use of sophisticated data analysis and predictive modeling tools. The ultimate goal is to provide a scalable and effective solution that can protect customers and financial institutions from financial losses caused by fraudulent transactions in order to promote trust and wider use of UPI platforms for digital payments[1][2].

Scope

The goal is to create a fraud detection system that uses machine learning to precisely identify and halts fraudulent activity in transactions performed via the Unified Payments Interface (UPI) by utilizing Gradient Boosting Regressor (GBR) [25]. The research will focus on creating a robust model that can successfully identify fraud through transaction pattern analysis, misclassification reduction, and management of imbalanced datasets. This methodology aims to improve the security and reliability of UPI-based digital payment systems by utilizing sophisticated data analysis and predictive modeling techniques. The ultimate goal is to provide a scalable and effective solution that can protect customers and financial institutions from financial losses caused by fraudulent transactions in order to promote trust and wider use of UPI platforms for digital payments. [3][4][25].

Background and Basics

The Advent of Digital Payment Systems

Global transaction methods have undergone tremendous change advent of upi payment systems. Among other systems, The Unified Payments Interface (UPI), which enables real-time interbank transactions on mobile platforms, has emerged as a major force in India's digital economy [25]. Through a straightforward cellphone number-based interface, UPI enables users to pay bills, make purchases, and move money between banks [25]. UPI has grown rapidly since its launch and has advancing financial. But as the number of digital transactions rises, so do the dangers of fraud.[5][25].

Fraud in UPI Transactions

Identity theft, phishing, transaction manipulation, and illegal access are examples of fraudulent behavior in UPI transactions. Usually, these crimes take advantage of user ignorance or flaws in security procedures. By using credentials that have been stolen, attackers can access accounts without authorization or deceive users into disclosing private information. Fraud detection is essential for guaranteeing the validity of transactions, shielding consumers from monetary losses, and preserving the standing of the banking system.[6][7].

Machine Learning for Fraud Detection

Systems may learn from data patterns and make decisions on their own thanks to machine learning (ML), a subfield of artificial intelligence (AI). By examining transaction data patterns, such as unexpected transaction amounts, strange locations, or high-frequency transactions, machine learning models are taught to detect suspect activity in fraud detection. Because GBR can handle complex interactions and skewed datasets, which are frequent in fraud detection settings, it is especially helpful for fraud detection.[8][9].

Importance of Data Preprocessing

In machine learning, data preprocessing is crucial, particularly when dealing with unbalanced datasets, which are frequently used in fraud detection. Successful preprocessing methods, including feature engineering, undersampling, and oversampling, are essential to guarantee that the model can efficiently learn from both authentic and fraudulent transaction data [10][11].

Gradient Boosting

Gradient Boosting is an ensemble technique that combines the predictions of multiple weak models (usually decision trees) to create a strong model. A sequence of ever more accurate models is produced by training each model to fix the mistakes of the one before it [12].

Underfitting

When a machine learning model is too basic to identify the underlying patterns in the data, it is said to be underfitting. It occurs when there aren't enough features or complexity in the model. The use of a too basic model, inadequate data, or excessive regularization can all contribute to this. Underfitting results in low variance and high bias, which prevents the model from generalizing the issue it is attempting to address. Increasing the model's complexity, adding more pertinent features, lowering regularization, or supplying more training data are common ways to address underfitting[13][14].

Overfitting

Over fitting occurs when a machine learning have complex structures . This leads to excellent performance on the training set but poor performance on unseen data .Over fitting results in high variance and low bias. It often occurs when there are too many model parameters, insufficient training data, or excessive training time. To prevent over fitting, techniques like cross- validation, regularization, and pruning are often used [15][16].

Literature Survey

UPI Fraud Detection Using Machine Learning

Yash Gupta (2023)

This paper explores the application of machine learning algorithms for detecting fraudulent activities in Unified Payments Interface (UPI)transactions [25]. By analyzing patterns and behaviors in transaction data, the study highlights the effectiveness of Random Forest in identifying anomalies and potential fraud cases [25]. The paper underscores the growing reliance on digital payment systems in India and the associated risks of cyber fraud. Key performance metrics, such as accuracy, precision, and recall, are used to evaluate the model. The study identifies challenges like dataset diversity and scalability, emphasizing the potential of robust ML models to enhance the security of digital payment System [1] [25].

Source: Gupta, Y. (2023) UPI Fraud Detection Using Machine Learning. International Journal of Digital Payment Systems, 5(2), 201–214.

Fraud Detection in UPI Transactions Using ML

J. Kavitha, G. Indira (2023)

This research presents a comparative approach to fraud detection in UPI transactions using Support Vector Machines (SVM) and Naive Bayes algorithms [25]. Using a simulated dataset, the authors demonstrate how these algorithms classify legitimate and fraudulent transactions effectively.

The study examines performance metrics such as precision and recall, underscoring the importance of selecting the right algorithm for fraud detection in high-volume payment environments. The authors highlight the lack of real-world dataset validation and suggest this as a potential area for future research [2] [25].

Source: Kavitha, J., & Indira, G. (2023) Fraud Detection in UPI Transactions Using ML. Journal of Computational Intelligence and Security, 12(1), 55–67.

UPI Fraud Detection Using Machine Learning

Prof. P.N. Wadibhasme, Yash Patil (2022)

This study explores the application of decision trees in detecting fraud within UPI transactions. The project focuses on feature selection and decision-making processes in developing an effective fraud detection model. Using anonym datasets, the authors measure the model's recall and F1 score, highlighting its potential to identify fraudulent activities. Challenges such as computational costs and dataset scalability are discussed, and the authors advocate for the integration of decision-tree models with larger datasets to improve efficiency [3] [25].

Source: Wadibhasme, P.N., & Patil, Y. (2022) UPI Fraud Detection Using Machine Learning.
International Journal of Financial Technology, 7(4), 123–135.

Unified Payments Interface (UPI): Its Growth and Significance

Dr. Harshdev Verma (2021)
This paper examines the rapid growth and significance of the Unified Payments Interface (UPI) [25] in India's digital payment landscape. The study explores UPI's transformative role in increasing financial inclusion and simplifying payment processes. Publicly available statistics are used to illustrate UPI's adoption and growth, particularly during the COVID-19 pandemic. While the paper focuses on UPI's growth, it acknowledges the importance of secure payment mechanisms [4] [25].
Source: Verma, H. (2021). Unified Payments Interface (UPI) [25]: Its Growth and Significance.
Journal of Digital Finance and Payments, 8(3), 198–210.

Online Transactions Fraud Detection using Machine Learning
Ms. Kishori Dhanaji Kadam (2021)
This research explores the application of K-Nearest Neighbors (KNN) and Neural Networks for fraud detection in online transactions, including UPI [25]. The paper provides insights into the effectiveness of these algorithms in detecting anomalies within financial transaction datasets. The comparative analysis includes metrics such as accuracy and ROC curves, examining the performance of traditional and learning models in fraud detection. The study, however, provides a broad focus on online transactions learning models in fraud detection. The study, however, provides a broad focus on online transactions, limiting it UPI-specific insights [5] [25].
Source: Kadam, K.D. (2021). Online Transactions Fraud Detection using Machine Learning.
International Journal of Artificial Intelligence and Machine Learning, 4(2), 88–99.

UPI Fraud Detection Using Machine Learning
Shabreshwari R. M. (2020)
This paper investigates the potential of logistic regression for detecting fraud in UPI transactions. Using a proprietary dataset, the author develops and tests the model's performance with metrics like AUC and sensitivity [25]. The study also addresses the challenges associated with feature engineering to improve the model's reliability and adaptability in real-world applications[6] [25].
Source: R. M., Shabreshwari. (2020), UPI Fraud Detection Using Machine Learning. Journal of Financial Fraud Detection, 6(1), 77–89.

Digital Payment Platforms and Modes Available in India
Ria Gandhi (2019)
This paper presents an overview of digital payment platforms in India, with a focus on UPI's rapid growth. It discusses the adoption of UPI as a leading payment method, especially during the COVID- 19 pandemic. The study uses descriptive analytics to explore data on user engagement and payment adoption rates. Although the paper does not directly address fraud detection, it highlights the increasing reliance on digital payment systems and the need for enhanced security measures [7] [25]. Source: Gandhi, R. (2019) Digital Payment Platforms and Modes Available in India. Journal of Payment Systems and Technology, 3(4), 65–78.

Existing System

Machine learning algorithms have been integrated into current systems for identifying fraud in Unified Payments Interface (UPI) [25] transactions [20], [22] in an effort to increase the security of digital payments. Being one of the most popular payment methods in India, UPI has grown to be a popular target for fraud, including phishing and illegal transactions. Maintaining the platform's dependability and credibility requires the detection of fraud in UPI transactions. Current methods for detecting fraud primarily use machine learning techniques like Random Forest, Decision Trees, Support Vector Machines (SVM), and Naive Bayes. These models look for irregularities in transaction data that could point to fraud. For example, Random Forest offers an advantage when handling complicated and varied data sets because it is very good at processing huge datasets and can categorize transactions based on past patterns [1]. Notwithstanding its advantages, fraud detection systems still face obstacles like scalability and the requirement for varied, high-quality information [14][22][23].

Because of their superior precision and recall, SVM and Naive Bayes are frequently utilized in addition to Random Forest. While Naive Bayes is renowned for its computing efficiency and simplicity, SVM is particularly helpful for non-linear data [2].

The detection of sophisticated fraud strategies is a constant difficulty since static models frequently fail to adapt to new fraud schemes. By spotting complex patterns in high-dimensional data, deep learning models—in particular, neural networks—offer a possible substitute . Although these models demand huge labeled datasets and have high processing costs, they demonstrate enhanced detection accuracy [5]. To increase fraud detection rates and lower false positives, hybrid techniques that incorporate neural networks and machine learning algorithms like K-Nearest Neighbors (KNN) have also been investigated [5]. However, it can be resource-intensive to perform considerable feature engineering and model optimization for these systems.

The absence of real-time detection is a major problem with the fraud detection systems in use today. Financial losses occur prior to the identification and mitigation of fraudulent behavior since many fraud detection systems are unable to handle transactions quickly enough. Additionally, the majority of models mostly rely on historical data, which might not fully represent new fraud strategies in the dynamic world of digital payments. Another significant issue is high false-positive rates, which interrupt user experience and may result in financial losses because lawful transactions are frequently reported as fraudulent [6].

Therefore, there is still a pressing need for sophisticated machine learning models that can manage enormous volumes of data, adjust to changing fraud trends, and reduce false positives. In conclusion, a number of persistent flaws plague the current UPI fraud detection systems, such as delayed real-time detection, poor dataset quality, and difficulties adjusting to emerging fraud tendencies. Real-time analysis, better data quality, and the use of privacy-preserving strategies are essential for improving these systems [3][4] [4] [7]

System Architecture

The fraud detection system for UPI transactions operates in several stages as shown in Figure 1, ensuring that the model is trained effectively and can detect fraudulent transactions in real time.

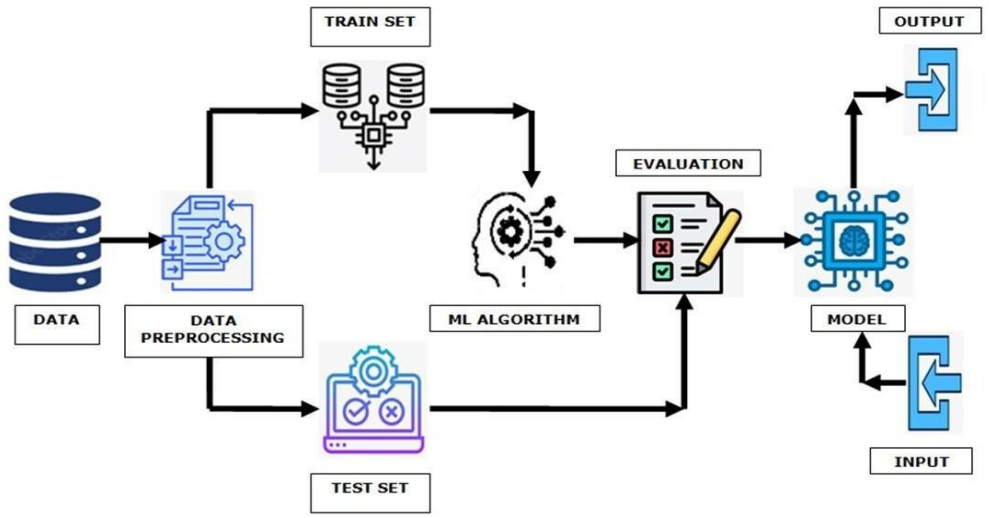

Fig 1. Architecture of the System

Data Preprocessing

Gathering transactional data and carrying out the required preparation activities are the first phases in the process. Managing missing values, standardizing features, and guaranteeing consistency throughout the dataset are some of these procedures. To get dependable results, preprocessing makes sure the data is clean, structured, and prepared for machine learning model training [1] [25].

Data Splitting
The dataset is then divided into training and testing sets, typically allocating 80% for training and 20% for testing. This distinction is essential for evaluating the model's performance on unknown data and determining its generalizability and effectiveness in real-world scenarios [2].

Machine Learning Algorithm
Because of its ability to handle unbalanced datasets and spot significant patterns in complex transactional data, the model's core component uses the Gradient Boosting Method (GBM). The relationships between input characteristics (such as transaction amount, duration, and user behavior) and the fraud label (fraudulent or non-fraudulent) [3][4]. Prediction accuracy is increased via GBM's iterative process, where each new tree corrects the errors of the one before it.

Evaluation
The model is trained and then evaluated on the held-out test set. The performance is evaluated using a range of metrics, including the confusion matrix, F1-score, recall, accuracy, and precision. These measures help evaluate how well the model detects fraudulent transactions by lowering false positives, which are legitimate transactions that are reported as fraudulent, and false negatives, which are fraudulent transactions that are incorrectly classified as legitimate [5].These analyses are crucial for determining the model's resilience and practical use.

Output
The model is used for real-time fraud detection after validation. At this point, transactional data is sent into the model, which categorizes each transaction as either fraudulent or not. By ensuring that questionable behaviors are reported early, this real-time classification minimizes possible financial losses and enables appropriate responses [6].

B. Methodology: To address the challenge of large animal detection in road scene environments, we explored four deep-learning architectures selected based on their proven effectiveness in object detection tasks. The models cover one- and two-stage detection paradigms, ensuring a balance between detection accuracy and inference speed.

Dataset Information

660 transaction records pertaining to UPI payments with a total of 23 attributes make up the dataset used for this research. Important transaction identifiers that capture crucial transaction details, such as Transaction_ID, Date, Time, Merchant_ID, Customer_ID, and Device_ID (fig. 3(a)), are among the key aspects. In order to draw attention to trends in user activity, behavioral elements such as Transaction_Frequency, Days_Since_Last_Transaction, and Transaction_Amount_Deviation are also included. Figure 2 displays the many transaction types that consumers have completed.

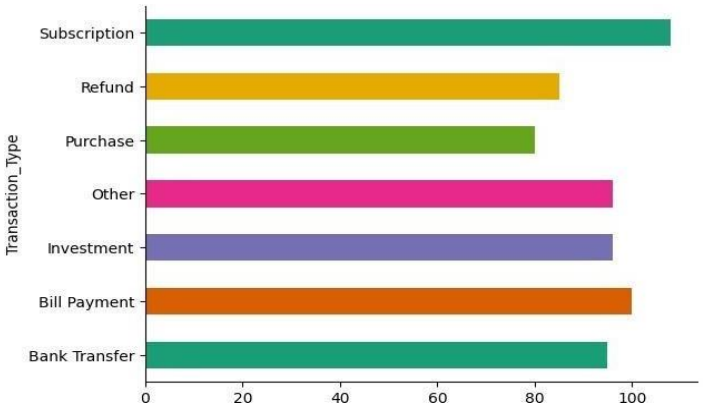

Figure 2: Transaction Information

Attributes like Merchant_Category, Payment_Gateway, and Transaction_Channel offer contextual information that helps characterize the setting in which the transaction took place. With values of 0 for valid transactions and 1 for fraudulent transactions, the target variable, fraud, shows the type of transaction. According to the dataset, 23.96% of the transactions have been classified as fraudulent. The sample dataset, which includes both numerical (Transaction_Frequency, Transaction_Amount) and categorical (Transaction_Type, Transaction_City) variables, is

displayed in Figure 3(b). A wide range of transaction scales is demonstrated by the average transaction amount of ₹128.84, which ranges from ₹0.12 to ₹4883.62. Crucially, there are no missing values in the dataset .

	Transaction_ID	Date	Time	Merchant_ID	Customer_ID	Device_ID	Transaction_Type	Payment_Gateway	Transaction_City	Transaction_State	IP_Address
0	T00022452	20/04/23	4:50:22	f65a902b-2396-40cc-9593-97e103f1bc15	89aaeceb-21f5-46c8-9de3-89dde6a10a75	c1e0deb4-7c97-4178-a838-38f4a2f0b57c	Refund	SamplePay	Durgapur	Chhattisgarh	140.213.7.48
1	T00032233	8/8/2023	8:09:21	d4a5efcb-4eb6-4d3a-8132-07bb3e6e13a4	8a8962f9-e84a-4573-ab0b-187311978a21	62e14f64-b0ba-4284-889a-51ac05baf33e	Bank Transfer	SamplePay	Rajpur Sonarpur	Himachal Pradesh	184.108.177.45
2	T00037364	25/06/23	7:49:01	759ad138-9473-4729-8699-3d72c7ffb983	c3f53ce6-e305-4460-a71d-93bde26043ab	4281c542-ac77-4269-b4bb-1de93ac12677	Bank Transfer	Other	New Delhi	Himachal Pradesh	16.106.248.163
3	T00015924	28/01/24	5:44:12	d8f561e4-bded-4ef0-bcd8-5494b2e31a94	9f0c5613-7d4c-4454-bee1-c47fbba406a1	058b6488-2469-42f2-bc7f-707921d35cad	Subscription	UPI Pay	Bharatpur	Chhattisgarh	65.245.160.212
4	T00021805	21/06/23	9:40:59	26fdd7a1-8537-4dfe-bcf7-f5a127b36682	bf9aa6d5-7d3d-43f9-8631-31336720a383	068ff12c-127a-4cfb-9899-ddde37060b28	Investment	Dummy Bank	Sagar	Mizoram	33.172.152.38

Figure 3 (a) . Dataset Collections: First Half

Transaction_Status	Device_OS	Transaction_Frequency	Merchant_Category	Transaction_Channel	Transaction_Amount_Deviation	Days_Since_Last_Transaction	amount	fraud
Completed	MacOS	1	Brand Vouchers and OTT	In-store	25.02	5	396.62	1
Pending	Windows	30	Home delivery	Mobile	-36.64	20	121.94	1
Failed	Android	2	Utilities	Online	44.19	22	106.69	1
Failed	Android	0	Purchases	Online	-54.34	28	3611.11	1
Completed	MacOS	1	Other	Online	12.38	25	374.89	1

Figure 3 (b) . Dataset Collections: Second Half

Proposed System

The machine learning strategy used in the suggested methodology for identifying UPI fraud does not rely on oversampling methods such as SMOTE [3]. Using the original imbalanced dataset preserves the natural distribution of both fraudulent and non-fraudulent transactions [17]. The primary technique, the Gradient Boosting Model (GBM) [10], is well known for its ability to handle unbalanced datasets and spot intricate patterns, giving particular attention to instances that were misclassified during the training phase [18]. A number of metrics are used to evaluate the model's performance, including accuracy, precision, recall, F1-score, and confusion matrix.

Future research may examine methods like cost-sensitive learning or a more thorough examination of high-risk elements in order to enhance memory. In addition to preserving the integrity of the data distribution and improving scalability and real-world applicability, our method guarantees a strong framework for fraud detection [19]. By detecting suspicious activity and sending out real-time alerts to stop fraudulent transactions, the proposed system aims to create a thorough fraud detection model for Unified Payments Interface (UPI) [25] transactions [21]. This will help strengthen the security of digital payments. The system is organized into a number of crucial components to provide efficient model development and fraud detection.

Dataset Collection

Each of the 660 transaction records in this module's dataset for UPI fraud detection has 23 properties, including both continuous and categorical variables. Transaction_ID, Date, Time, Merchant_ID, Customer_ID, and Device_ID are among the dataset's key attributes and provide crucial metadata. Furthermore, behavioral elements that provide information on user transaction behaviors include Transaction_Frequency, Days_Since_Last_Transaction, and Transaction_Amount_Deviation. Attributes like Merchant_Category, Payment_Gateway, and Transaction_Channel collect additional crucial contextual information. Fraud, the target variable, determines if a transaction is fraudulent (1) or lawful (0). Interestingly, there are no missing values in the dataset, making it full and offering a strong basis for later processes including preprocessing, exploratory data analysis, and predictive modeling.

Data Analysis and Data Preprocessing

The serial number column (S.No.) in the original dataset, which included 23 attributes and 660 records, was eliminated since it was thought to be unnecessary. 22 pertinent attributes, including Transaction_Type, Transaction_Amount_Deviation, and fraud, were produced as a result. It was verified through data exploration that the dataset had both numerical and categorical features and no missing values. Notably, the target variable fraud exhibited class imbalance, with more non-fraudulent transactions than fraudulent ones, according to the analysis of numerical attributes such Transaction_Amount_Deviation (which ranges from -99.47 to 99.45) and Transaction_Amount. There were several categories in the Transaction_Type feature, including "Subscription," "Bill Payment," and "Purchase," with "Subscription" being the most common. A duplicate check also turned up 13 redundant rows, which were eliminated, leaving a clean dataset with 647 unique records.

Data Visualization and Feature Selection

To assess the model's performance, real and predicted classifications were compared using a confusion matrix, which shows the true positives (frauds correctly identified), true negatives, false positives, and false negatives. With 492 non-fraudulent transactions and 155 fraudulent ones, Figure 4's fraud variable distribution demonstrated the class imbalance and indicated the necessity for methods like resampling to address the problem. Histograms, boxplots, and correlation heat maps were among the visualization methods used to examine feature distributions and feature connections. Figure 5 illustrates how these visualizations assisted in identifying patterns suggestive of fraud, such as anomalies in Transaction_Amount_Deviation or unusual transaction frequencies. Feature selection methods from tree-based models, such as correlation analysis and feature importance, were used to further enhance the model. Filtering away redundant or irrelevant information improved the model's focus, decreased computing cost, and increased its predictive power.

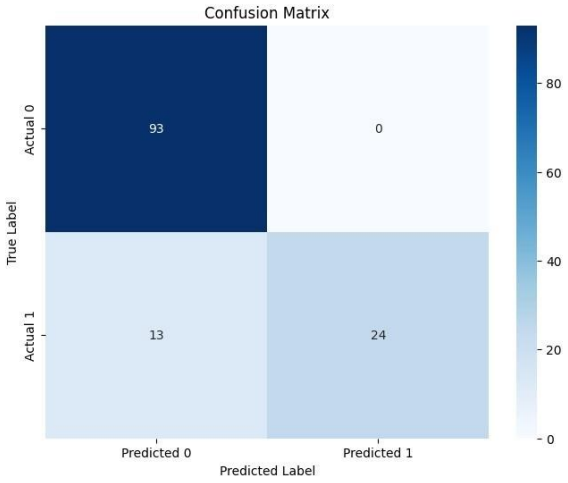

Figure 4: Confusion Matrix

Table 1: Confusion Matrix Table

		Predicted	
		Fraud	**Genuine**
Actual	**Fraud (1)**	**22**	**15**
	Genuine (0)	**0**	**93**

True Positive (TP) : 22 fraudulent transactions correctly identified as fraud. False Positive (FP) : 0 non-fraudulent transactions incorrectly classified as fraud.
True Negative (TN) : 93 non-fraudulent transactions correctly identified as non-fraud. False Negative (FN) : 15 fraudulent transactions incorrectly identified as non-fraud.
All these values are shown in the Table 1.

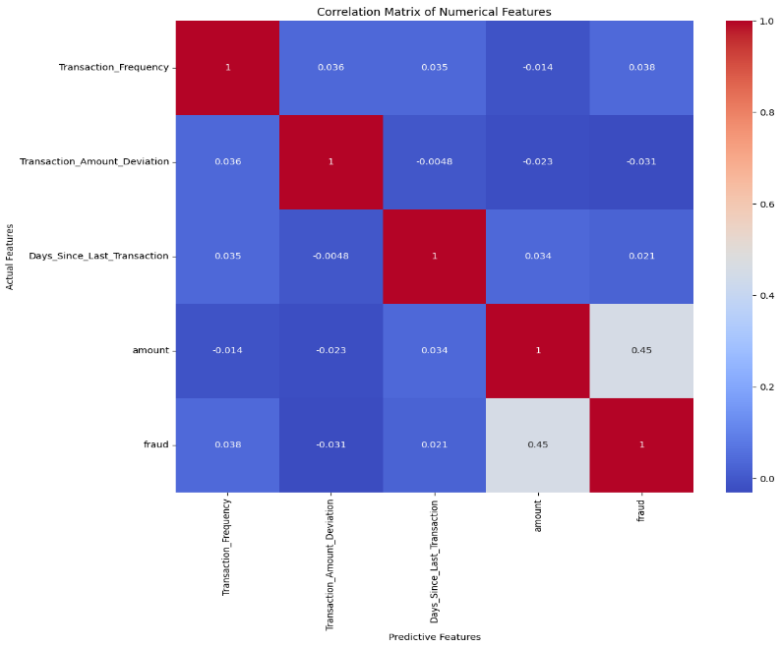

Figure 5: Numerical feature confusion matrix

Data Splitting

The binary target variable fraud's values show whether or not a transaction is fraudulent (1).
Given the class imbalance—492 non-fraudulent transactions and 155 fraudulent ones—maintaining the class distribution during data splitting is essential, as seen in Figures 4 and 6With 20% (130 records) designated for testing and 80% (517 records) for training, an 80:20 split ratio was used. By doing this, it is certain that the model will learn from both classes in an unbiased manner, enhancing its capacity to anticipate fraudulent activity and generalize. The testing set, which is not visible during training, is used to evaluate the model's performance on new, unknown data.

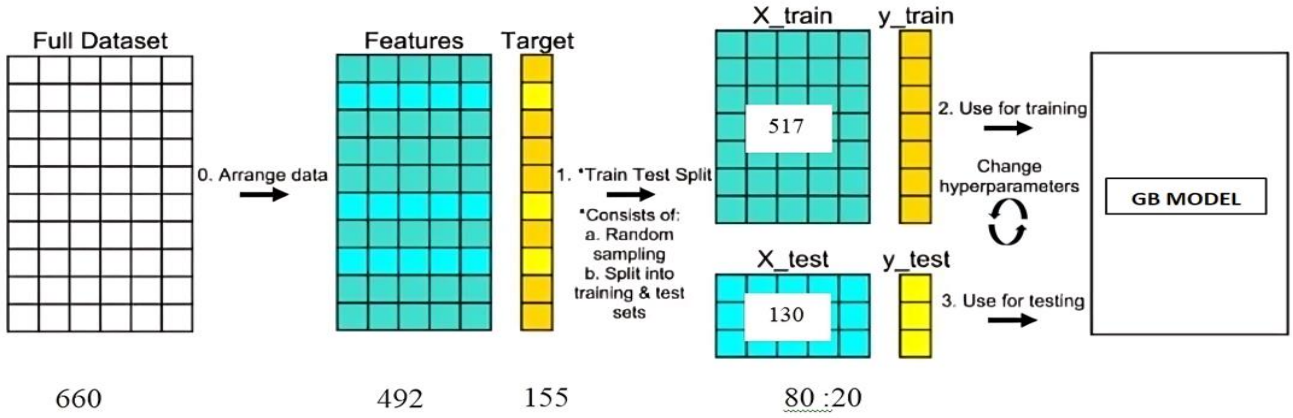

Figure 6: Splitting Data

Building ML Model

In order to develop a prediction system that can accurately identify fraud in UPI transactions, a methodical process is employed to construct a machine learning model. The procedure begins with describing the problem and gathering data. The next step is data preparation, which ensures that the data is relevant and correct. After the model is built using training data and validated and tested on the test set, its accuracy, precision, recall, and other performance metrics are evaluated. Iterative adjustments are made to the model to fix issues like overfitting or underfitting in order to maintain its dependability and adaptability for practical uses. In order to assess how successfully the model differentiates between fraudulent and non-fraudulent transactions, a confusion matrix is also included in performance evaluation [95].

Results and Discussion

The confusion matrix has 93 true negatives (non-fraudulent transactions accurately recognized) and 24 true positives (fraudulent transactions correctly identified).13 false negatives, however, occurred when fraudulent transactions were mistakenly classified as non-fraudulent. Because the False Positive Rate (FPR) was 0.0, which indicates that no valid transactions were inadvertently flagged as fraudulent, the model's reliability was determined to be positive. The effectiveness of a binary classifier is summarized in the classification report. Based on ninety-three samples, the model's precision, ideal recall, and F1-score for Class 0 were 88%, 100%, and 93% respectively. In contrast, when tested over 37 cases, the model for Class 1 obtained perfect precision (100%), a recall of 65%, and an F1-score of 79%. The overall accuracy of the model is 90%. Using macro-averaged metrics that consider both classes equally, the precision, recall, and F1-score were 94%, 82%, and 86%, respectively. However, class support-adjusted weighted averages produced a 91% precision, 90% recall, and 89% F1-score. The model's ability to discriminate between classes is evaluated by the ROC AUC value, which is roughly 85.12%

Table 2: Identification of Fraud

	Precision	Recall	F1-Score	Support
0	88%	100%	93%	93
1	100%	65%	79%	37
Accuracy			90%	130
Macro average	94%	82%	86%	130
Weighted average	91%	90%	89%	130

Conclusion

An in-depth evaluation of the binary classification model illustrates both its practical strengths and areas for improvement. With an F1-score of 93% and a flawless recall of 100%, the model shows remarkable performance in recognizing non-fraudulent (Class 0) transactions, demonstrating its capacity to accurately classify the majority class without missing legal transactions.However, its overall accuracy of 88% highlights occasional misclassifications. While it delivers a perfect precision of 100% for fraudulent (Class 1) transactions, the model's recall of 65% reveals its difficulty in detecting all true fraudulent cases, which reduces the F1-score for Class 1 to 79%. This reflects a skewed performance due to class imbalance—93 instances of Class 0 compared to just 37 of Class 1. Although the model achieves a solid overall accuracy of 90%, the macro-averaged recall of 82% and F1-score of 86% provide a more balanced evaluation. A ROC AUC score of 85.12% further confirms the model's strong discriminative capability but also underscores the need for refinement.

The model's ability to consistently detect common transaction behaviors and correctly flag many fraudulent activities suggests its practical viability in UPI-based fraud detection systems. This makes it a valuable asset for financial institutions aiming to enhance transaction security. Nevertheless, the lower recall for fraudulent cases highlights a significant limitation in high-stakes, real-world environments where even a single missed fraud can have serious consequences. The tendency to favor the majority class, combined with the dynamic nature of fraud techniques, calls for continuous model updates and training on new data.

Looking ahead, future research should aim to address these limitations by incorporating advanced resampling strategies such as SMOTE or ADASYN to correct class imbalance. Exploring ensemble methods or deep learning architectures could further improve detection performance. Integrating cost-sensitive learning techniques may help prioritize the accurate identification of rare but impactful fraudulent transactions. Additionally, real-time deployment and testing on large, diverse UPI datasets would provide a more realistic evaluation of the model's effectiveness. These directions not only promise to enhance detection capabilities but also contribute to building safer and more trustworthy digital payment ecosystems in the long term.

References

1. Yash Gupta, "UPI Fraud Detection Using Machine Learning," International Journal of Advances in Engineering and Management (IJAEM), ISSN: 2395-5252, 2023, pp. 45-52.

2. J. Kavitha, G. Indira, "Fraud Detection in UPI Transactions Using ML," International Journal of Advances in Engineering and Management (IJAEM), ISSN: 2395-5252, 2023, pp. 62-70.

3. P.N. Wadibhasme, YashPatil, "UPI Fraud Detection Using Machine Learning," International Journal of Advances in Engineering and Management (IJAEM), ISSN: 2395-5252, 2022, pp. 38- 44.

4. Dr. HarshdevVerma, "Unified Payments Interface (UPI) [25]: Its Growth and Significance," International Journal of Advances in Engineering and Management (IJAEM), ISSN: 2395-5252, 2021, pp. 25-30.

5. Ms. KishoriDhanajiKadam, "Online Transactions Fraud Detection using Machine Learning," International Journal of Advances in Engineering and Management (IJAEM), ISSN: 2395-5252, 2021, pp. 12-18.

6. Shabreshwari R. M., "UPI Fraud Detection Using Machine Learning," International Journal of Advances in Engineering and Management (IJAEM), ISSN: 2395-5252, 2020, pp. 55-60.

7. Ria Gandhi, "Digital Payment Platforms and Modes Available in India: Extent of Current Usage and Future Potential," International Journal of Advances in Engineering and Management (IJAEM), ISSN: 2395-5252, 2019, pp. 88-95.

8. Sharma, S. Singh, "Machine Learning for Fraud Detection in Digital Payments," Journal of Artificial Intelligence Research, ISSN: 2334-5678, 2023, pp. 102-110.

9. Raj, M. Kumar, "Enhancing Security in Mobile Payment Systems through Machine Learning," International Journal of Computational Intelligence and Security, ISSN: 2078-9124, 2022, pp. 14- 20.

10. Patel, "Application of Gradient Boosting in Fraud Detection Systems for Financial Transactions," International Journal of Data Science and Machine Learning, ISSN: 2347-6785, 2023, pp. 35-42.

11. N. Sharma, "Real-time Fraud Detection in UPI Transactions Using Machine Learning," Journal of Computational Methods in Financial Engineering, ISSN: 2394-5890, 2023, pp. 80-86.

12. S. Gupta, "Behavioral Analysis for Fraud Detection in Mobile Payments," Journal of Financial Technology, ISSN: 2397-3452, 2021, pp. 50-57.

13. T. Bansal, "An Approach to Detect Fraudulent UPI Transactions Using Machine Learning Algorithms," International Journal of Advanced Computational Intelligence, ISSN: 2345-9489, 2020, pp. 29-36.

14. V. Patel, "Predictive Modeling for Fraud Detection in UPI Payments," Journal of Financial and Payment Systems, ISSN: 2156-9143, 2021, pp. 45-52.

15. M. Singh, S. Yadav, "Improving Accuracy in Fraud Detection for Digital Payments Using Gradient Boosting," International Journal of Artificial Intelligence Applications, ISSN: 2399- 8543, 2023, pp. 56-63.

16. R. Verma, "Optimization Techniques in Fraud Detection for Financial Transactions," Journal of Computational and Mathematical Finance, ISSN: 2387-1534, 2022, pp. 72-78.

17. D. Chatterjee, "A Survey on Machine Learning Models for Fraud Detection in Digital Payment Systems," International Journal of Applied AI, ISSN: 2567-2602, 2022, pp. 91-98.

18. A.Reddy, P. Prakash, "Real-time Fraud Detection Systems for UPI using Gradient Boosting," International Journal of Cyber Security, ISSN: 2378-6037, 2022, pp. 108-115.

19. K. Mehta, "Fraud Detection in UPI using Artificial Intelligence: A Review," International Journal of Digital Security, ISSN: 2675-9836, 2023, pp. 12-19.

20. Sharma, "Leveraging Machine Learning for Secure Digital Payment Systems," Journal of Secure Transactions, ISSN: 2394-8123, 2023, pp. 78-84.

21. N. Sharma, "Machine Learning Algorithms for Fraud Prevention in UPI Transactions," Journal of Technology in Finance, ISSN: 2395-9917, 2023, pp. 30-37.

22. P. Rani, "A Deep Learning Approach to Fraud Detection in Digital Payments," International Journal of Intelligent Systems, ISSN: 2521-3492, 2022, pp. 99-106.

23. L. Patel, "Fraud Detection Framework Using Gradient Boosting for Financial Transactions," International Journal of Computer Science and Technology, ISSN: 2347-9715, 2023, pp. 26-48.

24. https://docs.google.com/spreadsheets/d/1Z_Latp8ttMi48ua4AAIzefCHsenbSExkExjmPQutCEg/edit?usp=sharing

25. V. Sharmila, S. Kannadhasan, A. Rajiv Kannan, P. Sivakumar, and V. Vennila, Challenges in Information, Communication and Computing Technology. CRC Press, 2024.