



An Ideal approach for Digital Transaction Fraud Detection using Machine Learning

Maibam Debina Devi¹ & Arpan Datta Roy²

*¹School of Cyber Security and Digital Forensics,
NFSU Tripura Campus, Agartala, Tripura*

*²Assistant Professor, School of Forensic Science,
NFSU Tripura Campus, Agartala, Tripura*

Abstract

This paper highlights the importance of machine learning-based solutions for finding the optimal approach for detecting credit card fraud. With the increasing number of digital transactions, identifying fraudulent activities has become a critical challenge. In this study, several machine learning models, including Random Forest, XGBoost, and LightGBM, are applied to detect fraudulent transactions. The experiments are conducted on the ULB Credit Card Fraud Detection dataset, which contains 284,807 transaction records with a fraud rate of 0.172%, making it a highly imbalanced dataset. The models are evaluated using performance metrics such as Precision–Recall Area Under the Curve (PR-AUC) and Receiver Operating Characteristic Area Under the Curve (ROC-AUC). The results show that all models perform effectively in fraud detection; however, LightGBM achieves the best performance with the highest PR-AUC score of 0.8764. Therefore, LightGBM is identified as the most effective model among the evaluated approaches for this dataset.

Keywords: *Credit Card Fraud, XGBoost, LightGBM, Random Forest, PR-AUC, Anomaly Detection. Machine Learning, Random Forest, LSTM*

1. Introduction

Considering the rapid advancement of technology and the availability of online services, digital transactions have become an essential part of our lives. There is an aspect of convenience and significant time savings that make digital transactions extremely convenient for livelihood. Aside from that, each digital transaction generates a record, which provides transparency and makes digital transactions easier to follow.

Nowadays, digital transactions serve as a support mechanism for small and online businesses, ultimately contributing to economic growth. As the quantity of digital transactions increases, so does the number of fraud incidents. According to reports, internet-based transactions account for a large portion of total bank fraud instances, indicating systemic vulnerabilities. There is a need for a solid security architecture to reduce or regulate the growth of fraud. User awareness and advanced technology engagement in the research of digital payment for fraud detection.

Digital payment platforms offer financial services like as money transfers, bill payments, and cashless transactions (Calderon, 2025). Digital transactions are the transfers of cashless funds using digital payment channels.

Digital transactions have become an essential part of everyday life, playing a significant role in activities ranging from small businesses to large-scale industries. The growth of digital payments has been influenced by several factors, including government initiatives promoting digitization, increased internet access, and the widespread use of smartphones. The expansion of online business and e-commerce has further accelerated this trend. In the context of the Indian economy, demonetization played a major role in boosting digital transactions. A study by [14] highlights the significant increase in the adoption of digital payments across India during this period. Due to the shortage of cash, platforms such as Google Pay, Paytm, and BHIM experienced rapid growth, making demonetization a catalyst for the expansion of digital payment systems in India.

However, with the rapid rise of digital payment mechanisms, cases of fraud have also increased. Among these, credit card fraud has emerged as a significant challenge in digital financial transactions. This paper focuses on exploring and developing a fraud detection mechanism for credit card transactions using machine learning algorithms.

This studies focus on finding an optimal model for detection of fraud in credit card data. Machine learning is widely used standard approaches for the model which is complex, non-linear patterns. The considered dataset is highly imbalanced, SMOTE mechanism is applied. The experiment make used of Random Forest, and Gradient Boost technique, LightGBost and XGBoost.

2. Literature Survey

In recent years, research on digital transactions has grown in importance. With the fast rise of online payment systems, assuring security and reliability has become a major concern. In this context, Artificial Intelligence (AI) has emerged as a critical solution provider for solving these difficulties, particularly in identifying and preventing fraudulent activity in digital financial systems.

According to [7] AI plays a crucial role in preventing fraud and maintaining trust in digital payment systems. Several studies, including [12], suggest that machine learning and deep-learning algorithms can effectively detect fraud in digital transactions. Another study by [13] compares the performance of several machine learning approaches on digital transactions.

Numerous studies demonstrate that artificial intelligence has demonstrated encouraging results in addressing the issue of fraud detection in online transactions. Credit card fraud is growing dramatically in the context of digital transactions [10]. A comparative analysis and a promising outcome are shown in [1] work on fraud detection using AI machine learning algorithms. Another study by [2] uses a granular computing framework that combines fuzzy rough set theory with reasoning techniques to detect credit card fraud. The study [16] explores several boost techniques, such as XGBoost and CatBoost. Because of its self-learning capabilities and algorithm-based detection approaches, artificial intelligence has become more important in credit card fraud detection [10, 1, 14]. Researchers

are concentrating more on creating AI-based models to enhance fraud detection systems. A report on a hybrid approach for detecting fraud in digital transactions may be found at [1]. In recent years, there has been a lot of interest in research on the use of machine learning algorithms and artificial intelligence for fraud detection. Traditional rule-based systems are no longer adequate to identify sophisticated fraudulent activities due to the explosive rise of digital payments and online transactions. Because of this, researchers are concentrating more on AI-based models [4] that can learn patterns from big datasets [8], adjust to new fraud tactics, and enhance the precision and effectiveness of fraud detection systems[17, 10].

This research focuses on implementing different machine learning algorithms and performing a comparative study to analyze their performance in credit card fraud detection.

3. Model

Credit card transactions done by European cardholders over two days in September 2013 are included in the ULB Credit Card Fraud Detection dataset. It is one of the most often mentioned benchmark datasets in the literature on fraud detection and is freely accessible on Kaggle (mlg-ulb/creditcardfraud).

The dataset exhibits a canonical extreme imbalance issue with a fraud rate of 0.172%. The degenerate strategy of forecasting all-legitimate is incentivized by optimizing for accuracy, and traditional metrics (accuracy, ROC-AUC)[9] provide an unduly optimistic image of model quality. For this reason, the main statistic used in this work is Precision-Recall AUC, which is only sensitive to minority-class performance.

3.1 Methodology

The first and most important stage in creating the fraud detection system is preprocessing. In order for machine learning algorithms to function well and yield trustworthy results, this step makes sure that the dataset is appropriately prepared. Feature scaling, which standardizes the range of the input variables, is the first step in the preprocessing procedure. Although it enhances model performance and prevents features with bigger values from dominating those with smaller values during training, this phase is very crucial.

To accurately assess the model's performance, the dataset is split into training and testing sets after the preprocessing step is finished. An 80:20 ratio is used to divide the data in this investigation. Consequently, 56,962 samples are set aside for testing, while 227,845 samples are used to train the model, enabling it to discover patterns and relationships within the data. The testing set is used to gauge the trained model's efficacy in identifying fraudulent transactions as well as how effectively it generalizes to new data. This methodical data preparation contributes to a trustworthy and objective assessment of the fraud detection model.

Over viewing the dataset, it is observed that the dataset possesses a class imbalance problem, which is one of the issues in most of the classification problems and eventually becomes biased toward the prediction model and eventually reduces the efficiency of the model. To overcome the issue, this model makes use of the SMOTE[5] (Synthetic Minority Oversampling Technique), which is applied over training samples in order to create a balanced class set over distribution to the ML (machine learning) models. Generally SMOTE creates synthetic samples of the minority class by interpolating among existing minority class samples. After the application of SMOTE, the training sample obtains uniform class distribution among the samples. Balancing the dataset plays an important factor in defining model performance. A balanced set allows models to effectively learn the patterns for the distinct class, helps in capturing better decision boundaries, and eventually reduces the risk of bias, overprediction, and improves the metrics score.

However, the testing remained unprocessed in order to reflect the true class distribution and retain the originality over class distribution. The evaluation remains unbiased and representative of real-world performance, which allows reliable comparison over models.

However, for XGBoost and LightGBM[11], they are trained upon the original imbalanced dataset; these models address class imbalance through cost-sensitive learning. Parameters responsible for XGBoost[6] and LightGBM are *scale_pos_weight* and *class_weight*, which adjust the learning process by managing greater weight for the underrepresented class instances.

This work considers 3 different models, namely Random Forest (RF)[3], for the detection mechanism. Table 1 gives the

ideas about the different parameters considered by the model for the experiment. *n_estimators* defines the total numbers of trees employed; 100 trees are considered with *class_weight* as balanced to compensate for the class imbalance, prioritizing the importance of minority samples, and *n_jobs=-1* with utilization of all available CPU cores.

XGBoost and LightGBM adopt 200 estimators to strengthen the boosting effectiveness, with a learning rate of 0.05 for a stable approach to learning to prevent overfitting and *max_depth* of 6 to control the model complexity.

Table 1. Model hyperparameters configurations

Model	n_estimators	Key Configuration
Random Forest	100	class_weight='balanced', n_jobs=-1
XGBoost	200	lr=0.05, max_depth=6, scale_pos_weight=ratio
LightGBM	200	lr=0.05, max_depth=6, class_weight='balanced'

4. Result and Discussion

Receiver operating characteristic-area under curve (ROC-AUC) is the performance statistic used in this experiment’s performance evaluation. Based on the sensitivity and specificity thresholds, the ROC assesses the model’s performance. However, the AUC provides an overview of the model’s overall performance based on class scores between 0.00 and 1.00. The outcome of the experiment is shown in figure 2. Metrics that take into account various aspects of the efficacy of the experiment in fruit detection are used to evaluate it.

Precision and recall are another mechanism for performance evaluation. Precision plays a vital role when errors are high, and recall reduces the false negatives. Figure 3 represents the place of the response of the model over the precision-recall graph.

The LightGBM model achieves the maximum PR-AUC of 0.8764 during training, with an execution time of 5.48 seconds , making it a natural fit for fraud production. It can identify intricate fraud patterns rapidly according to its histogram-based leaf-wise tree growth. Recall score of 0.8776 shows that 88% of the fraud cases in the collection could be identified. Conversely, out of all the models, the Random Forest model yields a strong F-score of 0.81

and precision of 0.81, indicating that the transactions that have been reported are fraudulent. However, as seen in figure 3, RM has an execution time of 242.88s, which is 49 times slower than LightGBM.

The XGBoost result is the fastest among the models, with 4.98 seconds of execution time, which is fractionally faster than LightGBM and robust. Overall model performance is shown in figure 1.

Table 2: Performance score of the models

Model	ROC-AUC	F1	Precision	Recall	Time (s)
LightGBM	0.9754	0.7611	0.6719	0.8776	5.48
Random Forest	0.9688	0.8103	0.8144	0.8061	242.88
XGBoost	0.9754	0.8000	0.7664	0.8367	4.98

5. Conclusion

This paper explains the process to use the ULB benchmark dataset to identify the optimal machine learning algorithm for credit card fraud detection. With the highest PR-AUC score of 0.8764, recall value of 0.8776, and training time of 5.48, LightGBM performed better than the other models during the testing as tabulated in table 2. However, gradient boosting XGBoost produced the fastest model (4.98 seconds) with accuracy on par with LightGBM. Random Forest, on the other hand, has the highest precision and F1-Score; but, due to the significant speed cost, it is better suited for offline batch scoring than real-time inference.

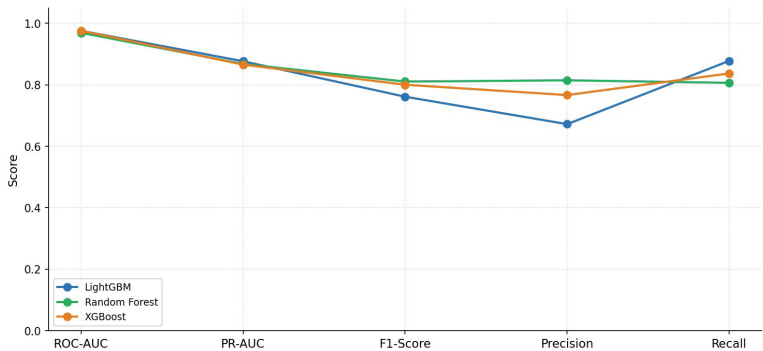
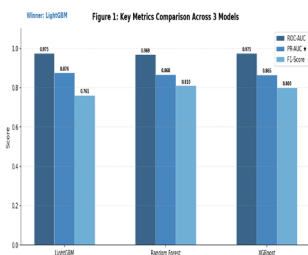
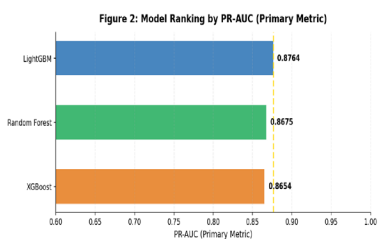


Fig. 1: Total metrics profile for the models

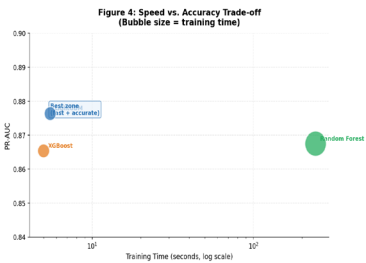


a. Metrics chart

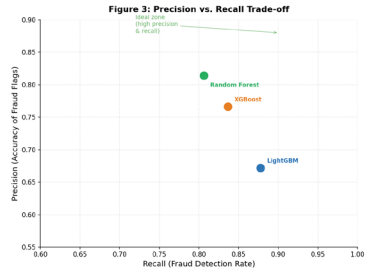


b. PR-AUC

Fig. 2: Models performance charts PR-AUC, RO-AUC AND F1-score



a. Speed vs accuracy trade graph



b. Models comparative analysis over Precision verse Recall

Fig 3: Models comparative analysis over Precision verse Recall

6. References

Masad A Alrasheedi. "Enhancing Fraud Detection in Credit Card Transactions: A Comparative Study of Machine Learning Models". In: Computational Economics (2025), pp. 1–27.

Leo Breiman. "Random forests". In: Machine learning 45.1 (2001), pp. 5–32.

Khyati Chaudhary, Jyoti Yadav, and Bhawna Mallick. "A review of fraud detection techniques: Credit card". In: International Journal of Computer Applications 45.1 (2012), pp. 39–44.

Nitesh V Chawla et al. "SMOTE: synthetic minority over-sampling technique". In: Journal of artificial intelligence research 16 (2002), pp. 321–357.

Tianqi Chen and Carlos Guestrin. "Xgboost: A scalable tree boosting system". In: Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining. 2016, pp. 785–794.

- Devendra Dahiphale et al. "Enhancing trust and safety in digital payments: an LLM-powered approach". In: 2024 IEEE International Conference on Big Data (BigData). IEEE. 2024, pp. 4854–4863.
- Andrea Dal Pozzolo et al. "Calibrating Probability with Undersampling for Unbalanced Classification." In: SSCI. 2015, pp. 159–166.
- Jesse Davis and Mark Goadrich. "The relationship between Precision-Recall and ROC curves". In: Proceedings of the 23rd international conference on Machine learning. 2006, pp. 233–240.
- Ibrahim Y Hafez et al. "A systematic review of AI-enhanced techniques in credit card fraud detection". In: Journal of Big Data 12.1 (2025), p. 6.
- Guolin Ke et al. "Lightgbm: A highly efficient gradient boosting decision tree". In: Advances in neural information processing systems 30 (2017).
- Zong Ke et al. "Detection of ai deepfake and fraud in online payments using gan-based models". In: 2025 8th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE. 2025, pp. 1786–1790.
- Ganesh Khekare, Shivam Sunda, and Yash Bothra. "A Comprehensive Performance Comparison of Traditional and Ensemble Machine Learning Models for Online Fraud Detection". In: arXiv preprint arXiv:2509.17176 (2025).
- Ankaj Kumar, Kapil Sethi, and Amit Verma. "A Comprehensive Review of Machine Learning Techniques in Fraud Detection". In: 2025 12th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE. 2025, pp. 1–7.
- Sahil Manocha, Ruchi Kejriwal, and Dr Akanksha Upadhyaya. "The impact of demonetization on digital payment transactions: a statistical study". In: Proceedings of International Conference on Advancements in Computing & Management (ICACM). 2019.
- Pooja Tiwari et al. "Credit card fraud detection using machine learning: a study". In: arXiv preprint arXiv:2108.10005 (2021).