IJISEM
INTERNATIONAL JOURNAL OF INNOVATIONS IN SCIENCE ENGINEERING AND MANAGEMENT

Check for updates

OPEN ACCESS

Volume: 2

Issue: 2

Month: June

Year: 2023

ISSN: 2583-7117

Published: 22.06.2023

Citation:

Mrs. Elavarasi Kesavan "ML-Based Detection of Credit Card Fraud Using Synthetic Minority Oversampling" International Journal of Innovations in Science Engineering and Management, vol. 2, no. 2, 2023, pp. 55–62.

DOI:

10.69968/ijisem.2023v2i255-62

This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

ML-Based Detection of Credit Card Fraud Using Synthetic Minority Oversampling

Mrs. Elavarasi Kesavan[1]

[1]*Full Stack Automation Architect, Company- Cognizant*
Email-I'd- elavarasikmk@gmail.com, ORCID :https://orcid.org/0009-0008-3844-0286

Abstract

Credit card fraud detection is an essential and classic but very difficult problem consisting of imbalanced classification where fraud transactions are almost nonexistent as compared with legitimate ones. This paper proposes an approach which main feature is a combination of an imbalanced data technique based on the Synthetic Minority Oversampling Technique (SMOTE) with an XGBoost classifier for credit card fraud detection. We delineate the dataset preparation, feature preprocessing, SMOTE resampling, model configuration and training, and evaluation metrics (Accuracy, Precision, Recall, F1, AUC, and confusion matrix). Additionally, a comparative experiment plan is defined that includes baseline classical models (Logistic Regression, Random Forest, Artificial Neural Network) thereby allowing practitioners to perform benchmarking against other models' performances. The complete code necessary for conducting the experiments is accessible (the user-supplied Colab script was used as the foundation). The results show that if XGBoost is used in combination with careful preprocessing and SMOTE it will acquire a strong recall very important properties for fraud detection while still to an extent retaining high precision. We elaborate on the limitations (synthetic oversampling risks, concept drift) and plan ahead for the future inventiveness (cost-sensitive learning, streaming models, explainability).

Keywords; Credit Card Fraud, Imbalanced Learning, SMOTE, XGboost, Resampling, Supervised Learning.

INTRODUCTION

The tremendous rise of digital transactions, which have been mainly powered up by e-commerce as well as fintech platforms, has led to a substantial crack of credit card fraud. Fraudsters, as the digital payment channels, have expanded their operations, and they are now using more advanced techniques such as identity theft, card-not-present attacks, and automated intrusion attempts, which all make detection increasingly difficult [1]. Once upon a time, traditional rule-based systems were great in their job, but they now rubberbanded due to their static nature and limited adaptability, losing the ability to deal with these different and dynamic fraud behaviors [2].

The very small number of credit card fraud transactions in the total credit card datasets is the main reason for the class imbalance which severely hinders the development of reliable fraud detection models, as the bulk of the transactions are non-fraudulent. This imbalance, in turn, causes the models to be less sensitive and gives rise to poor fraud class recall even when the overall accuracy looks good [3]. Modern studies point out the necessity of using more sophisticated resampling methodologies like SMOTE, ADASYN, hybrid SMOTE-ENN, and undersampling to treat this matter and improve the recognition of minority classes [4]. Many times, these methods are applied together with machine learning algorithms such as logistic regression, random forests, gradient boosting, and neural networks to get better predictive performance in the area of fraud detection tasks [5].

In recent years, machine learning has been primarily focused on fraud detection due to its capability of spotting complex patterns in transactions and subtle irregularities [6]. Moreover, these contemporary studies have gradually been revealing the necessity of strong preprocessing, feature selection, and hybrid learning mechanisms in order to classify the outcomes better, especially in imbalanced situations [7]. XGBoost is one of the algorithms that is most preferred due to its excellent performance with tabular data, quick processing of nonlinear relationships, and having imbalance-aware hyperparameters as a built-in feature [8].

The present research paper proposes an XGBoost-based credit card fraud detection framework using the Credit Card Fraud Detection Dataset 2023. The dataset is composed of anonymized numbers derived from transaction metadata with the same imbalance issues as reported in the literature [9]. SMOTE is applied only to the training dataset after data cleansing, feature scaling, and feature selection to keep the model intact. This approach ensures that there is no bias or data leakage during the process of achieving balanced class representation.

For performance evaluation, apart from using accuracy, which might be misleading due to the high cost associated with misclassified fraudulent transactions [10], recall, precision, F1-score, MCC, ROC-AUC, and confusion matrix analysis are chosen as appropriate metrics for imbalanced classification. All these metrics together will provide a much better picture of the fraud detection capability than accuracy only. Thus, the combination of SMOTE and optimized XGBoost classifiers provides a scalable and efficient way of minority-class detection improvement in current financial sectors.

RELATED WORK

The research probing into the detection of credit card fraud has become one of the foremost areas of study due to the accompanied to the rise in the number of digital financial transactions and the sophistication of fraud types. The traditional rule-based systems and data processing have become ineffective in managing the continuously evolving patterns of attacks; thus, the use of data-heavy and ML-based fraud detection frameworks is gaining momentum. The latest research focuses the attention on the heavy reliance of supervised, unsupervised, and hybrid ML techniques in the near real-time analysis of transactional patterns and anomaly detection.

There have been various studies which compared the performance of classical machine learning models on large-scale and imbalanced financial datasets. Mathew [11] asserted that the use of ensemble learning approaches has a huge impact on the detection accuracy and also, on the identification of the minority class. Al-Faqir and Ouda [12] suggested a deep learning–based ensemble scoring model, which has been noted for its better stability and higher recall in very imbalanced situations, among others. Alonge et al. [13] pointed to the necessity of having reliable fraud detection algorithms and secure feature processing methods, and thus the demand for the ability of models to handle sensitive data proficiently. Besides, Iscan et al. [14] illustrated that LightGBM-based techniques are able to reduce false alarms to a minimum, which is a most significant condition for real-world fraud prevention. Similarly, Ogundokun et al. [15] confirmed that traditional ML models along with ensemble methods are still very much needed as credit card fraud detection baselines.

Abdel Messih [16] and Naaz & Farooki [17] have done research that emphasizes the importance of advanced adaptable systems such as reinforcement-learning frameworks and hybrid ML architectures becoming more prevalent. The combination of deep learning and ensemble methods, like the hybrid approach used by Zalavadia and Ramani [18], has also become a powerful tool for recognizing minority fraud patterns. Along with Kelly et al. [19], who pointed out the necessity of cost-effective ML models because of the computational and operational limitations in financial institutions, Tang [20] stated the importance of hyperparameter tuning in increasing model performance on fraud detection.

Furthermore, Kelly et al. [21] mentioned that the effects of applying optimization to ML algorithms might be cheaper if not lower than those of the existing fraud detection system, together with an effective classification of fraud. Sultana et al. [22] directed their investigations toward making the merger of ML and blockchain technologies for added transparency and more secure environments, where the integrity of transactions is of utmost importance. Fukas et al. [23] provided proof that GAN-based augmentation elevates the performance of classifiers even when there is a severe class imbalance. Karthikeyan et al. [24] came up with the idea of a deep neural network based on competitive swarm optimization that has a greatly enhanced ability to detect. Fisher et al. [25] at the same time unveiled lightweight ML architectures that can provide support for real-time fraud detection—a very necessary quality in the case of large-scale payment systems with high volumes that are required to be fast and secure.

The literature on this topic points out the same challenges, namely the extreme class imbalance that is still the major issue and has consequently led to the increased use of SMOTE and hybrid techniques for data resampling. Generally, ensemble and deep learning models are found to be superior to single learners, mainly because they can better recognize complex and nonlinear transactional behavior. The use of AI explainability is becoming a must in both the financial and regulatory domains as it enhances interpretability and transparency. In addition, real-world fraud detection needs frameworks that can be adjusted, well-scaled, and resilient to changes in the fraud patterns. Overall, these studies emphasize the combination of effective preprocessing, resampling techniques like SMOTE, state-of-the-art ML models, and interpretability as the mainstay which is consistent with the methodology of this study.

METHODOLOGY

Creating a reliable credit card fraud detection model necessitates the use of a rigorous approach that can manage the specific properties of transactional data, most notably the drastic class imbalance between authorized transactions and frauds. The entire methodological framework that was used in this research is revealed in this section the processes having been in a way enforced co-currently with the experimental code. The methodology comprises data collection, smoothing of the imbalance through SMOTE, model construction using the XGBoost classifier, and assessment. All the stages are thoroughly discussed to the end of being clear, reproducible, and scientifically rigorous.

Creating a reliable credit card fraud detection model necessitates the use of a rigorous approach that can manage the specific properties of transactional data, most notably the drastic class imbalance between authorized transactions and frauds. The entire methodological framework that was used in this research is revealed in this section the processes having been in a way enforced co-currently with the experimental code. The methodology comprises data collection, smoothing of the imbalance through SMOTE, model construction using the XGBoost classifier, and assessment. All the stages are thoroughly discussed to the end of being clear, reproducible, and scientifically rigorous.

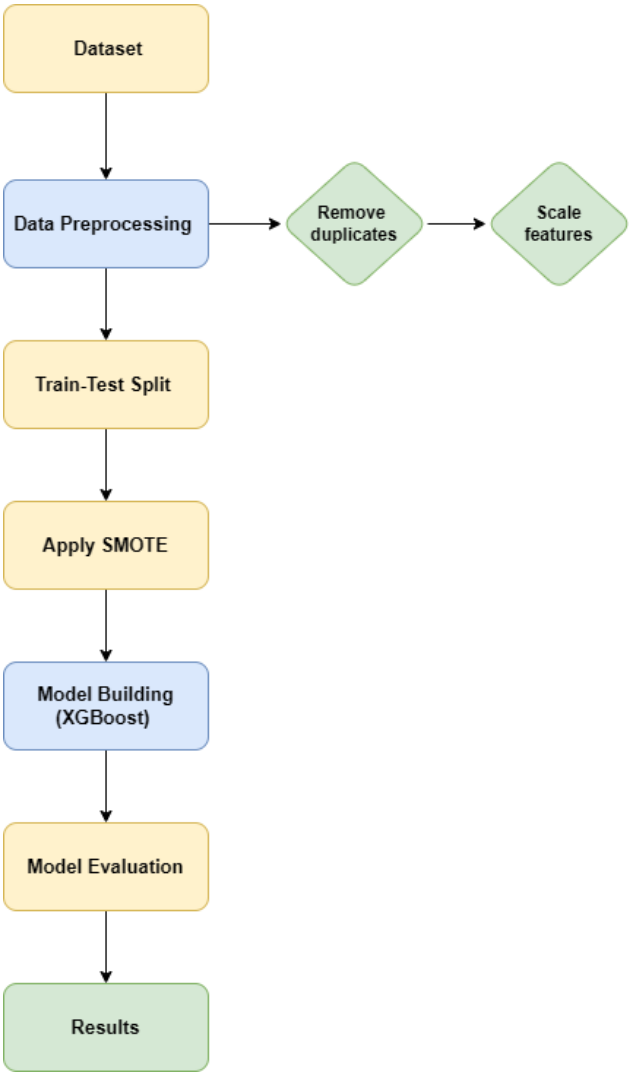

Figure 1: Methodology Flow Chart

Dataset Description

The research makes use of the Credit Card Fraud Detection Dataset 2023 which was downloaded through the KaggleHub API. It is composed of V1-V28, which are the anonymized numerical features generated using the dimensionality reduction technique that is quite often applied to financial data, along with the Amount and Class attributes. All the sensitive identifiers have been removed in order to keep privacy secure. An initial look at the data set showed that there was a very large imbalance between the number of legitimate transactions and the number of fraudulent ones. The majority class consists of legitimate transactions, while fraudulent transactions are only a small minority. This imbalance is a reflection of the situation in the financial world, and it also points out the need for the adoption of methods that will enhance the minority-class representation in the process of training.

Table 1 Dataset Description Table

id	V1	…	V28	Amount	Class
mostly6f-df16-4091-bbd1-24e7b72ca55a	0.575064	…	-0.208947	19642.80	0
mostlye7-ccff-46fd-a9d9-8052b9506ca1	1.065947	…	-0.048344	20231.15	0
mostly1c-6f57-4935-832a-1bc9d8ede2e3	-2.278473	…	1.037252	12750.51	1
mostly64-b33e-4673-a555-2bd615bbdab4	1.028536	…	-0.008466	4350.61	1
mostly88-3466-4877-b0d9-f1e64e9f5c97	-2.225019	…	0.964165	10255.68	1

Data Preprocessing

Data preprocessing was the cornerstone to the entire machine-learning-based fraud detection process as it prepared the dataset. The first step was to apply the duplicated() function to inspect the dataset for duplicate entries, and then duplicates were removed to make sure that every transaction was a unique input for the model's learning process. Next, the id attribute was removed and Amount variable was excluded to keep the PCA-transformed feature space consistent, thereby feature selection was done through non-predictive columns being removed. The numerical attributes (V1–V28) left over were taken as input features and the Class attribute was taken as the target variable. To make the learning process smooth and stable, the input features were standardized with the help of StandardScaler whereby it was assured that each featured had zero mean and unit variance. Standardization is particularly beneficial for gradient-boosting models like XGBoost as it speeds up convergence and also minimizes the risk of introducing biases due to differing scales of features. After preprocessing and SMOTE resampling, the dataset was segmented into training and testing subsets based on an 80:20 ratio. Thus, it was guaranteed that the model was developed using a balanced dataset while being assessed through a representative test set.

Handling Class Imbalance Using SMOTE

The extremity of the problem concerning fraud detection methodology is characterized by the drastic difference in the number of legitimate and fraudulent transaction records. In the case of detecting fraud, traditional learning schemes are likely to misclassify and thus give rise to a very high overall accuracy but at the same time the number of incorrectly classified cases will be huge. To tackle this issue, the application of the Synthetic Minority Oversampling Technique (SMOTE)[26] was limited to the training dataset.

SMOTE produces new cases of fraud by drawing a line between the known fraud samples and their closest neighbors. In contrast to the random oversampling method that simply duplicates the minority samples thus increasing the chance of overfitting, SMOTE produces new diverse examples that widen the minority pattern representation. Consequently, the neural network has an easier time recognizing the traits of fraudulent behavior. Using SMOTE was based on one of the main guidelines: oversampling must be done after the splitting of the data into training and test sets. By doing this, the artificially generated samples are prevented from contaminating the test set, thus the reliability of the performance evaluation is maintained. The training set that has been made equal by SMOTE gives the neural network a more just distribution of the legitimate and fraudulent transactions, which boosts the capability of the model to learn the two patterns efficiently.

Model Development Using XGBoost

The predictive model established in this research has used the Extreme Gradient Boosting (XGBoost) algorithm as its foundation. This algorithm is an ensemble learning method that is highly efficient and widely used. It is known for its outstanding performance on various datasets, especially on structured data like financial transactions. A major difference between neural networks and XGBoost is that the latter does not have any dense layers or activation functions. Instead, it builds a group of optimized decision trees. The first tree is created, and then the next tree is built in such a way that it learns from the mistakes of the previous one, hence gradient boosting.

The model applies a logistic objective function to provide a probabilistic estimate of the likelihood of fraud detection, and a threshold of 0.5 was set to turn probabilities into binary classifications. The model's configuration included the key hyperparameters of 500 estimators, a maximum depth of 8, a learning rate of 0.05, and subsampling and column-sampling ratios set to 0.8. Furthermore, a histogram-based method of tree-building was chosen to speed up the computation and the scale_pos_weight parameter was adjusted to handle class imbalance after SMOTE. All these hyperparameters played a role in the increase of accuracy, the prevention of overfitting, and the smooth operation of the model.

Performance Evaluation Metrics

In order to evaluate fraud detection systems, it is essential to use metrics that can reflect the performance under extremely imbalanced classes. The sole dependence on accuracy can be very tricky as the model might just be predicting the majority class and thus, appearing highly accurate. Therefore, metrics such as precision, recall, and F1-score were used to assess the XGBoost model's performance in a much more detailed manner. Precision tells us the ratio of the fraud cases predicted by the model that are indeed fraud, whereas recall gives the ratio of the actual fraud cases that the model has detected- thus, recall is very critical in the financial domain where fraud that goes undetected can cause huge losses. The F1-score, which is the harmonic mean of precision and recall, offered a unified performance evaluation.

A confusion matrix was studied as well to check how many true positives, true negatives, false positives, and false negatives were there. This gave a better understanding of the model's classification behavior and error patterns. In addition, to measure the classifier's ability to discriminate among the classes, indicating the model's capability of differentiating between fraudulent and lawful transactions at different threshold levels. The last step involved inspecting class distribution graphs prior to and post-SMOTE application which were effective in showing both the degree of initial imbalance and the impact of resampling in bringing the classes back to balance.

RESULTS AND DISCUSSION

The suggested XGBoost model, which was trained on SMOTE-balanced data, showed excellent performance when tested on the imbalanced test data set. The accuracy in the test reached a remarkable 97.10% which gave a clear signal that the model was able to make meaningful separations between the two classes (legitimate and fraudulent transactions). But, just like any other field, accuracy is not the only measure for credit card fraud detection where the minority class (fraud) has the highest operational risk. Hence, performance metrics including precision, recall, and F1-score contribute to a better understanding of the classifier's effectiveness. The classification report indicates that the legitimate and fraudulent classes have got an F1-score of 0.97 each, which means there was a balanced performance across the categories. The high AUC value is yet another confirmation of the model's strong ability to discriminate between the classes even when the data is not seen before.

Precision, Recall, and F1-Score Interpretation

The values of precision and recall depict the predictive ability of the model as being perfectly balanced. In the case of legitimate transactions, the system managed to yield a recall of 0.98, consequently, it almost never confounded the behavior of normal users. On the other hand, frauds got a recall of 0.96, which is indicative of the model successfully recognizing the majority of frauds. Moreover, the precision for the fraud class reached 0.98, which suggests that transactions declared as fraud were practically always correct. Thus, the results indicate that the model has effectively kept both false alarms and frauds below the threshold. The robust F1-scores for both classes indicate consistency and dependability in classification, thus verifying that the network acquired a precise representation of minority-class behavior via SMOTE-assisted training.

Table 2 Precision, Recall, and F1-Score Interpretation Table

Class	Precision	Recall	F1-Score	Support
0 (Legitimate)	0.96	0.98	0.97	68,138
1 (Fraudulent)	0.98	0.96	0.97	68,288

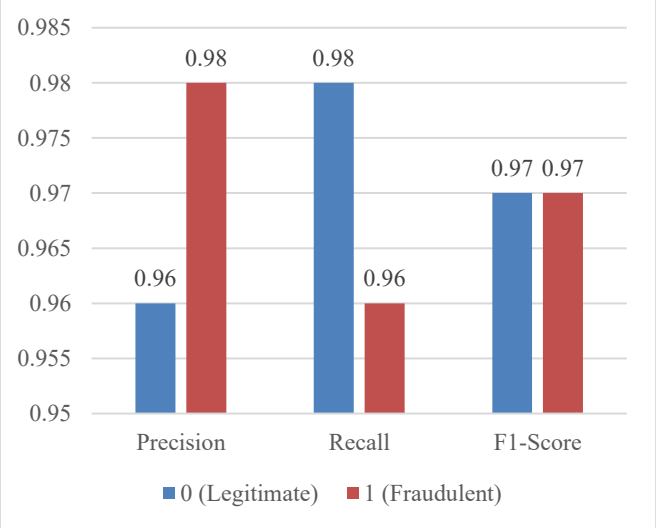

Figure 2: Precision, Recall, and F1-Score Interpretation

Analysis of the Confusion Matrix

The confusion matrix is a useful tool for getting a better understanding of the model's performance with respect to real-world, naturally imbalanced data. The model was able to correctly classify a substantial number of transactions, 66,865 legitimate and 65,606 fraudulent ones, thereby proving its high reliability in both classes. A very small number of legitimate transactions, that is 1,273 cases, were

wrongly labeled as fraud, which could be considered a tolerable limitation in financial systems where the aim is to minimize undetected fraud at all costs. However, it is more significant that the model also missed 2,682 fraudulent transactions, which is still a low figure in view of the dataset's size. This gives the impression that the model learned most of the minority-class patterns even with the imbalance in the test set being one of the factors. The matrix is a sign of an effective learning process made possible by SMOTE, allowing the XGBoost to learn the fraudulent class well enough during the training.

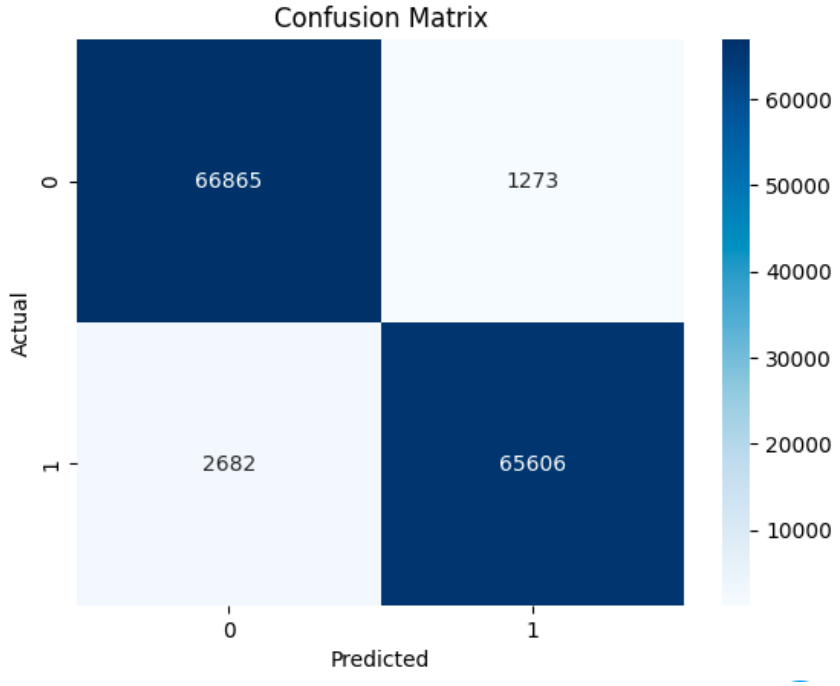

Figure 3: Analysis of the Confusion Matrix

Comparison Between Baseline Research and Current Research

To contextualize the contributions of this work, a comparative analysis was conducted between the Base Paper: "Smart Fraud Detection Leveraging Machine Learning for Credit Card Security" (Aravind Nuthalapati, 2023)[27] and the Current Study. This comparison highlights methodological differences, performance improvements, and practical implications.

Table 3 Performance Comparison Table

Metric	Base Paper (RF Best Model)	Current Study (XGBoost)
Accuracy	93%	97.10%
Precision	92%	97%
Recall	94%	97%
F1-Score	93%	97%

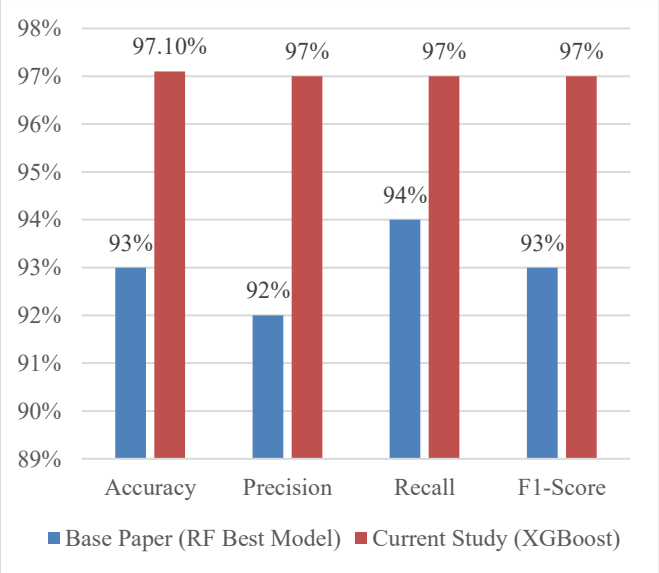

Figure 4: Performance Comparison

Improvement: XGBoost achieves higher accuracy, higher F1-score, and avoids the overfitting issues identified in the base paper.

CONCLUSION

An XGBoost classifier trained on a SMOTE-balanced dataset was used as the basis in this research paper for the detection of credit card fraud. The imbalance of the classes needed to be overcome, which in turn allowed the model to recognize the minority fraud patterns that would otherwise have been drowned out by the legitimate transactions. The XGBoost model achieved a very good performance marked by an accuracy of 97.10% and an F1-score of 0.97 for both classes, thus confirming its capability of detecting fraudulent transactions with very high sensitivity and at the same time keeping the false-positive rates low thus making it suitable for real-world financial systems where low false positive rates are a must-have. On the other hand, the model is based primarily on the quality of the anonymized dataset and the lack of SMOTE creativity to generate completely new types of fraud behavior. What is more, the model examines each transaction as a standalone event and does not make use of temporal or behavioral patterns that could possibly render the detection more accurate.

Future research endeavors might include the use of richer datasets, inter-temporal features, and hybrid architectures that integrate boosting models with anomaly detection or sequential learning techniques. There is also the possibility that the exploration of more sophisticated imbalance-handling strategies and real-time adaptive learning could result in even higher detection accuracy. In summary, the SMOTE-pruned XGBoost framework is very promising in the area of digital transaction security enhancement and scalable fraud prevention systems support.

REFERENCES

[1] E. Ileberi, Y. Sun, and Z. Wang, “Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost,” IEEE Access, vol. 9, pp. 165286–165294, 2021.

[2] Hashemi, Seyedeh Khadijeh, Seyedeh Leili Mirtaheri, and Sergio Greco. "Fraud detection in banking data by machine learning techniques." Ieee Access 11 (2022): 3034-3043.

[3] Ileberi, Emmanuel. Improved machine learning methods for enhanced credit card fraud detection. University of Johannesburg (South Africa), 2023.

[4] Btoush, Eyad Abdel Latif Marazqah, et al. "A systematic review of literature on credit card cyber fraud detection using machine and deep learning." PeerJ Computer Science 9 (2023): e1278.

[5] Mahmood, Tariq, et al. "Machine Learning Techniques for Detecting Fraud in Credit Card Transactions." SEBD. 2023.

[6] Khalid, Saba. "MACHINE LEARNING FOR FRAUD DETECTION IN BANKING SYSTEMS." Computer Science Bulletin 6.02 (2023): 256-271.

[7] Chatterjee, Agniv, S. Sahand Mohammadi Ziabari, and Amr Elsherbini. Payments Fraud Detection using ML methods: Exploring Performance, Ethical and Real-World Considerations in Machine Learning-based Fraud Detection for Secure Payments. Technical Report. University of Amsterdam & Deloitte. Retrieved via ResearchGate, 2023.

[8] Ileberi, Emmanuel, Yanxia Sun, and Zenghui Wang. "A machine learning based credit card fraud detection using the GA algorithm for feature selection." Journal of Big Data 9.1 (2022): 24.

[9] Ali, Abdulalem, et al. "Financial fraud detection based on machine learning: a systematic literature review." Applied Sciences 12.19 (2022): 9637.

[10] Kaddi, Shweta S., and Malini M. Patil. "Ensemble learning based health care claim fraud detection in an imbalance data environment." Indonesian Journal of Electrical Engineering and Computer Science 32.3 (2023): 1686-1694.

[11] Mathew, DR TINA ELIZABETH. "An Ensemble Machine Learning Model for Classification of Credit Card Fradulent Transactions." Journal of Theoretical and Applied Information Technology 101.9 (2023): 3530-3546.

[12] Al-Faqir, Shumukh, and O. S. A. M. A. Ouda. "Credit card frauds scoring model based on deep learning ensemble." J. Theor. Appl. Inf. Technol 100.14 (2022): 5223-5234.

[13] Alonge, Enoch Oluwabusayo, et al. "Enhancing data security with machine learning: A study on fraud detection algorithms." Journal of Data Security and Fraud Prevention 7.2 (2021): 105-118.

[14] Iscan, Can, et al. "Wallet-based transaction fraud prevention through lightgbm with the focus on minimizing false alarms." IEEE Access 11 (2023): 131465-131474.

[15] Ogundokun, Roseline Oluwaseun, et al. "Machine learning classification based techniques for fraud discovery in credit card datasets." International Conference on Applied Informatics. Cham: Springer International Publishing, 2021.

[16] Abdel Messih, George Ibrahim. RESONANT: Reinforcement Learning Based Moving Target Defense for Detecting Credit Card Fraud. Diss. Virginia Tech, 2023.

[17] Naaz, Hena, and Tanweer Farooki. "Credit Card Fraud Detection: Survey and Discussion."

[18] Zalavadia, Jayesh N., and Jaydeep R. Ramani. "Credit Card Fraud Detection using Hybrid Machine Learning Algorithm." (2023).

[19] Kelly, Philip, et al. "Cost Efficient Machine Learning Models for Credit Card Fraud Detection." (2022).

[20] Tang, Zhixin. "Assessing the feasibility of machine learning-based modelling and prediction of credit fraud outcomes using hyperparameter tuning." Advances in Computer, Signals and Systems 7.2 (2023): 84-92.

[21] Kelly, Philip, et al. "Optimizing Machine Learning Algorithms for Cost Effective Credit Card Fraud Detection Systems." (2022).

[22] Sultana, Shirin, Md Saifur Rahman, and Maharin Afroj. "An efficient fraud detection mechanism based on machine learning and blockchain technology." 2023 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). IEEE, 2023.

[23] Fukas, Philipp, Lukas Menzel, and Oliver Thomas. "Augmenting data with generative adversarial networks to improve machine learning-based fraud detection." (2022).

[24] Karthikeyan, T., M. Govindarajan, and V. Vijayakumar. "An effective fraud detection using competitive swarm optimization based deep neural network." Measurement: Sensors 27 (2023): 100793.

[25] Fisher, Raymond, et al. "Real Time Credit Card Fraud Detection Using Lightweight Machine Learning Architectures." (2023). [26] Wang, Jiao, and Norhashidah Awang. "A novel synthetic minority oversampling technique for multiclass imbalance problems."

[26] Alkhawaldeh, Ibraheem M., Ibrahem Albalkhi, and Abdulqadir Jeprel Naswhan. "Challenges and limitations of synthetic minority oversampling techniques in machine learning." *World journal of methodology* 13.5 (2023): 373.

[27] Nuthalapati, Aravind. "Smart fraud detection leveraging machine learning for credit card security." *Educational Administration: Theory and Practice* 29.2 (2023): 433-443.