Credit Card Fraud Detection based on Random Forest Model

1st Sorin-Ionuț Mihali
Faculty of Information Systems and Cyber Security
Military Technical Academy "Ferdinand I"
Bucharest, Romania
sorin.mihali@mta.ro

2nd Ștefania-Loredana Niță
Faculty of Information Systems and Cyber Security
Military Technical Academy "Ferdinand I"
Bucharest, Romania
stefania.nita@mta.ro

***Abstract*— Credit card fraud detection is a critical challenge in the financial sector, necessitating effective models for handling imbalanced data. This study explores the application of the Random Forest algorithm, emphasizing its performance in addressing the intricacies of data distribution. Building upon existing research, the model is refined through advanced data processing methods and optimized hyperparameters. The proposed solution encompasses detailed insights into data processing, tackles imbalanced data challenges using Synthetic Minority Over-sampling Technique (SMOTE), and employs Random Forest with entropy as the guiding criterion. Evaluation metrics, including accuracy, precision, recall, and F1-Score, assess model performance. Comparative results showcase the model's efficacy in reducing undetected fraudulent transactions, particularly in scenarios with imbalanced data. The discussion delves into the nuanced trade-offs between false positives and false negatives, highlighting the model's adaptability in diverse data distributions. The study concludes by outlining future research directions, emphasizing scalability, personalized detection capabilities, and real-world testing to enhance credit card fraud detection systems.**

Keywords*— *Random Forest, Credit Card, Fraud Detection, Imbalanced Data, Entropy

I. Introduction

Credit cards, originating in the early 20th century, have become essential for convenient and secure transactions worldwide, with their popularity and the availability for different options continuing to grow [1]. In today's digital era, credit cards extend beyond physical form into digital wallets like Apple Pay, Google Wallet, and Samsung Pay, enabling information to be stored on smartphones for contactless payments [2]. Credit card integration with online payment systems and e-commerce platforms has increased online shopping, easily enabling worldwide purchases. Technology such as tokenization, which protects card details, and two-factor authentication improves transaction security [3]. However, there are several concerns related to cybersecurity, including the risks of fraud, identity theft, or the security of transaction data [4]. The 2023 Payments Threats and Fraud Trends Report [5] highlights the increasing complexity of social engineering and phishing attacks, the persistence of malware threats, including advanced persistent threats (APTs), botnets, distributed denial-of-service (DDoS) attacks, and the persistent risk of malware, highlighting the financial sector's vulnerability and the need for robust cybersecurity measures. A representative report [6] shows the following statistics: a significant percent of global credit card fraud, nearly 46%, occurs in the United States. Projections indicate that by 2026, credit card fraud worldwide will grow up to $43 billion, with the U.S. experiencing losses exceeding $12.5 billion by 2025 alone. This growing concern is reflected in consumer attitudes, with 48% of them believing that merchants bear the responsibility to shield them from fraud. Interestingly, the majority of fraudulent credit and debit card transactions, about 55%, involve sums less than $100, suggesting that smaller transactions are often targeted by fraudsters.

In recent years, Artificial Intelligence (AI) and Machine Learning (ML) have gained significantly increasing applicability in different domains, including the financial sector. AI and ML algorithms are applied in different analytics, including online payment fraud detection. ENISA's opinion paper [7] has included machine learning as a possible way for financial fraud detection since 2018. Also, in 2019, VISA highlighted how financial institutions can use machine learning [8]. In this paper, we propose a credit card fraud detection technique based on the random forest algorithm based on work [9]. We show that the proposed method achieves better results in fraud detection of credit card transactions than related work [9], including evaluation metrics, such as accuracy, precision, recall, and F1-Score. While the related work [9] incorporated a specific set of features, preprocessing steps, and hyperparameter tuning techniques, we addressed this issue through significant adjustments in how the data was manipulated. Through intensive analysis and optimization of relevant features, we increased the overall accuracy of the Random Forest algorithm. Additionally, we made substantial adjustments to hyperparameters to optimize the trade-off between precision and recall. The rest of the paper is organized as follows: Section II provides an overview of representative related work, Section III discusses the proposed approach and the implementation, and Section IV discusses the results and comparison with related work. Finally, Section V presents the conclusions of the paper.

II. Related Work

In the pursuit of optimal and effective solutions for fraud detection, numerous algorithms have been explored and refined. As fraud methodologies continually evolve [10], the need for information systems capable of adapting to the increasingly diverse profiles of malevolent actors becomes imperative. One algorithm that has demonstrated remarkable performance in classification problems, as highlighted in [11], is the Random Forest algorithm.

The study [12] delves into an extensive exploration of various supervised machine learning algorithms for detecting fraudulent transactions in credit card data. The research aims to provide a comprehensive understanding of the strengths and weaknesses of different algorithms in the context of credit card fraud detection. By analyzing the comparative results, the study aims to shed light on the efficacy of each algorithm and

979-8-3503-4929-0/24/$31.00 ©2024 IEEE

identify potential candidates for robust fraud detection systems. Another relevant contribution to the field is found in the work [13]. This research encompasses both a literature review and a comprehensive survey of existing machine learning algorithms employed in the detection of fraudulent credit card transactions. By examining the current state of the art in fraud detection techniques, the study aims to provide insights into the evolving landscape of credit card fraud and the corresponding advancements in algorithmic approaches. A more recent study [14] analyzes the efficiency of logistic regression, random forest, and decision trees in scenarios for classification, prediction, and identifying instances of fraudulent credit card transactions. The authors evaluate the performance of different models and demonstrate that the random forest model has the highest accuracy in predicting and detecting fraudulent credit card transactions, with an accuracy of 96%. Research [15] has explored advanced machine learning techniques for detecting credit card fraud. One study applied hybrid models incorporating Ada Boost and majority voting strategies, introducing noise levels of 10% and 30% to improve effectiveness, with the voting system proving superior under noisy conditions. Another research [16] focused on using random forests to differentiate between typical and abnormal transactions, using data from a Chinese ecommerce platform to assess performance. Despite challenges like imbalanced data affecting efficacy on smaller datasets, random forests showed promising results. Further, an analysis of various machine learning algorithms [17] identified Random Forest, Xgboost, and Decision Tree as the most effective in predicting fraud, achieving high accuracy with by resampling methods to train the models.

III. The Proposed Solution

A. Data Processing

In this paper, we use the Credit Card Transactions Fraud Detection Dataset [18]. This dataset provides two different partitions used for the fundamental phases of machine learning: training and testing. The dataset contains simulated instances of both legitimate and fraudulent banking transactions. It is important to note that these transactional data are synthetically generated for the purpose of algorithm evaluation and do not contain real-world bank or customer data.

The dataset contains approximately 1.3 million rows of training data and 550,000 rows of test data, each characterized by 23 features free of missing values. During model training, an essential feature is the binary “is_fraud” label, where 0 represents a non-fraudulent transaction, and 1 signifies a fraudulent one.

The account holder's “age” is computed based on the “dob” feature of the dataset, while the “trans_date_trans_time” feature breaks down transaction timestamps into periods such as “Morning”, “Lunch”, “Afternoon”, and “Night”, aiding in establishing temporal patterns and time intervals between transactions by the same user, which is stored in “day_period”. The geographical distance (stored in the “distance”) between the payment location and the merchant's location, computed using the features “lat”, “long”, “merch_lat”, and “merch_long” of the dataset, is also a significant feature. The “cc_freq” feature represents the frequency of a specific card's usage for transactions by the user.

The data scaling process uses the Robust Scaler [19] for standardizing data across various features and minimizing the impact of outliers. The transformation of object-to-numeric values is based on the Weight of Evidence technique, particularly used in the financial domain for effective model training [20].

TABLE I. SELECTED FEATURES

Name	Description
amount	transaction amount
gender	cardholder’s gender
hour	hour of the transaction
day_period	period of the day of the transaction
age	cardholder’s age
distance	distance between merchant location and transaction location
hour_bet_trans	hour difference since last transaction
cc_freq	credit card usage frequency
category	category of the purchased product

B. Imbalanced Data

In machine learning, imbalanced datasets present a significant challenge, especially in contexts such as fraud detection. The imbalance in class distribution, with the minority class typically embodying fraud instances being less represented, can result in models biased towards the majority class.

To address this issue, the SMOTE (Synthetic Minority Oversampling Technique) technique is applied. By synthetically generating instances of the minority class (Fig. 1), SMOTE mitigates the imbalance, enhancing the model’s ability to distinguish patterns related to fraud. This technique proves to be essential in fraud detection scenarios where fraudulent activities are relatively rare compared to legitimate transactions [21].

Fig 1. Data before and after SMOTE

C. Random Forest Model

Random Forest, known for its improved prediction accuracy and reduced overfitting, is an effective ensemble learning method based on decision trees. This technique employs binary trees to iteratively divide datasets by features, effectively labeling instances and adeptly identifying intricate data relationships [22].

We have employed entropy as the guiding criterion for decision tree construction within Random Forest. Entropy, defined in Eq. (1), provides an essential measure of dataset impurity [23]. The optimization of decision tree splits by minimizing entropy at each node aligns with our goal of achieving robust decision structures.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using

a right tab stop. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

$$H(S) = -\sum_{i=1}^{c} p_i \, log_2(p_i) \quad (1)$$

The predilection for entropy over alternative criteria, such as Gini, is motivated by its capacity to provide a comprehensive metric for assessing dataset impurity and keeping diversity within decision trees. Prioritizing entropy in this context is intended to enhance the ensemble's generalization and robustness by evaluating probability distributions within the dataset [22]. Another essential aspect related to the Random Forest model involves efficient control of the number of features considered at each split, focusing on the overall quantity of features in the model. This strategic constraint, keeping diversity among decision trees, prevents overfitting to noise and contributes significantly to the ensemble's stability [24]. Another aspect that caused us to choose Random Forest is the ratio between the execution time and the value of the result obtained, avoiding overfitting.

D. Evaluation Metrics

As presented in [25], there are several quantitative metrics that we can assess in determining the performance of a fraud detection system, as well as for comparison with other existing research. For this study, following the computing of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN), we used the following evaluation metrics:

$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN) \quad (2)$$

$$\text{Precision} = TP / (TP + FP) \quad (3)$$

$$\text{Recall} = TP / (TP + FN) \quad (4)$$

$$\text{F1-Score} = 2 \times \text{Precision} \times \text{Recall} / (\text{Precision} + \text{Recall}) \quad (5)$$

$$\text{False Negative Rate} = FN / (FN + TP) \quad (6)$$

$$\text{False Positive Rate} = FP / (FP + TN) \quad (7)$$

In the context of fraud detection, our primary purpose is to minimize the False Negative Rate (FNR) to prevent unauthorized transactions. Simultaneously, we aim to avoid causing inconvenience to legitimate users, so the False Positive Rate (FPR) should also be minimal. Therefore, a suitable evaluation metric is the F1-Score, which establishes a balance between Precision and Recall. To overcome individual decision tree limitations, Random Forest employs an ensemble learning approach, constructing multiple trees and aggregating their predictions for improved generalization and robustness.

IV. Results And Discussion

The evaluation of our model's performance, as depicted in Tables II and III, aligns with the specified values and provides a comprehensive analysis of its capabilities in managing imbalanced and balanced datasets. A comparison model [9] is employed as a reference point to prove the effectiveness of our approach.

Our model exhibits robust performance in scenarios involving imbalanced data, where the negative class substantially outweighs the positive class. Table II summarizes the evaluation of our model for imbalanced data for six performance metrics by applying Eq. (2)-(7), as well as the comparison with reference [9] model, while Table III summarizes the results for balanced data. For imbalanced data, our model achieves a FPR of 0.62%, while the comparison model demonstrates a FPR value of 0.007%. This underscores the comparison model's proficiency in correctly identifying instances of the negative class while minimizing false positives. Further, the FNR value for our model is 20.37%, slightly higher than the comparison model's 30.17%. While a higher FNR signifies instances where the model fails to identify positive cases, it is essential to consider that our model attains a superior F1-Score of 0.86 compared to the comparison model's 0.81. This implies that our model strikes a more optimal balance between precision and recall. Our model's recall stands at 0.79, outperforming the comparison model's 0.69. The precision indicates the high accuracy of positive predictions made by our model, although the comparison model has a slightly better one.

TABLE II. IMBALANCED DATA

Performance Metric	Our Model	Comparison Model [9]
FPR (%)	0.62	0.007
FNR (%)	20.37	30.17
F1-Score	0.86	0.81
Recall	0.79	0.69
Precision	0.95	0.97
Accuracy	0.999	0.998

In the context of balanced data scenarios, our model consistently demonstrates high performance across key metrics, proving its adaptability and reliability. The FPR remains impressively low at 0.21%, showing our model's ability to maintain a balance between correctly identifying negative instances and minimizing false positives, comparable to the comparison model's FPR of 0.038%. A significant highlight is the substantial reduction in the FNR to 15.3%, outperforming the comparison model's FNR of 23.54%. This improvement underscores our model's efficacy in accurately identifying positive instances within a balanced dataset. Despite this, the F1-Score remains at a competitive 0.82, aligning closely with the comparison model's performance, proving a good balance between precision and recall. Our model's outstanding recall of 0.85 surpasses the comparison model's 0.76, indicating its superior ability to capture positive instances in the presence of balanced data.

TABLE III. BALANCED DATA

Performance Metric	Our Model	Comparison Model [9]
FPR (%)	0.21	0.038
FNR (%)	15.3	23.54
F1-Score	0.82	0.82
Recall	0.85	0.76
Precision	0.79	0.88
Accuracy	0.998	0.998

With the constraint of the chosen data set, as presented in Table II and III, our model obtains better results in terms of FNR, the basic metric of our study (decrease of 9.8% in the case of imbalanced data, respectively 8.24% in the case of those balanced), the rest of the evaluation metrics remaining at a competitive value with the comparison model.

The most important improvements that have contributed to obtaining the result are the use of Robust Scaler

in case of data preparation, to make the model resistant to outliners, and SMOTE for imbalanced data. Regarding the construction of the model, after several empirical attempts to set hyperparameters, we concluded that the criterion of entropy, in combination with setting the number of features for each tree as 4, have led to the best results in the validation stage.

V. Conclusion

This paper highlights the effectiveness of machine learning technologies in addressing financial fraud in the contemporary digital context. Our comparative results indicate that the enhanced Random Forest algorithm has achieved noteworthy performance in reducing the rate of undetected fraudulent transactions compared to the related work. This improvement has significant implications for critical metrics such as the F1-score, reflecting a better balance between recall and precision. In the context of the trade-off between the False Positive Rate (FPR) and False Negative Rate (FNR), there emerges a prioritization of preventing fraudulent transactions, even at the expense of potential inconveniences for users not involved in fraud. This approach reflects an increased focus on the financial safety of users, with the consequence of accepting temporary discomfort in the process of authentication of transactions.

Future research directions focus on improving personalized detection capabilities and expanding model testing in a real test environment involving direct interactions with clients, for a better evaluation of it. These efforts are essential for strengthening the efficiency of fraud detection systems, tailoring them specifically to the particular needs of users, and thus ensuring robust and personalized financial security.

References

[1] S. Madan, S. Sofat, and D. Bansal, 'Tools and Techniques for Collection and Analysis of Internet-of-Things malware: A systematic state-of-art review', Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 10, pp. 9867-9888, 2022.

[2] A. A. Al-Qudah, M. Al-Okaily, G. Alqudah, and A. Ghazlat, 'Mobile payment adoption in the time of the COVID-19 pandemic', Electron Commer Res, Jun. 2022, doi: 10.1007/s10660-022-09577-1.

[3] A. M. Sahi, H. Khalid, A. F. Abbas, K. Zedan, S. F. Khatib, and H. Al Amosh, 'The research trend of security and privacy in digital payment', in informatics, MDPI, 2022, p. 32. Accessed: Mar. 06, 2024. [Online]. Available: https://www.mdpi.com/2227-9709/9/2/32

[4] S. Badotra and A. Sundas, 'A systematic review on security of Ecommerce systems', International Journal of Applied Science and Engineering, vol. 18, no. 2, pp. 1-19, 2021.

[5] 2023 Payment Threats and Fraud Trends Report. [Online]. Available: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2023-12/EPC181-23%20v1.0%202023%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

[6] M. Rej, 'Credit Card Fraud Statistics (2024)'. [Online]. Available: https://merchantcostconsulting.com/lower-credit-card-processing-fees/ credit-card-fraud-statistics/

[7] Financial Fraud in the Digital Space. [Online]. Available: https: //www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/ financial-fraud-in-the-digital-space

[8] 'Machine Learning and Financial Institutions'. [Online]. Available: https://usa.visa.com/partner-with-us/visa-consulting-analytics/machine-learning-and-financial-institutions.html

[9] Ashraf, I., "Credit Card Fraud Detection", Kaggle, 28 Nov 2023, https://www.kaggle.com/code/islamashraaf/credit-card-fraud-detection.

[10] Cuccia, Joseph. "Fraud in Banking: A Review of Fraud Scams, Effects, and Antifraud Techniques in the Banking Industry." (2023).

[11] Trivedi, Naresh Kumar, et al. "An efficient credit card fraud detection model based on machine learning methods." International Journal of Advanced Science and Technology 29.5 (2020): 3414-3424.

[12] Dhankhad, Sahil, Emad Mohammed, and Behrouz Far. "Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study." 2018 IEEE international conference on information reuse and integration (IRI). IEEE, 2018.

[13] Sadineni, Praveen Kumar. "Detection of fraudulent transactions in credit card using machine learning algorithms." 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (ISMAC). IEEE, 2020.

[14] J. K. Afriyie et al., 'A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions', Decision Analytics Journal, vol. 6, p. 100163, Mar. 2023, doi: 10.1016/j.dajour.2023.100163.

[15] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, 'Credit Card Fraud Detection Using AdaBoost and Majority Voting', IEEE Access, vol. 6, pp. 14277-14284, 2018, doi: 10.1109/ACCESS.2018.2806420.

[16] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random Forest for credit card fraud detection", in 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), Mar. 2018, pp. 1-6. doi: 10.1109/ICNSC.2018.8361343.

[17] K. Ayorinde, A Methodology for Detecting Credit Card Fraud. Minnesota State University, Mankato, 2021. [Online]. Available: https://search.proquest.com/openview/59691d4dd638a54a88862f6c8ca9d494/1?pq-origsite=gscholar&cbl=18750&diss=y

[18] Shenoy, K., "Credit Card Transactions Fraud Detection Dataset", Kaggle, 5 Aug2020, https://www.kaggle.com/datasets/kartik2112/fraudetection.

[19] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., . . . & Vanderplas, J. (2011). Scikit-learn: Machine learning in Python. Journal of Machine Learning Research, 12, 2825-2830.

[20] Abdou, Hussein A. "Genetic programming for credit scoring: The case of Egyptian public sector banks." Expert systems with applications 36.9 (2009): 11402-11417.

[21] Chawla, Nitesh V., et al. "SMOTE: synthetic minority over-sampling technique." Journal of artificial intelligence research 16 (2002): 321357.

[22] Breiman, Leo. "Random forests." Machine learning 45 (2001): 5-32.

[23] Shannon, Claude E. "pA Mathematical Theory of Communication, qBell System Technical Journal." (1948): 379r423.

[24] Liaw, Andy, and Matthew Wiener. "Classification and regression by randomForest." R news 2.3 (2002): 18-22.

[25] Jain, Yashvi, et al. "A comparative analysis of various credit card fraud detection techniques." International Journal of Recent Technology and Engineering 7.5 (2019): 402-407.