DOI: 10.5748/20CONTECSI/PSE/ECO/7305

eLocator: e207305

MACHINE LEARNING IN ECOMMERCE FRAUD DETECTION: A SYSTEMATIC LITERATURE REVIEW AND COMPARATIVE ANALYSIS OF ADVANCED TECHNIQUES

Thiago Rocco – https://orcid.org/0000-0001-9580-8464
Instituto De Pesquisas Tecnológicas - Ipt

Adriano Galindo Leal – https://orcid.org/0000-0001-7114-6830
Instituto De Pesquisas Tecnológicas - Ipt

Machine Learning in E-Commerce Fraud Detection: A Systematic Literature Review and Comparative Analysis of Advanced Techniques.

ORCID:xxxx-xxxx-xxxx-xxx ORCID:xxxx-xxx-xxx-xxxx

Abstract—**In an era characterized by extensive credit use and rapidly advancing technology, mitigating fraud in online transactions is more critical than ever. This paper presents a systematic literature review (SLR) on applying Machine Learning Methods in fraud detection in online shopping.In addition, a comparative analysis of a more comprehensive array of Machine Learning techniques, including Logistic Regression, Decision Tree, Random Forest, SVM, KNN, and Neural Networks with CNN, ANN, Transformers, and Autoencoder, were applied to detect fraud in the heavily imbalanced dataset provided by IEEE-CIS**[1]**, a common characteristic in real-world fraud detection scenarios.This study explores the limitations, opportunities, and challenges ofapplying these machine learning models in detecting credit card fraud in e-commerce, shedding light on the significant potential and current limitations of such approaches.**

Our comparative analysis found that the Random Forest algorithm also demonstrated robust performance, attaining a close accuracy of 95,5%.Interestingly, the Transformers utilizing the pre-traineddistilbert-base-uncased model achieved the highest performance, reaching an accuracy of 90,1%. It also offers anoverview of machine learning applications in e-commerce fraud detection, emphasizing the importance of algorithm selection, data preprocessing, and ethical data handling. It underscores the potential of these strategies in minimizing financial fraud, thereby contributing to the security and trustworthiness of online transactions.

Keywords-MachineLearning,FraudDetectionSystem,E-commerce,CreditCardFraud.

I. INTRODUCTION

The advent of the COVID-19 pandemic has spurred a dramatic shift in consumer behavior, ushering in an era of unprecedented growth in e-commerce. As physical stores shuttered and consumers stayed home, the world turned to online shopping. This cultural shift towards the consumption of online goods is not a temporary change; it has laid the foundation for a new norm in the post-pandemic world. However, this surge in online transactions has increased the potential for fraud. This mounting threat poses significant challenges for e-commerce enterprises, financial institutions, and unsuspecting customers. Consequently, implementing robust and practical strategies to counteract fraud in online transactions has become more crucial than ever.

Machine learning techniques stand out among various strategies because they can process massive amounts of data and uncover patterns indicative of fraudulent activities. These techniques can continually adapt, honing their accuracy based on the most recent data, making them an invaluable tool in fraud detection.

Machine learning's versatility is evident through various techniques, including decision trees, SVM, logistic regression, and neural networks. However, the efficacy of each method depends on several factors, such as the volume and quality of data, sample characteristics, and the company's specific requirements. No single approach is universally practical, and the selection often necessitates careful consideration of these factors.

Combating e-commerce fraud necessitates a comprehensive approach that merges innovative technology with expert human analysis. It implies working alongside cybersecurity experts and machine learning specialists to create and maintain potent fraud detection systems. Moreover, staying abreast of evolving trends and techniques in fraud detection is pivotal to ensuring enduring customer protection.

E-commerce fraud detection is a crucial and complex task that demands constant vigilance and innovative solutions. Machine learning techniques offer a powerful tool in this fight against fraud, provided they are complemented by expert human analysis and an ongoing commitment to staying updated in this fast-evolving field.

II. RELATED WORKS

The methodology guiding the study presented in this paper was the Systematic Literature Review (SLR), as delineated in [2]. The primary objective of this SLR was to identify existing techniques and market-validated methods that can be applied to datasets, thereby augmenting the efficacy of fraudulent transaction analyses and pinpointing opportunities for fraud prevention in real-world scenarios.

The SLR process was segmented into three stages: planning, conducting, and reporting the results. During the planning stage, the research question was formulated, and the criteria for study selection were defined. The conduct phase entailed systematic literature exploration andselecting and evaluating relevant studies. Lastly, in the results stage, findings drawn from the analysis of the selected studies were presented.

III. SYSTEMATIC REVIEW PLANNING

The Systematic Literature Review (SLR) planning stage establishes the research protocol and identifies the necessity for the SLR. This stage comprises seven steps, which are detailed below:

A. Research Objective

This research aims to attain an elevated level of accuracy in analyzing fraudulent activities within e-commerce transactions involving credit card payments. This goal is achieved by applying Machine Learning techniques underpinned by a thorough systematic review.

B. Search Source Definition Criteria

The sources chosen for this research meet the criteria of being publicly available, providing full-text access, and being relevant in computer science, specifically for topics related to our research subject. For this study, we considered the globally recognized databases IEEE Xplore (https://ieeexplore.ieee.org/xplore/), Scopus Digital Library (http://www.scopus.com/), and ISI Web of Science (http://www.webofscience.com/). These data sources are widely known for their extensive collection of academic articles and journals, making them invaluable for conducting our systematic literature review on the machine learning methodsapplied in fraud detection.

C. Search String Criteria

The database search was performed in December 2022. Keywords were utilized to construct search queries, with the AND operator serving to refine and retrieve the most relevant works related to the topic. The search string was as follows: ("Machine Learning” and "Fraud Detection System" and "Credit Card Fraud" and "E-commerce")

D. Inclusion Criteria

The following criteria were established to select appropriate studies:

- Published in English or Portuguese.
- Regarding methods or techniques applicable within the field of machine learning.
- Regarding the methods applied in their experiments, along with the corresponding results.
- Performed a comparative analysis of machine learning techniques using metrics.

E. Exclusion Criteria

The following criteria were used to exclude unrelated or insufficiently informative studies:

- Duplicate entries, in which case the most recent version is considered, provided the content is similar.
- Incomplete documents.
- Studies without a clear overview or adequate information about the objectives.
- Studies that do not align with the objectives of this work.
- Studies that do not discuss Machine Learning techniques.
- Studies that do not describe techniques applicable to Machine Learning.
- Studies that do not apply relevant techniques by the research focus.
- Studies published after 2018.

F. Strategy for Study Selection

All the studies were cataloged and imported into JabRef for better visualization using a card system. The selection process involved an initial review of metadata (title, abstract, and keywords) and a pre-evaluation of the studies most relevant to the research, applying the inclusion and exclusion criteria. The selected texts were then earmarked for the extraction phase. An Excel file tracked which studies were included to enhance visibility.

G. Strategy for Data Summarization and Synthesis.

The data summarization and synthesis strategy involves writing a clear, concise summary of the results obtained from the systematic review. The results will be summarized and evaluated for quality and quantity to develop a comprehensive report encompassing pertinent considerations and observations. Data synthesis may also include supplementary reviews and statements, such as identifying literature gaps, emerging trends, limitations of the studies analyzed, and recommendations for future research. The aim is to convey a comprehensive overview of the systematic review results, emphasizing the most important and relevant information concisely and coherently.

IV.Analysis of Results

The Systematic Literature Review (SLR) was conducted from December 2022 to February 2023. During this interval, a total of ninety-four articles were identified and evaluated. The preliminary evaluation phase was based on the titles and abstracts of the articles, employing the previously defined inclusion and exclusion criteria. Consequently, five works were deemed relevant to the research topic and selected for further analysis.

Table 2 includes the critical studies related to the topic. For a comprehensive list of the analyzed literature, refer to the project's GitHub repository [3].Figure 1 visually represents the entire process adopted in the SLR.These results represent the set of studies that will be used as the basis for data analysis and synthesis.

Table 1 – Synthesisofpapersaccordingtoextractionfields

1stpaper
AnEfficientCreditCardFraudDetectionSystemusingDeep Learning-BasedApproaches [2].
Synthesis
[2]focuses on an efficient credit card fraud detection system utilizing deep learning-based methodologies. The authors propose a method, depicted in Figure 1, that leverages Naive Bayes (NB), Generative Adversarial Networks (GAN), and Neural Networks (NN) to scrutinize transactions and flag suspicious activities. This endeavor is geared towards maintaining customer confidence in the electronic payment system, which is frequently exploited by fraudsters. The article also integrates insights from other pertinent academic studies.
DataExtraction
Models and Techniques: The Paper highlights the application of Support Vector machines (SVM), Decision Trees, and Neural Networks (NN) in related studies. Additionally, the fraud detection system proposed by the authors employs Naive Bayes (NB), Generative Adversarial Networks (GAN), and Neural Networks (NN) for transaction monitoring and the identification of suspicious activities.
Conclusion and Results: The article puts forward a system employing techniques such as Naive Bayes (NB), Generative Adversarial Networks (GAN), and Neural Networks (NN) for transaction monitoring and fraud detection to enhance trust for users (both customers and suppliers). Despite the inherent complexity of fraud detection, using Naïve Bayes resulted in high rates of false positives and negatives, thereby impacting the model's accuracy due to data imbalance. A Neural Network with backpropagation was utilized to address this and achieve a superior balance, improving accuracy.

2ndpaper
AReviewofCreditCardFraudDetectionUsingMachineLearningTechniques. [4]
Synthesis
This paper concentrates on credit card fraud detection utilizing machine learning techniques. It elucidates the theoretical underpinnings of fraud detection systems, clarifies existing machine learning methodologies employed to confront banking fraud detection issues, and offers a comparative analysis of these techniques based on various criteria. The objective is to present comparative evaluations of existing procedures to mitigate credit card fraud and provide solutions predicated on machine learning techniques.
DataExtraction

Models and Techniques: ThePaper mentions a broad array of models and techniques, including Support Vector Machines (SVM), Logistic Regression, Decision Trees, Random Forest, Naive Bayes, Multiplayer Perceptron, K-Nearest Neighbors (KNN), Convolutional Neural Networks (CNN), Adaptive Boosting (ADB), Bagging (BAG), Neural Networks (NN), Extreme Gradient Boosting (XGBoost), and Gradient Boosted Trees.
Conclusion and Results: The Paper underscores the significance of machine learning in fraud detection and its potential benefits in real-world applications. Several techniques are presented as promising solutions, though they must continually evolve, given that fraudsters also exploit similar methods to commit fraud. The findings reveal that anomaly detection techniques and neural networks are most effective for detecting credit card fraud. However, the precision and sensitivity of these techniques can change depending on the dataset and the nature of the scam. Consequently, selecting the most suitable technique for the dataset's characteristics and the specific type of fraud to be detected is paramount.

3rdpaper
CCFD-Net: a novel deep learning model for credit card fraud detection. [5]
Synthesis
This study introduces a new deep learning model, the CCFD-Net, explicitly designed for credit card fraud detection. Developed by a global team of experts, this model aims to assist merchants and consumers in mitigating financial losses caused by credit card fraud. The model leverages sophisticated deep learning techniques, including the 1D-Conv process and the Resnet framework, to surpass traditional machine learning methods in fraud detection performance.
DataExtraction
Models and Techniques: The Paper discusses the use of K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Logistic Regression (LR), K-Means, Self-Organizing Map Hybrid (SOM-Hybrid), and Convolutional Neural Networks (CNN) with LeNet-5.
Conclusion and Results: Deep neural network learning emphasizes data balancing. The study used three classifications: Fraud, Non-Fraud, and Invalid Data. Although this approach resulted in a new model that performs more effectively on numerical data, with AUROC metrics of 0.9 and an f1-Score of 0.58, it is markedly superior to traditional models, which tend to falter when dealing with imbalanced data. In the neural network, this issue is better managed and classified. This proposed new model demonstrates the feasibility and opens doors for future enhancements.

4thpaper
Imbalanced data Classification in Credit Card Fraudulent Activities Detection using Multi-Class Neural Network. [5]
Synthesis
This paper proposes a method to manage imbalanced and misclassified data, where fraudulent credit card transactions can be easily mistaken for legitimate transactions, posing detrimental effects on the entire sales chain.
DataExtraction
Models and Techniques: The article focuses on Multi-class Neural Networks (MCNN) and

the Long Short-Term Memory (LSTM) method.

Conclusion and Results: initially, transactions are categorized into three types: fraudulent, non-fraudulent, and invalid records. The invalid records are ignored, reducing the time required to compare fraudulent and non-fraudulent transactions. However, a noted limitation of this work is its sole reliance on data from e-commerce sources.

5thpaper

Credit Card Fraud Detection Based on Machine Learning. [7]

Synthesis

A team of global experts developed this model to aid merchants and consumers in mitigating financial losses stemming from credit card fraud. The dataset consists of more than 410,000 credit card transaction records, from which 178,393 were chosen as test data. The fraud frequency represents 1.2% of the transaction frequency, highlighting the significant class imbalance within the credit card datasets. During data preprocessing, the Synthetic Minority Over-sampling Technique (SMOTE) manages imbalanced data, enabling a balanced 1:1 ratio between legitimate and fraudulent transactions. The proposed algorithm is juxtaposed against Random Forest and Gradient Boosting Machine algorithms, and cross-validation results, including average AUC score and training time, are obtained. The primary objective is detecting anomalies and analyzing data distribution to identify fraudulent transactions.

DataExtraction

Models and Techniques: The models and techniques mentioned in the paper include LightGBM, Random Forest, and Gradient Boosting Machine. Area Under the Curve (AUC) and Receiver Operating Characteristic (ROC) are applied metrics. Moreover, the SMOTE technique is employed as a data augmentation method to tackle the class imbalance issue in the dataset.

Conclusion and Results: The paper juxtaposes the effectiveness of three binary classification models: LightGBM, Random Forest (RF), and Gradient Boosted Machine (GBM). While both RF and GBM exhibit commendable performance in credit card fraud detection, the LightGBM model displays a slightly superior AUC score and can enhance the fraud detection rate by 1%. Another real-world dataset is trained to demonstrate the model's generalizability, showing the LightGBM model's robust performance on both datasets. Consequently, LightGBM outperforms the other models.

V. PROPOSED WORK

In this study, machine learning algorithms are used to process the available data, with the resulting outcomes being evaluated through metrics like accuracy, precision, recall, F1 score, sensitivity, and specificity. The proposed models include Random Forest, SVM, Logistic Regression, Convolutional Neural Networks, Autoencoder, Artificial Neural Networks, and Transformers. A pre-trained model from the Hugging Face company [8]is utilized for the Transformer model.The following steps outline the research procedure:

- Loading the transaction data and dividing it into training and test sets at an 80:20 ratio.
- Conducting Principal Component Analysis (PCA) on the data, retaining fifty components.

- Applying balancing, normalization, and cross-validation techniques using SMOTE [7] [9] and Stratified K Fold Cross Validation.
- Implementing the chosen algorithms, recording their performance metrics, including the confusion matrix, and conducting a final comparison among the models.

By following these steps, machine learning algorithms are applied to the transaction data, and their efficacy is evaluated using the specified metrics. Outcomes are then compared using a confusion matrix, offering a comprehensive analysis of the model's performance regarding true positives, true negatives, false positives, and false negatives.

VI. RESULTS

In this chapter, the focus is on analyzing and discussing the results of the metrics. The analysis examined the top performers in the IEEE-CIS Fraud Detection competition [1] to comprehend the techniques, methodologies, and strategies adopted. Most participants primarily used three algorithms: LightGBM, CatBoost, and XGBoost.

Our proposed research evaluates the results using various algorithms, including Support Vector Machines (SVM), Random Forest (RF), Logistic Regression (LR), K-Nearest Neighbors(KNN), Autoencoders (AE), Convolutional Neural Networks (CNN), Artificial Neural Network (ANN), and Transformers. Each algorithm presents distinct advantages and considerations, which we will explore more deeply.

The final stage involves a comparative evaluation using the accuracy metric. This metric is crucial as it shows the proportion of correct predictions, providing a general overview of the model performance. However, accuracy may only sometimes give a partial picture, particularly in imbalanced classes. Therefore, additional metrics such as precision, recall, and the F1 score might be needed to understand each model's performance more comprehensively. This will be discussed further in the subsequent sections.

A. Exploratory Data Analysis

The dataset utilized in this study comprises 590,540 observations and 434 variables. There is a noticeable substantial imbalance between fraudulent transactions (20.663 positive class) and legitimate transactions (569.877 negative type).

Addressing this imbalance during the data preprocessing stage is crucial because an unbalanced dataset can lead to biased predictions, where the model may be more likely to predict the majority class. Techniques like oversampling the minority class or undersampling the majority class can help mitigate this issue. It might also be beneficial to use specific metrics, such as the F1 score or the area under the receiver operating characteristic curve (AUC-ROC), that are more robust to class imbalance.

Further data exploration might reveal patterns, outliers, or other characteristics that can help refine the machine-learning models. It also plays a pivotal role in any data science project, allowing for a better understanding of the data at hand and guiding the subsequent preprocessing, modeling, and evaluation steps.To gain insights and identify patterns in the dataset, we performed the following preprocessing steps:

- Addressing NaN values: The dataset, consisting of approximately 45% NaN values, is cleaned by substituting these with zeroes.
- Standardizing Columns: Certain columns like 'Device Info' and 'Email Domain' provided by the vendor are standardized. This process reduces redundancy and ensures data consistency, contributing to more accurate analysis and prediction.

- Extracting Temporal Information: The 'TransactionDT' column is manipulated to extract crucial temporal details such as hours, days, weeks, months, and years. This data transformation provides valuable insights into transaction patterns that can be beneficial in identifying and predicting fraudulent activities.
- Learning from other participants: References are made to works of participants [10] [11]that align with the objectives of this article, which is to develop an effective anti-fraud model. This provides insights into methods that are effective in similar problems.
- Balancing and normalizing data: The Smote technique [12]balances and normalizes the data. Balanced and normalized data is crucial in machine learning algorithms to ensure the predictive model is unbiased and generalizes well to new data.

The preprocessing steps serve as the foundation for our analysis, addressing common issues that may impact the performance of machine learning algorithms. This is a vital stage in the data analysis pipeline, enhancing the model's accuracy by ensuring the data is in an appropriate format and potentially revealing additional insights or patterns.

Temporal characteristics were particularly informative, precisely the hourly pattern of transactions. There was a marked increase of over 50% in fraudulent transactions between 4 PM and 2 AM. Based on this pattern, we factored in the transaction hour as a key feature in our fraud detection model. By leveraging this temporal information, our model could be better equipped to identify potentially fraudulent transactions.

The dataset analysis further uncovered interesting characteristics regarding payment modalities and product categories. The balance between credit and debit payments was unusual, considering the e-commerce market and the population's purchasing power. Likewise, specific product categories, namely W and C, demonstrated higher volumes of fraudulent transactions. According to the Brazilian company Clearsale [13], fraudsters' preferences tend to focus on beverages and electronics.

These insights guided us in tailoring our fraud detection model, assigning a higher weight to features related to payment modalities and the mentioned product categories.

In the subsequent experiments, we applied machine-learning models to the preprocessed and feature-engineered dataset. The selected models included SVM, Random Forest, Logistic Regression, KNN, Autoencoders, CNN, ANN, and Transformers. The accuracy, precision, recall, and F1 score evaluated each model's performance.

Figure1provides visual representations of our findings:

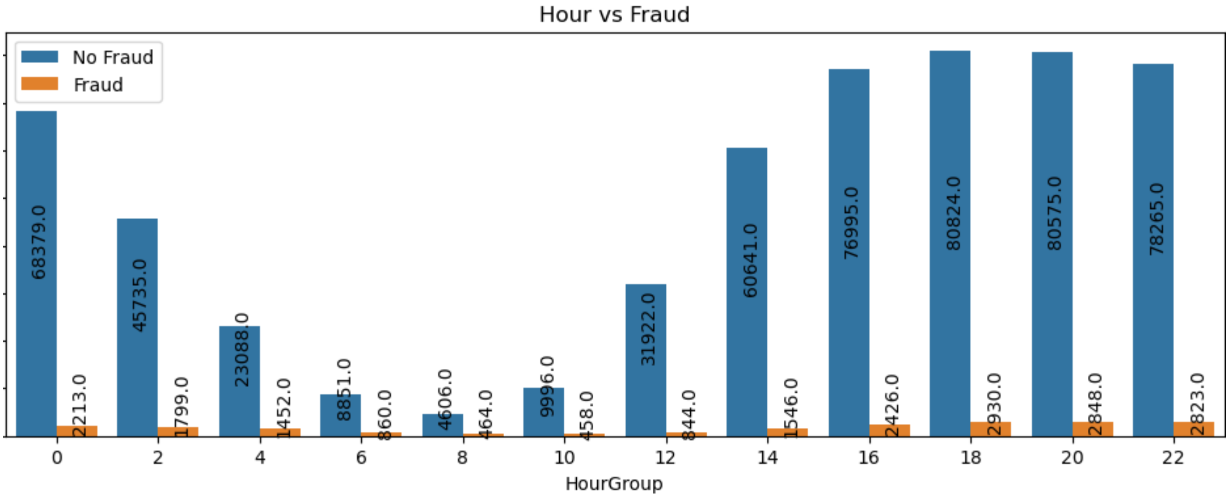

Figure 1 - TransactionDatetime (Hour) x Fraud

As a result, we noticed that the Transformer model outperformed the others, demonstrating its potential as a powerful tool for credit card fraud detection. However, the suitability of each model can significantly depend on the specifics of the task and the dataset at hand. Hence, we recommend selecting an appropriate model based on the dataset's unique characteristics and the type of fraud that needs to be detected.

In conclusion, our analysis highlights the potential effectiveness of machine learning techniques in credit card fraud detection. Our findings underscore the importance of careful preprocessing, feature engineering, and choosing the suitable model for the task. The insights gleaned from this study could be valuable to the broader AI community, particularly those in fraud detection and prevention.No further temporal analysis was considered as there was no valuable information for the study.

B. Results Evaluation

Table 2 and 3 presents a comparative analysis of the various models we used in our study, ranked by their accuracy performance.

Table 2 – Comparison of results

Model	Accuracy
Random Forest	95,5%
Transformer	90,1%
Decision Tree	89,7%
SVM	89,3%
KNN	86,1%
ANN	85,8%
Auto Encoders	84,4%
CNN	83,7%
Logistic Regression	73,3%

Table 3 – Matrix of Confusion

Model	TP	FN	FP	TN
Random Forest	47,9% 109.078	2,1% 4.856	1,8% 3.992	48,3% 110.025
Transformers	41,8% 8.130	8,5% 1.657	32,7% 6.369	17,0% 3.302
Decision Tree	44,3% 101.059	5,6% 12.875	3,6% 8.282	46,4% 105.735
SVM	43,8% 99.843	7,9% 18.094	2,8% 6.326	45,5% 103.689
KNN	44,9% 102.332	5,1% 11.602	1,4% 3.276	48,6% 110.741
ANN	45,7% 104.089	4,3% 9.845	4,9% 11.199	45,1% 102.818
Auto Encoders	82,6% 97.612	13,9% 16.363	1,8% 2.086	1,7% 2.047
CNN	43,3% 98.759	6,7% 15.216	9,7% 22.052	40,3% 91.924
Logistic Regression	41,0% 93.382	9,0% 20.552	17,7% 40.262	32,4% 73.755

The model resultsindicate the number of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN) observed. These metrics provide insight into how each model correctlyidentifiedfraudulent and non-fraudulenttransactions.

While accuracy is a crucial metric, it is also essential to consider the performance of the models in terms of False Positives and False Negatives. High numbers of False Positives (transactions flagged as fraudulent but legitimate) could lead to customer dissatisfaction. In contrast,increased False Negatives (fraudulent transactions missed by the model) could lead to economic loss. Thus, a balance between these aspects is necessary for an effective fraud detection system. The best model should have high accuracy andalower rate of false positives and negatives.

From our analysis, the Random Forest model demonstrated the highest accuracy [3].The following parameters were used: n_estimators = 100, max_depth = 20, and min_samples_split = 2.On the other hand, the Transformers modeled the parameters: AdamW optimizer, a learning rate of 1e-5, a batch size of 32, and 10 epochs [3]. However, the effectiveness of each model can significantly depend on the specifics of the task and the dataset at hand. Hence, we recommend selecting an appropriate model based on the dataset's unique characteristics and the type of fraud that needs to be detected.

In conclusion, our analysis underscores the potential effectiveness of machine learning techniques in credit card fraud detection. Our findings highlight the importance of choosing asuitable model for the task and adjusting it to best suit the data's unique characteristics.

C. Study Limitations

In the context of this article, due to the General Data Protection Law (LGPD) and the sensitivity of personal information, it washardto find companies willing to share accurate data for research purposes. Nowadays, organizations are concerned about the privacy and security of their customers' data, making it challenging to access real-world datasets.

Regarding bias, it is essential to acknowledge and address potential distortions in data collection, analysis, and interpretation. Discrimination can occur when the way data is collected is different from the studied population. This can lead to hasty or incorrect conclusions, impairing a precise understanding of the phenomenon under study.

In the case of this work, care was taken to avoid any bias related to characteristics such as ethnicity, social class, gender, or geographical location. The exclusion of such data may be adopted to ensure fairness and avoid unfair or discriminatory conclusions. It is important to consider ethics and equity when dealing with sensitive data and ensure that research is conducted fairly and responsibly.

By consciously avoiding selection bias and ensuring that the data used is representative and unbiased, efforts are made to ensure the reliability and validity of the research results.

VIII. Future Works

A critical aspect currently missing and could significantly improve the model's performance is the use of 'device fingerprint information. This could include data like device_id, device location, distance from residence address and delivery address, browser, migratory profile, and more related to purchases made through mobile devices. Collecting and integrating this type of information into future models could significantly enhance their fraud detection capabilities and represent a valuable area for further exploration in future research.

Even though transformers were used in this study, it is evident that their potential has not been thoroughly explored in the context of fraud detection.

IX. Conclusions

Machine learning algorithms offer an effective strategy to identify anomalous transactions in the dynamic fraud detection realm. Given the high volume and high dimensionality of transactional data, machine learning models find their niche in identifying patterns and anomalies effectively. This study explored multiple machine learning models to detect fraudulent activities in credit card transactions, presenting promising outcomes.

The Random Forest algorithm yielded the best performance with an accuracy of 95,5%. The Transformers algorithm, leveraging the pre-trained distilbert-base-uncased model from the Hugging Face library, yielded the second-best performance and demonstrated commendable results, achieving an accuracy of 95,5% after ten training epochs.

The robust performance of ensemble methods such as Random Forest in this high-dimensional task underscores their utility in classification tasks.

Interestingly, our analysis revealed that temporal features, precisely the transaction hour, play a significant role in identifying fraudulent transactions. This finding suggests that fraudsters may have preferred times for their illicit activities.

Nonetheless, it is crucial to note that striving for 100% fraud detection is unrealistic in practical settings, considering the dynamic nature of fraudulent behaviors, limitations related to data availability and quality, and the inherent trade-off between detecting as many frauds as possible and minimizing false alarms. The goal of an efficient fraud detection system should be to optimize this balance.

While pre-trained models, such as distilbert-base-uncased, exhibit the potential for enhancing model performance, their efficacy depends on the task's specific characteristics, the data quality, and the alignment between the data and the models' training data. Hence, it is vital to approach these models with an understanding of their limitations and strengths.

Acknowledging the challenges related to data privacy and potential biases, future research should concentrate on ethical data collection practices, ensuring confidentiality and fairness while obtaining robust, representative data for model training.

In conclusion, the domain of machine learning applications in fraud detection offers immense untapped potential. In an era of increasing digital transactions, such advancements could significantly enhance financial security and foster trust in digital platforms.Platforms.

Acknowledgment*(Heading5)*

Thepage is gray.

References

[1] I. C. I. Society, "IEEE-CIS Fraud Detection," [Online]. Available: https://www.kaggle.com/competitions/ieee-fraud-detection/data. [Accessed 18 03 2023].

[2] B. K. a. S. Charters, Guidelines for performing systematic literature reviews in software engineering, 2007.

[3] "GitHub - Thiago Rocco," [Online]. Available: https://github.com/thiagom128/Review-and-Application-of-Machine-Learning-Techniques-to-Detect-Fraud-in-Credit-Card-Transactions. [Accessed 22 03 2023].

[4] I. Ali, K. Aurangzeb, M. Awais, R. J. Ul Hussen Khan, and S. Aslam, "An Efficient

Credit Card Fraud Detection System using Deep-learning based Approaches," 2020.

[5] N. Boutaher, A. Elomri, N. Abghour, K. Moussaid, and M. Rida, "A Review of Credit Card Fraud Detection Using Machine Learning Techniques," in *Proceedings of 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech'20)*, 345 E 47th St, New York, NY 10017 USA, 2020.

[6] X. Liu, K. Yan, L. B. Kara, and Z. Nie, "CCFD-Net: a novel deep learning model for credit card fraud detection," in *2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science (IRI 2021)*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1264 USA, 2021.

[7] N. Prabha and S. Manimekalai, "Imbalanced data Classification in Credit Card Fraudulent Activities Detection using Multi-Class Neural Network," 2022.

[8] Y. Fang, Y. Zhang, and C. Huang, "Credit Card Fraud Detection Based on Machine Learning," *CMC - Computers Materials & Continua*, vol. 61, pp. 185-195, 2019.

[9] "Hugging Face – The AI community building the future," Hugging Face, [Online]. Available: https://huggingface.co/docs/transformers/model_doc/distilbert. [Accessed 30 04 2023].

[10] "Smote - Version 0.10.1," Imbalanced-learn.org, [Online]. Available: https://imbalanced-learn.org/stable/references/generated/imblearn.over_sampling.SMOTE.html. [Accessed 02 05 2023].

[11] "GitHub - Xiaoluoyfy," 13 11 2019. [Online]. Available: https://github.com/xiaoluoyfy/IEEE-CIS-Fraud-Detection. [Accessed 30 04 2023].

[12] Shejz, "GitHub - Shejz," 19 04 2020. [Online]. Available: https://github.com/shejz/IEEE-CIS-Fraud-Detection/blob/master/EDA/EDA_I.ipynb. [Accessed 30 04 2023].

[13] 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.

[14] C. Sale, "Mapa da Fraude - Resultados 2022 | ClearSale," Clear Sale, [Online]. Available: https://br.clear.sale/mapa-da-fraude. [Accessed 10 05 2023].