Forging the Future: Pioneering Approaches in Business, Management and Economics Engineering to Overcome Emerging Global Challenges - 2024

https://doi.org/10.24867/FUTURE-BME-2024-111 Original scientific paper

USING MACHINE LEARNING PRACTICES TO DETECT FRAUD AND RISK MANAGEMENT

Enio Yzeiri[1] *[0009-0000-4856-2916]*, *Egla Mansi*[2] *[0000-0002-1141-5020]*, *Nerajda Feruni*[3] *[0000-0002-0735-6486]*, *Aida Bitri*[4] *[0000-0002-3041-8833]*

Abstract

This paper presents a machine learning (ML) approach to detect credit card fraud and manage related risks in transactions. Traditional fraud detection systems struggle to adapt to evolving fraudulent patterns, leading to financial losses. ML techniques offer improved accuracy and efficiency in fraud detection. The proposed framework includes data preprocessing, feature engineering, model training, and evaluation. Key features such as transaction amount and location are extracted for analysis. ML models, including neural networks, decision trees, and logistic regression, are trained and evaluated using precision, recall, F1 score, and AUC-ROC. Cross-validation is employed for hyperparameter tuning, and a hybrid approach integrates supervised learning with anomaly detection to reduce false positives. Experiments use synthetic data to ensure privacy. This study contributes to safer and more transparent credit card transactions through advanced ML practices, enhancing fraud detection accuracy.

Key words: *Credit Card Fraud Detection, Machine Learning, Anomaly Detection, Risk Management.*

1. Introduction

Credit cards, widely used for transactions such as groceries, travel, and shopping, have become indispensable due to their convenience and perks like reward points (Tiwari et al., 2021). However, the rapid expansion of electronic commerce has also led to a rise in credit card fraud, involving identity theft and unauthorized transactions (Patil and Lilhore, 2018; Sharma et al., 2021). Fraudsters increasingly exploit digital tools such as VPNs and Tor networks, making it difficult

[1] Epoka University, Albania, eyzeiri21@epoka.edu.al
[2] Epoka University, Albania, emansi@epoka.edu.al
[3] Mediterranean University of Albania, Albania, nerajda.feruni@umsh.edu.al
[4] Epoka University, Albania, abitri@epoka.edu.al

to trace their activities. As society moves toward cashless payments, the need for robust fraud detection has intensified. This study explores the application of machine learning techniques—Artificial Neural Networks, Decision Trees, and Logistic Regression—to detect fraudulent activities using synthetic data. The findings demonstrate that synthetic datasets, when processed through machine learning classifiers, can effectively predict fraudulent transactions, safeguarding personal data and preserving privacy. This work builds on a rich body of literature that compares various fraud detection algorithms, with Random Forest, Decision Trees, and Neural Networks consistently demonstrating high accuracy (Afriyie et al., 2023; RB & KR, 2021; Kumar et al., 2022). The paper highlights the use of synthetic data to ensure privacy, offering insights into optimizing machine learning models for future studies in credit card fraud detection.

The paper is structured as follows: Section 1 reviews prior research on credit card fraud detection using machine learning. Section 2 details the data and variables used, while Section 3 outlines the methodology. Section 4 presents and discusses the results with graphical summaries. The paper concludes by summarizing findings, addressing limitations, and offering recommendations for future research.

3. Data

The study uses the "Credit Card Transactions Synthetic Data Generation" dataset by Rodrigues (2023), published on January 2, 2023. This synthetic dataset includes 5,000 customer profiles, 100 terminal records, and 1,785,308 transactions, containing no real credit card numbers, customer data, or personally identifiable information (PII). Key independent variables include daily transactions, transaction amount, terminals used, transaction time, and entry method. The dependent variable is fraud detection, while control variables such as customer profiles, spending behavior, bank identifiers, and location data provide additional context for analyzing fraudulent activities.

4. Methodology

The machine learning models were developed in Python using JupyterLab for efficient execution and result visualization. The process began by merging the datasets and removing irrelevant non-numeric columns. The imbalanced dataset was then balanced using the RandomOverSampler() function. Afterward, the dataset was trained on various machine learning models, with hyperparameter tuning applied to improve performance. Key performance metrics, including the Confusion Matrix, Classification Report, and AUC score, were gathered to evaluate and compare the models.

4.1 Measurement Metrics

The Confusion Matrix provides a detailed assessment of the model's classification performance by delineating four key outcomes: true positives (accurately identified fraudulent transactions), true negatives (correctly identified legitimate transactions), false positives (legitimate transactions incorrectly classified as fraudulent), and false negatives (fraudulent transactions not detected). The Classification Report offers a comprehensive summary of the model's efficacy through metrics such as accuracy (the proportion of correct classifications overall), precision (the proportion of accurately predicted fraud cases), recall (the model's capacity to detect actual fraud), and the F1 score (the harmonic mean of precision and recall, providing a balanced measure of performance). Additionally, the AUC score evaluates the model's discriminatory ability between fraudulent and legitimate transactions, with higher values signifying superior performance. The ROC curve, which plots the true positive rate against the false positive rate, serves as a visual representation of this capacity, with curves closer to the upper left corner indicating higher predictive accuracy.

4.2 Machine Learning Models

Three widely used machine learning models—Artificial Neural Networks (ANN), Decision Trees (DT), and Logistic Regression (LR)—were selected for analyzing fraudulent credit card transactions. ANNs, inspired by neural structures, were implemented using Keras and optimized through hyperparameter tuning to enhance accuracy, with performance measured by AUC, accuracy, confusion matrix, and classification report. Decision Trees, known for handling outliers and feature scaling, used the Gini Index for classification and were evaluated on similar metrics. Logistic Regression, effective for binary classification, provided interpretability by highlighting the influence of each variable on fraud detection, and its performance was also assessed using standard metrics.

5. Results and Discussion

The initial dataset comprised a total of 1,785,308 transactional records, out of which 3% were identified as fraudulent, while the remaining 97% consisted of legitimate transactions. Given this significant imbalance, it was necessary to balance the dataset before proceeding with model training. Figure 5.1 illustrates the frequency distribution of fraudulent and non-fraudulent transactions, providing both numerical and percentage representations. To further understand the relationships between fraudulent activities and other variables, a correlation analysis was performed using a correlation matrix. As depicted in **Figure 5.2**, no strong correlations were observed between the fraud variable and any other numerical variables in the dataset.

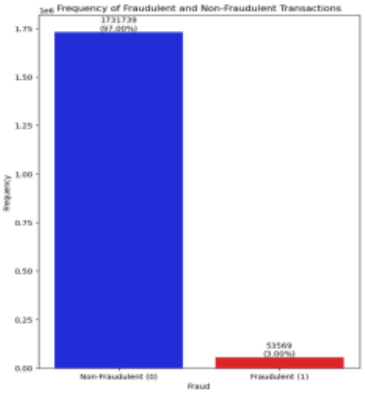

Figure 5.1: Frequency of Transactions

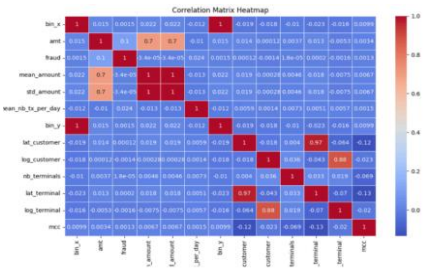

Figure 5.2: Correlation Matrix

The strongest correlation was observed between the fraud variable and the "amt" (transaction amount) variable, which demonstrated a weak positive correlation of 0.1. **Figures 5.3** display the distribution of transaction amounts for both fraudulent and non-fraudulent transactions. It is notable that fewer than one thousand transactions in either category exceeded an amount of 200 per purchase.

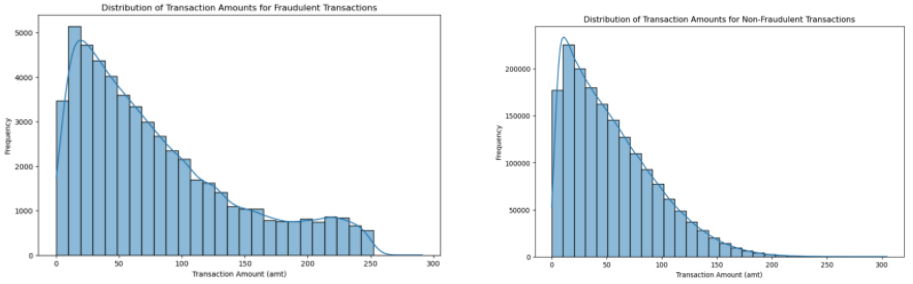

Figure 5.3: Distribution of Amount in Fraudulent and Non-Fraudulent Transactions

Based on the correlation analysis, no other significant relationships between fraudulent and non-fraudulent transactions were observed. Consequently, the next step involved training the machine learning models. For this purpose, a sample consisting of 20% of the overall dataset, amounting to 692,696 transactions, was used for analysis.

5.1 Results of the ANN Model

The confusion matrices for Artificial Neural Networks (ANN), Decision Trees (DT), and Logistic Regression (LR) reveal distinct performance levels in detecting fraud. ANN accurately classified 343,121 non-fraudulent transactions but struggled with fraud detection, achieving a low recall of 0.34%. In contrast, the DT model showed strong performance across all classifications, with an overall accuracy of

98%. The LR model performed the weakest, misclassifying 264,396 transactions and achieving only 61.8% accuracy. This comparison underscores the superior performance of the DT model, outperforming both ANN and LR in recall, precision, and accuracy.

Table 5.1: Comparison of Confusion Matrices for ANN, Decision Tree, and Logistic Regression Models

Model	Predicted Class	Actual Class: Not Fraud (0)	Actual Class: Fraud (1)
ANN	Not Fraud (0)	343,121	2,879
	Fraud (1)	228,900	117,796
DT	Not Fraud (0)	332,905	2879
	Fraud (1)	228,900	117,796
LR	Not Fraud (0)	235,928	110,072
	Fraud (1)	154,324	192,372

The classification reports for the ANN, Decision Tree (DT), and Logistic Regression (LR) models reveal notable differences in performance. The DT model excelled, with high precision, recall, and F1-scores of 0.98, indicating strong accuracy in identifying both fraud and non-fraud cases. In contrast, the ANN model, despite good performance on non-fraudulent transactions (0.99 recall), had poor fraud detection (0.34 recall), leading to lower weighted average recall and F1-score. The LR model showed the weakest performance, with precision, recall, and F1-scores around 0.62, highlighting its challenges in distinguishing between fraudulent and non-fraudulent transactions. Overall, the DT model outperforms both ANN and LR, particularly in handling unbalanced datasets.

Table 5.2: Comparison of Classification Report of Each Model

Class	*Metric*	*ANN*	*DT*	*LR*
Not Fraud (0)	Precision	0.60	1.00	0.60
	Recall	0.99	0.96	0.68
	F1-Score	0.75	0.98	0.64
	Support	346,000	346,000	346,000
Fraud (1)	Precision	0.98	0.96	0.64
	Recall	0.34	1.00	0.55
	F1-Score	0.50	0.98	0.59
	Support	346,696	346,696	346,696
Weighted Avg	Precision	0.79	0.98	0.62
	Recall	0.67	0.98	0.62
	F1-Score	0.63	0.98	0.62
	Support	692,696	692,696	692,696

The ROC curve analysis further differentiates the performance of the three models in detecting fraudulent transactions. The Decision Tree model demonstrated exceptional capability, achieving an AUC score of approximately 0.99. This result aligns closely with the findings of Afriyie et al. (2023) and RB & KR (2021), reflecting the model's high sensitivity and specificity in distinguishing between fraudulent and

non-fraudulent transactions. The ROC curve for the Decision Tree model is nearly identical to the ideal curve, indicating superior performance. In contrast, the Artificial Neural Network (ANN) model yielded an AUC score around 0.67, revealing a more modest performance with less effective separation between the classes. Similarly, the Logistic Regression (LR) model achieved an AUC score close to 0.66, demonstrating limited effectiveness in accurately classifying fraudulent transactions. These results corroborate the classification report findings, where the Decision Tree consistently outperforms both the ANN and LR models. This performance is in line with the conclusions of RB & KR (2021) and Afriyie et al. (2023), which highlight the Decision Tree's superior accuracy and reliability in detecting fraudulent transactions compared to the ANN and LR models.

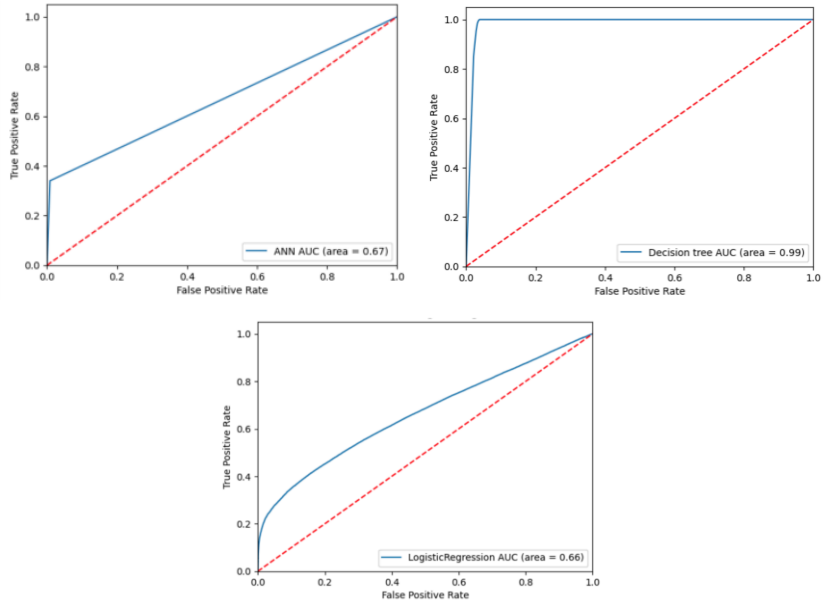

Figure 5.4: ROC Curve for the ANN, DT and LR Models

6. Conclusion

This study evaluated the effectiveness of synthetic credit card data for fraud detection using three machine learning models: Artificial Neural Networks (ANN), Decision Trees (DT), and Logistic Regression (LR). After balancing the dataset, the DT model achieved strong results, with accuracy, precision, recall, and F1-scores around 98% and an AUC of 99%. In contrast, ANN and LR showed lower accuracy at 66% and 61.8%, likely due to suboptimal hyperparameter tuning or difficulties with the imbalanced dataset. Future research should refine these models and explore additional algorithms, while companies could benefit from using Decision Trees with synthetic data to enhance privacy and security.

REFERENCES

[1] Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, *6*(100163), 100163. https://doi.org/10.1016/j.dajour.2023.100163

[2] Bakhtiari, S., Nasiri, Z., & Vahidi, J. (2023). Credit card fraud detection using ensemble data mining methods. *Multimedia Tools and Applications*, *82*, 29057-29075. https://doi.org/10.1007/s11042-023-14698-2

[3] Bing Chu, Y., Min Lim, Z., Keane, B., Hao Kong, P., Rafat Elkilany, A., & Hisham Abusetta, O. (2023). Credit card fraud detection on original european credit card holder dataset using ensemble machine learning technique. *Journal of Cyber Security*, *5*, 33–46. https://doi.org/10.32604/jcs.2023.045422

[4] Domor Mienye, I., & Sun, Y. (2023, March 27). A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection | IEEE Journals & Magazine | IEEE Xplore. Ieeexplore.ieee.org. https://doi.org/10.1109/ACCESS.2023.3262020

[5] Gupta, P., Varshney, A., Khan, M. R., Ahmed, R., Shuaib, M., & Alam, S. (2023). Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques. *Procedia Computer Science*, *218*, 2575–2584. https://doi.org/10.1016/j.procs.2023.01.231

[6] Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1). https://doi.org/10.1186/s40537-022-00573-8

[7] Kumar, S., Gunjan, V. K., Ansari, M. D., & Pathak, R. (2022). Credit Card Fraud Detection Using Support Vector Machine. Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications, 27–37. https://doi.org/10.1007/978-981-16-6407-6_3

[8] Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M.-S., & Zeineddine, H. (2019). An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection. *IEEE Access*, *7*, 93010–93022. https://doi.org/10.1109/access.2019.2927266

[9] Mittal, S., & Tyagi, S. (2019, January 1). Performance Evaluation of Machine Learning Algorithms for Credit Card Fraud Detection. IEEE Xplore. https://doi.org/10.1109/CONFLUENCE.2019.8776925

[10] Onyema, J. C., Betrand, C. U., & Benson-Emenike, M. (2023). Machine Learning Credit Card Fraud Detection System. *Applied Sciences Research Periodicals*, *1*(6), 19–28.

[11] Patil, V., & Lilhore, U. K. (2018). A Survey on Different Data Mining & Machine Learning Methods for Credit Card Fraud Detection International *Journal of Scientific Research in Computer Science*, *3*(5), 320–325. http://doi.org/10.13140/RG.2.2.22116.73608

[12] Asha, R. B., & Suresh Kumar, K. R. (2021). Credit Card Fraud Detection Using Artificial Neural Network. G*lobal Transitions Proceedings*, *2*(1) 35–41. https://doi.org/10.1016/j.gltp.2021.01.006
[13] Rodrigues, C. (2023, January). Credit Card Transactions Synthetic Data Generation. Www.kaggle.com. www.kaggle.com/datasets/cgrodrigues/credit-card-transactions-synthetic-data-generation
[14] Sailusha, R., Gnaneswar, V., Ramesh, R., & Rao, G. R. (2020, May 1). 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 1264–1270, https://doi.org/10.1109/ICICCS48265.2020.9121114
[15] Sarma, D., Alam, W., Saha, I., Alam, M. N., Alam, M. J., & Hossain, S. (2020). Bank Fraud Detection using Community Detection Algorithm. 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA). https://doi.org/10.1109/icirca48905.2020.9182954
[16] Sharma, P., Banerjee, S., Tiwari, D., & Patni, J. C. (2021, November). Machine Learning Model for Credit Card Fraud Detection - A Comparative Analysis. *The International Arab Journal of Information Technology*, *18*(6), 789–796. http://doi.org/10.34028/iajit/18/6/6
[17] Taha, A. A., & Malebary, S. J. (2020). An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine. *IEEE Access*, *8*, 25579–25587. https://doi.org/10.1109/access.2020.2971354
[18] Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., & Singh, A. K. (2021). Credit Card Fraud Detection using Machine Learning: A Study. ArXiv:2108.10005 [Cs]. https://doi.org/10.48550/arXiv.2108.10005