Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 2, April 2024
https://doi.org/10.47709/cnahpc.v6i2.3816

Submitted : May 02, 2024
Accepted : May 31, 2024
Published : June 03, 2024

Comparative Analysis of Machine Learning Models for Credit Card Fraud Detection in Imbalanced Datasets

Gregorius Airlangga[1)*]
[1)]Atma Jaya Catholic University of Indonesia, Indonesia
[1)]gregorius.airlangga@atmajaya.ac.id

ABSTRACT

This study presents a comprehensive evaluation of various machine learning models for detecting credit card fraud, emphasizing their performance in handling highly imbalanced datasets. We focused on three models: Logistic Regression, Random Forest, and Multilayer Perceptron (MLP), using a dataset comprising 555,719 transactions, each annotated with 22 attributes. Logistic Regression served as a baseline, Random Forest was evaluated for its high accuracy and low dependency on hyperparameter tuning, and MLP was tested for its capability to identify non-linear patterns. The models were assessed using ROC AUC, Matthews Correlation Coefficient (MCC), and precision-recall curves to determine their effectiveness in distinguishing fraudulent transactions. Results indicated that the Random Forest model outperformed others with a ROC AUC of 0.9868 and an MCC of 0.6638, showing substantial superiority in managing class imbalances and complex data interactions. Logistic Regression, although useful as a benchmark, exhibited limitations with a high number of false positives. MLP showed potential but was prone to a significant false positive rate, suggesting a need for further model refinement. The findings highlight the importance of choosing appropriate models and feature engineering techniques in fraud detection systems and suggest avenues for future research in real-time model deployment and advanced algorithmic strategies.

Keywords: Credit Card Fraud, Machine Learning, Imbalanced Datasets, Random Forest, Precision

1. INTRODUCTION

The rapid escalation of digital financial transactions globally has been accompanied by an equally significant rise in fraudulent activities, posing severe challenges for financial institutions and consumers alike (Alawida, Omolara, Abiodun, & Al-Rajab, 2022; Kanu et al., 2023; Zhu et al., 2021). Fraud detection, particularly in the domain of credit card transactions, is a critical area of focus due to the direct financial implications and the potential erosion of trust in payment systems (Ahmad, Khan, & Iqbal, 2024; Chung & Lee, 2023; Putrevu & Mertzanis, 2023). Traditional methods of fraud detection, predominantly rule-based systems, have increasingly been found wanting against the sophistication of modern fraudulent tactics (Alzahrani & Aljabri, 2022; Darwish, 2020; Reddy et al., 2024). These systems suffer from rigid detection rules that fraudsters can easily evade, highlighting the need for more adaptive and intelligent solutions (Almahmoud, Hammo, Al-Shboul, & Obeid, 2022; V. P. Kumar, Pallavi, & Prakash, 2021; Rusia & Singh, 2023). The literature on fraud detection is rich and varied, focusing largely on advancing methodologies that can cope with the complexities of transaction data and the clever disguises used by modern fraudsters (Saporta & Maraney, 2022). Early studies in this field relied heavily on statistical and data mining techniques that offered limited success in identifying complex fraud patterns (Kumaraswamy, Markey, Ekin, Barner, & Rascati, 2022). However, with the advent of machine learning, the landscape of fraud detection has shifted towards more dynamic and predictive modeling approaches. Machine learning offers the promise of not only capturing non-linear relationships in high-dimensional data but also adapting to new, previously unseen fraud tactics. Research such as (Alarfaj et al., 2022; Botchey, Qin, & Hughes-Lartey, 2020; S. Kumar, Gunjan, Ansari, & Pathak, 2022) has demonstrated the potential of various machine learning models, including decision trees, neural networks, and support vector machines, to significantly enhance the detection rates of fraudulent transactions.

Despite these advancements, several challenges remain. The primary issue is the imbalanced nature of fraud detection datasets, where fraudulent transactions are significantly outnumbered by legitimate ones (Kanchana, Naresh, Deepa, Pandiaraja, & Stephan, 2022). This imbalance can skew the performance of predictive models towards the majority class, resulting in a high number of false negatives. Furthermore, many existing models require extensive

* Corresponding author

Submitted : May 02, 2024
Accepted : May 31, 2024
Published : June 03, 2024

computational resources that may not be feasible in real-time transaction screening scenarios (Liang et al., 2022). Additionally, there is often a lack of comprehensive comparative studies that analyze the performance of different machine learning techniques across a uniform dataset (Merghadi et al., 2020). This research utilizes a publicly available credit card fraud dataset from Kaggle, which contains anonymized transaction data of stimulated banking transaction. This research aims to bridge these gaps by implementing and comparing a suite of advanced machine learning models, including Logistic Regression and Random Forest, on a robust dataset of credit card transactions. These models are selected for their ability to handle large, imbalanced datasets and their suitability for binary classification tasks like fraud detection. We hypothesize that these advanced models, coupled with appropriate preprocessing techniques and the Synthetic Minority Over-sampling Technique (SMOTE), will outperform traditional models in detecting fraudulent transactions (Mondal, Haque, Hassan, & Shatabda, 2021; Ni, Li, Xu, Wang, & Zhang, 2023).

The contributions of this research are threefold. First, it provides a detailed comparative analysis of both traditional and advanced machine learning models on a large, real-world credit card fraud dataset. Second, it evaluates the impact of SMOTE in addressing class imbalance within these models. Third, it offers insights into the trade-offs between different models in terms of accuracy, computational efficiency, and real-time applicability. The remainder of this article is structured as follows. The methodology section describes the dataset, feature engineering techniques, model selection, and evaluation metrics. The results and discussion section presents the findings of our experiments, comparing the performance of the models and discussing their implications for practical fraud detection systems. The conclusion summarizes the study's findings and suggests avenues for future research, including potential improvements in model training and feature selection techniques.

2. LITERATURE REVIEW

The complexity and severity of financial fraud, particularly in the context of credit card transactions, necessitate sophisticated detection techniques. As financial transactions increasingly migrate to digital platforms, the methods employed to detect and prevent fraud must evolve correspondingly. This literature survey reviews key developments in fraud detection, focusing on the transition from traditional methods to advanced machine learning techniques, and highlights the ongoing challenges and innovations in the field. Initially, fraud detection systems relied heavily on rule-based algorithms and simple statistical techniques. These methods were predicated on sets of rules crafted by experts, which were used to flag transactions that appeared anomalous or matched known fraudulent patterns (Hussein, Khairy, Najeeb, & Alrikabi, 2021) While effective for known fraud types, these systems lacked the flexibility to adapt to new fraud patterns, leading to high false positive rates and poor scalability under evolving fraud tactics.

The limitations of rule-based systems prompted researchers to explore machine learning (ML) techniques that could learn from data and identify hidden patterns indicative of fraud. Techniques such as decision trees, k-nearest neighbors (KNN), and logistic regression were among the first to be adopted (Udayakumar, Sreekumar, Nivedha, Sivasubramanian, & Umadevi, 2023). These methods offered improved detection capabilities overrule-based systems by adapting to changes in fraudster tactics over time. However, they often struggled with the high dimensionality of transaction data and the imbalanced nature of fraud datasets, where fraudulent transactions are vastly outnumbered by legitimate ones. To address the shortcomings of earlier ML approaches, researchers turned to more sophisticated algorithms, including Support Vector Machines (SVM) and ensemble methods like Random Forests and Gradient Boosting Machines (GBM). Ensemble methods, combining multiple learning algorithms, have shown promise in improving predictive performance and robustness, effectively handling the variance in transaction data and reducing overfitting (Craja, Kim, & Lessmann, 2020). With the resurgence of neural networks in the form of deep learning, newer models capable of learning complex, non-linear relationships in large datasets have been applied to fraud detection. Deep learning techniques, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have been explored for their ability to process sequences of transactions and extract spatial and temporal features that are indicative of fraudulent behavior (McIver, 2021).

One of the perennial challenges in fraud detection is the imbalanced nature of datasets. Techniques like Synthetic Minority Over-sampling Technique (SMOTE) and Adaptive Synthetic Sampling (ADASYN) have been developed to synthetically augment the minority class, helping models to learn more effectively from rare fraudulent cases (Vasantha et al., 2023). These methods have significantly improved the sensitivity of fraud detection systems to rare fraudulent transactions. Evaluating the effectiveness of fraud detection systems involves metrics that can accurately reflect the true performance in imbalanced datasets. Traditional accuracy measures are often misleading in this context;

* Corresponding author

thus, metrics like the Area Under the ROC Curve (AUC-ROC), Precision-Recall curves, and the Matthews Correlation Coefficient (MCC) are used to provide a more nuanced assessment of model performance (Ali et al., 2022). Recent studies are increasingly focusing on the integration of machine learning models into real-time fraud detection systems [29]. The challenge remains to balance detection accuracy with the need for fast decision-making that is critical in the financial sector. Furthermore, the integration of unsupervised learning techniques for detecting novel types of fraud where labeled data is not available presents an exciting frontier for research (Ren, Ma, Kong, Baltas, & Zureigat, 2022; Sarker, 2021). This literature survey underscores the dynamic evolution of fraud detection methodologies from simplistic, rule-based systems to sophisticated, learning-based models that leverage the power of artificial intelligence to safeguard financial transactions. The next sections of the research will build on these foundations, exploring how different machine learning models perform on a challenging dataset of credit card transactions, addressing both the class imbalance problem and the need for operational efficiency in real-world applications.

3. METHOD

The methodology of this research is designed to assess the effectiveness of various machine learning models in identifying fraudulent transactions within a credit card dataset as presented in the figure 1. This section details the dataset, preprocessing steps, feature engineering, model selection, and the evaluation framework used to measure performance.

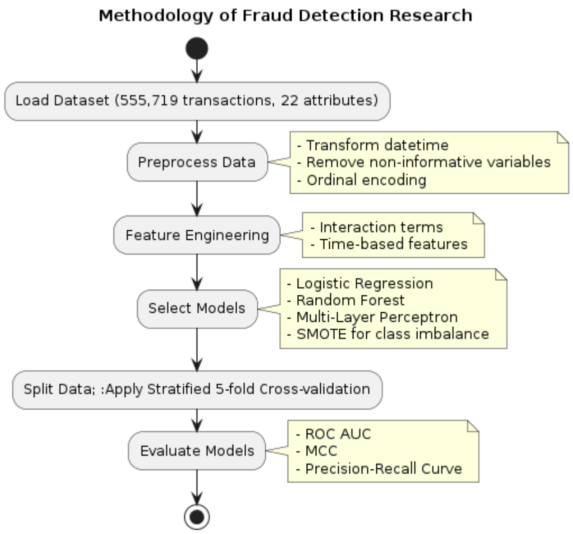

Fig. 1 Research Methodology of Fraud Detection

Dataset Description

The dataset used in this study is a comprehensive compilation of 555,719 transactions, each characterized by 22 distinct attributes that merge both categorical and numerical data types. This rich amalgamation of attributes includes key variables crucial for the analysis such as the transaction amount, detailed merchant information, customer demographics, and precise transaction timestamps. Each of these attributes plays a vital role in painting a complete picture of each transaction, which is essential for detecting patterns that may indicate fraudulent activity. The dataset's attributes cover a wide array, ensuring a thorough examination of factors that could influence or indicate fraud. The transaction amount (Amt) provides direct insight into the financial magnitude of each transaction, while merchant details offer context about the business entities involved, which can be critical for identifying potentially risky merchants or industries prone to fraud. Customer demographic information adds another layer of analysis, as certain trends or anomalies in customer behavior can be indicative of fraud. Additionally, the transaction timestamp is not merely a record of time but a gateway to understanding behavioral patterns based on transaction timing, which can vary significantly between legitimate and fraudulent activities.

Importantly, this dataset is meticulously curated to ensure no missing values, enhancing the reliability of the subsequent analysis. The absence of missing data points means that the dataset provides a complete view of each transaction without gaps, allowing for more accurate and confident application of machine learning models. This completeness is especially crucial in a field like fraud detection, where every detail may contribute to identifying fraudulent behavior more effectively. This dataset serves as a robust foundation for training and testing the machine learning models utilized in this study. Its comprehensive nature ensures that the models have access to a full spectrum of information, which is critical for learning to accurately differentiate between fraudulent and legitimate transactions based on a variety of indicators captured through the dataset's diverse attributes. Dataset can be collected from (Kelvin, 2023).

Data Preprocessing

Data preprocessing is an essential phase in preparing the raw dataset for effective model training, ensuring that the data fed into machine learning models is clean, comprehensive, and suitably formatted. This step is critical in transforming the raw data into a refined format that better suits the analytical models, which in turn can improve the accuracy and efficiency of the predictions. One of the initial steps in the data preprocessing phase involved the transformation of the 'trans_date_trans_time' field from a string format into a datetime object. This conversion is fundamental for the subsequent extraction of time-based features such as the hour of the day and the day of the week. Such features are invaluable as they allow the models to capture and learn from patterns related to the timing of transactions, which can be a significant indicator of fraudulent activity. For instance, fraudulent transactions may occur at unusual times that differ from the typical transaction patterns observed for a cardholder, making these features crucial for detecting anomalies.

```
df['trans_date_trans_time'] = pd.to_datetime(df['trans_date_trans_time'], format='%d/%m/%Y %H:%M')
```

This code snippet effectively converts the transaction timestamp into a Python datetime object, making it more accessible and useful for feature engineering tasks. Further, the dataset was streamlined by removing non-informative variables such as 'first name', 'last name', 'transaction number', and 'credit card number'. These attributes were excluded because they do not contribute meaningful predictive power to the fraud detection models. For instance, personal names and specific transaction numbers are unique to each transaction but do not inherently carry information about the legitimacy of a transaction. Additionally, categorical features within the dataset were transformed using ordinal encoding. This encoding method converts categorical variables into a machine-readable numeric format, maintaining the order where applicable. The transformation is crucial for the processing of categorical data by machine learning algorithms, which typically require numerical input. Encoding categorical features like merchant category or customer state allows the models to incorporate these factors into the predictive process, examining patterns and correlations that may suggest fraudulent behavior.

Feature Engineering

Feature engineering is a pivotal component of the data analysis process in our study, designed to enhance the dataset and improve the performance of the machine learning models. By developing more sophisticated features, we aim to capture the complexities and nuances inherent in the transaction data that might indicate fraudulent activity. During the feature engineering phase, interaction terms were generated from numerical features to explore potential non-linear relationships. These interactions can reveal combinations of numerical inputs that are unusually correlated with fraud. For example, the interaction between transaction amount and the time of day might expose certain patterns, such as high-value transactions occurring at unusual hours, which could be indicative of fraud. By modeling these non-linear relationships, the machine learning algorithms can learn to identify complex patterns that are not evident when considering individual features alone.

In addition to these polynomial features, the engineering process also focused on extracting and refining time-based features from the 'trans_date_trans_time' field. The transformation of this timestamp into more granular features such as 'hour_of_day' and 'day_of_week' allows the models to analyze transaction timing in depth. These temporal features are crucial as they help to uncover cyclical patterns in transaction activities. Fraudulent transactions may exhibit distinct temporal patterns compared to legitimate transactions. For instance, a higher frequency of fraudulent

Submitted : May 02, 2024
Accepted : May 31, 2024
Published : June 03, 2024

transactions might be observed during late-night hours or specific days of the week, which can significantly deviate from the norm observed in regular customer behavior.

Model Selection

In this study, we carefully selected a variety of machine learning models based on their effectiveness in binary classification tasks and their ability to manage the challenges presented by imbalanced datasets. The choice of models was guided by the need to comprehensively evaluate different approaches ranging from simple to more complex methodologies. Logistic Regression was chosen as a baseline model for its simplicity and interpretability, which makes it ideal for performance comparisons. It provides a straightforward, probabilistic approach to classification tasks and is often used as a starting point in binary classification to establish a benchmark for model performance. By using Logistic Regression, we can set a reference point against which the performance of more sophisticated models can be measured.

In contrast, the Random Forest Classifier and Multi-Layer Perceptron was selected for its proven efficacy in handling datasets with complex interactions and dependencies among features. Known for its high accuracy, Random Forest is an ensemble learning method that builds multiple decision trees and merges them together to obtain a more accurate and stable prediction. Its ability to perform both classification and regression tasks makes it particularly versatile. Importantly, Random Forest requires relatively less hyperparameter tuning, saving time and computational resources while still delivering robust results. This model is particularly adept at dealing with imbalanced datasets due to its inherent mechanism of constructing multiple trees and making decisions based on the majority voting system, which naturally reduces bias toward the majority class.

To further enhance the performance of these models, especially in the context of an imbalanced dataset typical of fraud detection scenarios, each model was integrated into a well-structured pipeline. This pipeline encompasses several stages, starting with data preprocessing to ensure that the models receive clean and well-formatted data. Following preprocessing, advanced feature engineering techniques were applied to develop a richer set of predictive features that capture the underlying patterns and anomalies indicative of fraudulent activities. Moreover, we incorporated the Synthetic Minority Over-sampling Technique (SMOTE) within the pipeline. SMOTE is an innovative approach that addresses the problem of class imbalance by creating synthetic samples from the minority class. This technique helps in balancing the dataset, which enhances the learning process and improves the predictive performance of the models regarding minority class predictions.

Training and Validation

In this study, the training and validation processes were meticulously designed to ensure that the machine learning models are accurately evaluated and validated. The dataset was methodically partitioned into training and testing sets, a crucial step that helps prevent model overfitting and ensures that the models can generalize well to new, unseen data. This division allows the training set to serve as the basis for building the models while the testing set functions as a tool for unbiased evaluation of model performance.

To further enhance the reliability and integrity of the model evaluations, Stratified 5-fold cross-validation was utilized during the training phase. This method of cross-validation involves dividing the entire dataset into five distinct subsets or folds. In each iteration of the validation process, four folds are used for training the model, and the remaining fold is used for testing. This cycle is repeated five times, with each of the five folds used exactly once as the testing set. Using stratified folds is particularly important in the context of fraud detection due to the typically imbalanced nature of the data. Stratification ensures that each fold is a good representative of the whole by maintaining approximately the same percentage of samples of each class as in the complete set.

```
StratifiedKFold(n_splits=5, shuffle=True, random_state=42)
```

This code configures the StratifiedKFold function to divide the dataset into five parts, with shuffling enabled to randomize the distribution of data points before splitting them into folds, and a random state set for reproducibility of the results. The application of Stratified 5-fold cross-validation provides several benefits. It not only maximizes the training data available (as each data point is used for both training and validation) but also minimizes bias and variance in estimating model performance. This approach is particularly valuable in handling datasets with an

Submitted : May 02, 2024
Accepted : May 31, 2024
Published : June 03, 2024

imbalanced distribution of classes, ensuring that each training set under the cross-validation framework is similarly distributed, which helps in achieving unbiased model performance metrics.

Training and Validation

In this research, the evaluation of model performance was comprehensively approached by employing multiple metrics, each designed to capture a distinct aspect of model effectiveness. This multi-metric evaluation is critical in providing a holistic view of how well the models perform under different conditions and criteria, which is particularly important in the complex field of fraud detection. One of the primary metrics used was the ROC AUC (Receiver Operating Characteristic Area Under the Curve). This metric is crucial as it measures the model's ability to discriminate between the fraudulent and legitimate classes over a variety of threshold settings. The ROC curve plots the true positive rate (sensitivity) against the false positive rate (1-specificity) at different threshold levels, providing insights into the trade-off between catching as many actual fraud cases as possible and minimizing false alarms. A higher AUC indicates a model that better distinguishes between the two classes, with an AUC of 1.0 representing a perfect model.

Another key metric utilized was the Matthews Correlation Coefficient (MCC), which offers a balanced measure that is particularly useful in the context of an imbalanced dataset like those typically found in fraud detection scenarios. Unlike simpler metrics such as accuracy, the MCC takes into account all four quadrants of the confusion matrix (true positives, false positives, true negatives, and false negatives), providing a more comprehensive assessment of model performance. It returns a value between -1 and +1, where +1 indicates a perfect prediction, 0 no better than random prediction, and -1 total disagreement between prediction and observation. This makes the MCC a robust metric that can convey a lot of information about the quality of binary classifications. Additionally, the Precision-Recall Curve was employed to further analyze model performance, particularly to evaluate the trade-offs between precision and recall. This curve is vital in scenarios where the consequences of false positives and false negatives carry significant costs. Precision (the proportion of positive identifications that were actually correct) and recall (the proportion of actual positives that were correctly identified) are particularly useful metrics for fraud detection, as they help to understand the effectiveness of the model in identifying only legitimate fraud cases without casting too wide a net.

4. RESULT

The evaluation of the machine learning models used in this study—Logistic Regression, Random Forest, and Multilayer Perceptron (MLP)—provided a detailed look at their effectiveness in detecting fraudulent transactions within a large dataset. The performance of these models was assessed using various metrics, including ROC AUC, Matthews Correlation Coefficient (MCC), and the Precision-Recall Curve, each providing insights into different aspects of the models' capabilities as presented in the table 1. The Logistic Regression model demonstrated moderate effectiveness with a ROC AUC score of 0.8572, indicating a fair ability to differentiate between fraudulent and legitimate transactions. However, the MCC value of 0.1894 suggests that the model's overall accuracy in predicting true positives and true negatives is relatively low in the context of an imbalanced dataset. The confusion matrix revealed a significant number of false positives (28,995), which could lead to many incorrect fraud alerts. The Precision-Recall Curve shows a general trend where recall is initially high at lower threshold values, but precision is very low, reflecting the model’s tendency to label too many transactions as fraudulent.

Table 1
The Comparison results of the Model

Model	ROC/AUC	MCC	False Positives	False Negatives
Logistic Regression	0.8572	0.1894	28,995	538
Random Forest	0.9868	0.6638	1,022	577
Multi-Layer Perceptron	0.9536	0.2763	14,076	506

Random Forest performed substantially better, with a ROC AUC of 0.9868, showcasing its strong discriminatory power. The MCC of 0.6638 is much higher than that of Logistic Regression, indicating a better balance in the classification performance across the four quadrants of the confusion matrix. The confusion matrix for this model

* Corresponding author

Submitted : May 02, 2024
Accepted : May 31, 2024
Published : June 03, 2024

shows fewer false positives (1,022) and false negatives (577), suggesting a more balanced approach to classifying transactions. The Precision-Recall Curve further confirms the model's robustness, displaying a much smoother and higher curve, which implies a better trade-off between precision and recall throughout the range of threshold settings. MLP showed a promising ROC AUC of 0.9536, which is indicative of good classification performance, though it falls short of the Random Forest model. The MCC score of 0.2763, while higher than that of Logistic Regression, still suggests there is room for improvement in how the model handles the imbalance in the dataset. The confusion matrix indicates a relatively high number of false positives (14,076), which is problematic for operational settings due to the potential for increased customer dissatisfaction due to erroneous fraud alerts. The Precision-Recall Curve for MLP indicates variability, with precision improving only at very high recall levels, suggesting that while the model can detect most fraudulent transactions, it does so at the expense of a higher false-positive rate. The results highlight the varying strengths and weaknesses of each model in handling a complex and imbalanced dataset. Random Forest emerged as the most effective model in terms of both its ability to distinguish between transaction classes and its balance of precision and recall. Logistic Regression, while useful as a benchmarking tool, showed limitations in handling the complexity and class imbalance of the dataset. MLP, though strong in identifying fraudulent transactions, still shows a tendency to generate a higher number of false positives, which could be mitigated with further tuning.

5. DISCUSSIONS

The results from the application of Logistic Regression, Random Forest, and Multilayer Perceptron (MLP) models on a large dataset of credit card transactions provide a nuanced view of the strengths and limitations of each approach in fraud detection. This discussion delves deeper into the implications of these findings, exploring how they align with the challenges inherent in fraud detection and suggest pathways for future research and practical application improvements. The moderate performance of Logistic Regression, as evidenced by its ROC AUC and MCC scores, highlights some fundamental challenges associated with simpler models in complex fraud detection scenarios. The significant number of false positives suggests that while the model can identify potential fraud, it lacks precision, which could lead to operational inefficiencies and customer dissatisfaction due to erroneous alerts. This model's performance underscores the need for more sophisticated techniques to handle datasets with complex patterns and severe class imbalances.

Random Forest's superior performance across all metrics—particularly its high ROC AUC and MCC—demonstrates its robustness and effectiveness in dealing with imbalanced data. The lower number of false positives and false negatives indicates that Random Forest is capable of maintaining a good balance between sensitivity and specificity, making it a preferable choice for environments where accuracy is crucial to maintaining customer trust and operational integrity. The success of the Random Forest model could be attributed to its ensemble method, which leverages multiple decision trees to arrive at more accurate and stable predictions by averaging out biases. While the MLP showed promising ability to detect fraudulent transactions as reflected in its ROC AUC, the high number of false positives highlighted by the Precision-Recall Curve and its overall MCC score suggest a trade-off between sensitivity and precision. This indicates that while MLPs are capable of modeling complex, non-linear interactions in high-dimensional data, they may require more careful tuning of thresholds or an enhanced feature set to improve precision without sacrificing recall. This could involve more advanced preprocessing techniques, feature selection methods, or the integration of domain-specific knowledge into the training process. The findings from this study have direct implications for the development and deployment of fraud detection systems. The trade-offs observed between sensitivity and recall across different models highlight the importance of model selection based on the specific operational context and the costs associated with false positives and false negatives. For instance, in high-stakes financial environments, a higher premium might be placed on minimizing false negatives, whereas in consumer-facing applications, reducing false positives might be prioritized to enhance customer experience.

6. CONCLUSION

In conclusion, while Random Forest proved to be the most robust model in this study, further research could explore the integration of additional advanced techniques such as ensemble methods combining multiple algorithms, hyperparameter tuning, and incorporating feature engineering strategies to enhance model performance further. Additionally, future studies might benefit from utilizing larger and more diverse datasets, including real-time data, to validate the generalizability and scalability of the models. Another promising direction would be the application of deep learning architectures, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), to

* Corresponding author

Submitted : May 02, 2024
Accepted : May 31, 2024
Published : June 03, 2024

capture temporal patterns and improve detection accuracy. These suggestions aim to build upon the findings of this research and contribute to the development of more sophisticated and reliable fraud detection systems.

7. REFERENCES

Ahmad, I., Khan, S., & Iqbal, S. (2024). Guardians of the vault: unmasking online threats and fortifying e-banking security, a systematic review. Journal of Financial Crime.

Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access, 10, 39700–39715.

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University-Computer and Information Sciences, 34(10), 8176–8206.

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., … Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. Applied Sciences, 12(19), 9637.

Almahmoud, S., Hammo, B., Al-Shboul, B., & Obeid, N. (2022). A hybrid approach for identifying non-human traffic in online digital advertising. Multimedia Tools and Applications, 81(2), 1685–1718.

Alzahrani, R. A., & Aljabri, M. (2022). AI-based techniques for Ad click fraud detection and prevention: Review and research directions. Journal of Sensor and Actuator Networks, 12(1), 4.

Botchey, F. E., Qin, Z., & Hughes-Lartey, K. (2020). Mobile money fraud prediction—a cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and na{\"\i}ve bayes algorithms. Information, 11(8), 383.

Chung, J., & Lee, K. (2023). Credit Card Fraud Detection: An Improved Strategy for High Recall Using KNN, LDA, and Linear Regression. Sensors, 23(18), 7788.

Craja, P., Kim, A., & Lessmann, S. (2020). Deep learning for detecting financial statement fraud. Decision Support Systems, 139, 113421.

Darwish, S. M. (2020). A bio-inspired credit card fraud detection model based on user behavior analysis suitable for business management in electronic banking. Journal of Ambient Intelligence and Humanized Computing, 11(11), 4873–4887.

Hussein, A. S., Khairy, R. S., Najeeb, S. M. M., & Alrikabi, H. T. S. (2021). Credit Card Fraud Detection Using Fuzzy Rough Nearest Neighbor and Sequential Minimal Optimization with Logistic Regression. International Journal of Interactive Mobile Technologies, 15(5).

Kanchana, M., Naresh, R., Deepa, N., Pandiaraja, P., & Stephan, T. (2022). Credit Card Fraud Detection Techniques Under IoT Environment: A Survey. In Transforming Management with AI, Big-Data, and IoT (pp. 141–154). Springer.

Kanu, C., Nnam, M. U., Ugwu, J. N., Achilike, N., Adama, L., Uwajumogu, N., & Obidike, P. (2023). Frauds and forgeries in banking industry in Africa: a content analyses of Nigeria Deposit Insurance Corporation annual crime report. Security Journal, 36(4), 671–692.

Kelvin, K. L. (2023). Credit Card Fraud Prediction.

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: ICMISC 2021, 27–37.

Kumar, V. P., Pallavi, L., & Prakash, K. B. (2021). Role of recent technologies in cognitive systems. Cognitive Engineering for next Generation Computing: A Practical Analytical Approach, 231–264.

Kumaraswamy, N., Markey, M. K., Ekin, T., Barner, J. C., & Rascati, K. (2022). Healthcare fraud data mining methods: A look back and look ahead. Perspectives in Health Information Management, 19(1).

Liang, S., Wu, H., Zhen, L., Hua, Q., Garg, S., Kaddoum, G., … Yu, K. (2022). Edge YOLO: Real-time intelligent object detection system based on edge-cloud cooperation in autonomous vehicles. IEEE Transactions on Intelligent Transportation Systems, 23(12), 25345–25360.

McIver, S. (2021). Can Generative Adversarial Networks Help Us Fight Financial Fraud?

Merghadi, A., Yunus, A. P., Dou, J., Whiteley, J., ThaiPham, B., Bui, D. T., … Abderrahmane, B. (2020). Machine learning methods for landslide susceptibility studies: A comparative overview of algorithm performance. Earth-Science Reviews, 207, 103225.

* Corresponding author

Submitted : May 02, 2024
Accepted : May 31, 2024
Published : June 03, 2024

Mondal, I. A., Haque, M. E., Hassan, A.-M., & Shatabda, S. (2021). Handling imbalanced data for credit card fraud detection. 2021 24th International Conference on Computer and Information Technology (ICCIT), 1–6.

Ni, L., Li, J., Xu, H., Wang, X., & Zhang, J. (2023). Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection. IEEE Transactions on Computational Social Systems.

Putrevu, J., & Mertzanis, C. (2023). The adoption of digital payments in emerging economies: challenges and policy responses. Digital Policy, Regulation and Governance, (ahead-of-print).

Reddy, S. R. B., Kanagala, P., Ravichandran, P., Pulimamidi, R., Polireddi, N. S. A., & others. (2024). Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics. Measurement: Sensors, 101138.

Ren, Y.-S., Ma, C.-Q., Kong, X.-L., Baltas, K., & Zureigat, Q. (2022). Past, present, and future of the application of machine learning in cryptocurrency research. Research in International Business and Finance, 63, 101799.

Rusia, M. K., & Singh, D. K. (2023). A comprehensive survey on techniques to handle face identity threats: challenges and opportunities. Multimedia Tools and Applications, 82(2), 1669–1748.

Saporta, G., & Maraney, S. (2022). Practical Fraud Prevention. " O'Reilly Media, Inc."

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN Computer Science, 2(3), 160.

Udayakumar, R., Sreekumar, K., Nivedha, C. S., Sivasubramanian, S., & Umadevi, V. (2023). A Predictive Analysis of Autism Spectrum Disorder Using Ensemble Techniques of Machine Learning. 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS), 558–565.

Vasantha, S. V, Thullimilli, S., Ganesh, V. S., Shankar, M. S., Reddy, M. V., & Hariharan, S. (2023). Application of Resampling Techniques on Sepsis Data to Balance Model Performance with Accuracy, AUC, Kappa and MCC. 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), 1174–1179.

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in post-pandemic era. The Innovation, 2(4).

* Corresponding author