IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306177|

Credit Card Fraud Detection: A Comparative Study

Prema Kadam, Vaibhavi Pathak, Dr. Ratna Patil, Pranav Wagholikar, Haazique Sayyed, Subhojit Talukdar

Department of Artificial Intelligence & Data Science, Vishwakarma Institute of Information Technology Pune, India

ABSTRACT: The prevalence of credit card fraud continues to pose significant challenges to financial security globally, necessitating advanced detection strategies. This study provides a comprehensive evaluation of several leading machine learning models to identify the most effective techniques for detecting fraudulent transactions. Through the analysis of transactional data characteristics and fraud detection metrics, we assess the performance, scalability, and operational efficiency of each model. Our findings reveal varied strengths and weaknesses, suggesting that the choice of model should be tailored to specific operational contexts and data environments. The study also discusses practical considerations for implementing these models in real-world systems, aiming to enhance predictive accuracy and reduce false positives. Overall, this research advances our understanding of machine learning applications in financial security, offering valuable insights for both academics and practitioners in the field.

KEYWORDS: Fraud Detection, Machine Learning, Financial Security

I. INTRODUCTION

In the realm of digital finance, credit card fraud remains a persistent and evolving threat, imposing significant economic burdens on individuals and institutions alike. As global reliance on electronic payment systems escalates, so too does the incentive for fraudsters to exploit these systems. The implications of credit card fraud are extensive, ranging from direct financial losses to indirect costs associated with heightened security measures and loss of consumer trust. Consequently, robust and effective fraud detection systems are crucial for maintaining the integrity and reliability of financial transactions.

The advent of machine learning has introduced a new frontier in fraud detection, providing powerful tools that can learn from complex datasets to identify potential fraud. Unlike traditional rule-based systems, which often struggle with the dynamic nature of fraud patterns, machine learning models adapt to new threats as they emerge. This adaptability is crucial in a landscape where fraudsters continuously refine their strategies to circumvent existing safeguards.

The effectiveness of machine learning in detecting fraudulent transactions relies heavily on selecting appropriate models that can handle specific challenges, such as imbalanced datasets where instances of fraud are rare compared to legitimate transactions. Moreover, the operational demands of real-time processing require models not only to be accurate but also efficient. The ability of a model to quickly evaluate transactions is paramount in preventing fraud before it causes harm.

This study focuses on comparing various machine learning techniques to ascertain their efficacy in identifying and preventing credit card fraud. By evaluating different models, the research aims to illuminate their respective strengths and weaknesses in dealing with the peculiarities of credit card transaction data. The study is structured to assess each model's performance based on accuracy, precision, recall, and computational efficiency—metrics that are critical in determining the practical applicability of a fraud detection system.

Furthermore, the paper discusses the implications of each model's results, offering insights into how they can be integrated into existing financial security frameworks to enhance fraud detection capabilities. The ultimate goal is to provide a nuanced understanding that aids stakeholders in selecting the most suitable machine learning approach based on their specific needs and operational contexts.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306177|

II. RELATED WORK

Recent advancements in machine learning for credit card fraud detection have centered on improving the accuracy and efficiency of various predictive models. A substantial body of research has focused on exploring different algorithms to enhance the identification and prevention of fraudulent transactions. For instance, studies like those by Lin et al. (2020) [1] and Costa & Pedreira (2022) [2] have examined the capabilities of decision trees and their optimizations to better handle the complexities of financial datasets characterized by non-linear patterns and class imbalances.

Further investigations, such as those by Izza, Ignatiev, and Marques-Silva (2022) [3], have sought to address the redundancy in decision tree explanations, aiming to streamline models for more efficient real-time processing. This is crucial in fraud detection where timely response is essential. Additionally, privacy concerns around data usage have prompted researchers like Akavia et al. (2022) [4] to develop privacy-preserving models that ensure user data security while still providing effective fraud detection capabilities.

The role of ensemble methods, particularly Random Forests and XGBoost, has been highlighted in several studies (e.g., Nanfack et al., 2022 [6]; Günlük et al., 2021 [7]) for their superior performance in handling overfitting and providing robustness against noise in transaction data. These methods have been shown to improve detection rates significantly, as noted by Goswami et al. (2021) [8], who explored the use of decision trees within a molecular memristor, demonstrating the potential for hardware-accelerated machine learning solutions.

Moreover, the application of novel techniques like GANs for data augmentation to address imbalances in fraud detection datasets has been explored (Strelcenia & Prakoonwit, 2023 [15]), indicating a growing interest in leveraging synthetic data to enhance model training processes. The integration of deep learning, as discussed by Mienye and Sun (2023) [18], offers another avenue where complex patterns inherent in transaction data are decoded more effectively than with traditional machine learning methods.

This body of work collectively illustrates a trend towards more sophisticated, adaptable, and secure machine learning frameworks that not only meet the operational demands of fraud detection systems but also push the boundaries of what these systems can achieve in terms of accuracy and speed. These studies provide a solid foundation for the ongoing development of machine learning applications in financial security, particularly in combating the ever-evolving threat of credit card fraud.

III. METHODOLOGY

A. Data Collection and Initial Processing

The study utilizes a widely acknowledged credit card dataset by Université Libre de Bruxelles, which encompasses a mix of transactions made with credit cards over a specific period. The dataset is primarily composed of numerical input variables transformed via PCA, with the exception of 'Time' and 'Amount', ensuring user confidentiality. The target variable, 'Class', identifies whether a transaction is fraudulent (1) or non-fraudulent (0), setting the stage for a binary classification problem.

B. Data Balancing Techniques

Given the skewed distribution of classes—where fraudulent transactions are significantly outnumbered—the study employs both under sampling and oversampling techniques to mitigate model bias:

- **Under Sampling:** The Random Under Sampler from the imbalanced-learn library was used to equate the number of samples in the minority class to those in the majority class by randomly eliminating excess majority class instances. This approach intended to prevent the model from being overwhelmed by the majority class but at the risk of losing valuable data.
- **Oversampling:** Conversely, the Random Over Sampler was applied to augment the minority class by replicating its instances, thus matching the majority class's size. This technique aimed to preserve all original data while providing balanced input for model training.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306177|

C. Feature Standardization

Critical to the preprocessing stage, the Standard Scaler was applied to normalize the 'Amount' and 'Time' features, which otherwise vary significantly in magnitude and could potentially skew the performance of certain algorithms. Standardization adjusts the features to have zero mean and unit variance, a prerequisite for algorithms like Logistic Regression and K-Nearest Neighbors that are sensitive to the scale of input data.

D. Model Selection and Training

The study evaluated the efficacy of four different machine learning models:

- **Logistic Regression:** A linear model used for binary classification tasks, known for its simplicity and interpretability.
- **Decision Tree Classifier:** A non-linear model that partitions the data space into regions with similar responses, offering easy interpretability.
- **K-Nearest Neighbors (KNN):** A distance-based algorithm that classifies new instances based on a plurality vote of its neighbors, with the class most common among its k nearest neighbors being assigned to it.
- **XGBoost:** An implementation of gradient-boosted decision trees, designed for speed and performance, which is particularly effective for large datasets and complex feature interactions.

Each model was trained on both the under sampled and oversampled datasets. This dual approach allowed the examination of how different data balancing techniques impacted model performance, providing insights into their suitability under various operational scenarios.

E. Evaluation Metrics

Model performance was assessed using several metrics crucial for imbalanced datasets:

- **Accuracy:** Measures the overall correctness of the model.
- **Precision:** Indicates the proportion of positive identifications that were actually correct.
- **Recall:** Reflects the proportion of actual positives that were correctly identified.
- **F1 Score:** Harmonic mean of precision and recall, providing a balance between the two in cases of uneven class distributions.
- **ROC-AUC:** Represents the likelihood that the model ranks a random positive example more highly than a random negative example.

IV. RESULTS AND DISCUSSION

The evaluation of the models deployed in this study was meticulously planned to gauge their effectiveness in identifying fraudulent transactions within the credit card dataset.

The models were trained using both under sampled and oversampled datasets to address the class imbalance inherent in the credit card transaction data. This dual approach allowed for a comparative analysis of how each sampling method affects model performance. Logistic Regression, Decision Trees, K-Nearest Neighbors, and XGBoost were each evaluated on these datasets. Experiments were conducted to optimize model parameters, such as the depth of the decision trees, the number of neighbors in KNN, and the learning rate in XGBoost, to find the best configuration for each model. The effectiveness of these configurations was then measured across the various performance metrics.

The results highlighted varied performance across models and configurations. Logistic Regression, often considered a baseline for binary classification tasks, showed respectable performance in terms of precision but struggled with recall, particularly when trained on the under sampled dataset. This indicates a tendency to miss fraudulent transactions—a critical flaw in fraud detection systems.

Decision Trees and XGBoost, both capable of modeling complex relationships, exhibited stronger performance on most metrics, particularly in recall and F1 score, suggesting better capability at identifying fraudulent transactions. The use of XGBoost with oversampling showed promising results, often achieving the highest ROC-AUC scores, indicating superior capability in distinguishing between classes.

K-Nearest Neighbors, while generally reliable, faced challenges related to its sensitivity to the local data structure, which can be adversely affected by noise and outliers in imbalanced datasets. Its performance varied significantly with the

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306177|

number of neighbors and was generally better with oversampling, where the increased number of minority class examples provided a more informative neighborhood.

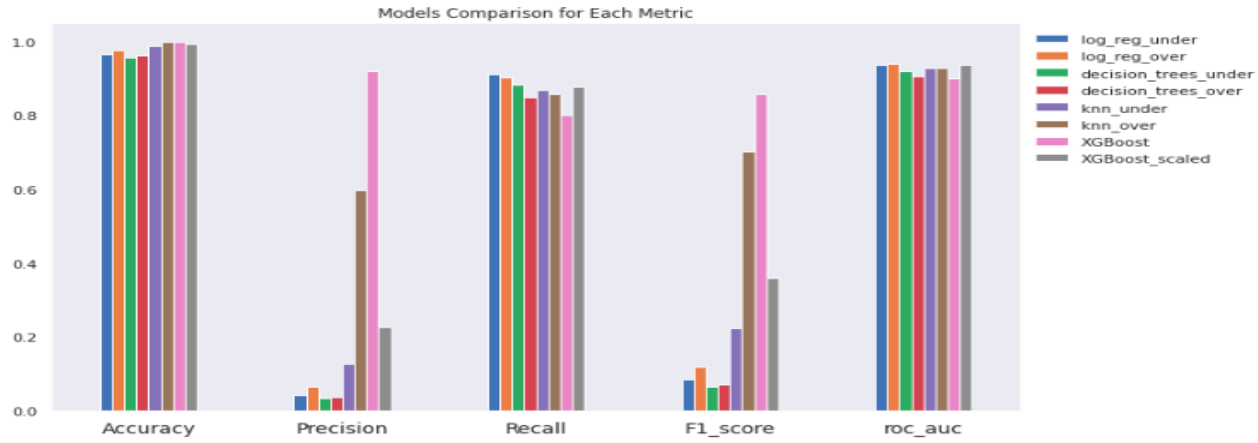

Fig. 1. Results of model comparison

V. CHALLENGES ENCOUNTERED

The primary challenge encountered was managing the skewed distribution of classes in the dataset, which can lead to models that are biased towards the majority class. Both undersampling and oversampling were used to address this, each with trade-offs. Undersampling led to a loss of valuable data, potentially omitting critical patterns necessary for identifying fraud. Oversampling, while preserving all data, increased the likelihood of overfitting, as models were more likely to learn noise from the duplicated minority class instances.

Additionally, the complexity of models like Decision Trees and XGBoost required careful tuning to avoid overfitting while maintaining the ability to generalize well on unseen data.

In summary, the experiments provided extensive insights into the strengths and weaknesses of each model in the context of fraud detection, guiding future efforts in model selection and tuning for optimal performance in real-world scenarios.

VI. CONCLUSION

The study embarked on a detailed exploration of various machine learning algorithms to tackle the persistent issue of credit card fraud, a formidable challenge in the financial sector. By employing diverse techniques such as Logistic Regression, Decision Trees, K-Nearest Neighbors, and XGBoost, the research aimed to ascertain the most effective methodologies for detecting fraudulent transactions. The use of both under sampling and oversampling strategies to prepare the data helped address the inherent class imbalance, a prevalent issue in fraud detection datasets that often skews model performance.

The findings from this comparative analysis reveal that while no single model uniformly outperformed others across all metrics, each model exhibited unique strengths and weaknesses. Logistic Regression, valued for its simplicity and interpretability, demonstrated high precision, making it suitable for scenarios where false positives are a significant concern. However, its lower recall suggests it might miss a considerable number of fraudulent transactions. Decision Trees and XGBoost, with their ability to capture non-linear relationships, proved effective in environments demanding high recall, though they require careful tuning to avoid overfitting.

K-Nearest Neighbors offered valuable insights into the importance of feature scaling and the influence of neighbors in classification accuracy. However, its performance was sensitive to the choice of 'k' and the method of sampling, underscoring the need for meticulous parameter optimization. The experimental results, particularly those involving ROC-AUC scores and F1 scores, emphasized the critical balance between sensitivity and specificity that financial

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306177|

security systems must achieve to be effective. The visualization of results through ROC curves and confusion matrices provided clear, actionable insights that can guide further research and practical implementations.

This study also highlighted the challenges associated with model training on imbalanced datasets, such as the potential for overfitting and the loss of valuable data. These challenges underscore the necessity for ongoing research into more sophisticated sampling and ensemble techniques.

In conclusion, this research contributes to the ongoing dialogue in the machine learning community about the best practices for fraud detection in credit card transactions. It provides a foundation for future work that could explore hybrid models combining the strengths of the examined algorithms or the application of novel machine learning techniques that could further enhance predictive performance. For practitioners, the study offers a roadmap for selecting and tuning machine learning models tailored to the specific dynamics of their operational environments, ensuring that they can effectively combat credit card fraud while minimizing adverse impacts on genuine transactions.

REFERENCES

[1] J. J. Lin, C. Zhong, D. Hu, C. Rudin, and M. Seltzer, "Generalized and scalable optimal sparse decision trees," in Int. Conf. Mach. Learn., 2020, pp. 6150-6160.
[2] V. G. Costa and C. E. Pedreira, "Recent advances in decision trees: An updated survey," Artif. Intell. Rev., vol. 56, pp. 4765-4800, 2022.
[3] Y. Izza, A. Ignatiev, and J. Marques-Silva, "On tackling explanation redundancy in decision trees," J. Artif. Intell. Res., vol. 75, pp. 261-321, 2022.
[4] A. Akavia, M. Leibovich, Y. S. Resheff, R. Ron, M. Shahar, and M. Vald, "Privacy-preserving decision trees training and prediction," ACM Trans. Priv. Secur., vol. 25, pp. 1-30, 2022.
[5] M. Arenas, P. Barcel'o, M. Romero, and B. Subercaseaux, "On computing probabilistic explanations for decision trees," Neural Inf. Process. Syst., 2022.
[6] G. Nanfack, P. Temple, and B. Frénay, "Constraint enforcement on decision trees: A survey," ACM Comput. Surv. (CSUR), vol. 54, pp. 1-36, 2022.
[7] O. Günlük, J. Kalagnanam, M. Li, M. Menickelly, and K. Scheinberg, "Optimal decision trees for categorical data via integer programming," J. Global Optim., vol. 81, pp. 233-260, 2021.
[8] S. Goswami, R. Pramanick, A. Patra, S. P. Rath, M. Foltin, A. Ariando, D. Thompson, T. Venkatesan, S. Goswami, and R. S. Williams, "Decision trees within a molecular memristor," Nature, vol. 597, pp. 51-56, 2021.
[9] Z. Qin, L. Yan, H. Zhuang, Y. Tay, R. K. Pasumarthi, X. Wang, M. Bendersky, and M. Najork, "Are neural rankers still outperformed by gradient boosted decision trees?" Int. Conf. Learn. Represent., 2021.
[10] A. Aboah, M. Shoman, V. Mandal, S. Davami, Y. Adu-Gyamfi, and A. Sharma, "A vision-based system for traffic anomaly detection using deep learning and decision trees," IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), pp. 4202-4207, 2021.
[11] Z. Salekshahrezaee, J. L. Leevy, and T. Khoshgoftaar, "The effect of feature extraction and data sampling on credit card fraud detection," Journal of Big Data, vol. 10, pp. 1-17, 2023. [Online]. Available: link
[12] M. Shraddha, K. Sumedha, and V. Veda Samhitha, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," International Journal For Multidisciplinary Research, 2023.
[13] Y. Xie, G. Liu, C. Yan, C. Jiang, and M. Zhou, "Time-aware attention-based gated network for credit card fraud detection by extracting transactional behaviors," IEEE Transactions on Computational Social Systems, vol. 10, pp. 1004-1016, 2023.
[14] I. D. Mienye and Y. Sun, "A deep learning ensemble with data resampling for credit card fraud detection," IEEE Access, vol. 11, pp. 30628-30638, 2023.
[15] E. Strelcenia and S. Prakoonwit, "A survey on GAN techniques for data augmentation to address the imbalanced data issues in credit card fraud detection," Machine Learning and Knowledge Extraction, vol. 5, pp. 304-329, 2023.
[16] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," Journal of Big Data, 2022.
[17] Y. Xie, G. Liu, C. Yan, C. Jiang, and M. Zhou, "Time-aware attention-based gated network for credit card fraud detection by extracting transactional behaviors," IEEE Transactions on Computational Social Systems, vol. 10, pp. 1004-1016, 2023.
[18] I. D. Mienye and Y. Sun, "A deep learning ensemble with data resampling for credit card fraud detection," IEEE Access, vol. 11, pp. 30628-30638, 2023.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306177|

[19] E. Strelcenia and S. Prakoonwit, "A survey on GAN techniques for data augmentation to address the imbalanced data issues in credit card fraud detection," Machine Learning and Knowledge Extraction, vol. 5, pp. 304-329, 2023.
[20] Z. Salekshahrezaee, J. L. Leevy, and T. Khoshgoftaar, "The effect of feature extraction and data sampling on credit card fraud detection," Journal of Big Data, vol. 10, pp. 1-17, 2023.
[21] H. Fanai and H. Abbasimehr, "A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection," Expert Systems with Applications, vol. 217, 2023.
[22] E. Esenogho, I. D. Mienye, T. Swart, K. D. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," IEEE Access, vol. 10, pp. 16400-16407, 2022.
[23] S. Xiang, M. Zhu, D. Cheng, E. Li, R. Zhao, Y. Ouyang, L. Chen, and Y. Zheng, "Semi-supervised credit card fraud detection via attribute-driven graph representation," AAAI Conference on Artificial Intelligence, 2023.
[24] L. Naik, K. Shekar, R Madhu, and T. Vinod, "Credit card fraud detection using random forest," International Journal of Advanced Research in Science, Communication and Technology, 2023.
[25] K. Laxmikant, R. Bhuvaneswari, and B. Natarajan, "An efficient approach to detect diabetes using XGBoost classifier," 2023 Winter Summit on Smart Computing and Networks (WiSSCoN), 2

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details