Original Article

Check for updates

Available online at
www.heca-analitika.com/ijma

Indatu Journal of Management and Accounting

Vol. 1, No. 1, 2023

Credit Card Fraud Detection for Contemporary Financial Management Using XGBoost-Driven Machine Learning and Data Augmentation Techniques

Teuku Rizky Noviandy [1], Ghalieb Mutig Idroes [2], Aga Maulana [1], Irsan Hardi [3], Edi Saputra Ringga [4] and Rinaldi Idroes [5,*]

[1] Department of Informatics, Faculty of Mathematics and Natural Sciences, Universitas Syiah Kuala, Banda Aceh 23111, Indonesia; trizkynoviandy@gmail.com (T.R.N.); agamaulana@usk.ac.id (A.M.)
[2] Energy and Green Economics Unit, Graha Primera Saintifika, Aceh Besar 23371, Indonesia; ghaliebidroes@gmail.com (G.M.I.)
[3] Economic Modeling and Data Analytics Unit, Graha Primera Saintifika, Aceh Besar 23371, Indonesia; irsan.hardi@gmail.com (I.H.)
[4] Department of Economics, Faculty of Business, Economics and Social Development, Universiti Malaysia Terengganu, Terengganu 21030, Malaysia; p5650@pps.umt.edu.my (E.S.R.)
[5] School of Mathematics and Applied Sciences, Universitas Syiah Kuala, Banda Aceh 23111, Indonesia; rinaldi.idroes@usk.ac.id (R.I.)

***** Correspondence: rinaldi.idroes@usk.ac.id

Article History

Received 30 July 2023
Revised 27 August 2023
Accepted 6 September 2023
Available Online 12 September 2023

Keywords:
Financial management
Imbalanced dataset
Tabular machine learning
SMOTE

Abstract

The rise of digital transactions and electronic payment systems in modern financial management has brought convenience but also the challenge of credit card fraud. Traditional fraud detection methods are struggling to cope with the complexities of contemporary fraud strategies. This study explores the potential of machine learning, specifically the XGBoost (eXtreme Gradient Boosting) algorithm, combined with data augmentation techniques, to enhance credit card fraud detection. The research demonstrates the effectiveness of these techniques in addressing imbalanced datasets and improving fraud detection accuracy. The study showcases a balanced approach to precision and recall in fraud detection by leveraging historical transaction data and employing techniques like Synthetic Minority Over-sampling Technique-Edited Nearest Neighbors (SMOTE-ENN). The implications of these findings for contemporary financial management are profound, offering the potential to bolster financial integrity, allocate resources effectively, and strengthen customer trust in the face of evolving fraud tactics.

1. Introduction

In the contemporary financial management landscape, digital transactions and electronic payment systems have completely changed how businesses and people handle their finances [1]. While this advancement has brought incredible convenience, it has also led to a significant problem of the growing risk of credit card fraud [2, 3]. The unauthorized use of credit card information for illegal activities causes financial losses for individuals and businesses and erodes people's trust in the integrity of financial systems [4].

To address credit card fraud, researchers have developed techniques for detecting it, which aim to prevent unauthorized purchases, whether they occur online or in physical stores. However, conventional fraud detection methods, which often rely on rule-based systems [5] and

static thresholds [6, 7], are insufficient to deal with modern fraudsters' ever-evolving and complex strategies. The complexity of fraudulent patterns and the vast number of digital transactions highlight the need for a new way of detecting fraud. This calls for a fundamental shift in identifying fraud, moving from traditional methods to more innovative solutions.

In recent years, machine learning has gained significant attention as a potential solution to the challenges posed by credit card fraud detection [8–11]. Machine learning is a subset of artificial intelligence that empowers systems to learn from data and improve their performance on specific tasks over time. It involves the development of algorithms that enable computers to identify patterns, make predictions, and make decisions based on the data they are exposed to [12–15]. By leveraging vast amounts of historical transaction data, machine learning algorithms can learn to discern intricate patterns and anomalies that might go unnoticed by traditional methods [16–18].

XGBoost is a powerful and widely used machine learning algorithm renowned for its efficiency and accuracy in handling various data types and complexities [17, 19–21]. It falls under the gradient boosting frameworks, which are ensemble learning methods that combine the predictive power of multiple models to create a stronger overall prediction [22]. XGBoost builds upon the principles of gradient boosting, enhancing the method with a focus on regularization [23]. It sequentially adds decision trees to an ensemble, iteratively correcting the errors made by the preceding models. This iterative process allows XGBoost to improve its predictive performance over time. XGBoost aims to find an optimal ensemble of weak learners (decision trees) that, when combined, produce a strong predictive model [24]. This is achieved by minimizing a loss function and quantifying the difference between predicted and actual values.

However, addressing the challenge of using machine learning for credit card fraud detection involves grappling with imbalanced datasets, where the abundance of legitimate transactions dwarfs the instances of fraud [25]. This disparity can skew model performance, favoring the majority class in classification [26]. Data augmentation techniques come into play to tackle this, aiming to enhance the representation of the minority class (fraudulent transactions) [27]. One such technique is oversampling, which entails duplicating instances from the minority class to balance its presence with the majority class [28]. This method exposes the algorithm to more examples of fraud during training, refining its ability to distinguish between legitimate and fraudulent activities. However, careful consideration is necessary to avoid overfitting, ensuring the model can generalize effectively to new, unseen data [29].

In this study, we aim to use machine learning for credit card fraud detection by employing a technique known as XGBoost with various data augmentation techniques to enrich the dataset with instances of fraudulent activities, enhancing the algorithm's capacity to learn and classify such cases. The findings of this study could potentially contribute to the development of more effective fraud detection systems, which are crucial for financial institutions and businesses to protect their customers and assets from fraudulent activities.

2. Materials and Methods

2.1. Dataset

The dataset comprises credit card transactions occurring in September 2013 among European cardholders. These transactions span two days, encompassing 492 instances of fraud out of 284,807 transactions. Notably, the dataset is heavily imbalanced, with fraud instances accounting for only 0.172% of all transactions. The dataset contains a total of 30 attributes. The dataset comprises 30 features, including time-related features that track elapsed time, an amount feature representing transaction values, and 28 numerical features labeled V1 through V28, obtained through a PCA transformation. Due to confidentiality, original features and background details remain undisclosed.

The dataset is split randomly into two parts: 80% is used as the training set, and the remaining 20% is used as the testing set. The training set teaches and refines the models, helping them understand the data's patterns and relationships. Meanwhile, the testing set, completely separate from the training data, acts as an unbiased test to assess how well the models can apply their learning to new, unseen data.

2.2. Data Augmentation

Due to the significant imbalance between classes in the dataset, it's crucial to utilize data augmentation methods. In this study, a particular focus is given to oversampling techniques, which are employed to address this issue. Oversampling involves generating additional instances of the minority class, aiming to balance out the class distribution and improve the model's performance. Doing so mitigates the skewed representation of fraudulent transactions, leading to more accurate fraud detection. In this study, we employ five distinct oversampling techniques:

- Random Oversampling is a method for handling imbalanced datasets. It involves randomly

duplicating instances from the minority class to balance class distribution. While this approach can help prevent bias, it might also lead to overfitting due to duplicate data [28].

- SMOTE (Synthetic Minority Over-sampling Technique) is a method for handling imbalanced datasets. It creates synthetic samples for the minority class by interpolating between existing minority class instances. By introducing new synthetic instances, SMOTE helps prevent the model from being biased towards the majority class and can lead to better performance on imbalanced data [30, 31].
- SMOTE Tomek is a technique that combines SMOTE and the Tomek links algorithm. It balances class distribution with SMOTE's synthetic instances and improves class separation by removing close, conflicting instances using Tomek links. This leads to enhanced model performance by simultaneously addressing class imbalance and increasing class separation [32].
- SMOTE-Edited Nearest Neighbors (ENN) is a technique for handling imbalanced datasets in machine learning. It combines SMOTE, which generates synthetic data for the minority class, with ENN, which cleans the data by removing misclassified instances. This helps balance class distribution and improve model training on imbalanced data [33].
- ADASYN (Adaptive Synthetic Sampling) is a method for handling imbalanced datasets. It generates synthetic samples for the minority class, focusing on areas of the dataset that are densely populated by the minority class. This adaptive approach aims to create synthetic samples that are more representative of the underlying data distribution and can improve the performance of models trained on imbalanced data [34].

2.3. Machine Learning Model

In this research study, we utilized the XGBoost machine learning technique. We implemented this technique using the XGBoost library within Python programming, version 3.10.11. To develop our predictive model, we maintained the default settings of XGBoost during the training phase for simplicity and consistency. We trained the model using both the original dataset and an augmented dataset.

2.4. Performance Evaluation

The effectiveness of the XGBoost model is assessed through a comprehensive set of metrics, including accuracy, precision, recall, and F1-score. These metrics are employed to rigorously evaluate the model's performance for credit card fraud detection. Accuracy measures the proportion of correctly classified instances from the total predictions, providing an overall gauge of the model's correctness. Precision assesses the ratio of correctly predicted positive instances to all predicted positives, focusing on the accuracy of positive predictions and helping to control false positives. Recall, also known as sensitivity or true positive rate, calculates the ratio of correctly predicted positive instances to all actual positives, emphasizing the model's ability to identify all relevant cases. F1-score, a harmonic mean of precision and recall, offers a balanced assessment of a model's performance by considering both false positives and false negatives, making it particularly useful when classes are imbalanced. The equations for accuracy, precision, recall, and F-1 score are presented in Equations 1, 2, 3, and 4, respectively:

$$Accuracy = \frac{TP + FN}{FP + FN + TP + TN} \quad (1)$$

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

$$Recall = \frac{TP}{FN + TP} \quad (3)$$

$$F1 - Score = 2\frac{Precision \times Recall}{Precision + Recall} \quad (4)$$

where TP corresponds to the quantity of accurate positive classifications, FN signifies the quantity of erroneous negative classifications, FP represents the quantity of erroneous positive classifications, and TN indicates the quantity of precise negative classifications [35].

3. Results and Discussion

In this study, we successfully trained machine learning models to detect credit card fraud using machine learning and data augmentation techniques. The performance of the trained model when tested on unseen data is presented in Table 1.

The XGBoost without data augmentation method demonstrates accuracy with a score of 99.96%. It maintains a high precision of 97.73%, indicating that many flagged fraud cases are genuine instances of fraud. The recall, or true positive rate, stands at 82.69%, indicating that a substantial portion of fraud cases are

Table 1. Performance of the XGBoost models.

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
XGBoost	**99.96**	**97.73**	82.69	**89.58**
XGBoost + Random Oversampling	**99.96**	96.63	82.69	89.12
XGBoost + SMOTE	99.95	89.69	83.65	86.57
XGBoost + SMOTE Tomek	99.95	87.00	83.65	85.29
XGBoost + SMOTE ENN	99.95	86.27	**84.62**	85.44
XGBoost + ADASYN	99.94	85.29	83.65	84.47

Bold indicates the best result

Table 2. Prediction result of the XGBoost models.

Methods	True Positive	False Positive	True Negative	False Negative
XGBoost	86	18	56856	2
XGBoost + Random Oversampling	86	18	56855	3
XGBoost + SMOTE	87	17	56848	10
XGBoost + SMOTE Tomek	87	17	56845	13
XGBoost + SMOTE ENN	88	16	56844	14
XGBoost + ADASYN	87	17	56843	15

correctly identified. The F1-score balances precision and recall, 89.58%, suggesting a harmonious trade-off between correctly identifying fraud cases and minimizing false positives.

The XGBoost with random oversampling technique achieved the same accuracy at 99.96%, yet the precision slightly decreased to 96.63%. The recall and F1-score also experience minor reductions to 82.69% and 89.12%, respectively, potentially implying a slightly higher false-positive tolerance in exchange for broader fraud detection coverage.

Adding SMOTE to XGBoost yields an impressive accuracy of 99.95%, but the precision drops to 89.69%. However, the recall increased to 83.65%, indicating improved identification of actual fraud cases. This change results in an F1-score of 86.57%, indicating a favorable balance between precision and recall. The XGBoost with SMOTE Tomek maintains the accuracy and recall levels observed in the SMOTE method, but the precision drops to 87.00%. The resulting F1-score is 85.29%, reflecting a more conservative approach to identifying fraud cases. The combination of SMOTE ENN with XGBoost showcases a similar accuracy of 99.95%. While the precision experiences a slight drop to 86.27%, the recall increases to 84.62%. These changes led to an F1-score of 85.44%, reflecting a balanced performance between precision and recall. Lastly, the XGBoost combined with ADASYN achieved an accuracy of 99.94%. The precision slightly declines to 85.29%, and the recall remains at 83.65%. Consequently, the F1-score is 84.47%, indicating a stable performance in detecting fraud cases.

Among the different methods we evaluated, the XGBoost with SMOTE ENN approach is the most effective for detecting credit card fraud. This is because it achieves the highest recall rate of 84.62%, which measures the model's ability to identify actual fraud cases. This is a crucial factor for fraud detection because it emphasizes the model's capability to catch real fraudulent activities. It might also mean that the model could sometimes flag a few valid transactions as suspicious, but that's a trade-off we're willing to make to ensure fraud detection. The SMOTE ENN approach forms a balanced strategy. SMOTE addresses the challenge of having an imbalanced dataset by creating artificial samples for the minority class, which helps the model learn from rare fraud cases. On the other hand, ENN helps eliminate any potential noise or outliers that SMOTE might have introduced.

Table 2. provides a detailed breakdown of the results for different methods applied to credit card fraud detection, showing the number of true positives, false positives, true negatives, and false negatives for each method. In this study, "true positives" refer to the number of actual fraud cases correctly identified as fraud, while "false positives" represent legitimate transactions incorrectly flagged as fraud. "True negatives" indicate legitimate transactions correctly identified as non-fraudulent, and "false negatives" represent actual fraud cases that were not identified as such.

Among the methods, the XGBoost with SMOTE ENN emerges as the most effective credit card fraud detection approach. It achieves the highest number of true positives (88) and the lowest number of false positives (16), indicating a strong capability to correctly identify

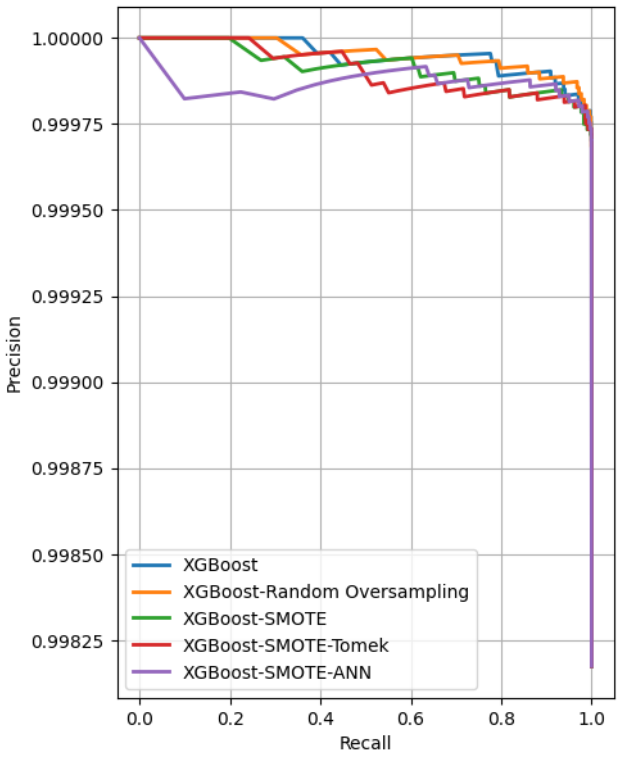

Figure 1. Precision-Recall curve.

actual instances of fraud while minimizing the misclassification of legitimate transactions as fraudulent. Although " the XGBoost with SMOTE ENN does have a slightly higher number of false negatives (14) compared to the XGBoost model without data augmentation (2), it is important to note that in credit card fraud detection scenarios, the emphasis is typically placed on maximizing the detection of fraud cases. In this context, more false negatives are more acceptable than false positives, as missing fraudulent transactions can lead to substantial financial losses. Considering the priorities of credit card fraud detection, "XGBoost + SMOTE ENN" offers a favorable balance between true positives and false positives. Its ability to significantly increase the detection of actual fraud cases while maintaining a low rate of false positives positions it as a more robust and suitable model for this specific application.

For further analysis, in Figure 1, we illustrate the precision-recall curve for all the models under consideration. The precision-recall curve is a graphical representation that provides insight into the trade-off between precision and recall as the discrimination threshold of a classification model varies. A higher precision indicates that when the model flags a transaction as fraudulent, it is highly likely to be an actual fraud case. A higher recall indicates that the model effectively captures a larger proportion of fraud cases, minimizing the chances of missing them. For the XGBoost model with SMOTE ENN, the recall and precision start high and decrease gradually as the curve progresses. This signifies that the model begins to miss some actual fraud cases as the discrimination threshold becomes more stringent. In summary, the model demonstrates its ability to achieve high precision while maintaining a relatively high recall rate. This suggests that the model effectively identifies many actual fraud cases with a low rate of false positives.

The study's results demonstrate that adopting this approach can greatly enhance financial management practices. This approach can help institutions improve their ability to detect and prevent fraudulent activities accurately. This, in turn, helps protect their financial environment and build trust with customers. One group that can particularly benefit from this implementation includes financial managers and accountants. They can utilize predictive models tailored to the complex patterns of fraudulent behavior. This empowers them to make well-informed decisions, allocate resources more efficiently, and proactively counter evolving fraud tactics. Moreover, the flexibility of machine learning models ensures that financial management systems remain adaptable and responsive to emerging fraud trends. This adaptability closes the gap between identifying new fraudulent strategies and implementing effective countermeasures. As a result, financial management practices become more resilient and better equipped to manage evolving risks.

4. Conclusions, Implications and Limitations

In this study, we successfully trained machine learning models to detect credit card fraud using a combination of machine learning and data augmentation techniques. Among the methods evaluated, XGBoost with SMOTE ENN emerged as the most effective approach for credit card fraud detection. This approach strikes a balanced strategy by addressing imbalanced datasets with SMOTE's artificial samples while eliminating potential noise with ENN.

These findings highlight the potential of this approach to significantly enhance financial management practices, particularly for financial managers and accountants. Predictive models tailored to fraud patterns empower better decision-making, resource allocation, and proactive fraud prevention. Moreover, the adaptability of machine learning models ensures that financial systems can stay responsive to evolving fraud tactics, enhancing overall resilience and risk management.

However, it is also important to acknowledge the limitations of this study. The dataset's specificity and the focus on a particular algorithm and augmentation technique could restrict the generalizability and

comprehensiveness of the findings. Moreover, the evolving nature of fraud tactics and unexplored socio-economic dimensions could impact the long-term viability of the proposed approach.

Author Contributions: Conceptualization, T.R.N., G.M.I., and R.I.; methodology, T.R.N., G.M.I., and I.H.; software, T.R.N. and A.M.; validation, E.S.R. and R.I.; formal analysis, T.R.N. and G.M.I.; investigation, T.R.N. and A.M.; resources, I.H. and E.S.R.; data curation, G.M.I., I.H., and R.I.; writing—original draft preparation, T.R.N, G.M.I., A.M., and I.H.; writing—review and editing, E.S.R. and R.I.; visualization, T.R.N. and A.M.; supervision, R.I.; project administration, R.I. All authors have read and agreed to the published version of the manuscript.

Funding: This study does not receive external funding.

Conflicts of Interest: All the authors declare that there are no conflicts of interest.

References

1. Barker, K. J., D'Amato, J., and Sheridon, P. (2008). Credit card fraud: awareness and prevention, *Journal of Financial Crime*, Vol. 15, No. 4, 398–410. doi:10.1108/13590790810907236.
2. Butaru, F., Chen, Q., Clark, B., Das, S., Lo, A. W., and Siddique, A. (2016). Risk and risk management in the credit card industry, *Journal of Banking & Finance*, Vol. 72, 218–239.
3. Almudaires, F., and Almaiah, M. (2021). Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation, *2021 International Conference on Information Technology (ICIT)*, IEEE, 732–738.
4. Limbu, Y. B., Huhmann, B. A., and Xu, B. (2012). Are college students at greater risk of credit card abuse? Age, gender, materialism and parental influence on consumer response to credit cards, *Journal of Financial Services Marketing*, Vol. 17, 148–162.
5. Leonard, K. J. (1993). Detecting credit card fraud using expert systems, *Computers & Industrial Engineering*, Vol. 25, Nos. 1–4, 103–106.
6. Kou, Y., Lu, C.-T., Sirwongwattana, S., and Huang, Y.-P. (2004). Survey of fraud detection techniques, *IEEE International Conference on Networking, Sensing and Control, 2004* (Vol. 2), IEEE, 749–754.
7. Bolton, R. J., and Hand, D. J. (2002). Statistical fraud detection: A review, *Statistical Science*, Vol. 17, No. 3, 235–255.
8. Asha, R. B., and KR, S. K. (2021). Credit card fraud detection using artificial neural network, *Global Transitions Proceedings*, Vol. 2, No. 1, 35–41.
9. Sailusha, R., Gnaneswar, V., Ramesh, R., and Rao, G. R. (2020). Credit card fraud detection using machine learning, *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, IEEE, 1264–1270.
10. Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., and Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection, *Information Sciences*, Vol. 557, 317–331.
11. Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., and Anderla, A. (2019). Credit card fraud detection-machine learning methods, *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, IEEE, 1–5.
12. Noviandy, T. R., Maulana, A., Idroes, G. M., Maulydia, N. B., Patwekar, M., Suhendra, R., and Idroes, R. (2023). Integrating Genetic Algorithm and LightGBM for QSAR Modeling of Acetylcholinesterase Inhibitors in Alzheimer's Disease Drug Discovery, *Malacca Pharmaceutics*, Vol. 1, No. 2, 48–54. doi:10.60084/mp.v1i2.60.
13. Agustia, M., Noviandy, T. R., Maulana, A., Suhendra, R., Muslem, M., Sasmita, N. R., Idroes, G. M., Rahimah, S., Afidh, R. P. F., Subianto, M., Irvanizam, I., and Idroes, R. (2022). Application of Fuzzy Support Vector Regression to Predict the Kovats Retention Indices of Flavors and Fragrances, *2022 International Conference on Electrical Engineering and Informatics (ICELTICs)*, IEEE, 13–18. doi:10.1109/ICELTICs56128.2022.9932124.
14. Noviandy, T. R., Maulana, A., Emran, T. B., Idroes, G. M., and Idroes, R. (2023). QSAR Classification of Beta-Secretase 1 Inhibitor Activity in Alzheimer's Disease Using Ensemble Machine Learning Algorithms, *Heca Journal of Applied Sciences*, Vol. 1, No. 1, 1–7. doi:10.60084/hjas.v1i1.12.
15. Maulana, A., Noviandy, T. R., Idroes, R., Sasmita, N. R., Suhendra, R., and Irvanizam, I. (2020). Prediction of Kovats Retention Indices for Fragrance and Flavor using Artificial Neural Network, *Proceedings of the International Conference on Electrical Engineering and Informatics* (Vol. 2020-Octob). doi:10.1109/ICELTICs50595.2020.9315391.
16. Idroes, R., Noviandy, T. R., Maulana, A., Suhendra, R., Sasmita, N. R., Muslem, M., Idroes, G. M., Kemala, P., and Irvanizam, I. (2021). Application of Genetic Algorithm-Multiple Linear Regression and Artificial Neural Network Determinations for Prediction of Kovats Retention Index, *International Review on Modelling and Simulations (IREMOS)*, Vol. 14, No. 2, 137. doi:10.15866/iremos.v14i2.20460.
17. Maulana, A., Faisal, F. R., Noviandy, T. R., Rizkia, T., Idroes, G. M., Tallei, T. E., El-Shazly, M., and Idroes, R. (2023). Machine Learning Approach for Diabetes Detection Using Fine-Tuned XGBoost Algorithm, *Infolitika Journal of Data Science*, Vol. 1, No. 1, 1–7. doi:10.60084/ijds.v1i1.72.
18. Noviandy, T. R., Maulana, A., Idroes, G. M., Suhendra, R., Adam, M., Rusyana, A., and Sofyan, H. (2023). Deep Learning-Based Bitcoin Price Forecasting Using Neural Prophet, *Ekonomikalia Journal of Economics*, Vol. 1, No. 1, 19–25. doi:10.60084/eje.v1i1.51.
19. Chen, T., and Guestrin, C. (2016). Xgboost: A scalable tree boosting system, *Proceedings of the 22nd Acm Sigkdd International Conference on Knowledge Discovery and Data Mining*, 785–794.
20. Rufo, D. D., Debelee, T. G., Ibenthal, A., and Negera, W. G. (2021). Diagnosis of Diabetes Mellitus Using Gradient Boosting Machine (LightGBM), *Diagnostics*, Vol. 11, No. 9, 1714. doi:10.3390/diagnostics11091714.
21. Maulana, A., Noviandy, T. R., Sasmita, N. R., Paristiowati, M., Suhendra, R., Yandri, E., Satrio, J., and Idroes, R. (2023). Optimizing University Admissions: A Machine Learning Perspective, *Journal of Educational Management and Learning*, Vol. 1, No. 1, 1–7. doi:10.60084/jeml.v1i1.46.
22. Dong, X., Yu, Z., Cao, W., Shi, Y., and Ma, Q. (2020). A survey on ensemble learning, *Frontiers of Computer Science*, Vol. 14, No. 2, 241–258. doi:10.1007/s11704-019-8208-z.
23. Al Daoud, E. (2019). Comparison between XGBoost, LightGBM and CatBoost using a home credit dataset, *International Journal of Computer and Information Engineering*, Vol. 13, No. 1, 6–10.
24. Li, H., Cao, Y., Li, S., Zhao, J., and Sun, Y. (2020). XGBoost model and its application to personal credit evaluation, *IEEE Intelligent Systems*, Vol. 35, No. 3, 52–61.
25. Kotsiantis, S., Kanellopoulos, D., and Pintelas, P. (2006). Handling imbalanced datasets: A review, *GESTS International Transactions on Computer Science and Engineering*, Vol. 30, No. 1, 25–36.
26. Chawla, N. V. (2010). Data mining for imbalanced datasets: An overview, *Data Mining and Knowledge Discovery Handbook*, 875–886.

27. Maharana, K., Mondal, S., and Nemade, B. (2022). A review: Data pre-processing and data augmentation techniques, *Global Transitions Proceedings*, Vol. 3, No. 1, 91–99.

28. Mohammed, R., Rawashdeh, J., and Abdullah, M. (2020). Machine learning with oversampling and undersampling techniques: overview study and experimental results, *2020 11th International Conference on Information and Communication Systems (ICICS)*, IEEE, 243–248.

29. Yap, B. W., Rani, K. A., Rahman, H. A. A., Fong, S., Khairudin, Z., and Abdullah, N. N. (2014). An application of oversampling, undersampling, bagging and boosting in handling imbalanced datasets, *Proceedings of the First International Conference on Advanced Data and Information Engineering (DaEng-2013)*, Springer, 13–22.

30. Chawla, N. V, Bowyer, K. W., Hall, L. O., and Kegelmeyer, W. P. (2002). SMOTE: synthetic minority over-sampling technique, *Journal of Artificial Intelligence Research*, Vol. 16, 321–357.

31. Suhendra, R., Arnia, F., Idroes, R., Earlia, N., and Suhartono, E. (2019). A Novel Approach to Multi-class Atopic Dermatitis Disease Severity Scoring using Multi-class SVM, *2019 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*, IEEE, 35–39. doi:10.1109/CYBERNETICSCOM.2019.8875693.

32. Jonathan, B., Putra, P. H., and Ruldeviyani, Y. (2020). Observation imbalanced data text to predict users selling products on female daily with smote, tomek, and smote-tomek, *2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, IEEE, 81–85.

33. Muntasir Nishat, M., Faisal, F., Jahan Ratul, I., Al-Monsur, A., Ar-Rafi, A. M., Nasrullah, S. M., Reza, M. T., and Khan, M. R. H. (2022). A comprehensive investigation of the performances of different machine learning classifiers with SMOTE-ENN oversampling technique and hyperparameter optimization for imbalanced heart failure dataset, *Scientific Programming*, Vol. 2022, 1–17.

34. He, H., Bai, Y., Garcia, E. A., and Li, S. (2008). ADASYN: Adaptive synthetic sampling approach for imbalanced learning, *2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*, Ieee, 1322–1328.

35. Tharwat, A. (2020). Classification assessment methods, *Applied Computing and Informatics*, Vol. 17, No. 1, 168–192.