ISSN 2776-8007

Optimization of Fraud Detection in E-Commerce: A CGAN Data Augmentation Approach to Address Class Imbalance

Zulham[1,*], Amru Yasir[2,]

[1]*Software Engineering, Dharmawangsa University, Indonesia*

[2]*Information Technology, Dharmawangsa University, Indonesia*

(Received: June 1, 2024; Revised: July 5, 2024; Accepted: October 1, 2024; Available online: December 1, 2024)

Abstract

The rapid growth of e-commerce has increased the risk of fraud in online transactions, resulting in significant financial losses and decreased consumer trust. One of the main challenges in fraud detection is data imbalance, where the number of legitimate transactions far exceeds fraudulent transactions. This imbalance causes machine learning models to fail in accurately identifying fraudulent transactions. This study aims to evaluate the effectiveness of Conditional Generative Adversarial Network (CGAN) in improving fraud detection performance in e-commerce through data augmentation. Two machine learning algorithms, Random Forest (RF) and XGBoost, were used to classify transactions in both the original imbalanced dataset and the dataset augmented with CGAN. The study uses key evaluation metrics, including accuracy, precision, recall, and F1-score, to measure the model's performance. The results show that data augmentation using CGAN significantly improved the performance of both models. RF on the augmented dataset achieved an accuracy of 99.96%, precision of 99.93%, recall of 99.99%, and F1-score of 99.96%. Meanwhile, XGBoost achieved an accuracy of 99.93%, precision of 99.91%, recall of 99.94%, and F1-score of 99.92%. The main contribution of this study is to demonstrate that CGAN can effectively address the challenge of data imbalance and improve the reliability of fraud detection systems in e-commerce. This approach has the potential to be applied in various sectors facing similar issues, such as anomaly detection in finance and cybersecurity.

Keywords: Fraud Detection, E-Commerce, CGAN, Data Augmentation, Machine Learning

1. Introduction

In recent years, e-commerce has become one of the most dynamic sectors in the global economy. According to Zhou et al. [1], e-commerce transactions increased by 110% in the United States in 2020, marking a significant acceleration of digital transformation across various industrial sectors. This rapid growth has brought convenience and efficiency to both consumers and businesses, but it has also introduced new challenges in the form of online fraud. Fraud in e-commerce not only leads to significant financial losses but also impacts consumer trust in digital payment systems [2], [3].

According to research by Zeng et al. [4], the proliferation of fraud in online payments has caused substantial economic losses, reduced customer trust, and complicated detection due to its dynamic and diverse nature. Fraud in e-commerce encompasses various forms such as identity theft, buyer fraud, and collaboration between buyers and sellers. To address this challenge, models capable of processing highly imbalanced data and identifying complex fraud patterns in real-time are needed [3].

Fraud detection in e-commerce is a major challenge due to the highly imbalanced nature of transaction data [5]. In such cases, the number of legitimate transactions far exceeds fraudulent ones, causing machine learning models to tend to ignore the minority class (fraud). Zarzà et al. [6] emphasized that data imbalance leads to predictive models failing to detect fraud patterns accurately, increasing the number of harmful false-negatives where fraudulent transactions go

***Corresponding author: Zulham (zullham@dharmawangsa.ac.id)**

DOI: https://doi.org/10.47738/ijaim.v4i4.90

undetected. This is further supported by Chu's findings [7], which stated that the inability of models to capture fraud patterns leads to significant financial losses and reputational risks for e-commerce platforms.

According to Khan et al. [8], the problem of data imbalance can cause bias towards the majority class, resulting in models failing to recognize important patterns from the minority class. To overcome this, machine learning-based approaches require effective data augmentation techniques to ensure that models can detect anomalies accurately and consistently across various application scenarios [9], [10].

To tackle the data imbalance challenge, various resampling methods have been developed [11], [12]. One widely used method is the Synthetic Minority Over-sampling Technique (SMOTE), which increases the number of minority class samples through linear interpolation [13]. However, SMOTE has limitations in capturing complex data distributions and may generate synthetic samples that are less representative [14]. A better alternative to address this issue is the use of CGAN. According to Lebichot et al. [15], CGAN has the ability to generate more realistic and complex synthetic data, enabling machine learning models to learn fraud patterns more deeply.

According to Lee et al. [16], the use of Generative Adversarial Networks (GANs) allows for the creation of high-quality synthetic data that resembles anomaly data. This technique is effective in enhancing detection capabilities because GANs can learn the complex distribution of actual data. Thus, the use of CGAN offers an innovative solution to balance datasets and reduce model bias towards the majority class [17].

CGAN works with two main components: the generator and the discriminator. The generator is responsible for creating synthetic data samples based on certain conditions (such as the fraud label), while the discriminator evaluates whether the sample is real or synthetic [18]. The interaction between these two components allows CGAN to generate data that is more varied and closer to the real data. Thus, the data augmentation process using CGAN can help balance datasets and enhance the model's ability to recognize fraud patterns [19].

2. Literature Review

2.1. Fraud Detection in E-Commerce

Fraud in e-commerce is a continuously evolving issue as the volume of online transactions increases. Zhou et al. [1] revealed that the surge in e-commerce transactions significantly raises the risk of fraud. Fraud in e-commerce directly impacts financial losses and decreases consumer trust in digital platforms. The growing complexity of fraud requires more adaptive detection methods. According to Moreira et al. [20], machine learning techniques such as Random Under Sampling, SMOTE, and ADASYN have been shown to improve the ability of models to detect fraud in banking systems. This research demonstrates that combining resampling techniques with machine learning algorithms such as Logistic Regression and KNN significantly enhances sensitivity to suspicious transactions and reduces the false-negative rate. Additionally, the implementation of these techniques in banking environments enables faster responses to anomalies, reducing the potential for large losses for financial institutions.

2.2. Data Imbalance in Machine Learning

Class imbalance is a key challenge in fraud detection. Zarzà et al. [6] highlighted that machine learning models tend to prioritize the majority class, leading to low accuracy in detecting the minority class (fraud). Chu [7] stated that the inability of models to recognize fraud patterns leads to an increase in false negatives, resulting in significant losses. According to Gupta et al. [21], oversampling methods such as Random Over-Sampling (ROS) and the XGBoost algorithm perform best in addressing data imbalance in credit card fraud detection. This study shows that using resampling techniques with algorithm-based models significantly improves accuracy and F1-score compared to conventional approaches. Recent research indicates that combining resampling techniques with ensemble models such as RF and XGBoost can substantially improve model performance in real-world environments.

2.3. Data Balancing Methods

Various approaches have been developed to address data imbalance. Mqadi et al. [13] introduced SMOTE as an effective oversampling technique, although it has limitations in capturing complex data distributions [14]. According to Azim et al. [22], an ensemble learning approach based on soft voting, combined with oversampling and under sampling techniques, can significantly enhance fraud detection accuracy. This research confirms that the combination of resampling techniques with ensemble learning models like RF and XGBoost provides the best performance in capturing rare fraud patterns. Moreover, a hybrid approach that combines resampling with hyperparameter fine-tuning on the model has been shown to yield more accurate predictions.

2.4. Generative Adversarial Network (GAN) Approach

The GAN-based approach offers an innovative solution for generating realistic synthetic data. Lebichot et al. [15] demonstrated that CGAN excels in generating data variations that resemble actual fraudulent transactions. Lee et al. [16] emphasized that the use of R-GAN with regularization significantly improves anomaly detection accuracy in imbalanced datasets.

3. Methodology

This study follows a systematic series of steps designed to evaluate the effectiveness of data augmentation using CGAN in improving fraud detection in e-commerce. The following are the research stages in accordance with the flow diagram in figure 1:

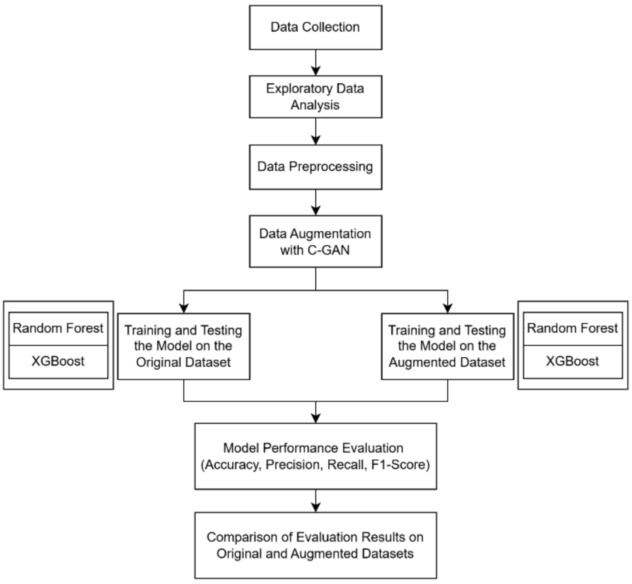
Data Collection
Exploratory Data Analysis
Data Preprocessing
Data Augmentation with C-GAN
Random Forest
XGBoost
Training and Testing the Model on the Original Dataset
Training and Testing the Model on the Augmented Dataset
Random Forest
XGBoost
Model Performance Evaluation (Accuracy, Precision, Recall, F1-Score)
Comparison of Evaluation Results on Original and Augmented Datasets

Figure 1. Research Methodology

3.1. Data Collection

The dataset was obtained from Kaggle and consists of 23,634 transactions. This dataset was chosen because it contains a variety of relevant attributes for detecting fraud patterns in e-commerce transactions. After downloading, the data underwent exploratory analysis to understand the distribution of each variable, check for missing values, and identify outliers that might affect the analysis results.

Subsequently, data cleaning was performed, including handling missing data, normalizing attributes, and encoding categorical variables into numerical form to meet the requirements of machine learning algorithms. Class imbalance in the dataset was addressed using resampling techniques such as oversampling the minority class or under sampling the majority class. This step ensures that the developed model can identify fraudulent transactions accurately without bias towards the dominant class.

3.2. Exploratory Data Analysis (EDA)

This process involves performing descriptive statistical checks, visualizing data distributions, identifying outliers, and detecting patterns that could affect model performance. Descriptive statistics were used to analyze key metrics such as mean, median, mode, and standard deviation to understand the data spread. Data visualization was carried out through graphs such as histograms, boxplots, and scatter plots to identify distributions and anomalies. This analysis helps detect data imbalances, correlations between variables, and features that have significant contributions to fraud prediction.

Additionally, techniques like heatmaps were used to map correlations between attributes, providing further insights into the relationships among variables. Understanding these patterns in the dataset allows for adjustments to features or transformations of variables to enhance model performance in subsequent stages. EDA is an essential step to ensure that the machine learning training process runs optimally and yields accurate predictions.

3.3. Data Preprocessing

The data preprocessing stage prepares the dataset to be compatible with the machine learning algorithm. The first step in preprocessing is handling missing values through imputation methods. For numerical features, the median is used as a substitute because it is more robust to outliers, while for categorical features, the mode is used as the most frequently occurring value.

Next, categorical variables were encoded using the one-hot encoding method. This technique transforms categorical variables into binary numerical representations, allowing machine learning models to process this information effectively. With one-hot encoding, each category is converted into a separate column containing values of 0 or 1, which prevents the model from assuming any ordinal relationships between categories that are inherently nominal.

The final step is normalizing the numerical features. Normalization ensures that all variables are on a similar scale, which is crucial for machine learning algorithms sensitive to scale differences, such as k-Nearest Neighbors (k-NN) or gradient-based algorithms. Normalization helps accelerate convergence during training and ensures that each feature contributes proportionately to the prediction process. With these steps, the data becomes cleaner, more consistent, and ready for building the fraud detection model.

3.4. Data Augmentation with CGAN

To address the class imbalance in the dataset, the CGAN method was used to generate synthetic data resembling fraudulent transactions. CGAN was chosen because it can generate high-quality data samples that reflect the true distribution of the minority class.

CGAN consists of two main components: the generator and the discriminator. The generator is tasked with creating synthetic data samples based on conditional labels, such as fraud or non-fraud status. Meanwhile, the discriminator's role is to distinguish between real and synthetic data. During training, the generator strives to produce data that increasingly resembles the real data, while the discriminator provides feedback to help the generator improve the quality of the synthetic data generated.

The synthetic data generated by CGAN is then combined with the original dataset to balance the proportion between legitimate and fraudulent transactions. With this data augmentation, the machine learning model can learn from a more balanced distribution, improving its ability to detect fraudulent transactions without bias towards the majority class. This technique is a crucial step in ensuring that the model performs accurately and generalizes well to new data.

3.5. Model Training

The model training stage used two main algorithms: RF and XGBoost. Both models were applied to two types of datasets: the original imbalanced dataset and the augmented dataset, which had a balanced proportion between legitimate and fraudulent transactions. The training process began by splitting the dataset into training and testing data using cross-validation. Cross-validation helps validate the model's performance thoroughly and reduces the risk of overfitting, especially with complex datasets. By splitting the data into several subsets (folds), the model is trained alternately on different subsets, ensuring that the performance evaluation includes the entire dataset.

Additionally, hyperparameter optimization was carried out using GridSearchCV to find the best parameter combination for each model. GridSearchCV evaluates various parameter combinations, such as the number of trees in RF or the learning rate in XGBoost, to improve prediction accuracy and model efficiency. With this approach, the resulting model is expected to perform optimally in detecting fraudulent transactions in the dynamic e-commerce environment.

3.6. Model Performance Evaluation

Model performance evaluation is conducted using several key metrics to measure the effectiveness of predictions. The metrics used include accuracy, precision, recall, and F1-score. The evaluation results are compared between the model trained on the original dataset and the model trained on the augmented dataset using CGAN. This analysis aims to assess the impact of data augmentation on improving fraud detection accuracy and to determine whether the CGAN approach successfully addresses class imbalance bias.

The primary goal is to evaluate how well the CGAN-augmented dataset improves the model's ability to detect fraud in e-commerce environments. The evaluation metrics, such as accuracy, precision, recall, and F1-score, will be used to compare both models and highlight any improvements achieved through data augmentation. By conducting this thorough evaluation, the best-performing model can be identified, one that demonstrates the ability to accurately and reliably detect fraud while addressing the challenges posed by class imbalance in the data. The results will provide insights into the effectiveness of using CGAN for fraud detection and whether it contributes to the model's robustness in detecting fraudulent activities.

4. Results and Discussion

4.1. Results for Imbalanced Dataset

Based on the classification results using RF on the original (imbalanced) dataset, the model's performance in classifying fraudulent and non-fraudulent transactions is as follows. The confusion matrix provides information about the model's performance in predicting correct and incorrect transactions for each class (fraudulent and non-fraudulent).

Table 1 shows that out of the total fraudulent transactions, only 47 transactions were correctly classified as fraudulent (True Positive). A total of 320 fraudulent transactions were incorrectly classified as legitimate transactions (False Negative), indicating that the model struggled to identify fraudulent transactions. Meanwhile, there were 6 legitimate transactions that were incorrectly classified as fraud (False Positive), and 6718 legitimate transactions were correctly classified (True Negative).

Table 1. Confusion Matrix for Random Forest Model on Imbalanced Dataset

	Predicted Positive (Fraud)	Predicted Negative (Non-Fraud)
Actual Positive (Fraud)	47	320
Actual Negative (Non-Fraud)	6	6718

Table 2 shows that the model has an accuracy of 95.35%, precision of 88.68%, recall of 12.81%, and F1-score of 22.36%. Despite having a high accuracy, the low recall value indicates that the model was ineffective in recognizing fraudulent transactions, as most fraudulent transactions went undetected.

Table 2. Evaluation Results for Random Forest Model on Imbalanced Dataset

Metric	Value (%)
Accuracy	95.35
Precision	88.68
Recall	12.81
F1 Score	22.36

Table 3 shows that the XGBoost model identified 48 fraudulent transactions correctly (True Positive), while 319 fraudulent transactions were incorrectly classified as legitimate transactions (False Negative). A total of 13 legitimate transactions were misclassified as fraudulent (False Positive), and 6711 legitimate transactions were correctly classified (True Negative). These results are similar to RF, where the low recall indicates that many fraudulent transactions were not detected.

Table 3. Confusion Matrix for XGBoost Model on Imbalanced Dataset

	Predicted Positive (Fraud)	**Predicted Negative (Non Fraud)**
Actual Positive (fraud)	48	319
Actual Negative (Non-Fraud)	13	6711

Table 4 shows that the model has an accuracy of 95.32%, precision of 78.69%, recall of 13.08%, and F1-score of 22.34%. The low recall value indicates that the model still struggles to recognize most fraudulent transactions, despite having high accuracy.

Table 4. Evaluation Results for XGBoost Model on Imbalanced Dataset

Metric	**Value (%)**
Accuracy	95.32
Precision	78.69
Recall	13.08
F1 Score	22.34

4.2. Results for Augmented Dataset

Table 5 shows a significant improvement, where the model successfully identified 6746 fraudulent transactions correctly (True Positive), only 1 fraudulent transaction was misclassified (False Negative), 5 legitimate transactions were misclassified (False Positive), and 6673 legitimate transactions were correctly classified (True Negative).

Table 5. Confusion Matrix for Random Forest Model on Balanced Dataset

	Predicted Positive (Fraud)	**Predicted Negative (Non Fraud)**
Actual Positive (Fraud)	6746	1
Actual Negative (Non Fraud)	5	6673

Table 6 and Figure 2 show that the RF model performed excellently on the augmented dataset across various evaluation metrics. The accuracy of the model reached 99.96%, which means almost all of the predictions made by the model were correct. This high accuracy indicates that the model has a very low error rate in classifying the data. Additionally, precision of 99.93% indicates that almost all positive predictions made by the model were correct. This suggests that the model performs excellently in avoiding false positives. On the other hand, recall reached 99.99%, meaning the model was able to detect almost all positive cases in the dataset. This high recall value reflects the model's ability to minimize false negatives. The combination of high precision and recall resulted in an F1 Score of 99.96%, demonstrating a good balance between both metrics. Overall, these evaluation results show that the RF model has a highly reliable and accurate performance on the augmented dataset. The data augmentation technique used proved to be effective in enhancing the model's performance, especially when dealing with class imbalance issues.

Table 6. Evaluation Results for Random Forest Model on Balanced Dataset

Metric	**Value (%)**
Accuracy	99.96
Precision	99.93
Recall	99.99
F1 Score	99.96

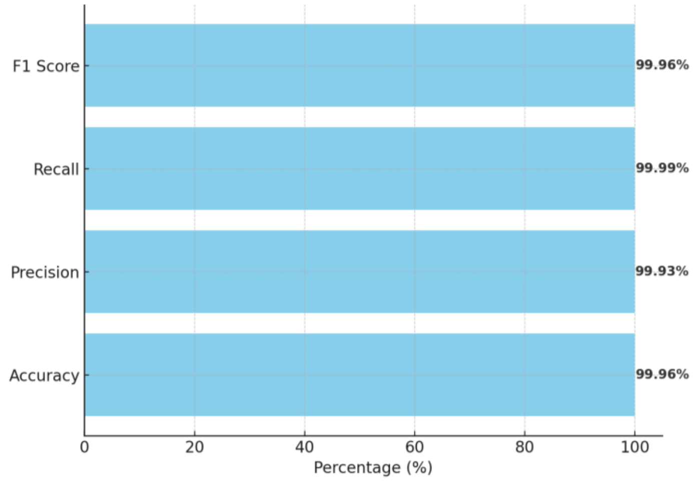

Figure 2. Evaluation Results for Random Forest Model on Balanced Dataset

Figure 3 shows the ROC curve for the RF model on the augmented dataset. The ROC curve is used to evaluate the model's classification performance by plotting the True Positive Rate (TPR) or sensitivity on the y-axis, and the False Positive Rate (FPR) or 1-specificity on the x-axis. In this curve, the blue line represents the ROC curve, with the area under the curve (AUC) recorded as 1.00, which is the ideal value. This AUC score indicates that the model has perfect discriminatory power, as the area under the curve ranges from 0 (random guessing) to 1 (perfect classification). The AUC score of 1.00 shows that the model is highly effective in distinguishing between the positive and negative classes. The gray dashed line represents a random classifier, where the TPR equals the FPR at all thresholds. Overall, the perfect AUC score of 1.00 demonstrates that the RF model on the balanced and augmented dataset performs exceptionally well in classifying both classes with minimal error.

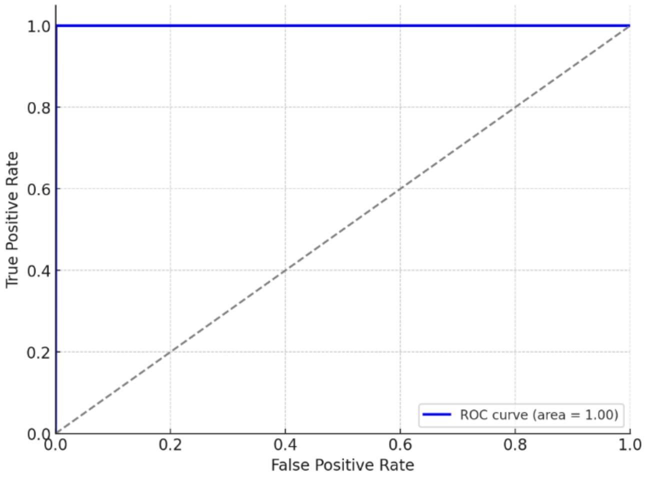

Figure 3. ROC Curve for Random Forest Model on Balanced Dataset

Table 7 shows that the XGBoost model successfully identified 6751 fraudulent transactions correctly (True Positive), only 4 fraudulent transactions were misclassified as legitimate (False Negative), 6 legitimate transactions were misclassified as fraud (False Positive), and 6706 legitimate transactions were correctly classified (True Negative).

Table 7. Confusion Matrix for XGBoos Model on Balanced Dataset

	Predicted Positive (Fraud)	**Predicted Negative (Non Fraud)**
Actual Positive (Fraud)	6751	4
Actual Negative (Non Fraud)	6	6706

Table 8 and figure 4 show the evaluation results for the XGBoost model on the augmented dataset show outstanding performance, almost matching that of the RF model. With an accuracy of 99.93%, the XGBoost model demonstrates excellent ability to classify data with minimal error. This indicates that almost all of the predictions made by this model were correct. Additionally, the precision of 99.91% shows that almost all positive predictions made were accurate. This indicates the model's low rate of false positives. The recall of 99.94% means the model was highly effective in detecting most of the positive samples in the dataset. The high recall value suggests that the model can identify nearly all positive cases, reducing the potential for errors in detecting the true positive class. The combination of high precision and recall results in an F1 Score of 99.92%, indicating an optimal balance between both metrics. Overall, the evaluation results show that the XGBoost model is highly effective in classification with a very low error rate on the augmented dataset. The data augmentation technique applied proved to have a positive impact on the model's performance, making it highly reliable and effective in classifying data.

Table 8. Evaluation Results for XGBoos Model on Balanced Dataset

Metric	Value (%)
Accuracy	99.93
Precision	99.91
Recall	99.94
F1 Score	99.92

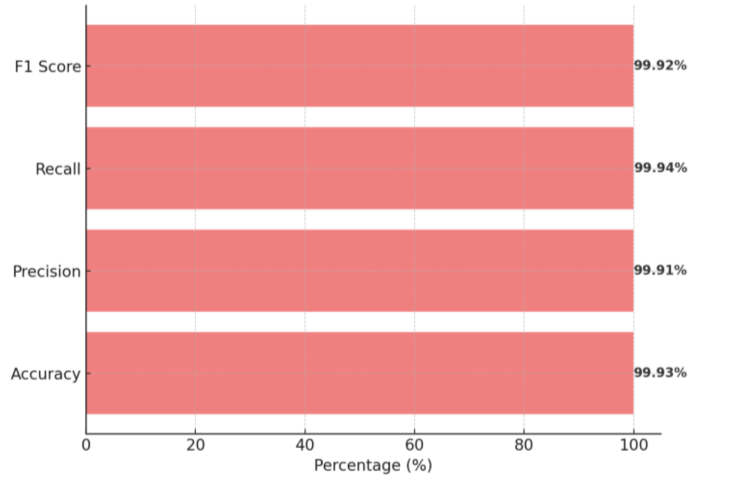

Figure 4. Evaluation Results for XGBoost Model on Augmented on Balanced Dataset

Figure 5 illustrates the relationship between the True Positive Rate (TPR) and the False Positive Rate (FPR). TPR measures the proportion of positives that are correctly identified, while FPR measures the proportion of negatives that are incorrectly identified as positives. In this graph, the ROC curve shows that the XGBoost model can effectively separate the positive and negative classes. The area under the curve (AUC) reaches 1.00, which is an indicator that the model is nearly perfect in separating the positive class from the negative class. AUC values close to 1.00 indicate that the model has very high predictive power, reflecting that nearly all positive cases are successfully detected with very few errors in predicting the negative class. Overall, this ROC curve confirms that the XGBoost model applied to the augmented dataset performs exceptionally well with near-perfect detection ability and very low prediction errors.

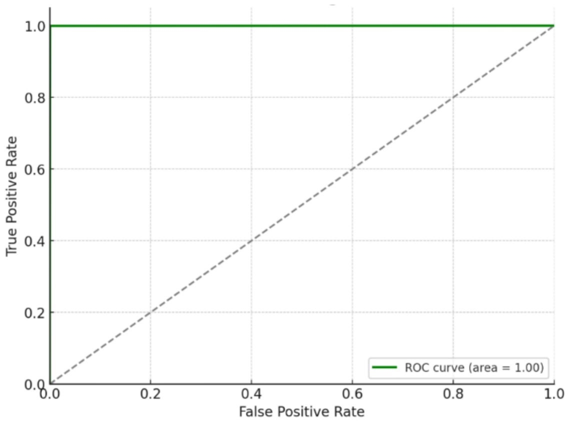

Figure 5. ROC Curve for XGBoost Model on Augmented on Balanced Dataset

Data augmentation using CGAN significantly improved fraud detection performance in both the RF and XGBoost models. In the original imbalanced dataset, both models had high accuracy (around 95%), but the recall performance was very low (12.81% for RF and 13.08% for XGBoost), indicating that many fraudulent transactions went undetected. After data augmentation, the performance of both models drastically improved. RF achieved an accuracy of 99.96%, precision of 99.93%, recall of 99.99%, and F1-score of 99.96%. The XGBoost model also showed improvement with an accuracy of 99.93%, precision of 99.91%, recall of 99.94%, and F1-score of 99.92%.

From these results, it can be concluded that data augmentation using CGAN effectively addresses the issue of data imbalance. Models trained on the augmented dataset have much better capabilities in recognizing fraudulent transactions while minimizing classification errors (false negatives and false positives). RFslightly outperforms XGBoost in recall, but both models show excellent performance overall. Thus, the application of CGAN provides a significant contribution to improving the reliability of fraud detection systems on e-commerce platforms.

4.3. Discussion

The results of the study indicate that CGAN significantly enhances fraud detection performance in e-commerce. This research compared the performance of two machine learning algorithms, RF and XGBoost, on both the original imbalanced dataset and the dataset augmented with CGAN. The key findings show that data augmentation with CGAN can address the challenge of class imbalance, which often causes models to struggle with detecting fraudulent transactions.

In the original imbalanced dataset, both models showed high accuracy (around 95%), but had very low recall values (12.81% for RF and 13.08% for XGBoost). The low recall values indicate that most fraudulent transactions went undetected by the models. This condition proves that without data balancing, the models tend to be biased toward the majority class (legitimate transactions) and fail to recognize fraudulent transactions effectively [13], [23], [24].

After data augmentation using CGAN, there was a significant improvement in performance across all evaluation metrics. The RF model trained on the augmented dataset achieved an accuracy of 99.96%, precision of 99.93%, recall of 99.99%, and F1-score of 99.96%. Meanwhile, the XGBoost model achieved an accuracy of 99.93%, precision of 99.91%, recall of 99.94%, and F1-score of 99.92%. This improvement demonstrates that data augmentation with CGAN not only enhances the model’s ability to detect fraudulent transactions (recall), but also maintains very low classification errors (false positives and false negatives) [15], [17].

The main advantage of CGAN over traditional oversampling methods such as SMOTE lies in its ability to generate more complex synthetic data that closely mirrors the characteristics of actual fraudulent transactions. Previous studies have shown that CGAN-based methods, such as K-CGAN, significantly outperform conventional oversampling techniques (SMOTE, B-SMOTE, and ADASYN) in improving fraud detection performance on imbalanced datasets. K-CGAN can generate high-quality synthetic datasets that help machine learning models capture more complex and varied fraud patterns [17]. As a result, machine learning models can learn more diverse and realistic fraud patterns, which improves model generalization when faced with new data.

Interestingly, RF showed an advantage in recall compared to XGBoost, indicating its superior ability to detect fraudulent transactions. However, XGBoost provided more balanced results across all metrics, showing high stability even after data augmentation. Previous research also indicates that RF tends to perform better in detecting fraudulent transactions after applying oversampling methods like SMOTE, which reduces bias toward the majority class and improves the model’s ability to identify the minority class [13]. This difference can be explained by the internal mechanisms of each algorithm: RF tends to produce more conservative predictions, while XGBoost uses optimized gradients to improve accuracy gradually [13].

The practical implications of this research are wide-ranging. With the increasing prevalence of fraud in e-commerce, the CGAN approach provides an innovative solution that can be applied in production environments to improve the security of online transactions. Moreover, this method can be adapted to various other industries facing similar challenges, such as anomaly detection in finance, healthcare, or cybersecurity. Previous research confirms that combining data augmentation techniques and hyperparameter optimization can yield optimal results in detecting fraudulent transactions across various e-commerce scenarios [6].

Although CGAN provides significant performance improvement, the training process for this model requires substantial computational resources and more time compared to traditional methods. Additionally, the effectiveness of CGAN heavily depends on the quality of the initial dataset and the parameters used in its training. Future research may explore the development of more efficient CGAN architectures or integrate this method with other techniques such as ensemble learning for even better results.

5. Conclusion

Based on the research findings, it can be concluded that the use of CGAN effectively improves fraud detection performance in e-commerce. Data augmentation using CGAN addresses the class imbalance issue, which is a major challenge in detecting fraudulent transactions.

The RF and XGBoost models showed significant improvements across all evaluation metrics after data augmentation. RF has an advantage in recall with a value of 99.96%, indicating its ability to detect more fraudulent transactions. On the other hand, XGBoost provides more balanced results across all evaluation metrics, reflecting stable and consistent performance.

The results of this study provide an important contribution to the development of more accurate and adaptive fraud detection systems. The CGAN approach can be widely applied in various industry sectors facing similar challenges in detecting anomalies or rare cases. Moreover, this study opens opportunities for further exploration in improving the efficiency and effectiveness of CGAN through architecture optimization and integration with other machine learning methods. Therefore, this study emphasizes that CGAN is an innovative and effective solution in addressing data imbalance and improving fraud detection performance in e-commerce environments.

6. Declarations

6.1. Author Contributions

Conceptualization: Z., A.Y.; Methodology: Z., A.Y.; Software: Z.; Validation: A.Y.; Formal Analysis: Z.; Investigation: Z.; Resources: A.Y.; Data Curation: Z.; Writing – Original Draft Preparation: Z.; Writing – Review and Editing: A.Y.; Visualization: Z.; All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H. Zhou, G. Sun, S. Fu, W. Jiang, and J. Xue, “A scalable approach for fraud detection in online e-commerce transactions with big data analytics,” *Comput. Mater. Contin.*, vol. 60, no. 1, pp. 179–192, 2019, doi: 10.32604/cmc.2019.05214.

[2] R. Damayanti and Z. Adrianto, “Machine Learning for E-Commerce Fraud Detection,” *J. Ris. Akunt. Dan Bisnis Airlangga*, vol. 8, no. 2, pp. 1562–1577, 2023, doi: 10.20473/jraba.v8i2.48559.

[3] G. Airlangga, “Evaluating the Efficacy of Machine Learning Models in Credit Card Fraud Detection,” *J. Comput. Networks,*

Archit. High Perform. Comput., vol. 6, no. 2, pp. 829–837, 2024, doi: 10.47709/cnahpc.v6i2.3814.

[4] Q. Zeng, L. Lin, R. Jiang, W. Huang, and D. Lin, "NNEnsLeG: A novel approach for e-commerce payment fraud detection using ensemble learning and neural networks," *Inf. Process. Manag.*, vol. 62, no. 1, pp. 103916, 2025, doi: 10.1016/j.ipm.2024.103916.

[5] A. Taherkhani, G. Cosma, and T. M. McGinnity, "AdaBoost-CNN: An adaptive boosting algorithm for convolutional neural networks to classify multi-class imbalanced datasets using transfer learning," *Neurocomputing*, vol. 404, pp. 351–366, 2020, doi: 10.1016/j.neucom.2020.03.064.

[6] I. de Zarzà, J. de Curtò, and C. T. Calafate, "Optimizing Neural Networks for Imbalanced Data," *Electron.*, vol. 12, no. 12, pp. 1–26, 2023, doi: 10.3390/electronics12122674.

[7] Y. Bing Chu, Z. Min Lim, B. Keane, P. Hao Kong, A. Rafat Elkilany, and O. Hisham Abusetta, "Credit Card Fraud Detection on Original European Credit Card Holder Dataset Using Ensemble Machine Learning Technique," *J. Cyber Secur*., vol. 5, no. 0, pp. 33–46, 2023, doi: 10.32604/jcs.2023.045422.

[8] A. A. Khan, O. Chaudhari, and R. Chandra, "A review of ensemble learning and data augmentation models for class imbalanced problems: Combination, implementation and evaluation," E*xpert Syst. Appl.*, vol. 244, no. 2023, pp. 122778, 2024, doi: 10.1016/j.eswa.2023.122778.

[9] R. K. L. Kennedy, Z. Salekshahrezaee, F. Villanustre, and T. M. Khoshgoftaar, "Iterative cleaning and learning of big highly-imbalanced fraud data using unsupervised learning," *J. Big Data*, vol. 10, no. 1, pp. 106, Jun 2023, doi: 10.1186/s40537-023-00750-3.

[10] X. Wang, Z. Liu, J. Liu, and J. Liu, "Fraud detection on multi-relation graphs via imbalanced and interactive learning," *Inf. Sci. (Ny)*., vol. 642, pp. 119153, 2023, doi: 10.1016/j.ins.2023.119153.

[11] T. R. Noviandy, G. M. Idroes, A. Maulana, I. Hardi, E. S. Ringga, and R. Idroes, "Credit Card Fraud Detection for Contemporary Financial Management Using XGBoost-Driven Machine Learning and Data Augmentation Techniques," *Indatu J. Manag. Accoun*t., vol. 1, no. 1, pp. 29–35, Sep 2023, doi: 10.60084/ijma.v1i1.78.

[12] D. Breskuvienė, and G. Dzemyda. Enhancing credit card fraud detection: highly imbalanced data case. *J Big Data*., vol. 11, no. 182, pp. 1-24, 2024, doi: 10.1186/s40537-024-01059-5

[13] N. Mqadi, N. Naicker, and T. Adeliyi, "A SMOTe based Oversampling Data-Point Approach to Solving the Credit Card Data Imbalance Problem in Financial Fraud Detection," *Int. J. Comput. Digit. Syst*., vol. 10, no. 1, pp. 277–286, 2021, doi: 10.12785/ijcds/100128.

[14] R. Bounab, K. Zarour, B. Guelib, and N. Khlifa, "Enhancing Medicare Fraud Detection Through Machine Learning: Addressing Class Imbalance With SMOTE-ENN," I*EEE Access*, vol. 12, pp. 54382–54396, 2024, doi: 10.1109/ACCESS.2024.3385781.

[15] B. Lebichot, T. Verhelst, Y.-A. Le Borgne, L. He-Guelton, F. Oble, and G. Bontempi, "Transfer Learning Strategies for Credit Card Fraud Detection," *IEEE Acce*ss, vol. 9, pp. 114754–114766, 2021, doi: 10.1109/ACCESS.2021.3104472.

[16] J. Lee, D. Jung, J. Moon, and S. Rho, "Advanced R-GAN: Generating anomaly data for improved detection in imbalanced datasets using regularized generative adversarial networks," *Alexandria Eng. J.*, vol. 111, no. Sept, pp. 491–510, 2025, doi: 10.1016/j.aej.2024.10.084.

[17] E. Strelcenia dan S. Prakoonwit, "A New GAN-based data augmentation method for Handling Class Imbalance in Credit Card Fraud detection," *Proc. 10th Int. Conf. Signal Process. Integr. Networks*, vol. 2023, pp. 627–634, 2023, doi: 10.1109/SPIN57001.2023.10116543.

[18] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[19] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, dan G. Obaido, "A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection," *IEEE Access*, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.

[20] M. Â. L. Moreira et al., "Exploratory analysis and implementation of machine learning techniques for predictive assessment of fraud in banking systems," *Procedia Comput. Sci*., vol. 214, pp. 117–124, 2022, doi: 10.1016/j.procs.2022.11.156.

[21] P. Gupta, A. Varshney, M. R. Khan, R. Ahmed, M. Shuaib, and S. Alam, "Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques," *Procedia Comput. Sci*., vol. 218, pp. 2575–2584, 2022, doi: 10.1016/j.procs.2023.01.231.

[22] M. Azim Mim, N. Majadi, and P. Mazumder, “A soft voting ensemble learning approach for credit card fraud detection,” *Heliyon*, vol. 10, no. 3, pp. e25466, 2024, doi: 10.1016/j.heliyon.2024.e25466.

[23] Z. Wu, H. Wang, J. Guo, Q. Yang, and J. Shao, “Learning evolving prototypes for imbalanced data stream classification with limited labels,” *Inf. Sci. (Ny).*, vol. 679, no. March, pp. 120979, 2024, doi: 10.1016/j.ins.2024.120979.

[24] M. M. Ahsan, M. S. Ali, and Z. Siddique, “Enhancing and improving the performance of imbalanced class data using novel GBO and SSG: A comparative analysis,” *Neural Networks*, vol. 173, no. Sept, pp. 106157, 2024, doi: 10.1016/j.neunet.2024.106157.