Jurnal Kecerdasan Buatan dan Teknologi Informasi
Vol. 5, No. 2, May 2026, pp. 279-287
e-ISSN: 2964-2922, p-ISSN: 2963-6191
DOI : https://doi.org/10.69916/jkbti.v5i2.478

XGBOOST-BASED FRAUD TRANSACTION CLASSIFICATION ANALYSIS IN ONLINE PAYMENT SYSTEMS

Sri Diantika[*1], Hiya Nalatissifa[2], Riki Supriyadi[3], Nurlaelatul Maulidah[4], Ahmad Fauzi[5]

[1,2,4,5]Faculty of Engineering and Informatics, Universitas Bina Sarana Informatika, Jakarta, Indonesia
[3]Faculty of Information Technology, Universitas Nusa Mandiri, Jakarta, Indonesia
Email: [1]sri.szd@bsi.ac.id, [2]hiya.hys@bsi.ac.id, [3]riki.rsd@nusamandiri.ac.id, [4]nurlaelatul.nlt@bsi.ac.id, [5]ahmad.fzx@bsi.ac.id

(Received: May 4, 2026; Revised: May 8, 2026; Accepted: May 14, 2026)

Abstract

The rapid development of online payment systems has significantly facilitated digital transactions; however, it has simultaneously increased the risk of fraudulent activities. Fraud detection has become a critical challenge due to the complex characteristics of transaction data and the imbalanced class distribution between legitimate and fraudulent transactions. This study aims to analyze the performance of the XGBoost algorithm in classifying fraudulent transactions within online payment systems. The research employs the Online Payments Fraud Detection Dataset obtained from the Kaggle platform. The research methodology consists of several stages, including dataset collection, data preprocessing, categorical data transformation using label encoding, feature engineering for the generation of new attributes, data partitioning through split validation with an 80:20 ratio, model development using the XGBoost algorithm, and performance evaluation using a confusion matrix, accuracy, precision, recall, F1-score, and Area Under the Curve (AUC). The experimental results demonstrate that the XGBoost model achieves excellent classification performance, with an accuracy of 99.98%, precision of 85%, recall of 100%, F1-score of 92%, and an AUC value of 0.9996. Furthermore, feature importance analysis reveals that errorOrig and newbalanceOrig are the most influential attributes in detecting fraudulent transactions. Based on these findings, it can be concluded that the XGBoost algorithm is highly effective for fraud transaction classification in online payment systems and exhibits strong potential for implementation in automated fraud detection systems to enhance the security of digital financial transactions.

Keywords: xgboost; classification; fraud detection; online payment; machine learning.

1. INTRODUCTION

The rapid advancement of digital technology has driven a major transformation in payment systems, where financial transactions are increasingly conducted online through various digital platforms such as mobile banking, e-wallets, marketplaces, and payment gateways. The convenience, speed, and flexibility offered by online payment systems have significantly increased transaction volumes [1] However, on the other hand, the growth of digital transaction activities has also intensified security threats in the form of fraudulent transactions, which may result in substantial financial losses for both users and financial service providers [2] Fraud in online payment systems has become one of the major challenges in modern digital finance, as attack patterns continue to evolve and become increasingly sophisticated, making them difficult to detect using conventional approaches [3].

Traditional fraud detection methods, which are generally based on rule-based systems, exhibit limitations in identifying new and dynamic fraudulent patterns [4]. Rule-based systems tend to be effective only in detecting previously known fraud patterns, rendering them less adaptive to continuously evolving fraud schemes [5]. This condition has encouraged the adoption of machine learning as a more adaptive solution for detecting suspicious transactions through historical data pattern analysis. Machine learning is capable of automatically learning transaction characteristics and performing more accurate classifications of legitimate and fraudulent transactions [6].

One of the major challenges in fraud detection is data imbalance, where the number of fraudulent transactions is significantly smaller than that of legitimate transactions [7]. This imbalance may cause classification models to become biased toward the majority class, thereby reducing their ability to optimally detect fraudulent transactions. Recent studies have demonstrated that addressing data imbalance through class weighting or resampling techniques significantly improves the performance of fraud detection models, particularly in terms of recall and F1-score, which are critical indicators in fraud detection systems[8].

Among various machine learning algorithms, XGBoost (Extreme Gradient Boosting) has emerged as one of the most widely adopted methods for fraud classification due to its strong capability in handling tabular data, mitigating overfitting through regularization, and delivering robust classification performance on imbalanced datasets [9].

Research in [10] demonstrated that XGBoost exhibits high effectiveness in detecting fraud in mobile payment systems and handling imbalanced data scenarios. Other studies have also reported that combining XGBoost with imbalance-handling techniques can achieve superior Area Under Curve (AUC) and F1-score performance compared to several other classification algorithms.

A previous study [10] analyzed the performance of several machine learning models in detecting fraudulent transactions in online payment systems, including Logistic Regression, Random Forest, XGBoost, and BiLSTM. The findings indicated that XGBoost and BiLSTM achieved the best performance based on evaluation metrics such as accuracy, precision, recall, F1-score, and ROC-AUC. The study also revealed that the application of data balancing techniques using SMOTE improved the model's ability to detect fraudulent transactions, particularly in terms of recall performance. Furthermore, XGBoost was considered superior in computational efficiency and interpretability compared to deep learning models, making it more suitable for real-time fraud detection implementation. Another study [11] demonstrated that an XGBoost model optimized through hyperparameter tuning achieved better classification performance than several other machine learning algorithms, such as Random Forest and Logistic Regression, particularly in terms of Area Under Curve (AUC) and precision. These findings further reinforce that XGBoost is one of the most effective algorithms for detecting abnormal transaction patterns in online payment systems.

Although numerous previous studies have demonstrated the effectiveness of XGBoost in fraud classification, limitations remain regarding the use of secondary datasets and the lack of in-depth analysis concerning the influence of class weighting on imbalanced data. Therefore, further investigation is required to comprehensively evaluate the performance of the XGBoost algorithm in detecting fraudulent transactions within online payment systems. Based on these considerations, this study aims to analyze the classification of fraudulent transactions in online payment systems using the XGBoost algorithm to evaluate the model's capability in accurately detecting fraud. This research is expected to contribute to the development of more effective fraud detection systems and serve as a reference for the implementation of machine learning in the digital transaction security sector.

2. RESEARCH METHOD

This research method section systematically describes the stages of the study, beginning with dataset collection, data processing, and ending with the classification analysis of fraudulent transactions in online payment systems using the XGBoost method. The research workflow is illustrated in Figure 1.

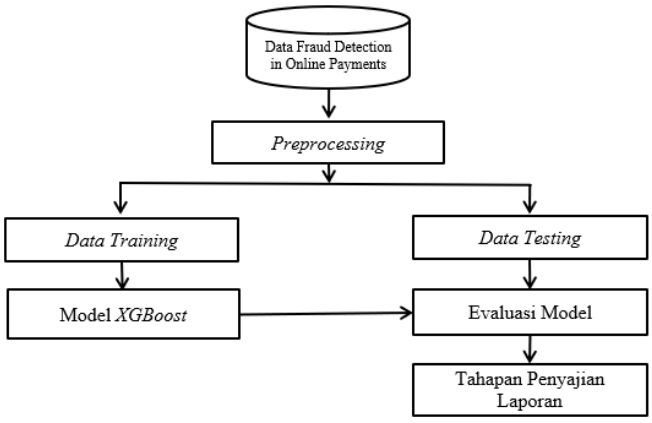

Figure 1. Research Workflow Diagram

2.1. Dataset Collection

The initial stage of this study involved collecting an online payment transaction dataset obtained from the Kaggle platform, namely the *Online Payments Fraud Detection Dataset*. This dataset contains historical digital payment transaction data consisting of both legitimate and fraudulent transactions. Several important attributes are included in the dataset for analytical purposes, such as *step*, *type* (transaction type), *amount* (transaction amount), *oldbalanceOrg* (sender's initial balance), *newbalanceOrig* (sender's final balance), *oldbalanceDest* (recipient's initial balance), *newbalanceDest* (recipient's final balance), and the classification label *isFraud*, which indicates whether a transaction is fraudulent or not.

2.2. Preprocessing

The preprocessing stage was conducted to prepare the dataset for optimal use in the classification modeling process using the XGBoost algorithm. This process aimed to improve data quality, reduce noise, and ensure that the data were formatted appropriately for model training. The preprocessing steps performed in this study include the following:

a. Data Inspection
At the initial stage, the dataset structure was examined to identify the total number of records, data types of each attribute, and the possible presence of missing values or inconsistent data.

b. Data Cleaning
The dataset was cleaned to remove invalid values, duplicate records, and anomalies that could negatively affect model performance. If missing values or irrelevant attributes were identified, appropriate handling procedures were applied according to the research requirements.

c. Categorical Data Transformation
The online payment transaction dataset contains a categorical attribute, namely type, which represents transaction categories such as CASH-IN, CASH-OUT, DEBIT, PAYMENT, and TRANSFER. Since the XGBoost algorithm can only process numerical data, this attribute was transformed into numerical form using the Label Encoding technique. This transformation assigns numerical representations to each transaction category, enabling its utilization during the model training process. This stage ensures that transaction type information remains useful for classification analysis.

d. Feature Engineering
At this stage, new features were generated to improve the model's capability in recognizing fraudulent transaction patterns. The newly created features include:
   1. errorOrig
      This feature represents the discrepancy between the sender's initial balance, sender's final balance, and the transaction amount.
   2. errorDest
      This feature represents the discrepancy between the recipient's final balance, recipient's initial balance, and the transaction amount.

   The purpose of creating these features is to identify inconsistencies in balance changes, which may indicate suspicious or abnormal transaction activities. The inclusion of these additional features enables the model to detect fraud patterns more effectively compared to relying solely on the original attributes.

e. Feature Selection
Following the transformation and feature engineering processes, the next stage involved selecting relevant attributes for the classification process.
The features utilized in this study include:
   1. type_encoded
   2. amount
   3. oldbalanceOrg
   4. newbalanceOrig
   5. oldbalanceDest
   6. newbalanceDest
   7. errorOrig
   8. errorDest

   Feature selection was conducted to ensure that the model only processes attributes relevant to fraud transaction detection.

f. Handling Imbalanced Data
Imbalanced data refers to a condition in which the distribution of class instances within a dataset is uneven, where one class significantly outnumbers the other. In this study, the online payment transaction dataset exhibits class imbalance between legitimate and fraudulent transactions, with legitimate transactions overwhelmingly dominating fraudulent transactions as the minority class. To examine the class distribution within the dataset, a data visualization process was performed, as shown in Figure 2. The visualization illustrates a substantial difference in the number of instances between the two classes.

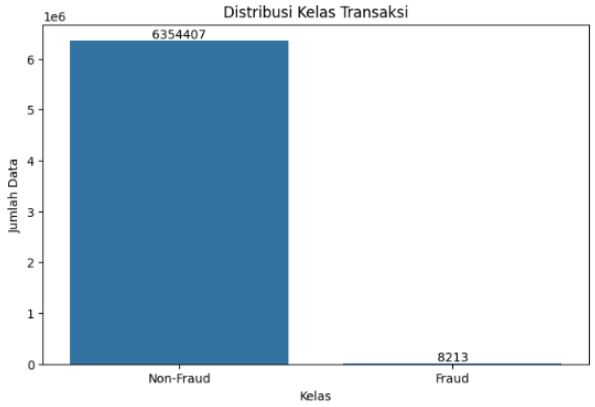

Figure 2. Imbalanced Data Visualization

Based on Figure 2, it can be observed that the number of legitimate transactions is significantly larger than fraudulent transactions. This condition indicates that the dataset possesses imbalanced characteristics. Such class imbalance may adversely affect classification model performance, as models tend to focus more on learning patterns from the majority class than from the minority class. Consequently, the model may achieve high accuracy while exhibiting poor capability in detecting fraudulent transactions. To address this issue, this study implemented a class weighting technique using the scale_pos_weight parameter in the XGBoost algorithm. This approach assigns a larger weight to the minority class, namely fraudulent transactions, allowing the model to pay greater attention to fraud-related patterns during the training process. The scale_pos_weight value was calculated based on the ratio between the number of majority-class samples and minority-class samples. This approach was selected because it efficiently addresses data imbalance without altering the original dataset distribution. The implementation of class weighting using scale_pos_weight is expected to improve the model's sensitivity in detecting fraudulent transactions, thereby optimizing classification performance for the minority class without compromising the model's ability to classify legitimate transactions.

2.3. Split Validation

After completing all preprocessing stages, the dataset was divided into two subsets, namely training data and testing data, using the *split validation* method. In this study, the dataset was partitioned using an 80:20 ratio, where 80% of the data were allocated as training data to train the XGBoost classification model, while the remaining 20% were used as testing data to evaluate model performance. This data partitioning strategy was implemented to ensure that the model could be evaluated using previously unseen data, allowing the evaluation results to objectively reflect the model's capability in classifying fraudulent transactions. Furthermore, this approach helps reduce the risk of overfitting in the developed model, thereby improving its generalization performance on new transaction data.

2.4. Modelling

The modeling stage involved the development of a classification model using the XGBoost (Extreme Gradient Boosting) algorithm. XGBoost is an ensemble-based machine learning algorithm that operates by sequentially constructing multiple decision trees using the gradient boosting technique [12] This algorithm was selected due to its strong performance in classification tasks, capability to handle large-scale datasets, and effectiveness in addressing class imbalance problems, particularly in fraud transaction detection cases.

In this study, the model training process was conducted using the training dataset obtained from the previous data partitioning stage. The model was trained to identify patterns of legitimate and fraudulent transactions based on features that had undergone preprocessing. To improve classification performance, the XGBoost model was configured using several parameters tailored to the characteristics of the dataset. Parameter determination in this study was performed manually based on recommendations from relevant literature and the official XGBoost documentation. Hyperparameter optimization methods such as Grid Search, Random Search, and Bayesian Optimization were not employed in this research. Parameter selection was carried out by considering a balance between classification performance, model generalization capability, and computational efficiency. The configuration of model parameters used in this study is presented in table 1.

Table 1. Model Parameters.

Parameter	Value	Description
scale_pos_weight	Based on calculation results	Handles class imbalance
n_estimators	200	Number of decision trees
max_depth	6	Maximum tree depth
learning_rate	0.1	Model learning rate

subsample	0.8	Proportion of training data per tree
colsample_bytree	0.8	Proportion of features per tree
random_state	42	Ensures result reproducibility
n_jobs	-1	Utilizes all processor cores

The parameters used represent empirical configurations commonly applied to imbalanced data classification problems and have been adjusted to meet the requirements of this study. After the parameter configuration process was completed, the model was trained using the training dataset and subsequently employed to perform predictions on the testing dataset during the model evaluation stage.

2.5. Model Evaluation

The model evaluation stage was conducted to measure the performance of the XGBoost algorithm in classifying fraudulent transactions in online payment systems. The evaluation process was performed using testing data, namely data that were not involved during the model training process, ensuring that the testing results objectively reflect the model's capability in predicting unseen data. In this study, model evaluation was carried out using a confusion matrix to compare the model's predicted results with the actual labels in the dataset. The confusion matrix was utilized to determine the number of correct and incorrect predictions generated during the classification process[13].

Based on the confusion matrix, model performance was assessed using several evaluation metrics, namely accuracy, precision, recall, and F1-score. The selection of these metrics aimed to provide a comprehensive understanding of the model's capability in detecting fraudulent transactions. Accuracy was employed to measure the overall correctness of the model in classifying transaction data. Precision was used to evaluate the accuracy of the model in predicting fraudulent transactions. Recall measured the model's ability to detect all fraudulent transactions present in the dataset. Meanwhile, the F1-score was applied to assess the balance between precision and recall. The use of precision, recall, and F1-score is particularly important in fraud detection research because transaction datasets generally exhibit imbalanced class distributions[14]. Under such conditions, a model with high accuracy does not necessarily possess strong capability in detecting fraudulent transactions. Therefore, recall and precision become the primary indicators for evaluating the effectiveness of the model. The evaluation results were subsequently analyzed to determine the effectiveness of the XGBoost algorithm in classifying fraudulent transactions in online payment systems. The obtained evaluation values were then used as the basis for drawing conclusions regarding the performance of the developed model[15].

3. RESULTS AND DISCUSSION

This chapter presents the results of testing the fraud transaction classification model in online payment systems using the XGBoost algorithm, along with a discussion of the performance of the developed model. The testing process was conducted using testing data obtained from the split validation process after undergoing preprocessing and model training stages. The research findings were analyzed using several evaluation metrics, namely the confusion matrix, accuracy, precision, recall, F1-score, *and* Area Under Curve (AUC). These metrics were employed to measure the model's effectiveness in identifying both legitimate and fraudulent transactions. The discussion in this chapter is systematically organized, beginning with the implementation of model testing, followed by testing results, model performance analysis, and an evaluation of the effectiveness of the XGBoost algorithm in detecting fraudulent transactions in online payment systems.

3.1. Model Testing Implementation

At this stage, the classification model was implemented using the XGBoost algorithm on the online payment transaction dataset that had undergone preprocessing. The dataset was divided into 80% training data and 20% testing data using the split validation method. The implementation process involved training the model using the training dataset to recognize patterns of legitimate and fraudulent transactions based on the selected features. The model was developed using parameters determined during the modeling stage, including adjustments to the *scale_pos_weight* parameter to address class imbalance distribution. After the training process was completed, the model was employed to perform predictions on the testing dataset. The prediction results were subsequently evaluated using several performance metrics to determine the model's effectiveness in classifying fraudulent transactions.

3.2. Model Testing Results

The model testing stage was conducted to determine the accuracy level and effectiveness of the XGBoost algorithm in classifying online payment transactions. Model evaluation was performed using a confusion matrix, classification report, ROC curve, and feature importance analysis to obtain a comprehensive understanding of model performance.

a. Confusion Matrix

To evaluate the model's performance in classifying fraudulent and non-fraudulent transactions, a *confusion matrix* analysis was conducted. This method was employed to compare the model's predictions with the actual labels in the testing dataset, thereby identifying the number of correct and incorrect predictions for each class.

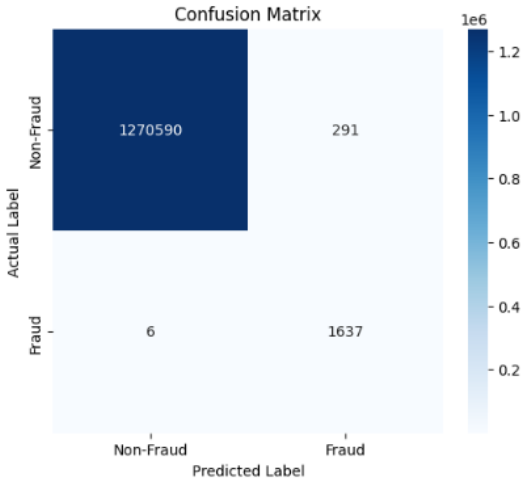

Figure 2. Confusion Matrix Results of the XGBoost Model

Based on the testing results, the confusion matrix indicates that the model successfully classified the majority of transaction data correctly. The model accurately identified 1,270,590 legitimate transactions and 1,637 fraudulent transactions. In addition, 291 legitimate transactions were incorrectly classified as fraudulent (false positives), while 6 fraudulent transactions were incorrectly classified as legitimate (false negatives).

These findings indicate that the model possesses excellent classification capability in distinguishing between legitimate and fraudulent transactions. However, the presence of 291 false positives should be considered carefully in real-world payment system implementation. Such classification errors may cause valid user transactions to be blocked or require additional verification procedures, potentially reducing user convenience, negatively affecting transaction experience, and lowering customer trust in the payment system. Although the number of false positives is relatively small compared to the total number of tested transactions, their impact should still be considered in fraud detection system development to maintain a balance between system security and transaction convenience.

b. Classification Report

To obtain a more detailed understanding of model performance, an evaluation using a classification report was conducted. This evaluation aimed to measure the model's performance based on several metrics, namely accuracy, precision, recall, and F1-score. These metrics were utilized to assess the model's capability in accurately detecting fraudulent transactions, particularly in datasets exhibiting imbalanced class distributions.

Table 2. Classification Report Results

Metric	Value
Accuracy	99,98%
Precision	85%
Recall	100%
F1-Score	92%
AUC Score	99,96%

Based on the evaluation results, the model achieved an accuracy of 99.98%, precision of 85%, recall of 100%, and an F1-score of 92%. These results demonstrate that the model is capable of detecting nearly all fraudulent transactions with a very high level of accuracy.

c. ROC Curve

In addition to the confusion matrix and classification report, model performance was also evaluated using the Receiver Operating Characteristic (ROC) curve. The ROC curve was employed to measure the model's ability to distinguish between fraudulent and non-fraudulent transaction classes across different classification threshold values. This evaluation generated an Area Under Curve (AUC) value, which indicates the model's classification capability.

A higher AUC value, particularly one approaching 1, signifies superior performance in distinguishing between the two classes.

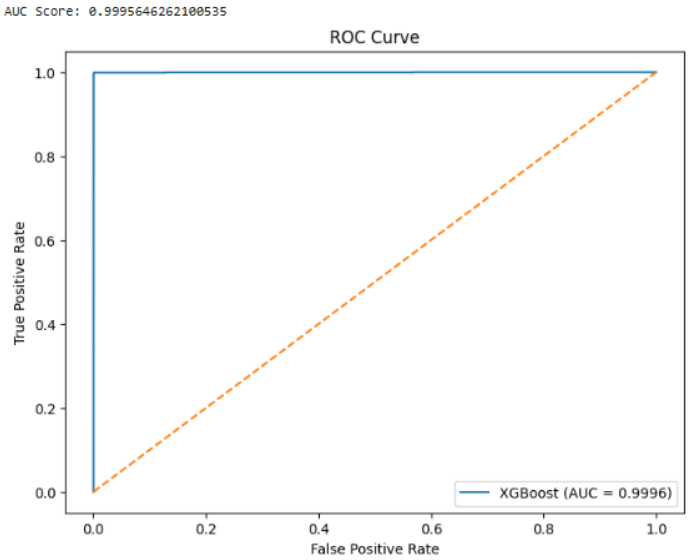

Figure 3 ROC Curve of the XGBoost Model

The ROC curve produced an AUC value of 0.9996, indicating that the model demonstrates excellent capability in distinguishing fraudulent and non-fraudulent transactions. An AUC value approaching **1** reflects highly optimal classification performance.

d. Feature Important

To determine the contribution level of each feature to the classification process, *feature importance analysis* was conducted on the XGBoost model. This analysis aimed to identify the attributes that most significantly influence the model in distinguishing fraudulent from non-fraudulent transactions. Through this analysis, the extent to which each feature contributes to the model's decision-making process can be identified.

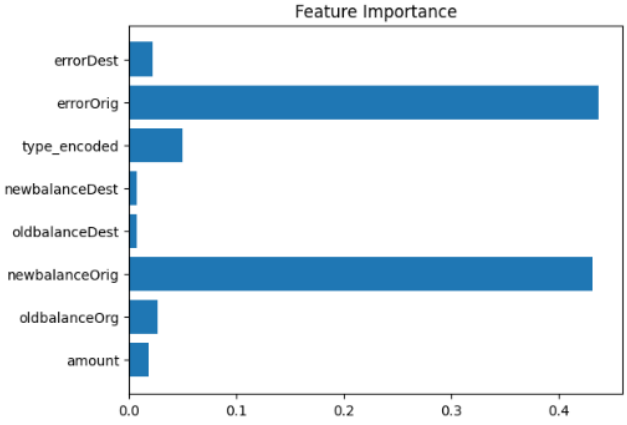

Figure 4. Feature Important

Based on the feature importance visualization results, errorOrig and newbalanceOrig were found to have the highest contribution values compared to other features. The dominance of the errorOrig feature indicates that inconsistencies in changes to the sender's balance relative to transaction amounts represent a major indicator of fraudulent transactions. This finding suggests that anomalies in sender balance changes have a strong relationship with suspicious transaction activities. Meanwhile, the high contribution of the newbalanceOrig feature indicates that the sender's ending balance after a transaction also plays an important role in helping the model identify fraud patterns. These findings suggest that the XGBoost model primarily utilizes sender-side balance change patterns to distinguish fraudulent transactions from legitimate transactions.

3.3. Analysis of Testing Results

Based on the evaluation results, the XGBoost algorithm demonstrated excellent performance in classifying fraudulent transactions in online payment systems. This is evidenced by an accuracy of 99.98%, precision of 85%, recall of 100%, F1-score of 92%, and an AUC value of 0.9996. The exceptionally high accuracy value indicates that the model successfully classified nearly all transaction data correctly. However, in fraud classification studies, accuracy cannot be considered the sole performance indicator because the dataset exhibits an imbalanced class distribution between legitimate and fraudulent transactions. The 100% recall value demonstrates that the model possesses excellent capability in detecting all fraudulent transactions within the testing dataset. This finding is further supported by the presence of only 6 false negatives, indicating that very few fraudulent transactions failed to be detected by the model. The 85% precision value indicates that most transactions predicted as fraudulent were indeed fraudulent. Although 291 false positives were still observed, this condition remains acceptable in the context of fraud detection systems, as flagging a number of legitimate transactions as suspicious is generally preferable to failing to detect fraudulent transactions that may lead to financial losses. The 92% F1-score indicates a strong balance between precision and recall, suggesting that the model not only detects fraud comprehensively but also maintains high prediction accuracy.

Furthermore, evaluation using the ROC curve demonstrated highly optimal performance with an AUC value of 0.9996. This value indicates that the model possesses exceptionally strong discriminatory capability in distinguishing fraudulent from non-fraudulent transactions. Additionally, feature importance analysis revealed that errorOrig and newbalanceOrig contributed most significantly to the classification process. These findings indicate that sender balance change patterns constitute the primary indicators in detecting suspicious transaction activities. Overall, the testing results demonstrate that the XGBoost algorithm is highly effective for fraud transaction classification analysis in online payment systems. Its high performance indicates that the model can serve as a reliable approach for supporting automated fraud detection systems.

3.4. Discussion

Based on the testing results obtained, the XGBoost model demonstrated excellent performance in classifying fraudulent transactions in online payment systems. The high evaluation scores indicate that the model is capable of effectively distinguishing between legitimate and fraudulent transactions. In the context of datasets with imbalanced class distributions, model performance should not be assessed solely based on accuracy, but also through precision, recall, F1-score, and ROC-AUC, which provide a more comprehensive understanding of the model's classification capability. The confusion matrix results indicate that the model successfully classified 1,270,590 legitimate transactions and 1,637 fraudulent transactions correctly. In addition, *291* legitimate transactions were incorrectly classified as fraudulent (false positives), while 6 fraudulent transactions were incorrectly classified as legitimate (false negatives). The extremely low number of false negatives demonstrates that the model possesses high sensitivity in detecting fraudulent transactions, thereby minimizing the likelihood of fraudulent activities bypassing the monitoring system. This capability is particularly important in online payment systems, as failure to detect fraudulent transactions may lead to financial losses for both users and service providers. On the other hand, the presence of 291 false positives indicates that a number of legitimate transactions were incorrectly identified as fraudulent. In real-world implementation, this condition may result in valid user transactions being delayed, temporarily rejected, or subjected to additional verification procedures. Consequently, this may affect user convenience and reduce trust in the payment system. Therefore, although the model demonstrates excellent performance, maintaining a balance between system security and seamless user transaction experience remains essential. The strong performance of the model was also influenced by the implementation of the scale_pos_weight parameter in XGBoost to address data imbalance. This approach enables the model to allocate greater attention to the minority class, namely fraudulent transactions, thereby improving detection capability without compromising overall classification accuracy. These findings are consistent with previous studies, which reported that imbalance handling techniques significantly contribute to improvements in recall and F1-score in fraud detection cases. The findings of this study are also consistent with previous research [10], [11] which reported that XGBoost is an effective algorithm for detecting fraudulent transactions. The advantages of this algorithm lie in its capability to process tabular data, reduce overfitting through regularization, and achieve high classification performance on imbalanced datasets.

Nevertheless, this study still has several limitations, particularly regarding the use of a secondary dataset, which may not fully represent real-world transaction conditions across various payment systems. Furthermore, this study did not directly compare the performance of XGBoost with other algorithms or evaluate computational efficiency in large-scale implementations. Therefore, future research may further extend this analysis by utilizing more representative datasets and conducting comparative evaluations with other machine learning and deep learning methods.

4. CONCLUSION

Based on the results of this study, the XGBoost algorithm demonstrated excellent performance in classifying fraudulent transactions in online payment systems. The model successfully distinguished between legitimate and

fraudulent transactions with high effectiveness, achieving an accuracy of 99.98%**,** precision of 85%, recall of 100%, F1-score of 92%**,** and an AUC value of 0.9996. These results indicate that XGBoost possesses strong capability in detecting fraudulent transactions, particularly in datasets characterized by imbalanced class distributions.

The confusion matrix results further revealed that the model correctly classified the majority of transactions, with only a small number of misclassifications. The very low number of false *negatives* indicates that the model has high sensitivity in detecting fraudulent transactions, thereby minimizing the risk of fraud escaping the monitoring system. However, the presence of false positives suggests that several legitimate transactions were incorrectly classified as fraudulent, highlighting the importance of maintaining a balance between transaction security and user convenience in real-world implementations. Additionally, the implementation of the scale_pos_weight parameter contributed significantly to improving model performance by addressing class imbalance without modifying the original data distribution. Feature importance analysis also revealed that errorOrig and newbalanceOrig were the most influential features in detecting fraudulent transactions, indicating that sender-side balance anomalies serve as major indicators of suspicious activities. Overall, the findings demonstrate that XGBoost is a highly effective and reliable approach for fraud transaction classification in online payment systems. The model shows strong potential for implementation in automated fraud detection systems to enhance the security and reliability of digital financial transactions. Future research is recommended to utilize more representative datasets, compare XGBoost with other machine learning and deep learning approaches, and evaluate computational efficiency in large-scale environments.

REFERENCES

[1] M. Susilawati, D. Meilandri, R. Semmawi, and N. S. Primasari, "Implementasi Sistem Pembayaran Digital untuk Peningkatan Perputaran Ekonomi di Pasar Tradisional," vol. 4, no. 3, pp. 15067–15075, 2026.

[2] S. L. Mulyana, "IMPLEMENTASI CYBER SECURITY DALAM SISTEM," vol. 2, no. 4, pp. 276–289, 2025.

[3] S. Arifin, "Tantangan dan Peluang yang Dihadapi Perbankan dalam Menghadapi Era Keuangan Digital," vol. 3, pp. 27–33, 2025.

[4] A. U. Z. Hesmi Aria Yanti, Indra Aulia, Rana Zaini Fathiyana, Alva Nurvina Sularso, Nurul Ilmi, Widang Muttaqin, Demi Adidrana, Syifa Nurgaida Yutia, Zuki Pristiantoro Putro, Haddad Alwi Yafie, Siti Zahrotul Fajriyah, Hertanto Suryoprayogo, Deny Haryadi, Desi Nurn, *Artificial Intelligence And Cybersecurity: Foundations, Applications, And Future Perspectives*. 2025.

[5] R. S. Ismanda, M. Tabita, A. Silitonga, and S. N. Hasanah, "Deteksi Hybrid Anomali Transaksi Digital dengan Optimasi Isolation Forest-K-Means untuk Peningkatan Keamanan Finansial," vol. 5, 2025.

[6] D. U. Khairah *et al.*, "Jurnal Computer Science and Information Technology (CoSciTech)," vol. 6, no. 3, pp. 392–398, 2025.

[7] N. N. Pradana, A. A. Subekti, E. Rilvani, U. P. Bangsa, and K. Bekasi, "DETEKSI TRANSAKSI MENCURIGAKAN MENGGUNAKAN DECISION TREE DAN LOGISTIC REGRESSION DENGAN DETEKSI TRANSAKSI MENCURIGAKAN MENGGUNAKAN DECISION TREE DAN LOGISTIC REGRESSION DENGAN," vol. 3, no. 8, 2025.

[8] B. N. Nuzululnisa and H. Hairani, "Analisis Kinerja Model Random Forest dengan Teknik Manhattan-SMOTE pada Deteksi Fraud Transaksi Kartu Kredit Imbalance," no. September 2025, pp. 65–71.

[9] A. C. Nugraha and I. Irawan, "Komparasi Deteksi Kecurangan pada Data Klaim Asuransi Pelayanan Kesehatan Menggunakan Metode Support Vector Machine (SVM) dan Extreme Gradient Boosting (XGBoost)," vol. 12, no. 1, 2023.

[10] M. M. Ibrahim, "ANALISIS KINERJA MODEL MACHINE LEARNING UNTUK MENDETEKSI TRANSAKSI FRAUD PADA SISTEM PEMBAYARAN ONLINE Universitas Terbuka 2 . 1 Konsep Dasar Deteksi Fraud dalam Transaksi Online dengan cara memanipulasi informasi transaksi untuk mendapatkan keuntungan se," vol. 2, no. 3, pp. 35–49, 2025.

[11] S. Dalal, B. Seth, M. Radulescu, C. Secara, and C. Tolea, "Predicting Fraud in Financial Payment Services through Optimized Hyper-Parameter-Tuned XGBoost Model," *Multivar. Data Anal. Mach. Model. Financ. Anal.*, vol. 10, p. 24, 2022, doi: https://doi.org/10.3390/math10244679.

[12] M. T. Kurniawan, I. Pratama, S. Informasi, U. Mercu, and B. Yogyakarta, "Implementasi xgboost untuk prediksi saham," vol. 10, no. 2, pp. 3569–3574, 2026.

[13] F. R. Valerian *et al.*, "Klasifikasi tingkat obesitas menggunakan metode gbm dan confusion matrix," vol. 9, no. 2, pp. 2242–2249, 2025.

[14] H. A. Irawan, "Deteksi Fraud Kartu Kredit Dengan Logistic Regression, Random Forest dan Gradient Boosting," vol. 11, no. 2, pp. 92–97, 2025.

[15] M. W. Hassan, A. Keshk, A. A. El-atey, and E. Alfeky, "Brain Stroke Detection Using Tensor Factorization and Machine Learning Models," *Int. J. Eng. Technol. Manag. Res.*, vol. 8, no. 8, pp. 1–12, 2021, doi: 10.29121/ijetmr.v8.i8.2021.1006.