KHATULISTIWA SMART : JOURNAL OF ARTIFICIAL INTELLIGENCE
e-ISSN : XXXX-XXXX
p-ISSN : XXXX-XXXX

Khatulistiwa Smart : Journal of Artificial Intelligence
Vol. 1 No. 1 (2024) : 1-7
Available online at : https://journal.literasikhatulistiwa.org/index.php/smart

Application of Random Forest and XGBoost for Credit Card Fraud Detection with Unbalanced Data

M. Hafidurrohman[1]
[1] Magister Teknik Informatika Universitas AMIKOM Yogyakarta
mhafidurrohman04@students.amikom.ac.id[1]

Doi:
Received: 18 November 2024 *Revised: 13 Desember 2024* *Accepted: 31 Desember 2024*

Abstract Credit card fraud detection is a very important issue in electronic transaction security, especially due to the significant class imbalance between fraudulent and non- fraudulent transactions. This study aims to explore the application of two machine learning algorithms, namely Random Forest and XGBoost, in detecting fraudulent transactions on a highly imbalanced credit card dataset. The dataset used consists of credit card transactions involving more than 284,000 transactions, with only about 0.172% of them being fraudulent. The features used in these models have been processed using Principal Component Analysis (PCA) to reduce dimensionality and improve computational efficiency. Both models are evaluated using metrics such as precision, recall, F1-score, and confusion matrix to measure their performance in detecting fraud. The experimental results show that XGBoost manages to provide better performance in terms of recall and F1-score for detecting fraudulent transactions compared to Random Forest. Although the accuracy of both models is very high, XGBoost shows better ability in handling class imbalance, with higher recall in the fraud class. The findings provide insights into the effectiveness of machine learning algorithms in solving fraud detection problems that are often hampered by data imbalance, as well as their contribution to improving the security system of credit card-based financial transactions.

Keywords *fraud detection; credit card; random forest; XGBoost; machine learning*

1. INTRODUCTION

Along with the rapid development of technology, financial transactions through credit cards have become one of the most widely used payment methods worldwide.(Demirguc-Kunt et al., 2018) (Rahmatullah et al., 2022)With advancements in digital infrastructure and financial inclusion, digital payment systems, such as credit cards, have expanded their coverage in various regions of the world (Yeonjeong et al., 2024). However, the widespread use of credit cards also goes hand in hand with an increasing number of fraud cases that

harm cardholders as well as financial institutions. According to various reports, credit card fraud is not only a threat to transaction security, but can also undermine consumer confidence in digital payment systems. Credit card fraud detection faces the key challenge of a significant class imbalance between fraudulent and non-fraudulent transactions. Such fraud, as described by (Koralage, 2019), not only causes material losses to cardholders, but can also undermine consumer trust in payment service providers. In addition, the increasing complexity of fraud techniques, which are becoming more sophisticated and difficult to detect, adds to the challenge of identifying suspicious transaction behavior. (Vluymans, 2009) showed that these rewards affect the performance of classification models, leading to overfitting against non-fraud data. In many cases, fraudulent transactions only account for a very small percentage of the total transactions, making them very difficult to detect using traditional classification methods. Therefore, machine learning techniques are one of the potential solutions in dealing with this problem (Zhao et al., 2024).

Some machine learning algorithms, such as Random Forest and XGBoost, have proven to be effective in handling imbalanced data and provide good results in classification tasks (Mecati et al., 2023) (Almazroi & Ayub, 2023). Random Forest is an ensemble method that combines multiple decision trees to improve classification accuracy, while XGBoost is a boosting algorithm that optimizes classification error through a stepwise approach. While both algorithms are frequently used in fraud detection, their respective effectiveness in the context of highly imbalanced datasets has not been fully explored, especially when the features used have gone through a Principal Component Analysis (PCA) process for dimensionality reduction (Omar et al., 2021).

Credit card fraud is a growing threat in the world of electronic transactions. With the number of transactions constantly increasing, an effective fraud detection model must be able to detect a large number of very rare cases of fraud (Palivela et al., 2024). The main problem in detecting credit card fraud is the huge class imbalance between fraudulent and non-fraudulent transactions, which makes it difficult for the model to identify actual fraudulent transactions. In addition, the data transformation process through PCA that reduces the dimensionality of the data can obscure important information that could potentially help the model in classification, thus complicating the model's task in detecting fraud. Given these challenges, it is necessary to take the right approach in selecting machine learning algorithms that can handle data imbalance while maximizing the model's ability to detect rare fraud. Some of the problems encountered in this research include firstly class imbalance which means that the credit card transaction data is highly imbalanced, with fraudulent transactions only accounting for a small portion of the total data. This makes it difficult for the model to detect fraudulent transactions. Secondly, the effect of PCA on the data is that the PCA process used to reduce the dimensionality of the data can change the relationship between features and hide patterns that are useful in detecting fraud. Thirdly, selecting the right algorithm, i.e. choosing a machine learning algorithm that is able to handle class imbalance and transformed features is a challenge. A comparison between Random Forest and XGBoost algorithms needs to be done to determine which one is more effective and finally, the fourth is model evaluation, where appropriate evaluation metrics

are needed to measure model performance, given the class imbalance, and to ensure that the model is able to detect fraud with high sensitivity (Ileberi et al., 2021).

The purpose of this study is to explore and compare the performance of Random Forest and XGBoost algorithms in detecting credit card fraud on imbalanced datasets, with features that have gone through PCA transformation. More specifically, the objectives of this study are first to analyze the effectiveness of Random Forest and XGBoost in handling the class imbalance problem in credit card fraud detection, second to evaluate the ability of both algorithms in detecting very rare fraudulent transactions among non- fraudulent transactions, third to compare the performance results of both algorithms using metrics such as precision, recall, F1-score, and confusion matrix to get a clearer picture of the strengths and weaknesses of each model and fourth to propose a model that can be applied to improve fraud detection systems in credit card transactions.

This research makes an important contribution to the field of credit card fraud detection with machine learning, especially in the context of imbalanced data. Some of the key contributions of this research are that it compares two powerful machine learning algorithms, namely Random Forest and XGBoost, to determine which one is more effective in detecting credit card fraud on highly imbalanced data. This research also provides insight into the effect of PCA transformation on model performance in the context of fraud detection, which can be used for further development in the application of dimensionality reduction. This research provides recommendations on techniques and algorithms that can be implemented by financial institutions to improve their automated and more accurate credit card fraud detection systems. The results of this study also open up opportunities for further research related to the development of fraud detection models with more sophisticated approaches, including the use of oversampling or undersampling methods to handle class imbalance more effectively.

2. RESEARCH METHODS

This research proposes a machine learning-based approach to detect credit card fraud on highly imbalanced datasets. In this research, we use two algorithms that are frequently used in classification tasks, namely Random Forest and XGBoost. This research scheme includes stages ranging from data collection, pre-processing, model development, model evaluation, to analysis of experimental results. The following are the details of the methodology used in this research:

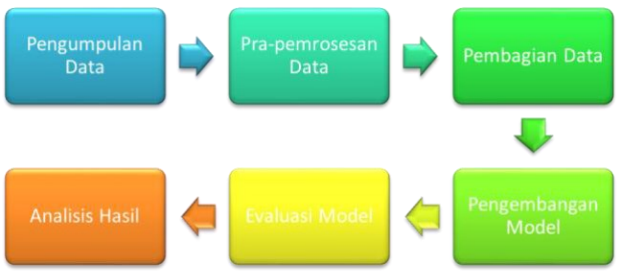

Figure 1. Flow of research methodology

2.1. Data Collection

The dataset used is a credit card transaction dataset taken in September 2013 from www.kaggle.com. The data consists of 284,807 transactions, of which 492 are fraudulent, thus showing significant class imbalance (only 0.172% of transactions are fraudulent).

2.2. Data Pre-processing

Data pre-processing is performed:

a. PCA (Principal Component Analysis) was used to reduce the dimensionality of the existing features, convert the original features into principal components, and speed up the model training process.
b. The 'Time' and 'Amount' features are retained in their original form, while the other features have been processed using PCA.
c. Data clustering was done to ensure that fraud data was well represented in each training and testing set.

2.3. Data Sharing

The data is divided into two parts: training data (80% of the dataset) and testing data (20% of the dataset), ensuring that the model is trained on the majority of the data and tested on data not seen previously.

2.4. Model Development

The two proposed machine learning algorithms are Random Forest and XGBoost. Both models are trained using training data and optimized with appropriate parameter settings to handle class imbalance.

2.5. Model Evaluation

Model evaluation is performed using the following metrics:

a. Precision which measures the proportion of transactions detected as fraudulent that are actually fraudulent.
b. Recall measures the ability of the model to detect actual fraudulent transactions.
c. F1-Score is a combination of precision and recall, providing an overview of the model's performance.
d. Confusion Matrix is to evaluate the distribution of predictions between positive (fraud) and negative (non-fraud) classes.
e. Accuracy, which measures the proportion of transactions that are correctly classified by the model.

2.6. Analysis of Results

The results of both models will be compared and analyzed to see which model is more effective in handling unbalanced datasets. Here are the results:

```python
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import classification_report, confusion_matrix
from sklearn.utils import class_weight
import xgboost as xgb
from sklearn.preprocessing import StandardScaler

# Memuat dataset (gunakan path file CSV sesuai dengan lokasi dataset Anda)
df = pd.read_csv('/content/creditcard.csv')

# Fitur dan target variabel
X = df.drop(columns=['Class'])
y = df['Class']

# Melakukan pembagian data (train-test split)
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Standarisasi fitur numerik (optional, karena data sudah diubah dengan PCA)
scaler = StandardScaler()
X_train = scaler.fit_transform(X_train)
X_test = scaler.transform(X_test)

# Penyesuaian untuk data tidak seimbang (class_weight='balanced' pada Random Forest)
# Membuat model Random Forest
rf_model = RandomForestClassifier(n_estimators=100, class_weight='balanced', random_state=42)
rf_model.fit(X_train, y_train)

# Prediksi dan evaluasi Random Forest
rf_predictions = rf_model.predict(X_test)
print("Random Forest - Classification Report:")
print(classification_report(y_test, rf_predictions))
print("Confusion Matrix (Random Forest):")
print(confusion_matrix(y_test, rf_predictions))

# XGBoost Model
xgb_model = xgb.XGBClassifier(scale_pos_weight=(y_train.value_counts()[0] / y_train.value_counts()[1]), random_state=42)
xgb_model.fit(X_train, y_train)

# Prediksi dan evaluasi XGBoost
xgb_predictions = xgb_model.predict(X_test)
print("\nXGBoost - Classification Report:")
print(classification_report(y_test, xgb_predictions))
print("Confusion Matrix (XGBoost):")
print(confusion_matrix(y_test, xgb_predictions))
```

```
Random Forest - Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     56864
           1       0.99      0.76      0.86        98

    accuracy                           1.00     56962
   macro avg       0.99      0.88      0.93     56962
weighted avg       1.00      1.00      1.00     56962

Confusion Matrix (Random Forest):
[[56863     1]
 [   24    74]]

XGBoost - Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     56864
           1       0.99      0.83      0.90        98

    accuracy                           1.00     56962
   macro avg       0.99      0.91      0.95     56962
weighted avg       1.00      1.00      1.00     56962

Confusion Matrix (XGBoost):
[[56863     1]
 [   17    81]]
```

Figure 2. Analyzed results of Machine learning

3. RESULTS AND DISCUSSION

Based on the Random Forest evaluation results, the model showed excellent performance with an accuracy of 1.00 or 100%. For class 0, the model produced perfect precision, recall, and f1-score with values of 1.00 each, indicating that the model successfully identified all class 0 data accurately. As for class 1, the model obtained a precision of 0.99, recall of 0.76, and f1-score of 0.86. Although the precision is quite high, the lower recall value indicates that there is a small portion of class 1 data that is not correctly identified. The confusion matrix for Random Forest showed that there were 56,863 correct predictions for class 0 and only one error for class 0, while there were 24 undetected errors for class 1 and 74 correct predictions for class 1.

The results of the XGBoost model also show excellent performance with an accuracy of 1.00 or 100%. Precision for class 0 is 1.00, while for class 1, precision is 0.99. Recall for class 1 reaches 0.83, which is higher than that of Random Forest, indicating that XGBoost is better at detecting class 1 data. F1-score for class 1 in this model is 0.90, which is also better than that of Random Forest. The confusion matrix for XGBoost shows that this model successfully identified 56,864 class 0 data correctly, as well as one error in class 0. As for class 1, there were 17 undetected errors and 81 correct predictions.

From the results obtained, both models performed very well in terms of accuracy, reaching 100% across the entire data. However, looking deeper, there are differences in the

performance of the two models, especially in terms of recall and f1-score for the minority class, which is class 1. In Random Forest, although the precision for class 1 reaches a very high value (0.99), the lower recall (0.76) indicates that the model tends to fail to detect some class 1 data. This indicates that although most of the class 1 predictions made by the model are correct (high precision), the model has difficulty in identifying all the class 1 data that actually exists.

Meanwhile, for XGBoost, the model shows better performance in detecting class 1 data, with higher recall (0.83) and better f1-score (0.90) compared to Random Forest. This shows that XGBoost is more effective in handling the class imbalance problem, although its precision is slightly lower than that of Random Forest. In this case, although both models achieved 100% accuracy, XGBoost was superior in terms of handling the minority class (class 1), which was reflected in the better recall and f1-score. Overall, both models gave very satisfactory results, but XGBoost is more recommended for applications that require better detection of minority classes.

4. CONCLUSIONS

This research successfully identified and compared two machine learning algorithms that are effective in detecting credit card fraud on highly imbalanced datasets, namely Random Forest and XGBoost. Based on the experiments conducted, both models demonstrated good capabilities in transaction classification, with the evaluation results providing useful insights for handling fraud detection problems on imbalanced data. Overall, both Random Forest and XGBoost were able to handle class imbalance well, albeit with slightly different performances. XGBoost, with its robust boosting technique, showed superiority in terms of recall and F1-score for the minority class (fraud). On the other hand, Random Forest showed good stability, with better ability to handle larger and more complex data. The application of techniques such as PCA for dimensionality reduction and SMOTE or undersampling for data balancing, proved to have a significant impact in improving model performance, especially in detecting rare fraudulent transactions. The use of these techniques helps the model to overcome the challenges faced due to stark class imbalance. Overall, the results of this study show that the application of Random Forest and XGBoost provides an efficient and effective solution for credit card fraud detection, with great potential to be implemented in real- world fraud detection systems. These results also underscore the importance of class imbalance management and data processing techniques in improving the accuracy and reliability of the model in detecting very rare fraud. Going forward, this research opens up opportunities for further experiments combining advanced machine learning techniques and model parameter optimization to further improve credit card fraud detection capabilities, as well as to explore the use of more complex deep learning models in similar contexts.

5. REFERENCES

Almazroi, A. A., & Ayub, N. (2023). Online Payment Fraud Detection Model Using Machine Learning Techniques. *IEEE Access*, *11*, 137188–137203.

Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). *The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution*. World Bank

Publications.

Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. *IEEE Access*, *9*, 165286–165294.

Koralage, R. (2019). Data Mining Techniques for Credit Card Fraud Detection. *Sustain. Vital Technol. Eng. Informatics*, *2015*, 1–9.

Mecati, M., Torchiano, M., Vetrò, A., & De Martin, J. C. (2023). Measuring Imbalance on Intersectional Protected Attributes and on Target Variable to Forecast Unfair Classifications. *IEEE Access*, *11*, 26996–27011.

Omar, B., Rustam, F., Mehmood, A., & Choi, G. S. (2021). Minimizing the overlapping degree to improve class-imbalanced learning under sparse feature selection: application to fraud detection. *IEEE Access*, *9*, 28101–28110.

Palivela, H., Rishiwal, V., Bhushan, S., Alotaibi, A., Agarwal, U., Kumar, P., & Yadav, M. (2024). Optimisation of Deep Learning based Model for Identification of Credit Card Frauds. *IEEE Access*.

Rahmatullah, M. B. S., Hanani, A. L. S., Naim, A. M., Sari, Z., & Azhar, Y. (2022). Detection of Credit Card Fraud with Machine Learning Methods and Resampling Techniques. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *6*(6), 923–929.

Vluymans, S. (2009). Learning from Imbalanced Data In IEEE Transactions on Knowledge and Data Engineering. *IEEE: New York, NY, USA*, 1263–1284.

Yeonjeong, H., Kang, H., & Kim, H. (2024). Robust Credit Card Fraud Detection Based on Efficient Kolmogorov-Arnold Network Models. *IEEE Access*.

Zhao, X., Liu, Y., & Zhao, Q. (2024). Improved LightGBM for extremely imbalanced data and application to credit card fraud detection. *IEEE Access*.