Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 3, 2482-2494
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i3.5823

Fraud credit card transaction detection using hybrid multilayer perceptron-random forest method

Alexander Subagio[1*], Ditdit Nugeraha Utama[2]
[1,2]Computer Science Department, Binus Graduate Program – Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia; alexander012@binus.ac.id (A.S.) ditdit.utama@binus.edu (D.N.U.)

Abstract: Credit card fraud is a leading crime with rapid growth in the world. This is due to credit cards being one of the most popular payment options worldwide. To address this problem, there needs to be a robust and efficient method to accurately identify fraudulent transactions. This study aims to investigate the performance of a hybrid method that combines Multilayer Perceptron (MLP) as a feature extractor and a Random Forest (RF) classifier for detecting fraudulent credit card transactions. The MLP is used to capture complex patterns in the transaction data, while the RF classifier is used to make robust and accurate predictions. The performance of the proposed model was compared with standalone MLP and RF using several evaluation metrics. The proposed method achieved the best performance among other methods, with an accuracy of 99.949%, precision of 87.097%, recall of 82.653%, and F1-score of 84.817%. This result shows the ability of the proposed method by combining the strengths of MLP as a feature extractor and RF as a classifier, offering an effective and robust method for fraud detection. This research shows the potential of hybrid methods in addressing financial challenges and provides further advancement in fraud detection systems.

Keywords: *Credit Card Fraud Detection, Machine Learning, Multilayer Perceptron, Random Forest.*

1. Introduction

Credit card is one of the most popular payment options in the world. Based on [1] the market size of credit card in 2023 was USD 572.34 billion. In 2024, the market size has increased to USD 622.76 billion. The market size of credit card has increased exponentially and will be expected to reach around USD 1,331.50 billion by the year 2033. However, with such rapid growth, there are both positive and negative impacts that it causes. The example of this negative impact is credit card fraud, which continues to increase due to the advances in cybercrime methods and the adoption of online payment systems. According to Rej [2] global losses due to credit card fraud reached $32.4 billion in 2021 and are expected to grow to $43 billion by 2026.

A credit card fraud transaction is an illegal or unauthorized activity that aims to gain financial advantage by using the credit card without the owner's permission. This act can be committed both involving the use of physical credit card or other methods that do not require physical card ownership. These methods are Lost or Stolen Card Fraud, Application Fraud and Cardholder Not Present Fraud. Lost or stolen card fraud is common crime that uses unauthorized physical credit card that has been lost or stolen to make as many and as large transactions as possible until the card is blocked. Application Fraud is a type of credit card fraud where the fraudster creates a credit card with false personal information. Application Fraud is hard to detect because the fraudster usually does not make large transactions right away. Cardholder Not Present Fraud is a type of fraud that does not need physical credit card and usually committed through online transactions or over the phone sales [3]. Traditional fraud detection systems generally use rule-based or statistical methods. These approaches often have

History: Received: 16 January 2025; Revised: 5 March 2025; Accepted: 11 March 2025; Published: 27 March 2025
* Correspondence: alexander012@binus.ac.id

weaknesses in terms of scalability and adaptability which makes them struggle to keep up with the ever-evolving cybercrime tactics that attackers use and may fail to capture complex and non-linear patterns in a transaction data [4].

With the growth of technology, Machine Learning has become popular for detecting fraud due to its ability to analyze big datasets and its capability to identify the complicated and complex patterns in real-time. Fraud detection system that is based on machine learning can adapt and evolve as time goes on, making them a suitable choice for dealing with the dynamic nature of fraud behavior. Machine learning is divided into several types based on their training approach. One of the most used types of machine learning for fraud detection system is supervised learning. Supervised learning is a machine learning approach that uses labelled data to train its model. With this approach, the model can study the given historical transaction data and identify patterns related to fraud. There are several often-used supervised learning methods such as logistic regression, decision trees, random forest, neural network, and others [5].

This research will focus on exploring a hybrid model for credit card fraud detection system. The proposed hybrid model will combine both MLP Neural Network and Random Forest methods. MLP will be used to perform feature extraction to identify complex patterns from the dataset. Afterwards, the extracted features will be used by the Random Forest model to perform classification and prediction. Research related to fraud detection systems using neural networks has been done by researchers like Varmedja, et al. [6]; Sadgali, et al. [7] and Andrade, et al. [8]. However, in those research, neural network has not been able to beat the performance of other methods. Neural network, especially Multilayer Perceptron (MLP), is a type of neural network that consists of several layers of neurons that connect with each other. MLP excels at identifying non-linear relationships in high-dimensional data and able identify complicated patterns that cannot be captured by simple statistical methods or linear methods [9]. Research using Random Forest related to fraud detection has also been done by previous researchers such as Agarwal and Usha [10] and Jain, et al. [11] where it produces good results. Random Forest is an ensemble method that combines multiple decision tree models to improve performance and is popular because of its effectiveness in performing regression and classification.

2. Literature Review

Research that use machine learning to detect fraud transaction has already been done. Previously Varmedja, et al. [6] researched the application of various machine learning models for detecting fraudulent transactions in credit card usage. This paper discussed the critical problem of credit card fraud due to increasing digital transactions. The research underlined the challenges of imbalance datasets which make preprocessing steps like SMOTE and feature selection a necessity. The research tested multiple algorithms such as Logistic Regression (LR), Naïve Bayes (NB), Random Forest (RF), and Artificial Neural Networks (ANNs). The result showed that among other models, RF and ANNs model performed better overall with accuracy of 99.96% and 99.93%, recall of both 81.63%, as well as precision of 96.38% and 79.21%. The study concluded that machine learning models especially ensemble and deep learning methods can significantly improve fraud detection when paired with effective preprocessing techniques.

Other research like [12] discussed utilizing deep learning techniques to identify fraudulent credit card transactions. The study used Convolutional Neural Network with 6 convolutional layers. The result of the experiment showed that CNN model got an accuracy of 99.62% without using max pooling layer and 95.93% with max pooling layer. The study concluded that CNN model has excellent performance with good stability.

In the area of supervised learning technique, Sadgali, et al. [7] explored the application of neural network for the topic of fraud detection. The study used a generated dataset that mimic real financial condition with significant imbalances which includes approximately 60.000 transactions. The study tested various machine learning models, including Decision Tree, Support Vector Machine (SVM), Random Forest, and K-Nearest Neighbour. The result of the study showed that the best performing model was Support Vector Machine with MSE score of 0.0021 for training dataset and 0.0024 for test dataset as well as an accuracy 99.7%.

However, SVM is proven to be defeated by Random Forest in other cases like in the study by Swetha, et al. [13]. The study explored the challenges of enhancing credit card fraud detection by applying advanced machine learning algorithms. A performance analysis was made based on three different algorithms, including SVM, Decision Tree and Random Forest. The analysis was split between 3 different feature selection which were "For 5 variables", "For 10 variables" and "For all variables". The result showed that the accuracy for SVM, Decision Tree and Random Forest model were 90.0, 94.3, and 95.5. This number indicated that the Random Forest classifier is better than the SVM and Decision Tree model. The study used different dataset and feature selection, which could be the contributing factor to the different results.

Other research on machine learning was done by Andrade, et al. [8] where the performance of four machine learning models, including K-Nearest Neighbors (KNN), Random Forest (RF), Support Vector Machines (SVM) and Neural Network (NN) was evaluated. The result showed that Random Forest has the highest score in all metrics indicating that Random Forest has the best performance. Random Forest achieved a precision of 94.24%, Recall of 92.04% and F1-score of 92.98%. The potential of Random Forest has also been proven by several research like the study by Bhattacharyya, et al. [14] where the authors utilized various data mining techniques including Logistic Regression, Support Vector Machines (SVM) and Random Forests to analyzed the performance of each technique. The authors used several measures of classification performance such as Accuracy, Sensitivity, Specificity, Precision, F-measure, G-mean and wtdAcc. The results showed that Random Forest has the best performance compared to the other two methods.

Another research that proved the excellent performance of Random Forest is the research by Aftab, et al. [15]. The research aimed to identify the best supervised machine learning method for credit card fraud detection. The methods that were compared include Logistic Regression, Random Forest, Support Vector Machine, and Decision Trees. Furthermore, the research also used SMOTE to address the imbalance in dataset. The result of the research showed that Random Forest have the best performance compared to other methods. Other than that, Agarwal and Usha [10] also conducted a research that investigate the usage of machine learning technique for detecting fraud credit card transactions. The research utilized a large dataset that consisted of credit card transactions and identified the suspicious patterns in the data that may resulted to fraudulent activity. The authors used Random Forest as the algorithm which performed extremely well. The result showed that the algorithm performed extremely well with a high accuracy, precision and recall of 0.999, 0.999, and 1.0. The result indicated that to significantly reduce the amount of fraud credit card transactions, Random Forest is a great option.

Other than Random Forest, there is another algorithm that has excellent performance which is XGBoost algorithm. In the study by Singh and Mahrishi [16] the authors explored and compared the various methods for credit card fraud detection. The study used K-means clustering, Logistic Regression, Random Forest and XGBoost models. The study used dataset with 284,807 transactions which were obtained from Kaggle. The models were tested and compared using precision as the comparison metric. The result showed that XGBoost were more accurate than other models thus making it preferable over the other models. Unlike the previous papers, the study shows that XGBoost performs better than Random Forest. To determine the superiority of XGBoost over Random Forest, there are other research that also showed that XGBoost has the better performances. In the study by Jain, et al. [11] the authors analyzed the role of machine learning to detect fraudulent patterns effectively. The study used a credit card transaction dataset that are preprocessed first to address the class imbalance. The study compared the performance of 3 machine learning algorithms, such as Decision Tree, Random Forest and XGBoost. The prediction accuracy of each algorithm was 99.923% for Decision Tree, 99.957% for Random Forest and 99.962% for XGBoost. Same with the previous paper, the result showed that XGBoost is the best out of all three with a slight difference with Random Forest model.

3. Methods

In this research, the workflow of the proposed methodology can be seen in Figure 1, which starts with preprocessing the dataset. Preprocessing dataset includes cleaning the dataset and splitting the dataset into train and test sets. Then, because of the imbalance in the dataset, SMOTE will be used to address the problem. StandardScaler will also be applied for standardization. The train data set will then be used to train the Multilayer Perceptron standalone model, Random Forest standalone model and the proposed Multilayer Perceptron – Random Forest model. Each model will then be used to predict the fraudulent transaction using the test data set that has been split at the beginning. Lastly the performance of each prediction model will then be evaluated using several evaluation metrics to make an analysis.

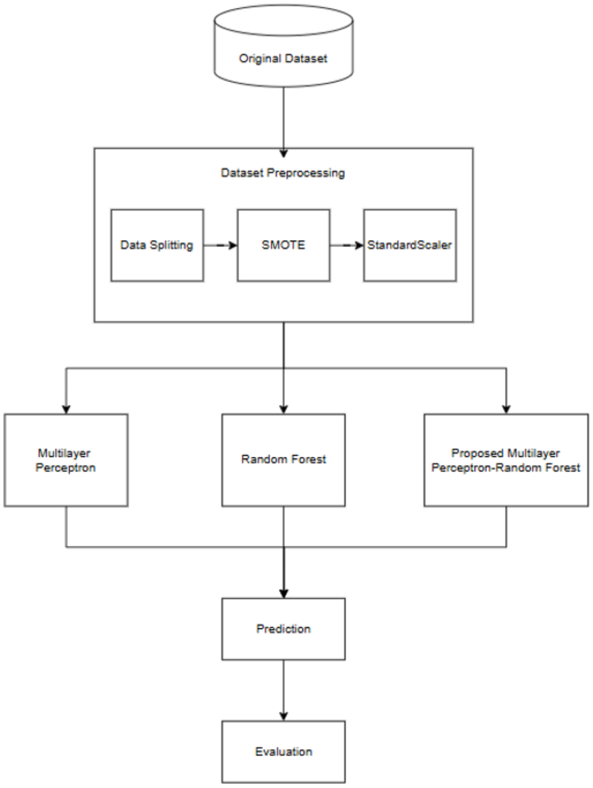

Figure 1.
System architecture of the proposed methodology.

3.1. Dataset and Preprocessing

The dataset used in this study was from Kaggle which contains the data of credit card transactions made in two days by European cardholder in September 2013. The dataset contains a total of 284,807 transactions with 492 of them were labelled as fraud. The dataset consists of 31 attributes in which 28 of them were the result of a dimensionality reduction technique called PCA transformation named V1, V2, … V28. Due to privacy issues, the original features cannot be provided thus the anonymized features were given. The "Time" feature represents the time that has passed between each transaction and the initial transaction. The "Amount" feature is the amount made in each transaction. Lastly, the "Class" feature shows whether the transaction is fraudulent or not by labelling it with 1 for fraud transaction and 0 for genuine transaction. In this study, the dataset was split into 80% of train set and 20% of test set. The train set was used for training the models and the test set was later used for evaluating the

DOI: 10.55214/25768484.v9i3.5823

performance of each model. With only 0.1729% of the total transactions being fraud, this clearly shows that the dataset is extremely imbalanced as depicted in Figure 2.

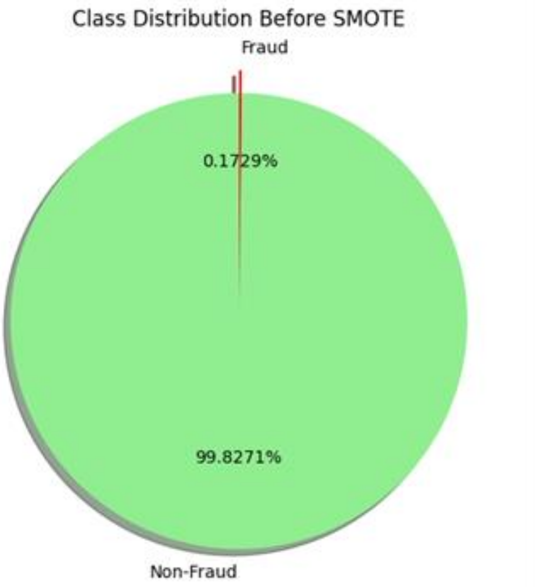

Figure 2.
Pie Chart of Class Distribution before applying SMOTE.

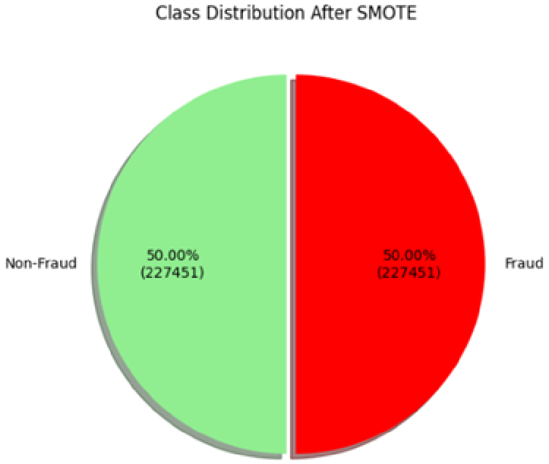

Figure 3.
Pie Chart of Class Distribution after applying SMOTE

The imbalanced in data can prove to be a problem for training the machine learning algorithms [6]. Therefore, Synthetic Minority Oversampling Technique (SMOTE) was utilized to addresses this problem. SMOTE is a preprocessing algorithm that is widely used due to its simplicity and robustness for handling imbalanced data [17]. In this study, SMOTE algorithm was used for the train set only to balance the class distribution of the data. As depicted in Figure 3, the class distribution has been successfully balanced with 227,451 transactions labelled as Non-Fraud and 227,451 transactions also labelled as Fraud. After balancing the class distribution, StandardScaler was also used to standardized

DOI: 10.55214/25768484.v9i3.5823

the data. StandardScaler is a standardization method that scale the features by removing the mean and scaling the features to unit variance (standard deviation of 1) [18].

3.2. Model Training

In this study, the proposed method will use MLP for feature extraction and then Random Forest will be used for prediction. The proposed method will then be compared to the standalone MLP and Random Forest. The comparison will be used to evaluate each performance of the method.

MLP is a feed-forward Artificial Neural Network (ANN) where the network is made of multiple layers of neurons that are linked together by connecting weights [19]. MLP transforms a set of given inputs into the desired output. MLP consists of three layers such as Input Layer to receive data inputs, Hidden Layer to process the data and Output Layer which will output the final prediction. Each layer consists of a number of neurons where the weight and bias are used to connect the neurons between each layer. In this study, the standalone MLP method used the default parameter which had 1 hidden layer with 100 neurons.

Random Forest is an ensemble-based machine learning algorithm introduced by Breiman [20]. This technique is a development of the bagging method by introducing the concept of random feature selection at each split node in the decision tree. Random Forest builds many decision trees during training and combines the results of each tree to produce more accurate and stable predictions. Random Forest has two main concepts which are bootstrap sampling and random feature selection. Bootstrap sampling is used to ensure that each tree is trained with different subsets of data thus reducing overfitting. Random feature selection selects a random subset for consideration to determine the best splits thus ensuring that the model is diverse. In this study, the standalone random forest that was used for comparison used the default parameter. These parameters consisted of several parameters including number of trees of 100, minimum number of samples to split of 2 and minimum samples at a leaf node of 1.

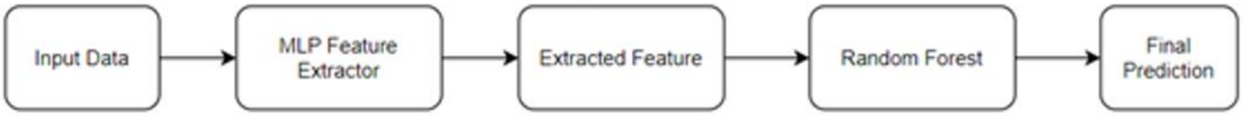

Figure 4.
System architecture of the proposed methodology.

For the proposed method, Figure 4 is used to visualize the flow of the proposed architecture. First, the input data was used to train the MLP model as a feature extractor. The parameters used for the MLP feature extractor were obtained through exhaustive search starting from small number of neurons to higher numbers. At the end, the parameters that produced the best result were 1 hidden layer with 256 neurons, activation function of tanh and adam optimizer. Random state of 42 was also used to ensure consistency in training the model.

After training the MLP feature extractor, the extracted features were then obtained and used to train the Random Forest. The parameters that were used to train the Random Forest were obtained through Grid Search with 3 Cross Validation over a range of hyperparameter combinations using the following parameters based on F1-score. The number of estimators/trees in the forest were evaluated using values of 100, 200, and 300. The tree's maximum depth was tested at 10, 20, and 30. For the minimum samples required to split a node, values of 2, 5, and 10 were considered, while the minimum samples required per leaf node were tested with values of 1, 2, and 4. Lastly, there are two options tested for the maximum number of features considered for a split which are sqrt and log2. The combination of parameters that produce the best result for Random Forest model were 100 estimators, maximum depth of 10, minimum samples to split of 2, 4 minimum samples required in a leaf and maximum features using sqrt. Additionally, a random state of 42 is also used to ensure consistency during training.

3.3. Metric of Evaluation

To evaluate the performance of each model, there are several metrics that were used in this research, including accuracy, precision, recall and F1-score. These evaluation metrics are obtained from the Confusion Matrix. Confusion Matrix is method that is commonly used to evaluate the performance of machine learning classification [21]. Confusion Matrix consists of four values which are True Positives, True Negatives, False Positives, and False Negatives. The table of confusion matrix can be seen in Table 1.

Table 1.
Confusion Matrix Table.

Class	Predicted Negatives	Predicted Positives
Actual Negatives	True Negatives	False Positives
Actual Positives	False Negatives	True Positives

Using the confusion matrix, the evaluation metrics then can be obtained. Accuracy is an evaluation metric that calculates the overall accuracy of a model by dividing the number of correct predictions by the total number of predictions. After the explanation, the formula can be written as Equation 1, where TP is true positives, TN is true negatives, FP is false positives, and FN is false negatives. The second metric is precision which is an evaluation metric that measures the proportion of positives predictions that were correct by dividing the number of correctly identified positive predictions to the sum of all predicted positives. The equation for the precision metric can be seen in Equation 2. The next metric used in the research was recall which is an evaluation metric that measures the proportion of actual positives that were correctly predicted by dividing the correctly identified positive predictions to the sum of the actual positives. The equation for recall can be written as in Equation 3. The last metric is F1-score which is the harmonic mean of precision and recall and is used especially in the case of imbalanced class distribution. In an imbalanced dataset, the balance of precision and recall is necessary thus making this metric useful to determine the performance of the prediction models. The equation for F1-score can be written as in Equation 4.

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

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

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

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

4. Results

To evaluate the performance of the proposed MLP-Random Forest model, a comparison based on evaluation metrics is needed. Using the confusion matrix, the evaluation metrics can be calculated. All the models were tested on 20% of the dataset which consists of 56962 instances.

The first test was conducted to the standalone MLP model. The MLP model achieved an evaluation metric result of 99.993% accuracy, 81.914% precision, 78.571% recall and 80.208% F1-score. The confusion matrix for the MLP model can be seen in Figure 5 which had 56847 transactions labelled as True Negatives, 21 transactions labelled as False Negatives, 17 transactions labelled as False Positives, and 77 transactions labelled as True Positives.

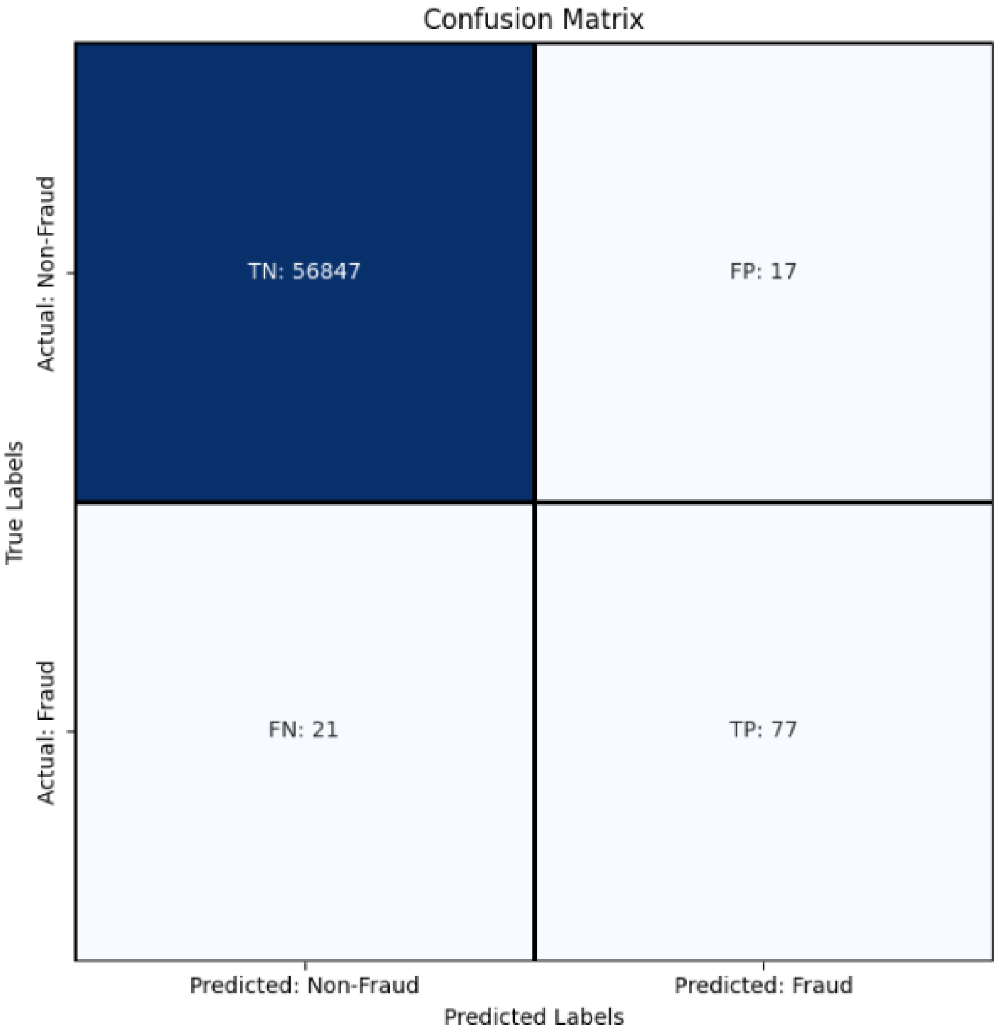

Figure 5.
Confusion Matrix for Standalone MLP model.

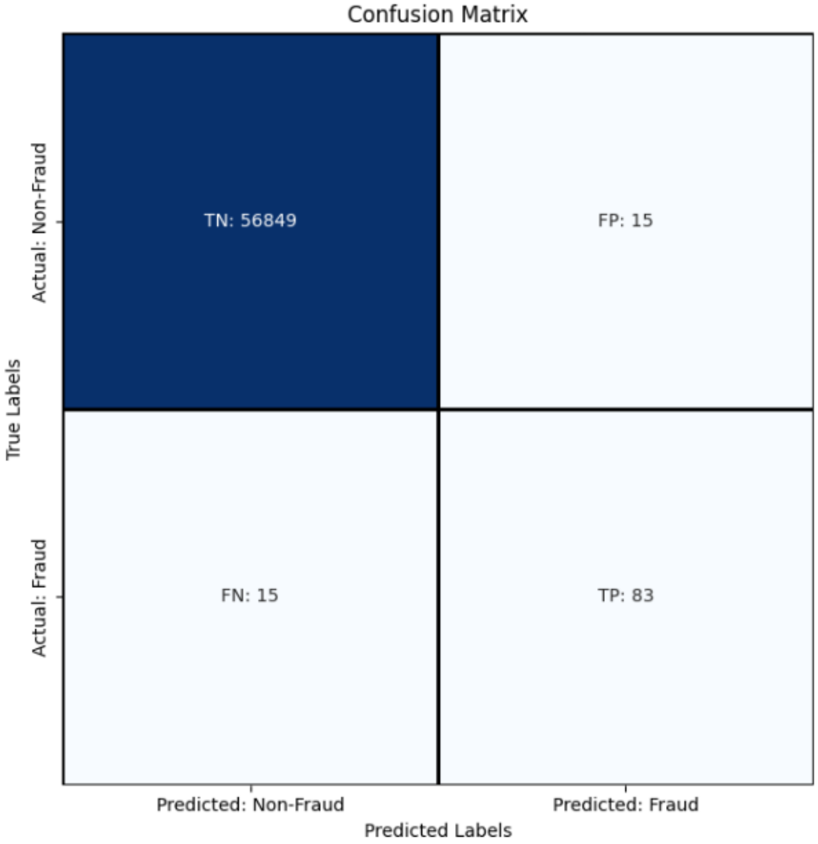

Figure 6.
Confusion Matrix for Standalone RF model.

For the standalone Random Forest model, the model achieved an evaluation metric score of 99.947% accuracy, 84.694% precision, 84.694% recall and 84.694% F1-score. The confusion metric of the Random Forest model can be seen in Figure 6 where there were 56849 transactions labelled as True Negatives, 15 transactions labelled as False negatives, 15 transactions labelled as False Positives, and 83 transactions labelled as True Positives.

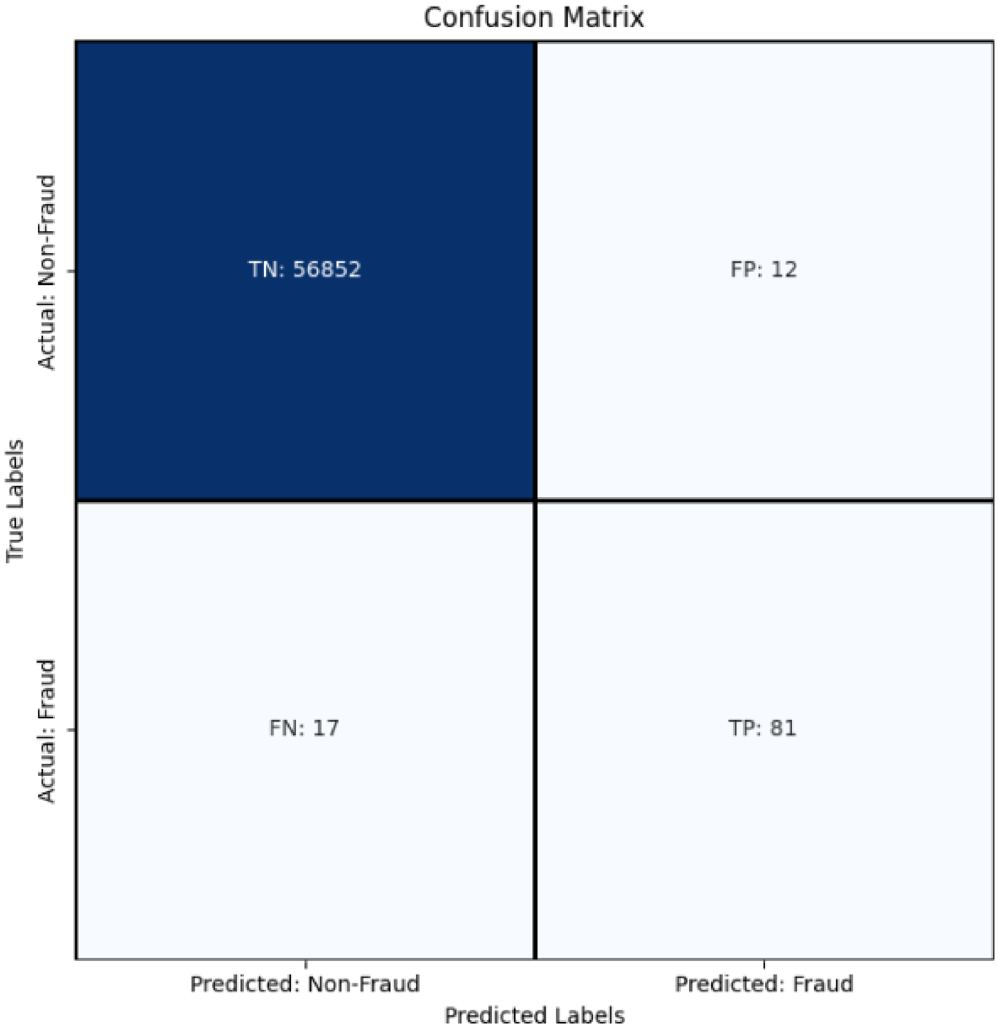

Figure 7.
Confusion Matrix for Proposed MLP-RF model

Lastly, the proposed MLP-Random Forest model achieved an evaluation metric result of 99.949% in accuracy, 87.097% in precision, 82.653% in recall and 84.817% in F1-score. The confusion matrix for the proposed MLP-Random Forest can be seen in Figure 7. The confusion matrix showed that the proposed MLP-Random Forest model was able to correctly identify 56852 transactions as non-fraud (True Negatives), 17 transactions were mistakenly identified as non-fraud (False Negatives), 12 transactions mistakenly identified as fraud (False Positives) and 81 transactions correctly identified as fraud (True Positives).

Table 2.
Performance Comparison for Each Model.

	Accuracy	Precision	Recall	F1 Score
Standalone MLP	99.933%	81.914%	78.571%	80.208%
Standalone RF	99.947%	84.694%	84.694%	84.694%
Proposed MLP-RF	99.949%	87.097%	82.653%	84.817%

DOI: 10.55214/25768484.v9i3.5823

5. Discussion

To analyze the performance of each model, a performance comparison is done in the form of Table 2. For the accuracy metric, all of the models had a similar but great performance. The proposed MLP-RF model had the best performance of 99.949% accuracy which means that the proposed model was able to correctly classifies almost all transactions. Although only a slight improvement, the proposed model had a better performance against MLP model with 99.933% and RF model with 99.947%.

In the precision metric, the proposed MLP-RF model had the best performance with good precision of 87.097%. This indicates that the proposed model had superior capability to minimize false positives. Compared to the accuracy of MLP model with 81.914% and RF with 84.694%, it is a significant improvement that shows that combining the two standalone methods can improve the precision capability. However, for the recall metric, the RF model was able to beat the standalone MLP and proposed MLP-RF model and achieved the best result. The RF model achieved 84.694% while with a slightly lower recall, the proposed MLP-RF model achieved a score of 82.653% and the MLP achieved an even lower recall of 78.571%. With only slightly lower recall, the proposed model still had a good recall and still able to identify a good portion of fraudulent transactions.

For the last metric, which is F1 Score, the proposed MLP – RF model had the best performance followed up by RF model with a slight difference and in the last place was MLP model with the worst performance. The proposed model achieved 84.817% in F1 Score and the RF model achieved 84.694% which demonstrated that both the model had a really good balance of precision and recall, thus indicating that the models are better at minimizing false positives while also able to correctly identify fraudulent cases. Meanwhile, MLP had the worst F1 Score with 80.208% due to its relatively lower precision and recall.

Based on the result of the performance comparison, the proposed MLP-RF model has the best overall result compared to standalone MLP and RF models. The proposed model combines the MLP's capabilities at extracting features to identify the complex patterns in data and the effective classifying capabilities of RF. By leveraging the strength of each standalone model, the proposed model is able to further enhance the performance by reducing false positives which is evidenced by its high result in precision while still maintaining a good recall. This good performance of the proposed model is influenced directly by the parameter of both the MLP feature extractor and the RF classifier.

Based on the experiment that have been done, MLP feature extractor was influenced by the assigned number of neurons in a hidden layer. With higher number of neurons, MLP was able to capture complex patterns in the input data more effectively. Other than that, using tanh activation function allows MLP to model both positive and negative relationships which can be found in the input data. Furthermore, using the adam solver also improves the model performance by optimizing weight efficiently and are more suited for larger dataset like the transaction data used in this study.

For the RF classifier, the parameter that influenced the model greatly is the number of trees and maximum depth which with the balance of the two, the model is more balanced and can generalize better. Furthermore, by increasing the number of minimum samples in a leaf node, the model can be further generalized by preventing the trees from being overly sensitive. With these parameters' optimization, the proposed model is trained to be accurate and robust as well as reliable at predicting fraudulent transactions.

6. Conclusions

This research was conducted to test the performance of the proposed method which combines Multilayer Perceptron Neural Network with Random Forest to detect fraud credit card transaction. The MLP was used to effectively capture the complex patterns in the data by extracting the meaningful features, while the RF classifier used these features to make a robust and accurate classifications.

The proposed MLP – RF method was compared with the standalone MLP and Random Forest method using several metrics that includes accuracy, precision, recall and F1 score. The result of the research concluded that the proposed MLP – RF method achieved the best result with an exceptional accuracy of 99.949%, great precision of 87.097%, good recall of 82.653% and great F1 Score of 84.817%. These results indicated that the proposed MLP – RF method was able to balance the detection of fraudulent transactions with minimum false positives, which is critical in fraud detection systems. This research demonstrated the potential of hybrid machine learning models in addressing real-world challenges in fraud detection, opening up further advancement in this field.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

References

[1] Precedence Research, "Credit card payments market size to hit USD 1,331.50 Bn by 2033. Precedenceresearch.com," Retrieved: https://www.precedenceresearch.com/credit-card-payments-market, 2024.

[2] M. Rej, "Credit card fraud statistics (2023) | Merchant Cost Consulting. Merchantcostconsulting.com," Retrieved: https://merchantcostconsulting.com/lower-credit-card-processing-fees/credit-card-fraud-statistics/, 2023.

[3] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Statistical Science*, vol. 17, no. 3, pp. 235-255, 2002. https://doi.org/10.1214/ss/1042727940

[4] P. T. S. Ningsih, M. Gusvarizon, and R. Hermawan, "Analysis of credit card transaction fraud detection system with machine learning algorithm," *Jurnal Teknologi Informatika Dan Komputer*, vol. 8, no. 2, pp. 386-401, 2022. https://doi.org/10.37012/jtik.v8i2.1306

[5] Z. Zhu, Q. Zhao, J. Wang, and A. Yang, *A comparative study of machine learning methods.* Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-546-1, 2024.

[6] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Credit card fraud detection - machine learning methods," in *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH 2019) - Proceedings. https://doi.org/10.1109/INFOTEH.2019.8717766*, 2019.

[7] I. Sadgali, N. Sael, and F. Benabbou, "Fraud detection in credit card transaction using neural networks," in *ACM International Conference Proceeding Series. https://doi.org/10.1145/3368756.3369082*, 2019, pp. 1-4.

[8] J. P. A. Andrade *et al.*, "A machine learning-based system for financial fraud detection," in *Encontro Nacional de Inteligência Artificial e Computacional (ENIAC)*, 2021: SBC, pp. 165-176.

[9] G. E. Hinton, S. Osindero, and Y. W. Teh, "A fast learning algorithm for deep belief nets," *Neural Computation*, vol. 18, no. 7, pp. 1527–1554, 2006. https://doi.org/10.1162/neco.2006.18.7.1527

[10] S. Agarwal and J. Usha, "Detection of fraud card and data breaches in credit card transactions," *International Journal of Science and Research Archive*, vol. 9, no. 2, pp. 576-582, 2023. https://doi.org/10.30574/ijsra.2023.9.2.0603

[11] V. Jain, M. Agrawal, and A. Kumar, "Performance analysis of machine learning algorithms in credit cards fraud detection," in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, 2020: IEEE, pp. 86-88.

[12] A. M. Babu and A. Pratap, "Credit card fraud detection using deep learning," in *2020 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, 2020: IEEE, pp. 32-36.

[13] T. Swetha, N. N. Bellam, G. N. Manjunath, and K. H. V. Naveen, "Detection of credit card fraud transactions using machine learning-based algorithm," *International Journal of Advanced Research in Science, Communication and Technology*, 2022. https://doi.org/10.48175/ijarsct-5742

[14] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602-613, 2011. https://doi.org/10.1016/j.dss.2010.08.008

[15] A. Aftab, I. Shahzad, M. Anwar, A. Sajid, and N. Anwar, "Fraud detection of credit cards using supervised machine learning techniques," *Pakistan Journal of Emerging Science and Technologies*, vol. 4, pp. 38-51, 2023. https://doi.org/10.58619/pjest.v4i3.114

[16] B. Singh and M. Mahrishi, "Comparing different models for credit card fraud detection," *Skit Research Journal*, vol. 10, no. 2, pp. 8–12, 2020. https://doi.org/10.47904/ijskit.10.2.2020.8-12

[17] A. Fernández, S. García, F. Herrera, and N. V. Chawla, "SMOTE for learning from Imbalanced data: Progress and challenges, marking the 15-year anniversary," *Journal of Artificial Intelligence Research*, 2018. https://doi.org/10.1613/jair.1.11192

[18] Scikit-Learn, "StandardScaler," Retrieved: https://scikit-learn.org/1.6/modules/generated/sklearn.preprocessing.StandardScaler.html, 2025.

[19] B. Kasasbeh, B. Aldabaybah, and H. Ahmad, "Multilayer perceptron artificial neural networks-based model for credit card fraud detection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 1, pp. 362-373, 2022. https://doi.org/10.11591/ijeecs.v26.i1.pp362-373

[20] L. Breiman, "Random forests," *Machine Learning*, vol. 45, pp. 5-32, 2001. https://doi.org/10.1023/A:1010933404324

[21] L. S. Hasugian, "Fraud detection for online interbank transaction using deep learning," *Journal of Syntax Literate*, vol. 8, no. 6, p. 4267, 2023. https://doi.org/10.36418/syntax-literate.v8i6.12627