Credit card Fraud Classification using an Optimized Ensemble Learning Technique

Altyeb Taha [1] Ahmed Hamza Osman [2] Ahmed AbdulQadir AlRababah [3] Yakubu Suleiman Baguda [3]
aaataha@kau.edu.sa ahoahmad@kau.edu.sa aahmad13@kau.edu.sa ysoleman1@kau.edu.sa
Department of Information Technology, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah 21911, Saudi Arabia[1]
Department of Information Systems, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah 21911, Saudi Arabia[2]
Department of Computer Science, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah 21911, Saudi Arabia[3]

Abstract
Recent advancements in e-payment and e-commerce methods have resulted in rising the quantity of credit card transactions that are fraudulent, which cause significant massive financial losses and become a potential security issue. There is an urgent need for efficient methods for identifying fraudulent credit card transactions. This paper presents an effective ensemble learning technique that utilizes the grid search optimization approach for identifying credit card fraud. The suggested approach consists of two phases. First, base learners consist of multiple machine learning classifiers, including Decision Tree (DT), K-nearest neighbor (KNN), AdaBoost (ADA), Gradient Boosting (GB) and Logistic Regression (LR), are utilized to find the fraudulent transactions probabilities. Second, a meta learner that integrates the Random Forest with the Grid Search (RF-GS) is applied to categorize the probabilities of predictions produced by the base learners. RF-GS uses the Grid Search (GS) optimization technique to tune the parameters of Random Forest (RF) method, to get the maximum credit card fraud detection accuracy. A real-world dataset was utilized to evaluate the effectiveness of the suggested approach. The findings of the experiment show the effectiveness of the suggested optimized ensemble-learning strategy for identifying the fraudulent credit card transactions, which performed better than the other approaches and obtained superior accuracy of 99.01%.

Keywords:
Credit card fraud identification; Random Forest; Machine learning; ensemble learning.

1. Introduction

The number of enterprises, online services, and internet users has increased because of recent developments in communication and information technology. People can conveniently use online banking services for money transfers, debit and credit cards for shopping, and bill payment services. When someone utilizes another person's credit card without his authorization, credit card fraud occurs. This can happen with or without the actual card when the essential information, such as the PIN, password, and other credentials, are stolen. Modern credit card fraud does not require the attackers to be present at the scene of the crime. They have a variety of techniques to conceal their identity and execute their illegal activities from their homes. These personality-hiding methods, which are difficult to trace, include utilizing a VPN and transmitting the victim's traffic over the Tor network [1].

According to Statista [2], the global cost of fraudulent payment card transactions in 2021 is estimated to be more than 32 billion US dollars, it is expected that this amount would rise to 38.5 billion by 2027. Thus, the credit card fraud can cause huge financial losses, as an example, the total yearly losses from card-not-present (CNP) fraud for credit and debit cards approved in the United Kingdom (UK) in 2020 were 452.6 million British pounds [3].

In order to reduce losses and combat rising fraud and fraud expenses, fraud detection systems are crucial. Even though cases of credit card fraud are rare, accounting for only 0.2% of all card transactions, they can still cause substantial financial losses due to high transaction values. Given the nature of people, it is impossible to completely avoid fraud; instead, early identification is employed to reduce the harm [4]. Many fraud detection approaches, such as data mining and predictive analytics, help to avoid fraud in the financial industry. All these strategies, however, cannot be carried out without the use of machine

Manuscript received November 5, 2024
Manuscript revised November 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.11.5

learning algorithms, whether unsupervised or supervised, which can be successful in the classification of credit card fraudulent transactions [5].

Due to its numerous applications, shorter learning times, and higher accuracy of results, machine learning is well-known and widely used approach. Although the identification of credit card fraud based on one machine learning algorithm has been extensively studied, the achievement of every algorithm varies due to variances in training datasets and the techniques used for selecting the features. Each classifier also has inherent restrictions and unpredictability. In order to lower the variation of anticipated errors and increase classification accuracy, employing a set of classifiers is preferable than using a single algorithm. Ensemble learning is a machine learning scheme that utilizes multiple approaches rather than depending on just one to create a single reliable model; successfully it has been applied in several different industries. It has been shown both theoretically and practically that ensemble learning methodologies perform better than poor individual techniques, particularly when tackling challenging and large-scale forecast issues [6]. The three more common ensemble learning strategies are bagging [7], boosting [8], and stacking [9]. Stacking is an integration technique that combines various artificial intelligence techniques grouped in one step before applying a separate machine learning technique to produce a categorization scheme that is more precise [10].

The purpose of this study is to investigate the utilization of the ensemble learning based on the grid search optimization for the credit card fraud identification. The suggested technique is separated into two phases. First, base learners consist of multiple machine learning algorithms, such as Gradient Boosting (GB), Logistic Regression (LR), AdaBoost (ADA), K-nearest neighbor (KNN) and Decision Tree (DT) is utilized to find the fraudulent transaction's probabilities. Second, a meta learner RF-GS is used to categorize the probabilities of prediction from the base learners. The grid search optimization approach is employed to tune the RF method's specifications to get the maximum credit card fraud detection accuracy. The following is a summary of the contributions of the suggested research:

• An enhanced ensemble learning strategy based on grid search optimization is suggested to classify the fraudulent credit card transactions.

• The grid search optimization algorithm is utilized to tune the meta learner's settings to raise the accuracy of credit card fraud detection.

• Compared to previous techniques, the proposed technique achieved the highest accuracy of categorization.

The remainder of the research is structured as follows: Section 2 presents research related work; Section 3 presents the suggested method for credit card identification; The experimental outcomes and analysis are presented in Section 4. This study's conclusion and recommendations for further research are provided in Section 5.

2. Related Work

Numerous research efforts have been suggested to address the challenge of classifying fraud in credit card transactions, including advanced and cutting-edge machine learning techniques.

In prior work [11], we employed LightGBM to perform experiments using two datasets UCSD-FICO and ECCFD. We estimated the average results from different classifiers using 5-fold cross validation and contrasted it with Optimized Light Gradient Boosting Machine (OLightGBM), which includes hyperparameter optimization as well as other cutting-edge methods. We observed that OLightGBM had the greatest results in the two datasets. OLightGBM obtained area under the curve (AUC) of 90.94%, 40.59% in Recall, 98.40% in Accuracy, 56.95% in F1-Score and 97.34% in Precision in the first dataset. In the second dataset, OLightGBM obtained 98.35% Accuracy, 92.88% AUC, 91.72% Precision and 28.33% Recall. Prusti and Rath [12] created an application that used machine learning approaches including Extreme learning machine (ELM), KNN, DT, SVM and Multilayer perceptron (MLP) to classify the credit card fraud.

They suggested a hybrid classifier that used the techniques of DT, SVM, and KNN. They analyzed the outcomes from five methods for machine learning based on the accuracy measure. SVM outperformed

other methods by 81.63%, while their hybrid approach achieved a higher accuracy of 82.58%.

Kumar et al. [13] proposed an approach that used Random Forest algorithm for classifying fraudulent credit card transactions. Random forest method is a supervised machine learning method that utilizes DT to classify fraudulent credit card transactions. The proposed method has a 90% accuracy rating. Awoyemi et al. in [14] proposes three credit card fraud classification approaches: LR, KNN and NB. The KNN algorithm with k = 3 produces the highest accuracy of 96.91%. The k-NN technique is a supervised machine learning approach that can be utilized for regression and classification.

Pumsirirat and Yan in [15] proposed Two unsupervised machine learning approaches using the Auto Encoder (AE) model and the Restricted Boltzmann machine (RBM) model for credit card fraud detection. Since no data labels are required for model training, both techniques are unsupervised. With an obvious input layer and an invisible layer, RBM may be compared to a two-layer neural network. It can determine the distribution's probability of the supplied data and use that knowledge to learn how to re-structure the data. AE obtained the highest accuracy of 97.05%. John and Naaz [16] suggested a method for classifying credit card fraud using the Isolation Factor and Local Outlier Factor algorithms. They conducted their experiments using Kaggle credit card fraud dataset. The Local Outlier Factor algorithm obtained the top accuracy of 97%. Prusti et al. [17] presented a fraud identification approach using graph database architecture. The graph's features are obtained utilizing the Neo4j tool and then integrated with other transaction database characteristics in their model. They then used five supervised and two unsupervised learning techniques. They evaluated the achievement of these techniques using features collected from graph and transaction databases.

Seera et al. [18] used actual public transaction records to construct several machine learning algorithms and mathematical approaches for detecting credit card fraud. To determine if the characteristics produced by the genetic algorithm outperformed standard features for fraud detection, researchers utilized a probabilistic assessment of hypotheses. Results from the aggregated attributes were reliable. Alharbi et al. [19] used the Kaggle dataset to build a deep learning (DL) based technique to detect credit card fraud based on solving the text data issue. A text2IMG transformation approach that produces small images is proposed. To address the issue of class disparity, the inverse frequency technique is used to feed the pictures into a CNN structure with class scores. To validate the strength and reliability of the suggested approach, ML and DL approaches were utilized.

3. The suggested method for credit card fraud detection based on optimized ensemble learning

The proposed scheme is an ensemble learning method for identifying the fraudulent credit card transactions that utilizes an optimized random forest algorithm (meta learner) which uses the predictions of the base learners as inputs. There are five algorithms in the base learners: DT, ADA, KNN, LR and GB. To obtain the highest detection accuracy for the fraudulent credit card transaction, the grid search optimization is applied to tune the settings of the base learners. The proposed scheme is illustrated in figure 1.

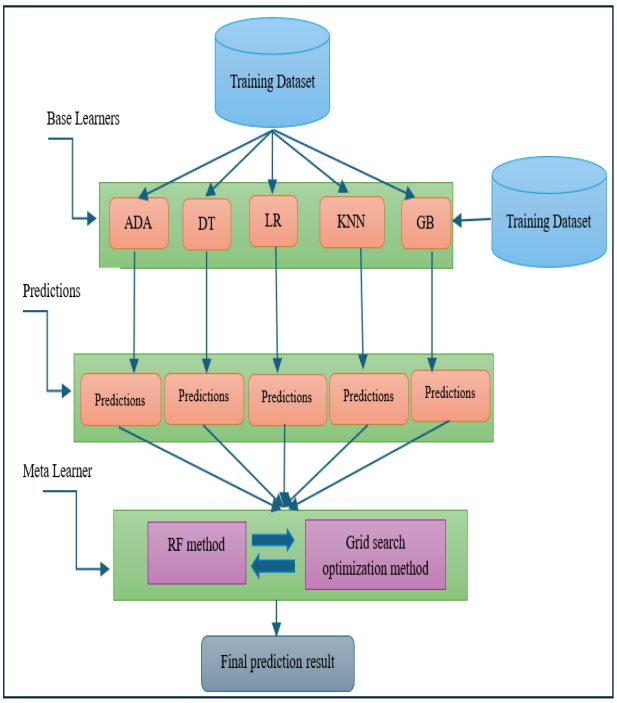

Figure 1. Suggested approach for Credit card fraud detection.

A. Dataset and Features Selection

This research utilized publicly available real-world dataset of online purchases to build various experiments for assessing the suggested scheme for identifying unauthorized use of credit cards. The goal of the dataset was to classify fraudulent e-commerce transactions.

In the used dataset [20], there are 94,683 transactions in total, 2,094 of which are fraudulent. The dataset gathered from 73,729 credit cards. It has 20 features, category is included, with the following fields: hour1, amount, zip1, state1, custAttr1, eld1, custAttr2, eld2, hour2, ag1, total, eld3, eld4, indicator1, indica-tor2, ag2, ag3, ag4, ag5, and Class. The Class field is the classification variable, one denotes event of credit card fraud and zero denotes legitimate transaction. Choosing important and crucial features is significant for successful classification of credit card fraud [21]. The proposed method employs the information gain (IG) algorithm to choose the significant characteristics and minimize the training data's dimensionality. Information gain works by identifying similar patterns in online purchases and then giving the great score to the important characteristics based on the classification of valid and unauthorized use of credit cards. Due to its processing effectiveness and superior precision [22], information gain is used for selecting the significant features in the suggested scheme.

B. Random Forest

Random Forest is an ensemble approach in artificial intelligence that uses bagging as an ensemble strategy and decision trees as individual models. The main reason for choosing Random Forest is because it is an incredibly popular and widely used machine learning method. Furthermore, it is extensively applicable and produces good performance results for classification and regression-based predictive modeling challenges. Moreover, its reliance on fewer hyper-parameters makes it simple to use and deploy [23].

C. Random Forest Optimization using Grid search Algorithm

Adjusting the settings is a significant phase in constructing reliable ML models. Tuning a machine learning model decreases overfitting and enhances the model's adaptation to new data. Moreover, selecting the proper hyperparameters is also an important factor in enhancing the model's accuracy [24]. The RF parameters are critical to how effectively they function: if the proper values are set for these parameters, the model's performance can improve significantly. The grid search algorithm utilized in the suggested ensemble learning scheme to adjust the settings of the meta leaner, by finding RF settings that improve the precision of detecting the fraudulent credit card transactions classification. The hyper parameters from the Grid Search method and forecast probabilities derived from the base learners were used as input to the random forest classifier, as illustrated in figure 1.

Grid Search finds the parameters that contribute to the best performance from a set of given ranges of values for some parameters. The obtained optimal parameters used for RF classification are summarized in Table 1.

Table 1. Optimal parameters used for RF classification

Parameter	Range of values	Optimal value
'max_depth’	[7, 15]	15
'max_features'	[0, 17]	17
'min_samples_leaf'	[1, 2, 4]	1
'min_samples_split'	[5, 10]	5

D. Performance Measures

It is standard practice to evaluate the efficacy of machine learning methods using the matrix of confusion, it includes the following details:

TP: The proportion of the payments with credit cards that are fraudulent and are identified as fraudulent.

TN: The proportion of the payments with credit cards that are normal and are classified as normal.

FP: The proportion of the payments with credit cards that are normal but are identified as fraudulent.

FN: The proportion of the payments with credit cards that are fraudulent but are classified as normal.

The proportion of properly categorized data split by the entire number of classification possibilities is the definition of accuracy. Accuracy may be expressed numerically as:

Accuracy = (TP + TN) / (TP + TN + FN+ FP)

Precision assesses how frequently the machine learning method is accurate. The computational formula for precision is:

Precision = TP / (FP + TP)

A measure of genuine positive rates is recall. The formula for recall in mathematics is:

TP = TP/ (TP + FN)

The harmonic average of recall and accuracy is defined as the F-measure:
F-measure = (2 × Recall × Precision)/ (Recall +Precision)

The achievement of the classifier at each classification threshold is depicted on a graph called a receiver operating characteristic (ROC) curve. Two metrics, the false positive percentage and the real positive percentage, are shown on this graph:
As a synonym for recall, true positive rate (TPR) is explained in the formula below:
TPR = TP/(TP + FN)
The rate of false positives (FPR) is explained below:
FPR = FP / (TN + FP)

The FPR and TPR are visually represented by the area under the ROC curve (AUC) using different folds. AUC is more accurate when evaluating performance because it is not based on a threshold. A classifier often performs better when its AUC value is near to 1. Metrics like accuracy, recall and AUC were utilized to assess the efficacy of the suggested approach.

To fully assess the efficiency of the suggested strategy, AUC was employed in this study along with other important performance indicators including accuracy and recall. Although accuracy gauges the total percentage of accurate predictions, unbalanced datasets may cause it to be deceptive. Conversely, recall assesses the sensitivity of the model and its capacity to accurately detect positive cases. Combining these measures allows us to get a more detailed picture of the model, making sure that it works effectively in both general and particular circumstances where different kinds of mistakes could have greater consequences [25]. This comprehensive assessment enables a more thorough examination of the model's efficacy.

4. Results and discussion

In this part, using data from the experiments, we assessed the performance of the suggested technique by contrasting it with five fundamental classifiers. The fundamental classifiers include RL, ADA, GB, KNN and DT.

The proposed scheme obtained the top accuracy score of 99.01 %, showing its capability to differentiate between the fraudulent credit card transactions and legitimate transactions as explained in Table 2 and Figure 2. In addition, the proposed method obtained a recall score of 99.01%, demonstrating its capability to appropriately classify 99.01% of the fraudulent credit card transactions while decreasing false positives. The DT method achieved the second top accuracy of 98.51%, whereas AdaBoost obtained the lowest accuracy of 97.66%. The suggested scheme achieved the best recall, F1 and precision scores of 99.01%, 98.70% and 98.70% respectively.

Table 2: Performance assessment of the suggested strategy in comparison to other artificial intelligence methods.

Approach	Accuracy	Precision	Recall	F1-measure
Decision Tree	0.98518	0.97335	0.97191	0.9726
Logistic Regression	0.97661	0.96751	0.97761	0.96835
K-Nearest Neighbors	0.9786	0.97185	0.9786	0.97154
Gradient Boosting	0.98106	0.97729	0.98106	0.97631
AdaBoost Classifier	0.97768	0.95586	0.97768	0.96665
The proposed optimized approach	0.99012	0.98702	0.99012	0.98709

The AUC, which was utilized to evaluate the recommended approach, is shown in Figure 3. The AUC is a useful and pertinent assessment of general achievement. An increased AUC score shows a more powerful capacity for categorization. According to Figure 3, the suggested method's AUC is 93.6%, indicating that it effectively separates authentic credit card transactions from fraudulent ones. Figure 3 also shows that our suggested ensemble classifier outperformed the classifiers that utilized as basis models.

The suggested approach's achievement is contrasted with current approaches. Table 3 contrasts the achievements of the proposed method to that of other methods.

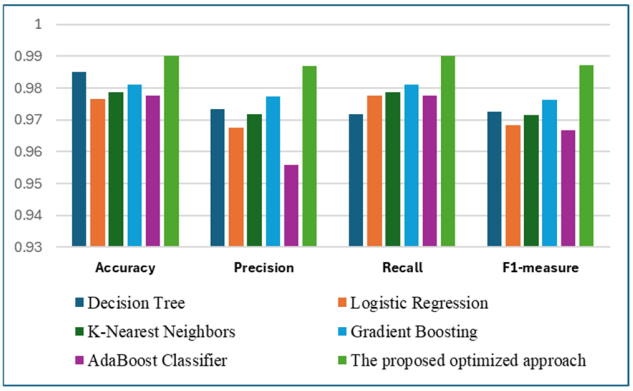

Figure. 2. Performance evaluation of suggested scheme and other machine learning methods.

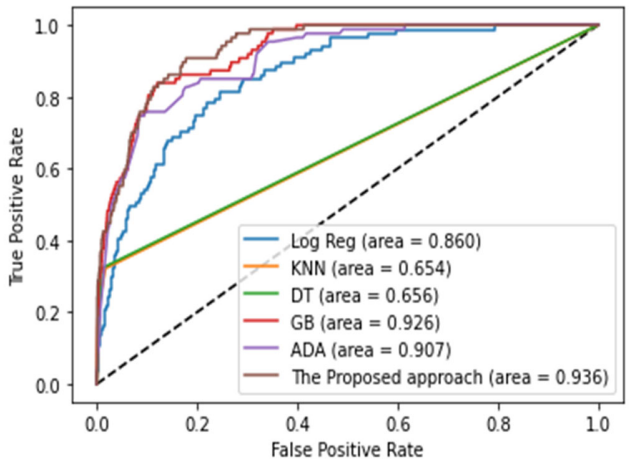

Figure 3. AUC for suggested scheme and some other machine learning methods.

Table 3. Comparison between the suggested technique with past works.

Approach	Accuracy
[11]	0.9840
[12]	82.58%
[13]	90%
[14]	96.91%
[15]	97.05%
[16]	97%
The proposed approach	99.01%

5. Conclusions

Because credit card theft causes significant financial losses, effective classification systems are crucial. This work presents a technique for credit card fraud categorization using optimal ensemble learning. The suggested technique includes two phases. First, base learners are built to accommodate several machine learning methods, such as DT, ADA, KNN and LR. Second, a meta learner RF-GA is utilized to categorize the probabilities of prediction from the base learners, which applies the grid search algorithm (GS) to improve the RF method's parameters.

GS were used to fine-tune the parameter values of the RF method to achieve the greatest credit card fraud categorization. The experiments' results show that the proposed strategy for credit card fraud classification using random forest and gird search methods, outperforms the other techniques and attained the greatest level of accuracy of 99.01%. For future research, more advanced techniques will be considered to optimize the ensemble learning scheme.

Acknowledgment

This research work was funded by Institutional Fund Projects under grant no. (IFPIP: 281-830-1443). The authors gratefully acknowledge technical and financial support provided by the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

References

[1] Alfaiz, Noor Saleh, and Suliman Mohamed Fati. "Enhanced credit card fraud detection model using machine learning." Electronics 11, no. 4 (2022): 662.

[2] Statista, Value of fraudulent payment card transactions worldwide from 2021 to 2027. Available online: https://www.statista.com/statistics/1264329/value-fraudulent-card-transactions-worldwide/ (Accessed on 5 SEP 2024).

[3] Statista, Value of annual losses on "Card-not present" fraud on UK-issued debit and credit cards in the United Kingdom (UK) from 2002 to 2020. Available online: https://www.statista.com/statistics/286245/united-kingdom-uk-card-not-present-fraud-losses/ (accessed on 5 SEP 2024).

[4] Sohony, Ishan, Rameshwar Pratap, and Ullas Nambiar. "Ensemble learning for credit card fraud detection." In Proceedings of the ACM India joint international conference on data science and management of data, pp. 289-294. 2018.

[5] Sinap, Vahid. "Comparative analysis of machine learning techniques for credit card fraud detection: Dealing with imbalanced datasets." Turkish Journal of Engineering 8, no. 2 (2024): 196-208.
[6] Dong, X., Yu, Z., Cao, W., Shi, Y. and Ma, Q., 2020. A survey on ensemble learning. Frontiers of Computer Science, 14, pp.241-258.
[7] Breiman, Leo. "Bagging predictors." Machine learning 24 (1996): 123-140.
[8] Schapire, Robert E., and Yoram Singer. "Improved boosting algorithms using confidence-rated predictions." In Proceedings of the eleventh annual conference on Computational learning theory, pp. 80-91. 1998.
[9] Wolpert, David H. "Stacked generalization." Neural networks 5, no. 2 (1992): 241-259.
[10] Sagi, Omer, and Lior Rokach. "Ensemble learning: A survey." Wiley interdisciplinary reviews: data mining and knowledge discovery 8, no. 4 (2018): e1249.
[11] Taha, Altyeb Altaher, and Sharaf Jameel Malebary. "An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine." IEEE access 8 (2020): 25579-25587.
[12] Prusti, Debachudamani, and Santanu Kumar Rath. "Web service based credit card fraud detection by applying machine learning techniques." In TENCON 2019-2019 IEEE Region 10 Conference (TENCON), pp. 492-497. IEEE, 2019.
[13] Kumar, M. Suresh, V. Soundarya, S. Kavitha, E. S. Keerthika, and E. Aswini. "Credit card fraud detection using random forest algorithm." In 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), pp. 149-153. IEEE, 2019.
[14] Awoyemi, John O., Adebayo O. Adetunmbi, and Samuel A. Oluwadare. "Credit card fraud detection using machine learning techniques: A comparative analysis." In 2017 international conference on computing networking and informatics (ICCNI), pp. 1-9. IEEE, 2017.
[15] Pumsirirat, Apapan, and Yan Liu. "Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine." International Journal of advanced computer science and applications 9, no. 1 (2018).
[16] John, Hyder, and Sameena Naaz. "Credit card fraud detection using local outlier factor and isolation forest." Int. J. Comput. Sci. Eng 7, no. 4 (2019): 1060-1064.
[17] Prusti, Debachudamani, Daisy Das, and Santanu Kumar Rath. "Credit card fraud detection technique by applying graph database model." Arabian Journal for Science and Engineering 46, no. 9 (2021): 1-20.
[18] Seera, Manjeevan, Chee Peng Lim, Ajay Kumar, Lalitha Dhamotharan, and Kim Hua Tan. "An intelligent payment card fraud detection system." Annals of operations research 334, no. 1 (2024): 445-467.
[19] Alharbi, Abdullah, Majid Alshammari, Ofonime Dominic Okon, Amerah Alabrah, Hafiz Tayyab Rauf, Hashem Alyami, and Talha Meraj. "A novel text2IMG mechanism of credit card fraud detection: A deep learning approach." Electronics 11, no. 5 (2022): 756.
[20] UCSD: University of California, San Diego Data Mining Contest 2009. Available online : https://www.cs.purdue.edu/commugrate/data/credit_card/ (accessed on 5 March 2024).
[21] Bahnsen, Alejandro Correa, Djamila Aouada, Aleksandar Stojanovic, and Björn Ottersten. "Feature engineering strategies for credit card fraud detection." Expert Systems with Applications 51 (2016): 134-142.
[22] Theng, Dipti, and Kishor K. Bhoyar. "Feature selection techniques for machine learning: a survey of more than two decades of research." Knowledge and Information Systems 66, no. 3 (2024): 1575-1637.
[23] Belgiu, Mariana, and Lucian Drăguţ. "Random forest in remote sensing: A review of applications and future directions." ISPRS journal of photogrammetry and remote sensing 114 (2016): 24-31.
[24] Morales-Hernández, Alejandro, Inneke Van Nieuwenhuyse, and Sebastian Rojas Gonzalez. "A survey on multi-objective hyperparameter optimization algorithms for machine learning." Artificial Intelligence Review 56, no. 8 (2023): 8043-8093.
[25] Rainio, Oona, Jarmo Teuho, and Riku Klén. "Evaluation metrics and statistical tests for machine learning." Scientific Reports 14, no. 1 (2024): 6086.