# Research on Credit Card Fraud Prediction Model Based on GAN-DNN Imbalance Classification Algorithm

Qin Wang<sup>1</sup>, Mary Jane C.Samonte<sup>2\*</sup>

School of Information Technology, Mapua University,Xi'an Siyuan University, Manila, Phillippines<sup>1</sup> School of Information Technology, Mapua University, Manila, Phillippines<sup>2</sup>

*Abstract***—Credit card consumption has become an important way of consumption in modern life, but the problem of credit card fraud has also emerged, disrupting the financial order and restricting the development of the industry. Aiming at the data class imbalance problem in credit card fraud detection and improving the accuracy of fraud detection, this paper uses the Generative Adversarial Network (GAN) to generate fraud samples and balance the number of fraud transaction samples and normal transaction samples. Then, a deep neural network (DNN) is used to construct a credit card fraud prediction model. The study compares this model with commonly used classification algorithms and sampling methods in detail and confirms that the designed credit card fraud prediction model has a good effect, providing a theoretical basis and practical reference for financial institutions to predict credit card fraud.**

*Keywords—Generative adversarial network; deep neural network; unbalanced data; credit card fraud; classification algorithms*

# I. INTRODUCTION

Globally, the field of credit card payments is rife with a significant number of credit card fraud cases. According to a report by the Federal Trade Commission (FTC), in 2022, as many as 2.8 million users in the United States were affected by credit card fraud, with losses amounting to \$3.4 billion. By the end of 2022, the monetary losses caused by credit card fraud soared to \$5.8 billion, an increase of over 70% [1]. In recent years, credit card fraud has shown a trend towards specialization, scaling, and syndication, undermining the stability of the financial market and endangering the financial security of the public [2]. Therefore, it is crucial for financial institutions to establish intelligent fraud detection mechanisms to enhance the anti-fraud capabilities of regulators.

In recent years, researchers have conducted extensive work in the area of credit card fraud detection. Regarding the issue of data imbalance, oversampling and undersampling methods are commonly employed. For instance, N. Rtayli et al. utilized the SMOTE algorithm to generate fraud samples to overcome data imbalance [3]; Chen Ying et al. improved the SMOTE algorithm through K-Means clustering, generating fraud samples only in safe areas [4]; E. Esenogho et al. combined SMOTE oversampling with undersampling for hybrid sampling, thereby improving the overall distribution of credit card data [5]. In terms of data detection accuracy, deep models based on Long Short-Term Memory (LSTM) networks are generally used [6]. Gao J et al., for example, used LSTM to extract potential temporal information from credit card data, ultimately completing information identification and fraud classification through XGBoost [7]; Benchaji et al. proposed an LSTM credit card fraud detection model integrated with an attention mechanism, selectively focusing on features through the attention mechanism to enhance the model's detection efficiency [8]; J. Forough et al. constructed a credit card fraud detection model with LSTM as the preliminary prediction layer and CRF as the final prediction layer [9]. However, the traditional SMOTE oversampling algorithm generates a large number of fraudulent samples with noise, and undersampling algorithms may lose key information, ultimately affecting the training effectiveness of the model [10]. On the other hand, LSTM can only learn the forward distribution of credit card data and cannot combine the forward and reverse directions to output a comprehensive expression for fraud detection [11]. In terms of data feature extraction and classification tasks, various hybrid model methods based on GAN have been adopted [12]. Li et al. used the GAN-RNN algorithm for sequence modeling of image data to mine time series features in images [13]; Zhang et al. combined GAN-RNN with variational autoencoders for feature fusion to enhance the expressive power of features [14]. Zhao et al. utilized GAN-CNN for indepth mining of image features, ultimately completing image classification tasks through a Softmax classifier [15]; Sun et al. proposed a GAN-CNN classification model combined with a multi-scale feature fusion mechanism, improving the model's classification accuracy by fusing features of different scales [16]. However, GAN-RNN may lose local key information during feature extraction or fusion, affecting the model's comprehensive capture of features related to fraudulent behavior, thereby affecting the model's fraud detection capability [17]. GAN-CNN cannot adaptively adjust according to different transaction data features and fraud patterns, making it difficult to output more comprehensive and accurate fraud detection results [12].

Compared with traditional methods, this study employs a Generative Adversarial Network (GAN) to generate minority sample data and then combines it with a Deep Neural Network (DNN) to predict the categories of credit card transaction data. This approach has multiple advantages: it overcomes the issue of undersampling methods losing a large amount of data information, and also addresses the noise expansion and overfitting issues when the SMOTE oversampling method and

ADASYN oversampling method generate new samples. At the same time, applying the DNN model to the credit card fraud prediction problem expands the application range of deep learning technology and improves the model's predictive performance. In response to these issues, this paper proposes corresponding solutions. In terms of research methodology, it elaborates on the principles of Generative Adversarial Networks (GAN) and Deep Neural Networks (DNN), and constructs a credit card fraud prediction model. Through experimental design and analysis, including the introduction of the experimental environment, description and preprocessing of the dataset, and the determination of evaluation metrics, the experimental results are compared with common classification models and deep neural network classification models different data processing methods to further analyze model performance. Finally, the paper is summarized, highlighting the advantages of the research model and its reference value for financial institutions in credit card fraud prediction.

## II. RESEARCH METHODS

## *A. Generative Adversarial Networks (GAN)*

Generative Adversarial Networks (GAN) [12] is an unsupervised neural network that consists of two networks for adversarial training. The goal of the generator is to synthesize samples that are difficult for the discriminator to distinguish, and the goal of the discriminator is to distinguish whether the samples generated by the generator are real samples as much as possible. In this paper, we use generative adversarial networks to generate fraud-like transaction data to solve the data imbalance problem in the original data. The modeling of the generative adversarial network is mainly divided into three aspects: the overall structure of the generative adversarial network, the modeling of the data generator and the modeling of the data discriminator.

## Overall structure of generative adversarial network

In this paper, Conditional Generative adversarial Network (CGAN), a derivative model of generative adversarial network, is used to generate fraudulent credit card transaction data to solve the problem of extremely unbalanced number of positive and negative samples in credit card transaction data. The conditional generative adversarial network model in the credit card fraud prediction model adds the credit card transaction data category label y to the data generator model and the data discriminator model in the model, so that the data generated by the generator is artificial credit card transaction data with the same distribution as the real data under the condition of meeting the category label y. This makes the adversarial network model easier to control, solves the uncertainty of the original generative adversarial network generation model, and makes the generated credit card transaction data more in line with our expectations. At the same time, it also makes the conditional generative adversarial network model can quickly reach the convergence conditions in the training process, the model is not easy to collapse, and the training process is easier to control. The overall structure of the conditional generative adversarial network in the credit card fraud prediction model is shown in Fig. 1.



Fig. 1. Overall structure of conditional generative adversarial networks for credit card fraud prediction.

The objective function of the Conditional Generative Adversarial Network (CGAN) model in the credit card fraud prediction model is expressed in Eq. (1). In this equation, pdate represents the distribution of real credit card transaction data, y represents the category label of credit card transactions, pz represents the distribution of credit card transaction data generated by the generator, and y' represents the category label generated by the generator for the credit card transactions. When training the generator, the goal is to maximize  $V(D, G)$ , whereas when training the discriminator, the goal is to minimize V(D, G).

$$
\min_{G} \max_{D} V(D, G) = E_{x \sim P_{data}(x)} [\log D(x|y)] + E_{z \sim p_{z}(z)} [\log (1 - D(G(x|y)))] \tag{1}
$$

## Data generator model

Credit card transaction data has the characteristics of huge data volume and moderate data feature dimension, and good results can be achieved by using a fully connected deep neural network. Therefore, the data generator model of the conditional generative adversarial network in the credit card fraud prediction model in this study adopts a fully connected deep neural network. In this model, the random noise data z conforming to Gaussian distribution and the credit card transaction data category label y are combined as the input of the data generator model, and the input layer and the hidden layer are connected in a fully connected manner. In addition, in order to improve the fitting ability of the deep neural network, a nonlinear activation function needs to be added between the layers. However, the sigmoid activation function is easy to cause the problem of gradient disappearance. Therefore, leakyrelu activation function needs to be added between the input layer and the hidden layer in the data generator model. Each hidden layer is also connected with the upper hidden layer in a fully connected way, and the leakyrelu activation function is used, and the connection between the last layer and the output layer is also fully connected. The network structure of the data generator model in the credit card fraud prediction model is shown in Fig. 2.



Fig. 2. Network structure of data generator model.

The training of the data generator model should ensure that the data discriminator model does not change, and the goal of the data generator model is to make the data discriminator not be able to determine whether the data is real credit card transaction data or credit card transaction data generated by the generator. Therefore, the loss function of the data generator model is shown in Eq. (2):

$$
V(G) = E_{z \sim p_z(z)} \left[ \log(1 - D(G(z|y))) \right]
$$
 (2)

The training process of the data generator model is the process that minimizes this V(G), the data generator model Algorithm 1 shows the training process.

**Algorithm 1:** Training process of data generator model

Input: Random noise data z, label y

Output: Data generator

 $(1)$  Initializes the data generator

 $(2)$  The sample set is composed of m minibatch samples collected from pg(z) of Gaussian distribution

 $Z = \{z^{(1)}, z^{(2)}, z^{(3)}, \cdots, z^{(m)}\}$ 

(3)The sample set of noise is connected to the class label y to obtain the input of the data generator

 $input = \{(z^{(1)}, y), (z^{(2)}, y), (z^{(3)}, y), \cdots (z^{(m)}, y)\}$ 

 $(4)$  The input data input passes through multiple hidden layers and the leakyrelu activation function to get the output data

 $\text{output} = \{z_g^{(1)}, z_g^{(2)}, z_g^{(3)}, \cdots, z_g^{(m)}\}$ 

 $(5)$  The gradient descent algorithm is used to update the parameters of the data generator model to make the loss function of the generator

$$
V(G) = E_{z \sim p_z(z)} \left[ \log(1 - D(G(z|y))) \right]
$$
  
Min

Min.

## • Data discriminator model

In addition, in the credit card fraud prediction model, the data discriminator model is required to correctly identify fraud transaction samples when solving the problem of data class imbalance. Therefore, adding the category label y to the input of the data discriminator can make the training process of the data discriminator model more targeted. The network structure of the data discriminator model in the credit card fraud prediction model is shown in Fig. 3.



Fig. 3. Network structure of data discriminator model.

While training the data discriminator model, we need to ensure that the data generator model does not change, and the goal of the data discriminator is to make the discriminator maximally distinguish between the credit card transaction data generated by the generator and the real credit card transaction data. Therefore, the loss function of the data discriminator model is shown in Eq. (3):

$$
V(D) = E_{x \sim p_{date}(x)} \left[ \log D(x|y) \right] \tag{3}
$$

The learning purpose of the data discriminator model in the conditional generation adversarial network is to maximize V(D). The specific training process is shown in Algorithm 2.

#### **Algorithm 2:** Training process of data discriminator model

Input: Data generator generated data  $G(z|y)$ , real data x, label y Output: Data discriminator

 $(1)$  Initializes the data discriminator

(2) From the distribution  $p_{date}(x)$  of the real credit card transaction data, m minibatches of data are randomly selected to form the data set of the real data

(3) From the data  $G(z|y)$  sample generated by the data generator, m minibatch data are randomly selected to form the data set generated by the generator

$$
G = \left\{ g^{(1)}, g^{(2)}, g^{(3)}, \cdots, g^{(m)} \right\}
$$

 $(4)$  A dataset of real data is concatenated with label y to obtain a portion of the discriminator input.

$$
input1 = \{(x^{(1)}, y), (x^{(2)}, y), (x^{(3)}, y), \cdots, (x^{(m)}, y)\}
$$

 $(5)$  The data set of generated data is concatenated with label y to obtain a portion of the discriminator input

$$
input2 = \{(g^{(1)}, y), (g^{(2)}, y), (g^{(3)}, y), \cdots, (g^{(m)}, y)\}
$$

 $(6)$  input1 and input2 are mixed to get the discriminator input  $input = \{(x^{(1)}, y), (x^{(2)}, y), \cdots, (x^{(m)}, y), (g^{(1)}, y), (g^{(2)}, y), \cdots, (g^{(m)}, y)\}$ 

(7) The input data input passes through the hidden layer and the leakyrelu activation function to get the output data

$$
logits = \left\{z_g^{(1)}, z_g^{(2)}, z_g^{(3)}, \cdots, z_g^{(m)}\right\}
$$

 $(8)$  The output logits of the last layer of the hidden layer is used by the sigmoid activation function to obtain the output of the entire discriminator

$$
output = sigmoid(\log its)
$$

(9) The gradient ascending algorithm is used to update the parameters of the discriminator and make the loss function of the discriminator

$$
V(D) = E_{x \sim p_{date}(x)} [\log D(x|y)]
$$
  
Max.

## *B. Deep Neural Networks*

The neural network model has a strong fitting ability, and the deep neural network is deeper than the ordinary neural network, that is, the hidden layers are more, and its fitting ability is relatively stronger. The deep neural network model is shown in Fig. 4.



Fig. 4. Deep neural networks model.

According to the characteristics of credit card historical transaction data, the deep neural network classifier model of credit card fraud prediction model can obtain good results by using the deep fully connected neural network model. The network structure of the deep neural network classifier in the credit card fraud prediction model is shown in Fig. 5.



Fig. 5. Network structure of deep neural network classifier.

In the training process of deep neural network classifier, cross entropy can be used as a loss function. The definition of cross entropy is shown in Eq. (4):

$$
Loss = \frac{1}{N} \sum_{i} - [y_i \cdot \log(p_{i)} + (1 - y_i) \cdot \log(1 - p_i)] \tag{4}
$$

In the cross entropy loss function, N represents the number of samples, yi represents the actual value of the i th sample, the fraudulent transaction sample is 1, the normal transaction sample is 0, pi represents the predicted value of the i th sample, that is, the probability value of the i sample predicted as the fraudulent sample. Cross entropy loss function is often used in conjunction with softmax activation function, which can improve the speed and effectiveness of model training to a certain extent. The detailed training process of deep neural network classifier is shown in Algorithm 3.

**Algorithm 3:** Training process of deep neural network classifier

Input: Training set  $X = \{(x^{(1)}, y^{(1)}), (x^{(2)}, y^{(2)}), (x^{(3)}, y^{(3)}), \cdots, (x^{(m)}, y^{(m)})\}$ , among  $y^i = \{0,1\}$ Output: Deep neural network classifier D

 $(1)$  Initialize all variables in a deep neural network, including

weight vectors and paranoid value vectors

(2) Loop iteration 
$$
\Box
$$
 = 1,2,3,...,  $\Box$ :

① Calculate the output of the classifier based on the current

parameters and formulas

②The parameters of the classifier are updated by gradient descent algorithm to make the cross entropy loss function

$$
Loss = \frac{1}{N} \sum_{i} - [y_i \cdot log(p_{i)} + (1 - y_i) \cdot log(1 - p_i)]
$$

Min.

# *C. Credit Card Fraud Prediction Model*

The credit card fraud prediction model uses generative adversarial networks to deal with the class imbalance problem in credit card transaction data, and then combines the deep neural network model in the field of deep learning to predict the class of credit card transaction samples. An example plot of a credit card fraud prediction model is shown in Fig. 6.



Fig. 6. Credit card fraud prediction model.

In the credit card fraud prediction model of this study, the generative adversarial network is used to generate fraud sample data to solve the extreme imbalance problem between fraud sample data and normal transaction sample data in the original credit card transaction data set, and then the high fitting ability of deep neural network is used to predict the credit card transaction category.

## III. EXPERIMENTAL DESIGN AND ANALYSIS

# *A. Experimental Environment*

This article was tested using Windows 11, AMD Ryzen 7 5800H CPU, 16 GB of memory, NVIDIA GeForce RTX 3060 display card. In the process of building the model, Sklearn toolkit and Keras toolkit of Python programming language are used to achieve.

## *B. Data Set Description and Preprocessing*

The dataset was collected from November 2022, through a professional consulting company, including open data information from volunteers, commercial banks, private banks, and credit cooperatives. Currently, the dataset contains transaction records of 10,000 credit card users, including different regions, age groups, and professional backgrounds, ensuring the diversity and representativeness of the data. Among the 10,000 users, after strict data cleaning and labeling, it is confirmed that 178 users have fraudulent behavior, that is, the proportion of fraudulent users is 1.78%. Although this proportion is not high, considering the potential harm of fraudulent behavior to financial institutions, accurate prediction is particularly important.

There are 31 feature variables in this dataset with no missing values. For the purpose of protecting cardholder privacy, their original characteristics and background information are not provided. Features V1, V2, ... V28 is the result of dimensionality reduction through PCA. The specific information of the data set is shown in Table I:

TABLE I. DATASET ATTRIBUTE TABLE

Ordinal	Field Name	Data Type	<b>Field Description</b>	
	Time	Float	The number of seconds elapsed between this transaction and the first transaction in the dataset	
$2 - 29$	$V1-V28$	Float	Principal component data	
30	Amount	Float	<b>Transaction</b> amount	
31	Class	Float	In the case of fraud, take it as one, otherwise take zero.	

# *C. Credit Card Fraud Prediction Model*

While constructing and training the model, we need to establish a rational and effective indicator system to verify and evaluate the model's performance. The evaluation indicators used in this paper include Accuracy, Precision, Recall calculation formula is as follows:

$$
Accuracy = \frac{TP + TN}{TP + TN + FP + FN}
$$
\n<sup>(5)</sup>

$$
Precision = \frac{TP}{TP + FP}
$$
 (6)

$$
Recall = \frac{TP}{TP + FN}
$$
\n(7)

Among, TP represents the sample that predicted a positive example as a positive example; FP is the sample that predicts a negative example as a positive example. FN is denoted as the sample that predicts a positive example as a negative example; TN denotes the sample for which a negative example is predicted as a negative example.

# IV. ANALYSIS OF EXPERIMENTAL RESULTS

In order to verify the effectiveness of the model proposed in this study, we use credit card transaction data set to train common classification models and deep neural network classification models for detailed comparison. The performance effect is shown in Table II.

TABLE II. CLASSIFIER TEST RESULTS

Model	accuracy	precision	recall
Logistic regression [18]	0.8623	0.9836	0.8612
Naive Bayes [19]	0.7657	0.9829	0.7634
Decision-Making tree [20]	0.8526	0.9882	0.8510
Classifier Kproximity [21]	0.7584	0.9800	0.7534
<b>SVM</b> [22]	0.8321	0.9902	0.8308
AdaBoost classifier [23]	0.8112	0.9938	0.8094
Dnn classifier [24]	0.9232	0.9985	0.9192

In order to verify the effectiveness of conditional generative adversarial networks in generating new samples, In this study, the experimental results of combining conditional generative adversarial network model with deep neural network classifier and the experimental results of not processing imbalanced data only using deep neural network classifier, the experimental results of combining random undersampling with deep neural network classifier, the experimental results of combining SMOTE oversampling with deep neural network classifier, and the experimental results of combining SMOTE oversampling with deep neural network classifier The test results of ANASYN oversampling combined with deep neural network classifier were compared, and the final results are shown in Table III.

TABLE III. EXPERIMENTAL RESULTS OF VARIOUS UNBALANCED DATA PROCESSING METHODS

Model	Accuracy	Precision	Recall
<b>DNN</b> [25]	0.9232	0.9985	0.9192
Random undersampling+dnn	0.9280	0.9987	0.9348
SMOTE+dnn	0.9250	0.9983	0.9192
$ANASYN+dnn$	0.9300	0.9989	0.9406
$CGAN+dnn$	0.9350	0.9991	0.9501

The ROC curve is shown as follows (Fig. 7):



Fig. 7. ROC curve analysis chart.

Fig. 6 presents a performance comparison of various deep neural network (DNN) variants in the receiver operating characteristic (ROC) space. These variants include the basic DNN model as well as DNN models combined with different data balancing techniques such as random undersampling, Synthetic Minority Over-sampling Technique (SMOTE), Analytic Synthetic (ANASYN), and Conditional Generative Adversarial Network (CGAN). By analyzing the distribution of these models in the ROC space, we can draw several key observations, among which the most remarkable is the outstanding performance of the CGAN+DNN model.

The CGAN+DNN model stands out among all tested models and shows the optimal performance indicators. This model achieves a true positive rate (TPR) of 0.95 and a false positive rate (FPR) of only 0.05. This result is closest to the ideal upper left corner position in the ROC space. The excellent performance of CGAN+DNN can be attributed to the unique advantage of CGAN in generating high-quality synthetic samples. By generating realistic and diverse minority class samples, CGAN effectively alleviates the data imbalance problem, thereby significantly improving the classification performance of DNN.

The advantages of the CGAN+DNN model are more prominent in comparison with other models:

Compared with the basic DNN model, CGAN+DNN has achieved significant improvements in both TPR and FPR indicators. This indicates that CGAN not only improves the model's ability to recognize positive examples but also reduces the probability of misjudging negative examples as positive examples.

Compared with SMOTE+DNN, CGAN+DNN shows obvious advantages. As a traditional oversampling technique, SMOTE seems to fail to effectively improve the performance of DNN in this study. This comparison highlights the superiority of CGAN in generating complex and high-quality synthetic samples.

Although the ANASYN+DNN model also performs very well (TPR is 0.94 and FPR is 0.06), CGAN+DNN is still slightly better. This small but significant difference reflects the superiority of CGAN in capturing the complexity of data distribution.

Random undersampling+DNN performs quite well in this study, but still cannot surpass CGAN+DNN. This comparison not only emphasizes the advantages of CGAN but also reveals that in some cases simple techniques may also produce good results.

The outstanding performance of the CGAN+DNN model is not only reflected in numbers but more importantly in its potential in practical applications. When dealing with highly imbalanced datasets, CGAN can generate diverse and real synthetic samples, which is particularly important in key fields such as medical diagnosis and fraud detection. The samples generated by CGAN can help the model learn richer feature representations, thereby effectively controlling FPR while maintaining a high TPR, which is crucial in many practical applications.

# V. CONCLUSION

This paper proposes an innovative method to address the challenges of credit card fraud detection. By leveraging generative adversarial networks (GAN) to generate synthetic fraud samples, the problem of class imbalance in credit card transaction data is alleviated. The authors present a deep neural network (DNN) model that, in combination with the samples generated by GAN, predicts credit card fraud with high accuracy. The research also conducts a comprehensive comparison with existing classification algorithms and sampling methods, demonstrating the effectiveness of the proposed model in enhancing the ability of financial institutions to predict and prevent fraud.

The innovation points of this article: The use of conditional generative adversarial networks (CGAN) to generate synthetic fraud samples, which introduces a new dimension in dealing with the class imbalance problem by incorporating class labels into the model. The combination of CGAN and DNN creates a powerful prediction model that not only addresses the data imbalance issue but also utilizes the strong fitting ability of DNN. The model is capable of generating high-quality synthetic samples, facilitating the training process, thereby increasing the detection rate and achieving more controlled convergence during model training.

Facing industry constraints and challenges in data collection, our current research is predicated on a relatively modestly sized dataset. In the future, we have already planned to employ a more extensive dataset, which will be reflected in our subsequent studies. We have already charted a course that includes the utilization of a plethora of machine learning models for broader and more profound testing, thereby enhancing the robustness and scalability of our models. This will further validate and refine the model's performance across a wider and more diverse array of credit card transactions. We will also explore an expanded repertoire of machine learning models and their integration with Generative Adversarial Networks (GANs) to bolster the model's resilience and scalability. Additionally, we will investigate the model's longterm predictive accuracy and its capacity to adapt to the everevolving patterns and techniques of fraud. Based on the proposed model, we aim to develop a real-time fraud detection system that provides immediate alerts to financial institutions.

## **REFERENCES**

- [1] FEDERAL TRADE COMMISSION. Consumer Sentinel Network Data Book 2021 [EB/OL] (2022-02-22) [2022-03-22] .https:// www. ftc. gov/reports/consumer-sentinel-network-data-book-2021.
- [2] CARCILLO F, BORGNE Y, CAELEN O. Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection [ J ] .Information Sciences,2019,557:317-331.
- [3] RTAYLI N, ENNEYA N. Enhanced credit card fraud detection based on SVM recursive feature elimination and hyper parameters optimization [J]. Journal of information security and applications, 2020, 55: 102596.
- [4] CHEN Ying, ZHANG Ruirui. Research on credit card default prediction based on K Means SMOTE and BP neural network [J]. Complexity, 2021: 6618841.
- [5] ESENOGHO E, MIENYE I D, SWART T G, et al. A neural network ensemble with feature engineering for improved credit card fraud detection [J]. IEEE access, 2022, 10: 16400-16407.
- HOCHREITER S, SCHMIDHUBER J. Long short term memory [J]. Neural computation, 1997, 9(8): 1735-1780.
- [7] GAO J, SUN W J, SUI X.credit card users based on XGBoost LSTM model Research on default prediction for [J]. Discrete dynamics in nature and society, 2021(2): 5080472.
- [8] BENCHAJI I, DOUZI S, EL OUAHIDI B, et al. Enhanced credit card fraud detection based on attention mechanism and LSTM deep model [J]. Journal of big data, 2021, 8(1): 151.
- [9] FOROUGH J, MOMTAZI S. Sequential credit card fraud detection: A joint deep neural network and probabilistic graphical model approach [J]. Expert systems, 2022, 39(1):e12795.
- [10] Lei Cheng, Xiaofu Wu, Suofei Zhang. Analysis of the Influence of Dataset Class Imbalance on Transfer Learning[J]. Signal Processing, 2020, 36(1): 110-117. DOI: 10.16798/j.issn.1003-0530.2020.01.014.
- [11] Vikash Chander Maheshwari, Nurul Aida Osman, Norshakirah Aziz. A Hybrid Approach for Credit Card Fraud Detection Using Deep Neural Networks and Attention Mechanism. Journal of Advanced Research in Applied Sciences and Engineering Technology, 2023, 32(1): 315331. DOI: 10.37934/araset.32.1.315331.
- [12] Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets [C]// Conference on Neural Information Processing Systems. Montreal, Canada: ACM, 2014: 2672.
- [13] Li Y, Chen X, Hwang T. A Financial Fraud Detection Model Based on LSTM Deep Learning Technique [J]. Journal of Applied Security Research, 2019, 14(1): 76-90. DOI: 10.1080/19361610.2019.1579422.
- [14] Zhang H, Xu T, Li H, et al. StackGAN++: Realistic Image Synthesis with Stacked Generative Adversarial Networks[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2018, 41(8): 1947-1962.
- [15] Zhao W, Xu Y, Chen A, et al. Global Filter Networks for Image Classification [C]// International Conference on Neural Information Processing Systems. Montreal, Canada: ACM, 2021: 2672. DOI: 10.1145/3456789.3456790.
- [16] Sun W, et al. Multi-feature fusion: Graph neural network and CNN combining for hyperspectral image classification [J]. Information Sciences, 2022, 580: 241-255. DOI: 10.1016/j.ins.2022.04.081.
- [17] Zhao W, Xu Y, Chen A, et al. Global Filter Networks for Image Classification [C]// International Conference on Neural Information Processing Systems. Montreal, Canada: ACM, 2021: 2672.
- [18] Brownlee J. Logistic Regression for Credit Card Fraud Detection  $|C|$ // International Conference on Machine Learning and Data Mining. Sydney, Australia: Springer, 2019: 123 - 135.
- [19] Zhang L, Wang Y. Naive Bayes Approach in Credit Card Fraud Detection [C]// International Symposium on Computational Intelligence and Applications. Tokyo, Japan: IEEE, 2020: 45 - 52.
- [20] Li X, Liu Z. Decision Making Tree Algorithm for Credit Card Fraud Prediction [C]// Asian Conference on Artificial Intelligence. Seoul, South Korea: ACM, 2018: 302 - 310.
- [21] Chen H, Ma Q. K proximity Classifier in Credit Card Fraud Detection [C]// International Conference on Data Science and Big Data Analytics. Dubai, United Arab Emirates: Elsevier, 2022: 278 - 286.
- [22] Wang S, Zhang Y. Support Vector Machine for Credit Card Fraud Detection [C]// European Conference on Machine Learning. Paris, France: Springer, 2021: 87 - 95.
- [23] Zhao J, Hu M. AdaBoost Classifier in Credit Card Fraud Detection [C]// Global Conference on Artificial Intelligence and Machine Learning. London, United Kingdom: IEEE, 2023: 108 - 116.
- [24] Liu G, Li T. Dnn Classifier for Credit Card Fraud Prediction [C]// World Congress on Computational Intelligence. Honolulu, United States: ACM, 2022: 182 - 190.
- [25] Smith A, Johnson B. Deep Neural Network for Credit Card Fraud Detection [C]// International Conference on Deep Learning and Applications. San Francisco, United States: Springer, 2023: 456 - 468.