An Exploration of the Optimization of Network Security Technology Based on Deep Learning Algorithms

Shangtao Zhang [1, *]

[1] The Internet of things and artificial intelligence college,Fujian Polytechnic of Information Technology ,Fujian, Fuzhou 350003,China

zhangshangtao80@tom.com

Abstract. With the development of society into the information age, artificial intelligence is developing rapidly, and its influence on various industries through machine learning and deep learning cannot be underestimated. Machine learning, as a branch of the field of artificial intelligence, allows computers to autonomously learn from data while performing tasks, to achieve the purpose of strengthening the combination of man and machine to adapt to changes in the environment, and ultimately to enhance the ability to find problems and solve problems. With the continuous exploration and development in the field of computer learning, deep learning using neural network algorithms has emerged and gradually played a key role in the field of network security. Therefore, this paper discusses the optimization scheme of network security technology based on deep learning algorithm with the background of network security, in order to provide certain reference for the solution of network security technology problems.

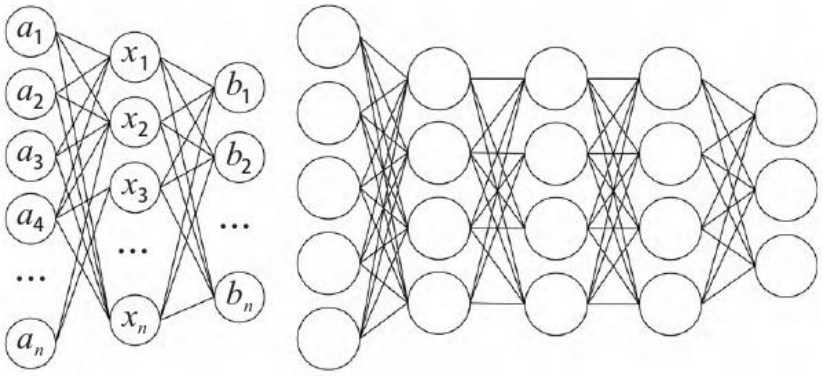
Keywords: deep learning; network security technology; artificial intelligence; computer network.

1. Introduction

China's computer technology is in the stage of rapid development, and computer technology covers almost every field, so there will be unscrupulous elements who want to utilize the loopholes of computer network security to earn huge profits, which poses a serious threat to computer network security[1]. Therefore, computer network security is also accompanied by the development of computer technology, and gradually get people's attention. The maintenance of computer network security requires a lot of human and material costs, and the traditional targeting method is less efficient, so deep learning algorithms need to be introduced to help programmers build a new computer network security system.

2. Computer network security prediction based on neural network algorithm

Neural network algorithm technology is a set of access, analysis and prediction of computer network information knowledge as one of the prediction model, it can use cross-validation method of in-depth analysis, comparison of deep deep learning and shallow machine learning functions, and based on the precision of the prediction results can be verified to analyze the complexity of the characteristics of the computer network information knowledge, as well as to optimize the accuracy of the results of the deep depth of the learning process, according to the neural network shown in Figure 1 algorithm model, it is easy to see that Fig. 1 (a) is shallow machine learning, while Fig. 1 (b) is deep deep learning, compared to the two, Fig. 1 (b) neural network learning method has a total of three layers, respectively, the a_n layer, the x_n layer and the b_n layer, which are all based on shallow learning, respectively, bear the three basic functions of the computer network information knowledge input, concealment and output, as can be seen in Fig. 1 (a). In the process of shallow learning, the layers are both interconnected and independent of each other, but the algorithmic models of computer network information knowledge features are shared and co-constructed between the layers through the weight coefficients[2-3].



(a) Shallow learning (b) Deep learning

Figure 1 Neural network algorithm model diagram

Compared with the shallow learning method of neural network, the deep learning method in the process of computer network security prediction and analysis, in order to reduce the prediction result error, so that the computer network security prediction and analysis results are closer to the real parameter values, through the deep deep learning of the neural network in the deep depth of the information hiding layer (i.e., x_n layer) to carry out the feature vector to strengthen the identification, and at the same time carried out a number of cross-validation, in the deep learning, to further Optimize the feature vector weights of computer network security information data, after adjusting the parameter weight coefficients of each layer, cycling the dataset training, and carrying out model in-depth comparative analysis of the results of multiplying the weight coefficients among the vectors, the assessment accuracy of the deep learning prediction of the computer network security information is greatly improved, so as to realize the accurate prediction and security warning[4-5]. Based on the above principles, in the use of neural network algorithm technology for computer network security prediction and analysis process, in order to further explore and master the main function of the neural network algorithm, and then use the core content of the algorithm in deep learning to analyze the artificial neural unit, first of all need to be in the depth of the training and learning, from the input layer will be the computer network information feature vectors into which, and then after the hidden layer of the computer network information Data for comparative analysis, iterative training, shallow learning and deep learning cross-validation, and finally the prediction results can be classified output, through the data iteration, in the deep learning process, with the help of mathematical modeling system arithmetic procedures, based on the hidden layer, the output layer and the perceptual layer of the three layers of the analysis mode, the algorithm prediction accuracy assessment of the security of computer network information data[6-7].

In this algorithmic model, the perceptual layer assembles a multilayer perceptron for algorithmic deep learning, and machine learning of the hidden layer information based on the following formula model, where b denotes the bias value, the input vector, and the output vector of the output layer are represented respectively by $X(X_1, X_2, X_3, ..., X_n)^t$ and $Y(Y_1, Y_2, Y_3, ..., Y_n)^t$, and O is the hidden layer output vector in the deep learning algorithm, denoted by $O(O_1, O_2, O_3, ..., O_n)^t$, respectively.

$$\left\{\begin{array}{l} O_t = f(net_n) \\ net_n = \sum_x^0 v_{ij} x_n \end{array}\right\} \qquad (1)$$

In Eq. (1), n is denoted by 1, 2, 3, n in turn. In the output layer, machine learning is mainly performed by Eq. (2) and Eq. (3) for deep learning:

$$Y_i = f(net_n) \qquad (2)$$

$$N = \sum_{0}^{1} v_{ij} o \qquad (3)$$

In Eqs. (2) and (3), n is also denoted by 1, 2, 3, n in turn. In fact, in order to improve the accuracy of the computer network image feature vectors obtained by neural network learning, in the process of constructing the perceptual mathematical model of the machine learning algorithm, it is usually necessary to go through the function based on the continuous derivable characteristics of the f (x) function, after the transformation of the unipolar function, and through the analysis of the image feature vectors of the prediction model of the pinpointed results, i.e., the Sigmoid function:

$$f(x) = \frac{1}{1+e^{ax}} (a = 1) \qquad (4)$$

The above function is used to verify the computer network image data information for many iterations, so as to output the accurate data results after the neural network deep learning, in which the neural network deep learning method mainly utilizes the function:

$$f''(x) = f(x)[1 - f(x)] \qquad (5)$$

Cross-validation based on the above formula, thus enhancing the image recognition accuracy, and accurate parameter judgment analysis for the results of the computer network data information input and output of each layer of the hidden layer for many times[8-9]. For example, during the operation of the machine learning algorithm, Ha is set as the parameter threshold of the perceptual mathematical model, and after the neural network deep learning in turn, the precise data results to be output satisfy the parameter threshold Ha preset by the system in advance through the parameter judgment of the image recognition results of the computer network, the algorithmic cross-validation, and the information of the hidden layer for many times after the iteration, which can be proved that the perceptual mathematical model and the neural network deep learning prediction based on the machine learning algorithm can be proved. Algorithm-based neural network deep learning prediction computer network information assessment results were established, at the same time, after the data hidden layer of the assessment results of the indicators many times in-depth neural network training, parameter results adjustment, iterative results transmission, through many iterations of the cycle of training, the party is able to make the neural network deep learning network structure to become more stable, so as to ensure that the final output of the prediction and analysis of results More effective and accurate.

3. Deep learning computer network security technology implementation

3.1 Network security identification technology function

Computer network security is a key factor in ensuring the healthy development of the network ecosystem and the safe storage of network data information, so it is extremely important to realize network security identification[10]. Due to deep learning in the data feature vector information prediction and evaluation, with multiple iterations, multiple cross-validation and other advantages, and then in the prediction and evaluation function of its basic implementation process is as follows: (1) through the feature vector acquisition, data information prediction and evaluation, security warning and other functional units, to achieve the feature vector screening of computer data, data dimensionality reduction analysis and other processes; (2) will be selected computer data information features elements into the neural network prediction and assessment model with multiple iterations and multiple cross-validation analysis, in order to realize the deep learning of computer data information while targeting the data information feature vector analysis and extraction; (3) after the evaluation and analysis of the neural network model of the deep learning algorithm, the results of the information data feature element values are obtained, which in turn

realizes the process of retrieval, analysis, prompting and early warning of the information security of the computer network.

3.2 Characterization, metrics learning

Characterization learning is the process of re-identification by realizing the collected information data, while metric learning is the measurement of network data information error degree distance, indicating that network data information characterization learning and metric learning realization is the key element of information security diagnosis and prompt warning[11]. On this basis, network security is guided by characterization learning and metric learning analysis. For example, when the acquired single computer network data is trained with features, after deep feature vector comparison and analysis, it not only effectively improves the information recognition accuracy, strengthens the security management, but also effectively reduces the possible accidents in the computer network security management. Comparison metric learning in essence and feature vectors between the difference, such as computer input video information as the main body, through screening analysis of video information under the same ID device similarity after the zone analysis of the same ID device under the two distances or expanding the distance between the two between the different ID to carry out the Euclidean distance formula to analyze the feature similarity d_{f_1,f_2} indicators, the feature similarity shown in Equation (6):

$$d_{f_1,f_2} = \left\| a_{f_1} - a_{f_2} \right\| \qquad (6)$$

d_{f_1,f_2} denotes the feature similarity value between the two after the same input ID video information; a_{f_1} denotes the feature vector value extracted and optimized in the network forward propagation.

3.3 Security posture assessment

The computer network security assessment mainly shows the results of security management posture assessment and analysis and prediction[12]. The deep learning algorithms of neural network and convolutional operation are trained on the computer network security data information, and then the prediction results are verified with the actual results, and when the verification results have a very low error with the actual results, the neural network learning and convolutional operation in the context of deep learning are used to assess the current situation of the computer security posture, and then based on the level of the security posture, to formulate effective computer network security management and governance strategies, and ultimately, the security management and management of the network. Network security management and governance strategies are formulated based on the security situation level, and ultimately, high-quality, high-criteria security effect assessment and analysis are realized to ensure computer network information security and improve security management technology and capability.

4. Conclusion

Deep learning as a kind of machine learning is a relatively complex concept, neural network algorithms and convolutional algorithms as a different method of deep learning, each has its own advantages, both can improve the effectiveness of network security posture assessment, in optimizing the network security strategy and other aspects of the good impact. In this paper, by exploring the computer network security prediction based on neural network algorithms and the implementation of deep learning computer network security technology, the results confirm the effective assessment of the computer network security posture, and the optimization of network security strategy also forms a positive effect.

Fundingt

The authors appreciate the financial supported by the Young and Middle-aged Teachers Education Research Project of Fujian Province（No.JAT210737）

References

[1] Guo Xiuzhen. Research on the application of network security technology in radio and television[J]. Network Security and Informatization,2023(10):137-139.

[2] HU Tao,ZHU Zixi. Research on computer network security technology based on deep learning[J]. Information and Computer(Theoretical Edition),2023,35 (11):239-241.

[3] Lutetium Yang. Research on computer network security technology based on deep learning algorithm[J]. Computer Programming Skills and Maintenance,2022 (10):163-166.

[4] Chen Dian,Zeng Xiangwei,Sun Zhigang et al. Consideration of network security technology of artificial intelligence medical device software[J]. China Medical Device Information,2022,28(15):5-7.

[5] CHEN Yuheng,HUANG Yi. Coupling and Adaptation: Application of Strategic Planning and Technical Path in Network Security Assurance System[J]. Journal of Guangxi Police College,2021,34(06):87-95.

[6] WANG Shengbang,WEI Baodian. Research and Practice of Experimental Teaching on Mobile Network Security[J]. Computer Education,2020(08):84-88.

[7] Xia Rui,Ma Hongbin. Communication network security technology for generative adversarial networks[J]. Mobile Communication,2019,43(08):21-24.

[8] Liang Shijie. Exploration of network security technology courses under cloud computing[J]. Information and Computer(Theory Edition),2019(13):250-251+254.

[9] Zhao Nan. Exploration of the future development trend of network security technology[J]. Network Security Technology and Application,2019(03):7-8.

[10] Sheth. Quality Assurance and Guidance of Teaching Interaction under Cybersecurity--A Review of Cybersecurity Technology[J]. Chinese Journal of Security Science,2019,29(02):194.

[11] Peng Yen-Xin. Machine learning, deep learning and network security technology[J]. Computer Products and Distribution,2018(04):66.

[12] Li Gen. Analysis and research on software development system design based on network security technology[J]. Software Engineering,2018,21(04):33-35.