ISSN: 2710-0588

Industrial Internet Intrusion Detection Method based on Cloud-Edge Collaboration

Jinhai Song[1, 2, *], Zhiyong Zhang[1, 2]

[1]School of Information Engineering, Henan University of Science and Technology, Luoyang 471000, China

[2]Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science and Technology, Luoyang 471023, China

*18331665373@163.com

Abstract

Industrial Internet security incidents occur frequently, and the amount of industrial data is increasing exponentially. Efficient and correct detection of attacks is critical to industrial Internet security. The method is based on the concept of cloud-edge collaboration to detect malicious behaviors. Firstly, the data is normalized and preprocessed to reduce the differences caused by different feature scales, then the deep neural network(DNN) is used to extract the features of massive data, and finally the softmax function is used for classification. In order to verify the effectiveness of the model, it is evaluated on the NSL-KDD dataset and the GAS dataset, and compared with other traditional models, the model has higher precision and recall. This method integrates edge-cloud collaboration and deep learning models, which can effectively reduce edge load and improve model performance, and has a good application prospect.

Keywords

Cloud Edge Collaboration; Industrial Internet; Deep Learning; Intrusion Detection; Deep Neural Network.

1. Introduction

During the vigorous development of the Industrial Internet, the amount of industrial data has increased exponentially compared with the past, and a large amount of industrial data is collected and stored in the industrial network. As each module in the industrial network is more closely related, it is also more complex, and the probability of being attacked by unpredictable also increases. These cyber attacks may bring disasters such as industrial data leakage and property loss to industrial enterprises. The traditional network attack identification mode can no longer guarantee the continuous and stable operation of industrial application scenarios. The essential goal of the industrial control system is control, and the core goal of the Internet is exchange. Compared with the point-to-point transmission mode of equal relationship adopted by the traditional Internet, the industrial Internet mostly adopts the non-peer network based on the master-slave relationship. The security challenges faced by the Industrial Internet need to be viewed from the perspective of the security protection capabilities of industrial control systems. From the perspective of industrial control system design ideas, the traditional design of industrial control systems uses dedicated, relatively closed and reliable communication lines. However, with the transfer of industrial control systems to the Internet and the integration with other business applications of enterprises, they are also more and more vulnerable to attacks from the Internet, exposing many inherent defects.

From the perspective of industrial control system operation and maintenance, many companies have opened up the remote debugging function because the industrial control system is closed.

ISSN: 2710-0588

At the same time, they did not consider the access control of remote debugging. Many attacks exploit the access control loopholes of remote debugging to achieve penetration. From the perspective of industrial control system communication protocols, the vast majority of industrial control system communication protocols do not consider confidentiality issues at the beginning of design, and basically use plaintext transmission, and most countries have not yet established their own, secure industrial Internet communication protocols, Data exchange protocol.

Through intrusion detection technology, it is possible to monitor abnormal data on the edge side such as hosts and networks. With the widespread application of cloud computing, cloud computing centers have gathered a large amount of data. Cloud centers have powerful processing performance and can handle massive amounts of data. But cloud computing has two limitations. One is the weight of the data. Because the data requires a large amount of storage space and bandwidth, the communication transmission is congested. The other is the delay. It takes time to transmit massive data, and it also takes time for the cloud center to process the data, which will increase the request response time. With the development and perfection of technologies such as edge computing, artificial intelligence, and cloud computing, research in many fields adopts a cloud-edge collaboration approach. Different from ordinary intrusion detection, this paper proposes a cloud-edge collaborative industrial Internet intrusion detection method. This method fully considers possible false positives and other problems and ensures a high accuracy rate.

The rest of this paper is organized as follows. Section 2 contains the analysis and discussion of related work. In Section 3, we propose a development method for creating an industrial Internet intrusion detection scheme based on cloud-edge collaboration. The validation and experimental validation results of the case study are presented in Section 4. Finally, in Section 5, we provide concluding observations and guidelines for future work.

2. Related Work

With the proposal and development of the Internet of Everything, security and privacy challenges have become major concerns for billions of IoT smart devices. Among them, the security of the industrial Internet needs to be paid attention to urgently. Due to the inherent security problems of industrial equipment, it is more vulnerable to external malicious attacks and other destructive behaviors.

In order to solve the problem that high-dimensional and large-scale data significantly increase training, retraining and detection time, resulting in low scalability, Chen et al. [1] proposed a method based on deep belief network (DBN) and long-term short-term A detection algorithm for memory (LSTM) networks. Latif et al. [2] proposed a lightweight Dense Random Neural Network (DnRaNN) intrusion detection method, which is very suitable for resource-constrained Internet of Things (IoT) due to its inherent generalization ability and distributed characteristics. Implemented in the network, fast and flexible, and verified on the ToN_IoT dataset. Han et al. [3] proposed an improved temporal multi-graph convolutional network for false data injection attack detection. False data injection attack (FDIA) detection is of great significance to the stable operation of modern smart grids.

Comprehensive analysis, low false positive and high-precision detection methods are the key to malicious behaviors such as intrusion. However, the parameter calculation of the detection algorithm consumes resources of the edge controller and affects its performance, and the resources of the edge controller are extremely limited and cannot undertake a large number of computing tasks. Therefore, we propose a new cloud-edge collaborative architecture, which separates the preprocessing calculation of abnormal traffic data detection such as malicious intrusion from the edge device, improves the efficiency and stability of detection, and selects a

ISSN: 2710-0588

deep neural network (DNN) that can theoretically fit all functions for experimental demonstration.

3. Method Design

First, the captured data is uploaded to the cloud, and then the detection model deployed on the cloud processes it and obtains the evaluation results. However, uploading the captured data to the cloud may not be able to obtain evaluation results more efficiently, because the delay between the cloud server and the edge device is large, and the model and results cannot be transmitted to the edge in a timely and fast manner. Therefore, this paper proposes a A new cloud-side collaborative intrusion detection framework.

3.1. Cloud-edge Collaborative Intrusion Detection Method

In this paper, a cloud-edge collaboration framework based on the industrial Internet is used to detect anomalies using data from industrial networks. The whole framework mainly includes edge and cloud. The edge end is an edge computing platform close to the data source and an extension of the cloud server. The cloud is the main platform, using technologies such as cloud computing, big data analysis, and machine learning. The specific implementation of the cloud-edge collaborative intrusion detection method is: first upload the data collected by the edge detection equipment to the cloud for storage and analysis, and then train the intrusion detection model on the cloud and send it to the edge for intrusion detection, realizing the collaboration between the cloud and the edge. The general cloud-edge collaboration method is to train the model on the cloud. After the model is trained, it is sent to the edge, and then the edge detects it. The cloud-side collaboration proposed in this paper, on the basis of the above, the edge should also have its own lightweight detection model, a large amount of data captured by the edge is uploaded to the cloud for evaluation, and the lightweight detection model at the edge can quickly analyze the traffic data. Process, train and evaluate. The architecture of the cloud-side collaborative detection model is shown in **Figure 1**. In actual production, it is tested in parallel with the model delivered by the cloud, and the final detection result is weighted and averaged by combining the probability values of the detection results of the two models, and finally the evaluation result of the detection is given. The cloud model is regularly updated and sent back through the data continuously collected at the edge, and the lightweight model at the edge is also regularly updated to ensure the performance of the model.

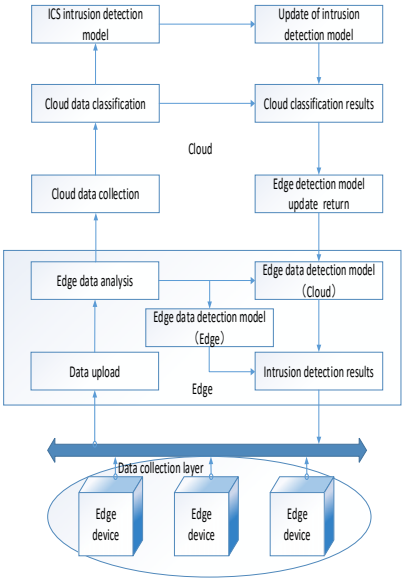

Figure 1. Industrial Internet intrusion detection model for cloud-edge collaboration

ISSN: 2710-0588

3.2. Cloud Training

The cloud collects and manages large amounts of data that can be used for training. The data collected from each edge device has different data scope and format. Therefore, it is necessary to convert the collected data into an appropriate format and preprocess it for use in machine learning models. This article mainly focuses on the model sent from the cloud to the edge.

3.3. Edge Test

Through the model delivered by the cloud and the lightweight model at the edge end, the data is jointly detected at the edge end and a reasonable evaluation is given.

3.4. Data Description

The selected data sets are the NSL-KDD [4] data set and the GASpipeline data set [5]. These two data sets are relatively representative of the traffic data that will appear in the industrial Internet, and both have sufficient data for learning and training , in order to simulate the problem of massive industrial flow data faced by the cloud. See Table 1 and
Table **2** for the labels and label values of the data sets selected in this paper.

Table 1. Samples label of data set KDD

Label Name	Label Value
DoS	0
Normal	1
Probing	2
R2L	3
U2R	4

Table 2. Samples label of data set Gaspipeline

Label Name	Label Value
Normal	0
NMRI	1
CMRI	2
MSCI	3
MPCI	4
MFCI	5
DoS	6
Reconnaissance	7

3.5. Data Preprocessing

In the data preprocessing, the data is balanced first, so that the category distribution of the training set and the test set converge, and the two do not overlap each other, so as to simulate the real traffic data. The features in the original data are normalized so that they are distributed in (0, 1), so as to avoid affecting the performance of the model due to the occurrence of large or small extreme values among the features. The character features in the data are processed by one-hot encoding, and the digital features are standardized by min-max. Then the processed data is input into the DNN model for feature learning, and the learned data is used for modeling, and finally the detection model is constructed through multiple rounds of training.

3.6. Build DNN Model

A deep neural network can also be called a multi-layer perceptron. A multilayer perceptron is a very powerful neural network model that can learn nonlinear functions of complex data. The

ISSN: 2710-0588

method uses forward propagation to build weights, then calculates the loss, and backpropagation is used to update the weights, thereby reducing the loss. In theory it can describe problems of any complexity. Because each activation function implements nonlinear processing of the input, and then superimposes through a multi-layer network, as long as the parameters are appropriate, it can theoretically fit any function. The larger the number of hidden layers, the higher the complexity that can be expressed. A foreign team proposed an architecture that abandons convolution and self-attention and fully uses a multi-layer perceptron [6]. Its performance is comparable to CNN and ViT. Although it is in the field of computer vision, it also proves that DNN has superior solutions problem ability. Therefore, in this paper, we decided to choose DNN to extract features of network behavior data. The intrusion detection process of this model is shown in Figure 2.

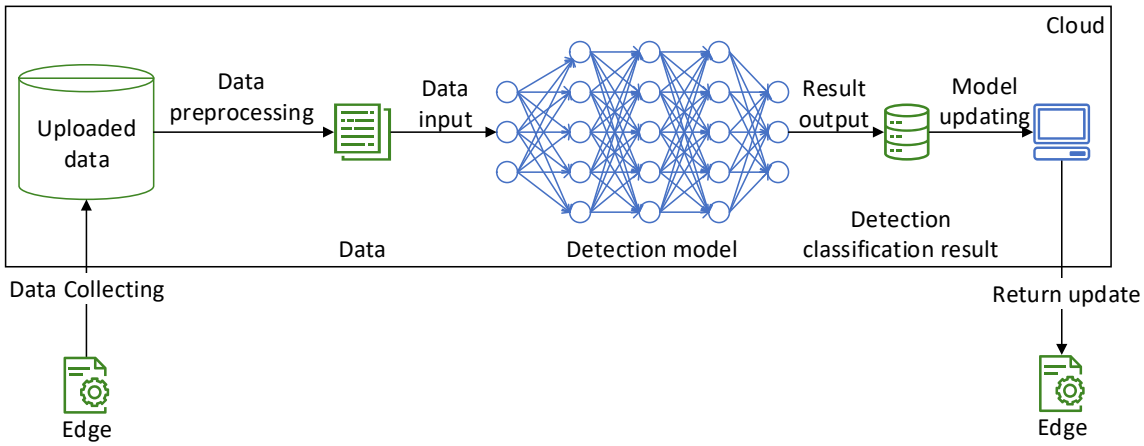

Figure 2. Flow chart of IDS

4. Experiment

4.1. Experiment Environment

The experimental test environment in this article is Windows 10 PC, Intel(R) Core (TM) i5-7300HQ CPU @ 2.50GHz, 8.00GB RAM. Use Sklearn, keras, tensorflow libraries in the Python language to implement algorithms.

4.2. Model Parameters

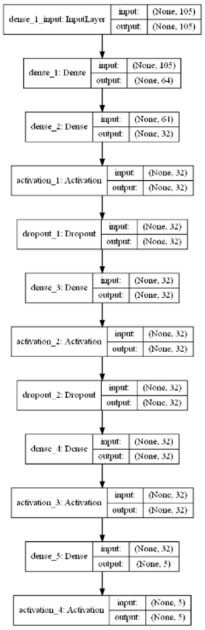

Figure 3. Algorithm model diagram. Network layer and its input and output

ISSN: 2710-0588

The overall structure of the model and the parameter settings of each layer of the DNN network selected in this paper are shown in **Figure 3**. In order to avoid model overfitting, a Dropout layer is added. The Dropout layer will randomly discard neurons, get rid of the dependence between neurons, and improve Generalization performance. The activation function uses the LeakyRelu function to avoid the gradient disappearance that may occur in the deep neural network. Its expression is shown in formula (1), a is a constant between (0,1):

$$f(x) = \max(ax, x) \tag{1}$$

4.3. Experimental Results

Put the preprocessed KDD data into the selected model for fitting training, choose categorical crossentropy as the loss function, and choose adam as the optimizer. Under the same conditions, compared with other traditional models, the experimental results are shown in Table 3. Comparing the numerical values of each indicator, it can be seen that the selected DNN model has a better performance, and has a higher accuracy rate and recall rate. The accuracy curve and loss curve of DNN are shown in Figure 4 and Figure 5.

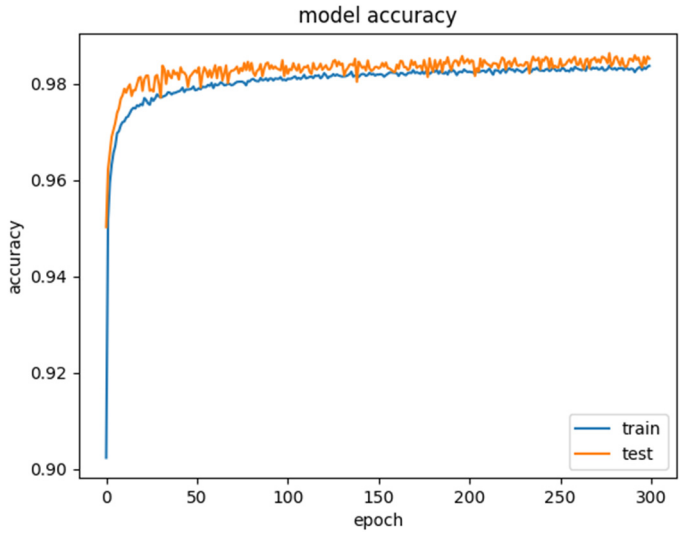

Figure 4. Training curves of the KDD

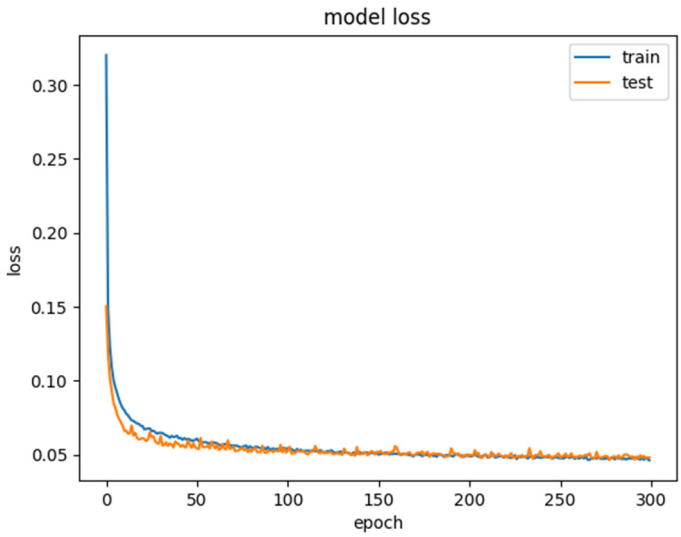

Figure 5. Loss curves of the KDD

ISSN: 2710-0588

Table 3. Multi-Classification accuracy of KDD (%)

	Accuracy	F1-Score	Precission	Recall
RandomForest	97.95	85.83	94.83	81.44
NaiveBayes	73.18	56.28	56.50	76.08
SVM	95.15	65.11	89.53	62.60
DNN	98.50	91.07	92.67	89.71

At the same time, we put the same preprocessed GAS data set into the DNN model, modify the corresponding input and output, and conduct training and testing. Good evaluation indicators have also been achieved on the GAS dataset, indicating that the model selected in this paper has a certain generalization ability. The experimental results are shown in Table 4, and the accuracy curves and loss curves are shown in Figure 6 and Figure 7.

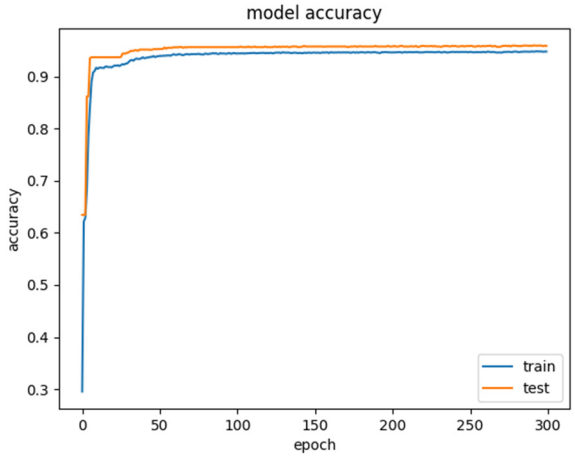

Figure 6. Training curves of the GAS

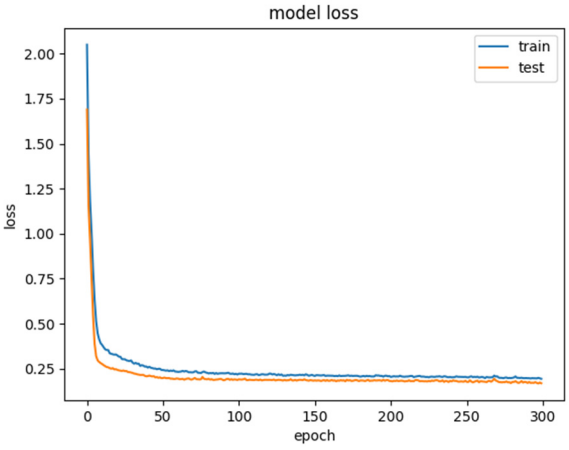

Figure 7. Loss curves of the GAS

Table 4. Multi-Classification accuracy of GAS (%)

	Accuracy	F1-Score	Precission	Recall
DNN	94.16	83.44	85.55	81.94

Based on the above experimental results, it can be seen that DNN performs well on these two data sets. In the KDD data set, the comprehensive performance is better than that of RF, SVM and NB models; followed by the RF model, its detection accuracy is 97.95%, and other

ISSN: 2710-0588

indicators are higher than 80%. In terms of recall rate, these models can reach higher than 60%, but in the other three evaluation criteria, only DNN has better performance, and the values are all higher than 90%.

5. Conclusion

This paper proposes an industrial Internet intrusion detection method based on cloud-edge collaboration. The model selected in this article is more suitable for the cloud. The edge end uploads the data, and the cloud classifies the data and returns the model. Perform normalization and other preprocessing on the data set in the cloud, extract the complex features in the massive data through DNN, and classify them according to the extracted features, and then send the built model to the edge device from the cloud to ensure the accuracy rate; At the same time, the advantages of DNN itself and the powerful computing power of the cloud can modify the depth of the model when facing more complex problems to better fit actual problems. Experimental verification shows that the accuracy and recall of this method on the KDD and GAS datasets are both good. However, this model has obvious deficiencies. In the face of new unknown attacks, it may need to be retrained. The next step is to consider introducing incremental learning and adding a lightweight intrusion detection model on the edge side to achieve complete cloud-side collaborative intrusion detection and optimize learning performance, improve generalization and improve training efficiency.

References

[1] Ag Chen, Y Fu, X Zheng and G Lu: An efficient network behavior anomaly detection using a hybrid DBN-LSTM network, Computers & Security, Vol. 114(2022), p.102600.

[2] S. Latif et al.: Intrusion Detection Framework for the Internet of Things Using a Dense Random Neural Network, IEEE Transactions on Industrial Informatics, Vol. 18 (2022) No.9, p.6435-6444.

[3] Yh Han, Ht Feng, Kk Li and Q Zhao: False data injection attacks detection with modified temporal multi-graph convolutional network in smart grids, Computers & Security, Vol. 124 (2023), p. 103016.

[4] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani: A detailed analysis of the KDD CUP 99 data set, IEEE International Conference on Computational Intelligence for Security & Defense Applications (2009).

[5] T. Morris, W. Gao: Industrial Control System Traffic Data Sets for Intrusion Detection Research, International Conference on Critical Infrastructure Protection (2014), p.65–78.

[6] I. Tolstikhin, N. Houlsby, A. Kolesnikov, et al.: MLP-Mixer: An all-MLP Architecture for Vision, Neural Information Processing Systems (2021).