Quantitative selection of secure access policies for edge computing side terminals

Aidong Xu[1], Qianru Wang[2], Yixin Jiang[1], Runfa Liao[2], Yunan Zhang[1], Yi Chen[3], Hong Wen[2], Jinran Du[1]

1. Electric Power Research Institute, China Southern Power Grid Co., Ltd. Guangzhou, China

2. School of Aeronautics and Astronautics, University of Electronics Science and Technology of China, Chengdu 611731, China

3. National Key Lab of Comm., University of Electronics Science and Technology of China, Chengdu 611731, China

Keywords: edge computing security, terminal access, quantitative assessment, strategy selection

Abstract: As a new computing model in the era of Internet of things, edge computing has the characteristics of distributed, “data first entry”, relatively limited computing and storage resources, which make it not only face the widespread network attacks in information systems, but also inevitably introduce some new security threats, which need to implement end-to-end protection. Therefore, this paper mainly studies the terminal access security in the edge computing system, and puts forward the terminal security access strategy selection scheme based on BP neural network, which can comprehensively evaluate the security risks and threats faced by the terminal and data, select the appropriate algorithm according to the actual needs of the system, and select the security access strategy of the terminal on the edge computing side through quantitative objective standards, so as to realize the edge computing side Maximum optimization of safety performance of edge computing system.

1. Introduction

With the rapid development of centralized processing methods, the Internet of Things technology has gained widespread popularity in recent years [1]. In addition, the fifth generation (5G) network era has achieved more flexible, intelligent, efficient, and open network connections, and has promoted the Internet of Everything (IoE) [2]. The core of the Internet of Things is to collect massive data from terminal devices [3]. The number of terminal devices that need to be connected reaches billions or even trillions. Traditional cloud computing models have been unable to meet heterogeneous, low-latency, dense network connections. Access and service needs [4]. In this context, edge computing has emerged. However, the rise of edge computing also brings new security challenges. Due to the openness and heterogeneity of edge-side terminal equipment and relatively limited computing and storage resources (compared to cloud computing), the breadth and difficulty of access control and protection has increased significantly, and end-to-end protection needs to be implemented [5].

At present, most of the research on terminal security access strategies in edge computing systems draw on traditional information security protection technologies, without fully considering the characteristics of edge computing systems such as low latency, limited device resources, and massive terminal heterogeneity [6]. In order to solve these problems, a more feasible method is to use physical layer security technology [7]. A commonly used technology is radio frequency fingerprint identification [8].

Based on the above analysis, this paper mainly studies the terminal access security issues in edge computing systems, and proposes a terminal security access policy selection scheme based on BP neural network. According to the actual application requirements of the edge computing system terminal side, under the limited computing environment resources, flexible and targeted terminal security access is achieved to meet the requirements of low latency of edge computing systems. In the second section it is going to present the algorithm of selecting secure access strategy of edge

  DOI: 10.25236/icicta.2019.013

computing side terminal. In the third section, it is going to give a numerical example based on BP. Then, the article ends with a comment.

2. Method for selecting secure access strategy of edge computing side terminal

This article mainly studies the quantitative method for selecting secure access to terminals on the edge computing side. The research content includes comprehensive assessment of terminal security risks and threats based on the analytic hierarchy process [9]. A quantitative objective criterion is proposed for selecting secure access to terminals on the edge computing side, including steps:

1) Set the quantified security risks and corresponding security risk levels for terminals and data applications under the edge computing system. Each type of security risk consists of three dimensions: system risk, destructive power, and vulnerability. Evaluation matrix of security threats for various threats:

$$A=\begin{Bmatrix} a_1^1 & a_2^1 & a_3^1 \\ a_1^2 & a_2^2 & a_3^2 \\ \vdots & \vdots & \vdots \\ a_1^s & a_2^s & a_3^s \end{Bmatrix} \tag{1}$$

In the matrix, a_t^v is the quantified value of the t dimension of the v security risk facing the terminal or data application, $t=1,2,3, v=1,2,\cdots s$, s is the total number of security risks, and v is the serial number of the security risk type;

2) Quantitative risk of each terminal W_i:

$$W_i=\left\{w_1^i, w_2^i, \cdots w_s^i\right\}$$

$$w_v^i=\frac{\sum_{t=1}^{3} a_t^v}{\sum_{v=1}^{s}\sum_{t=1}^{3} a_t^v} \tag{2}$$

In formula (2), w_v^i is the quantified value of the vth security risk faced by the ith terminal or data application, $i=1,2,\cdots k,\ v=1,2,\cdots,s$, k is the total number of terminals and data applications, and i is the terminal serial number variable;

3) Evaluation matrix of security policy set on the edge side:

$$B=\begin{Bmatrix} b_1^1 & b_2^1 & \cdots & b_p^1 \\ b_1^2 & b_2^2 & \cdots & b_p^2 \\ \vdots & \vdots & \ddots & \vdots \\ b_1^s & b_2^s & \cdots & b_p^s \end{Bmatrix} \tag{3}$$

b_j^v indicates that the edge side adopts the jth security policy for the vth security risk, p is the number of security policy types, and j is the serial number of the security policy type;

4) Calculate the security protection quantification value Z^i after applying the security policy to each terminal or data on the edge side:

$$Z^i=W_i\cdot B=\left\{Z_1^i \quad Z_2^i \quad \cdots Z_j^i \quad \cdots \quad Z_p^i\right\} \tag{4}$$

In Formula (4), Z_j^i is a quantified value of security protection after applying the jth security policy to the ith terminal or data;

5) The edge side selects a security policy based on the actual security protection quantified value Z^i .When only a single security policy is selected, the maximum value of Z_j^i in Z_j^i is directly

selected. When a combination of two or more security policies is required, a machine learning method and a deep learning algorithm are used to select based on the quantitative protection value Z_j^i of the security protection [10].

3. Implementation scheme based on BP neural network

3.1 Terminal security access policy selection process

The technical solution of this article is described in further detail in combination with the method of BP neural network.

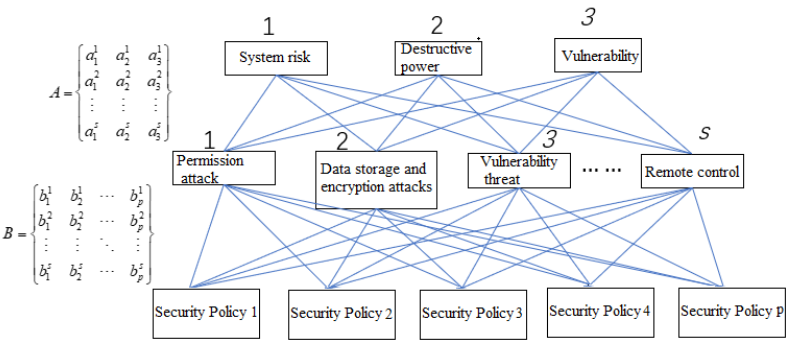

Figure 1. Terminal security risk-policy relationship model

First, establish a relationship model between the security policy of the edge computing device and the risk of the terminal or data application, as shown in Figure 1. The edge computing system includes an edge-side computing device and a terminal device, and the connection between the edge-side computing device and the terminal device is a wireless connection or a wired connection. Possible security risks of terminal or data applications include: permission attacks, data storage and encryption attacks, vulnerability threats, and remote control [11]. Edge computing devices need to respond to the risks of terminal or data applications according to security policies. The security policy method and the number of security policies adopted by the edge-side computing device can be set according to the requirements of the network system.

According to the terminal and data application requirements and the security risks faced by the edge computing system, quantified values and classifications are shown in Table 1. The quantified security risk of each threat can be determined by methods such as empirical value and expert assessment.

Table 1. Security level division table

Security Risk Grade		Quantitative value of security risk				
		0～2	2～4	4～6	6～8	8～10
Security risk dimension	System risk	Very low	Low	Medium	High	Very high
	Destructive force	Very weak	Weak	Medium	Strong	Very strong
	Vulnerability	Very low	Low	Medium	High	Very high

An example of specific terminal quantification is given below.

1) Based on Table 1 and expert experience, it is assumed that the security threats that the terminal faces under the edge computing system include permission attacks, data storage and encryption attacks, vulnerability threats, and remote control. Each type of security risk is composed of three dimensions: system risk, destructive power and vulnerability. The risk assessment matrix is:

$$A=\begin{bmatrix}1 & 3 & 7\\ 5 & 7 & 9\\ 3 & 5 & 1\\ 1 & 5 & 7\end{bmatrix} \tag{5}$$

2) The terminal's quantified risk is calculated according to equation 2:

$$W=\{0.204,0.389,0.167,0.241\} \tag{6}$$

3) Provide a set of security access policies based on system security requirements. And adopt an evaluation standard of 1-9 to obtain the security access policy evaluation matrix:

$$B=\begin{bmatrix}1 & 5 & 7\\ 5 & 7 & 3\\ 3 & 5 & 1\\ 5 & 1 & 7\end{bmatrix} \tag{7}$$

4) Calculate the security protection quantification value Z after the terminal adopts the corresponding security access policy:

$$Z=W\bullet B=\{3.855,4.819,4.449\} \tag{8}$$

5) The terminal selects a security policy based on the actual security requirements of the system in which it is located, based on the quantified security protection value Z obtained. Based on the quantitative evaluation of the risk of the terminal, a third security access policy should be considered at this time to achieve the terminal security Access and the system's security performance is maximized.

3.2 BP neural network Model ensemble and training

The edge device can select multiple security policies from p security policies to protect the terminal at a time. According to the complexity of each security policy, the BP neural network method is used to select according to the quantitative value of equation (4), the model ensemble and training process is as follows:

A. The edge device determines the number of terminals k according to the number of data sets, the number of security policy types p, and the security policy is expressed as y_j^i $(i=1,2,\cdots k;\ j=1,2,\cdots p)$, obtain training samples according to the steps in section 3.1, that is to say, adopt the jth security policy for the ith terminal. That is to say, the jth security policy is adopted for the ith terminal, and the security quantified value in formula (4) is the security policy y_j^i is combined into a data set $D=\{(Z_1,y_1),(Z_2,y_2),\ldots,(Z_k,y_k)\}$.

B. Divide the data set D, take the first m items of data set D as the training set T, and the next n items as the test set S, $k=m+n$. That means, the training set $T=\{(Z_1,y_1),(Z_2,y_2),\ldots,(Z_m,y_m)\}$, the proportion of the data set is $\frac{m}{m+n}*100\%$, the test set $CHE=\{(Z_{m+1},y_{m+1}),(Z_{m+2},y_{m+2}),\ldots,(Z_{m+n},y_{m+n})\}$, the proportion of the data set is $\frac{n}{m+n}*100\%$.

C. Determine the BP neural network structure, as shown in Figure 2. The BP neural network includes an input layer of N1 nodes, a hidden layer containing N2 nodes, and an output layer containing N3 nodes. The output layer passes the calculated loss back to the nodes in the network.

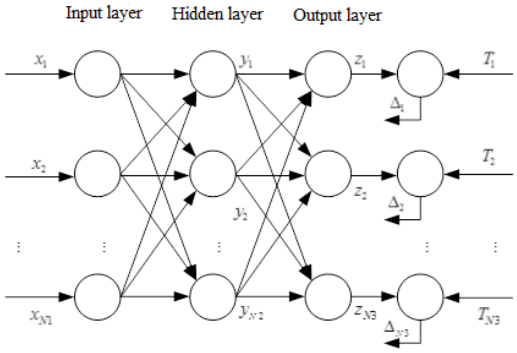

Figure 2. BP neural network structure diagram

D. Use the training set $T=\{(Z_1,y_1),(Z_2,y_2),\ldots,(Z_m,y_m)\}$ to train the BP neural network.

E. After training, input the test set $CHE=\{(Z_{m+1},y_{m+1}),(Z_{m+2},y_{m+2}),\ldots,(Z_{m+n},y_{m+n})\}$ into the BP neural network to get the corresponding security policy.

4. Conclusions

This article discusses terminal security under edge computing, and proposes a quantified method for selecting security access policies for edge-side terminals. It can achieve security performance and complexity through the quantified relationship between the security policies of edge computing devices and the risks of terminals or data applications. Comprehensive evaluation to achieve the most resource-saving and maximum optimization of edge computing system security performance under security requirements.

Acknowledgement

This work is supported by National major R&D program (2018YFB0904900, 2018YFB0904905).

References

[1] Fei Pan, Zhibo Pang, Michele Luvisotto, Ming Xiao, Hong Wen, Physical-Layer Security for Industrial Wireless Control Systems: Basics and Future Directions, IEEE Industrial Electronics Magazine, vol. 12, Issue 4, pp. 18-27, Dec. 2018.

[2] Jie Tang, Hong Wen, Kai Zeng, Run-fa Liao, Fei Pan, Lin Hu, Light-weight physical layerenhanced security schemes for 5G Wireless Networks, IEEE Network. Volume: 33, Issue: 5, pp. 126 – 133, Sep. 2019.

[3] Feiyi Xie, Hong Wen, Yushan Li, Songlin Chen, Lin Hu, Yi Chen, and Huanhuan Song，Optimized Coherent Integration-Based Radio Frequency Fingerprinting in Internet of Things, IEEE Internet of Things Journal, Vol. 5, Issue 5, pp. 3967-3977, Oct. 2018.

[4] Yuanpeng Xie, Hong Wen, Bin Wu, Yixin Jiang, Jiaxiao Meng, A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing， IEEE Transaction on Cloud Computing, vol.7, no2, PP. 383 - 391, April 2019.

[5] Songlin Chen, Hong Wen, Jinsong Wu, Wenxin Lei, Wenjing Hou, Wenjie Liu, Aidong Xu, Yixin Jiang, Internet of Things Based Smart Grids Supported by Intelligent Edge Computing, IEEE Access, vol.7, pp. 74089 – 74102, 03 June 2019.

[6] Liufei Chen, Yushan Li, Hong Wen, et al. Block Chain Based Secure Scheme For Mobile Communicatio, CNS2018.

[7] Fei Pan, Zhibo Pang, Ming Xiao, Hong Wen, Run-Fa Liao, "Clone Detection Based on Physical Layer Reputation for Proximity Service", IEEE Access, vol. 7, pp. 3948-3957, Feb. 2019.

[8] Yi Chen, Hong Wen, Huanhuan Song, Songlin Chen, Feiyi Xie, Qing Yang, Lin Hu, Lightweight one-time password authentication scheme based on radio frequency fingerprinting, IET Communications, 12(12): 14477-1484, March 2018.

[9] G Wang, Q Song, X Zhu. An improved data characterization method and its application in classification algorithm recommendation, Applied Intelligence, 2015, 43(04):892-912.

[10] Qing Yang, Yixin Jiang, Aidong Xu, Hong Wen, Feng Wang, LiuFei Chen, Kai Ouyang, Xinping Zhu, “A Model Divides the Mobile Security Level Based on SVM,” in Proceedings of IEEE CNS 2017, LasVegas, USA, 7-9 Oct., 2017.

[11] Idrees F , Rajarajan M , Conti M , et al. PIndroid: A novel Android malware detection system using ensemble learning methods[J]. Computers & Security, 2017, 36-46.

[12] Q. Jia, L. Guo, Z. Jin, et al. Privacy-preserving data classification and similarity evaluation for distributed systems, 2016 IEEE 36th International Conference on Distributed Computing Systems, 2016, 690-699.

[13] Yushan Li, Liufei Chen, Jie Chen, et al. A Low Complexity Feature Extraction for the RF Fingerprinting Process, CNS2018.