International Journal of Intelligent Information and Management Science
ISSN: 2307-0692, Volume 9, Issue 3, June, 2020

Adaptive Security Model of Dynamic Network Information Communication in Cloud Computing

Zhiqiang Wang
Department of Information Engineering, Jiyuan Vocational and Technical College, Jiyuan, 459000, China

Abstract: Under cloud computing, the structure that traditional model predicts the virus in dynamic network information communication can't satisfy its accuracy. Therefore, the optimization design of dynamic network information communication security adaptive model under cloud computing is carried out. Through dynamic network attack signal data acquisition, the data collection results classify the communication security adaptive virus data, and finally through the network information communication security situation prediction the dynamic network information communication security assessment can be achieved. By comparison experiments, it is proved that the predicted results obtained by the optimized model are closer to the actual virus level with higher prediction accuracy, so it is more suitable for the information communication security detection of dynamic networks in cloud computing environment, providing a more secure and reliable transmission environment for data information.

Keywords: Cloud computing; Dynamic network; Information communication; Security adaptation

1. Introduction

Cloud computing is a technology to transfer computing and data from traditional computers to the big data center. Computer devices in the entire network environment can be virtualized into a completed pool of resources, sending various applications and related basic settings to the network as service content through pay-as-you-go. Computer users can use equipment and applications of different sizes and reliability over the Internet at a small cost, without having to consider the complex operating content of facilities and installation, maintenance, etc. With the spread of big data technology, cloud computing environments are home to a large number of cheap, low-reliability infrastructures. Because these facilities are fragmented in a cloud computing environment, the security and reliability of data information is bound to be threatened. Therefore, in order to ensure the security and stability of the cloud computing environment, the distribution of data information storage is usually used to ensure the security of data, and by increasing a large amount of storage space and higher performance computing power ensure better service quality. Information security detection in cloud computing is an important basis for resource allocation, task scheduling, load balancing and other operational links. It can not only find out specific problems in the cloud computing environment on a node, but also achieve real-time monitoring of data status to find problems quickly, and to save more time for repair. Based on this, this paper conducts a study on the design of the adaptive mode of dynamic network information and communication security under cloud computing.

2.Dynamic Network Information Communication Security Adaptive Model Design under Cloud Computing

Environment under the cloud computing is the network operating environment that virtualizes the storage of a large number of Internet computing resources. The adaptive model of dynamic network information communication security in cloud computing is proposed. The model is divided into four levels and a center. The four levels are the signal acquisition layer, the data classification layer, the security situation prediction layer and the third-party regulatory layer; the center refers to the adaptive system for dynamic network information construction. Because the third-party regulatory layer and the dynamic network information system cannot be changed in technology, this paper design and describe the signal acquisition layer, the data classification layer, the security situation prediction layer on the basis of the traditional model of information system and the existing third-party regulatory layer.

2.1. Dynamic network attack signal data acquisition in cloud computing environment

The signal acquisition layer design for the dynamic network information communication security adaptive model under cloud computing is mainly used to collect the data generated in the network attack signal. In this paper,

the whole dynamic network information communication security adaptive model is regarded as a typical autonomous model of continuous three-dimension, using the three-dimensional continuous autonomy method to simulate the typical network attack mode existing in the cloud computing environment. Based on the typical network attack pattern, the threat index of various servers in the dynamic network and the threat index on the host are calculated. The calculation formula is shown in (1):

$$\begin{cases} m_a = g(m_{a-1}) + i_a \\ n_a = h(m_a) + j_a \end{cases} \tag{1}$$

In the formula (1), m_a represents the time of sampling virus data in the event of an attack on a dynamic network in a cloud computing environment; n_a represents the logging information used for intrusion detection devices in a cloud computing environment; g represents the sampling time series of virus data generated when a dynamic network is attacked in a cloud computing environment; h representsa directory when a dynamic network is attacked in a cloud computing environment, i_a and j_a represents interference item detected by an intrusion detection device in a cloud computing environment. The range for m_a and n_a is within the maximum threat tolerance of dynamic networks. According to formula (1), the security situation index for information communication in the event of an attack on a dynamic network is calculated:

$$y(\alpha_a) = \frac{\theta\Gamma(\frac{u_a}{2}) \cdot |u_a\pi|^{-\frac{1}{2}}}{\Gamma(\frac{u_a}{2})} \tag{2}$$

In formula (2), $y(\alpha_a)$ is represented as the security situation index of information communication in the event of an attack on a dynamic network; α_a is represented as an information feature; θ is represented as a feature of reconstructed network virus data, u_a is represented as a state in the detection of dynamic network situation risk; Γ represents Γ function. By using phase spatial reconstruction method, data acquisition of dynamic network attack signal is reconstructed, and the available formula (3) for dynamic network attack signals in a cloud computing environment is obtained:

$$\begin{aligned} z(x) &= y(\alpha_x)[s(x) + v(x)] \\ &= y(\alpha_x)[\sum_{i=1}^{K} A_i \cos(\alpha_i x + \varphi) + \sum_{j=0}^{\infty} h(j)] \end{aligned} \tag{3}$$

In the formula (3), $z(x)$ stand for the data collected for the dynamic network attack signal in the cloud computing environment; $s(x)$ is represented as the signal characteristic when the dynamic network information communication is attacked; $v(x)$ is expressed as the interference item when the interference signal of the dynamic network information communication is attacked; the signal K is represented as the fuzzy feature when the dynamic network is attacked by virus; A stand for the interference factor in the cloud computing environment; j stand for the total number of dynamic network attack signals. The dynamic network attack signal is collected and represented in concrete data form by formula (3). The network attack signal in the function-first lightweight program will go through the variable assignment, transmission and other links into the inner. Choosing to collect the attack signal data at this time can effectively improve detection performance.

2.2. Communication security adaptive virus data classification

Dynamic network attack signal data acquisition in cloud computing environment can classify communication security adaptive virus data. According to the collected attack signal data, this paper uses adaptive data classification to cluster the dynamic network information communication data. According to the topology of dynamic network, the virus data in the attack signal can be classified. The dynamic network topology contains two channels for information communication. The physical layout of the cloud computing environment can be implemented. The infrastructure in different regions can be connected through communication lines, and shares and transmits data information. Based on the virus data entered into the dynamic network, the specific amplitude and frequency distribution are judged, and the virus data response to the pulse in two bilinear curves. According to the classification method of adaptive data and the data calculation formula of dynamic network attack signal above, the total amount of specific energy for dynamic network information virus data in a cloud computing environment is obtained. Then the specific virus number in the dynamic network server layer and host layer is analyzed in peripherality, so as to obtain the fuzzy relationship between virus data and attack signal. The immunity of information communication to virus data can be optimized and the data performance can be detected. The adaptive resonance acquisition data stream of attack signal in the input and output nodes can be obtained.

In cloud computing, the characteristic information traffic of virus data in dynamic networks is composed of random signals related to multi-dimensional mean information flows and multiple unknown means. Therefore, this paper uses multi-product adaptive resonance detection method to classify communication security adaptive virus data. According to the calculation of self-correlation functions, the correlation variables of dynamic network

virus data are obtained, so as to classify the virus data according to the composition of different variables.

2.3. Network information and communication security posture prediction

On the basis of the communication security adaptive virus data which is classified above, the network information communication security situation prediction is realized by extracting and analyzing the infection membership of information communication. According to the characteristics of time-shifting and frequency-shifting invariance when dynamic network information communication attacked, as well as the total energy of the virus data derived from the above-mentioned in this paper, the total energy of the server layer in the dynamic network and the total energy of the virus data in the host layer are decomposed, and the degree of relevance of the virus data is obtained. Using the time-frequency scaling characteristics of the attack signal, the situational orientation function of virus data is:

$$n(x) = \sqrt{k}n(kx) \tag{4}$$

According to the dynamic pointing function of formula (4), the historical measurement results of attack signal virus data in dynamic network information communication channel in cloud computing environment are gradually eliminated. The noise suppression of the signal is combined with cascading filtering, so as to obtain the specific video response characteristics in the analysis of dynamic network information communication security situation. According to the characteristics, combined with the special nature of Gaussian function limit separation, each independent variable is characterized to the maximum extent. The characteristic virus data in dynamic network information communication can be predicted in the network threat situation, so as to realize the secure adaptive analysis of dynamic network information communication under cloud computing and achieve the prediction of virus level.

3. Analysis of Experimental Demonstration

3.1. Experimental preparation

In order to verify the feasibility of dynamic network information communication security adaptive model in the actual application of cloud computing, it is compared with the traditional model. First of all, the experimental operating environment of two models is constructed by using simulation experiment software. Other parameter settings for the simulation experiment operating environment are shown in Table 1.

Table 1. Simulation experiment operating environment parameter settings

Parameter	Value	Parameter	Value
Simulation experiment duration	248ticks	Cloud computing environment communication channel	75.24b/s
Number of unit information channel attacks	Adjustable25~105dB	Attack type	Multi-channel common attack
Information communication range	Before and after information 4 patches	Network transmission speed	55.67b/dB

The algorithms in both models are mathematically programmed using commercial mathematical software. The attack virus data provided by Armadillo software is added in the experimental environment of two model analysis. By using two models the information communication security adaptation in the dynamic network environment is analyzed.

3.2. Experimental results and analysis

According to the above experiment preparation, the simulation comparison experiment is completed. The virus flow prediction results of the dynamic network information communication obtained by the two models are plotted into a comparative picture of the experimental results shown in Figure 1.

It can be seen from the experimental results in Figure 1 that the two completely different virus level prediction curves are obtained by the security adaptive analysis of the same set of dynamic network information communication by the model and the traditional model. Comparing the two result curves with the actual virus level, we can see that the model is closer to the actual virus level result curve, while the traditional model is far from the actual virus level. The overall trend of the curve is quite different from the actual virus level curve. The main reason for the analysis is that the traditional model is disturbed by the cloud computing environment during the experiment, which affects the calculation accuracy of the model. Therefore, by comparing experiments, it is proved that the prediction result of the adaptive model of dynamic network information communication security under

cloud computing is more accurate, more in line with the actual needs of dynamic network information communication security in the cloud computing environment, and can effectively guarantee the safe and reliable transmission of information data.

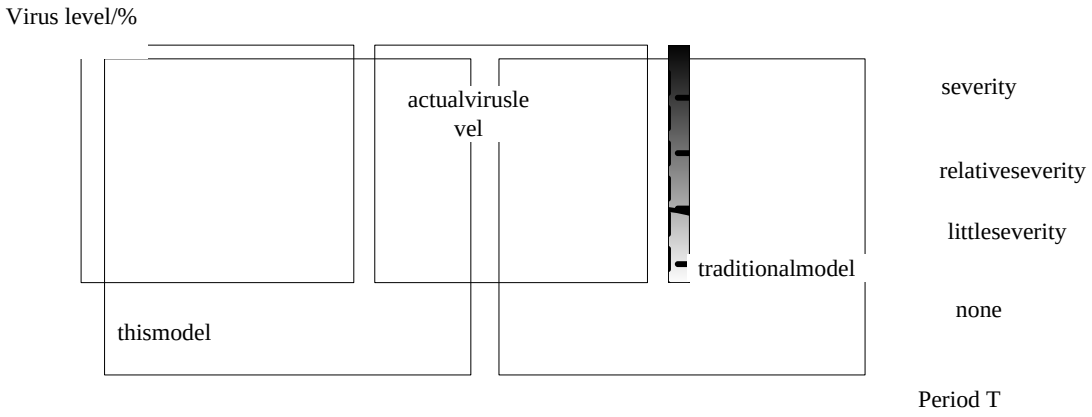

Figure 1. Comparison of experimental results

4. Conclusions

The adaptive model of dynamic network information communication security under cloud computing can effectively predict the communication security of the current dynamic network information. Taking the prediction result of this model as the basis can effectively improve the testability of dynamic network countermeasures, and further improve the ability of dynamic network to resist risks. At the same time, the model can also be used in different scenarios to predict and monitor dynamic network viruses, so as to realize the overall security estimation of the network, with good application value.

References

[1] Cao Xiang, Zhang Yang, Song Linchuan. Design and realization the forward isolation device based on deep message detection and safety enhancement. Automation of Electric Power Systems. 2019, 43(02), 162-169.

[2] Chen Wenwei, Yu Zhuozhi, Zhang Yefeng. The design of the intelligent secure private network wireless communication module based on Linux system. Electronic Design Engineering. 2019, 27(05), 121-126.

[3] Wang Gang, Zhang Xiangdong, Chen Shunli. Relying on gray-related projection of the distribution network automation communication network security evaluation study. Electrical Technology. 2019, 20(06), 066-069.

[4] Sun Yong. Appearance and essenceof the problem of network security --the reflection on the Internet security problem of frontier science field. Journal of Social Sciences, Hunan Normal University. 2020, 49(01), 032-039.

[5] Yu Baoquan, Cai Yueming, Hu Jianwei. Cognitive radio non-orthogonal multi-access random network physical layer security performance analysis. Journal of Electronics and Informatics. 2020, 42(04), 950-956.