Research on Information Security Risk Analysis and Prevention Technology of Network Communication Based on Cloud Computing Algorithm

Yonghong Li1*, Ruifeng Liu1, Xiaoyu Liu1, Hong Li2, Qingwen Sun1
1Seismological Bureau of Shandong Province, Jinan, Shandong, 250014, China
2China Earthquake Networks Center, Beijing, 100036, China

*Corresponding author: eqwww@163.com

Abstract. Data communication network must use telephone, cable or optical fiber as transmission medium and computer as information receiving, output and communication tool. Customers can not only process the received information, but also realize information sharing through the network. With the wide application of network communication in daily life, network security issues have higher requirements. In order to solve the problems of subjectivity, long modeling time and low classification accuracy of information security risk assessment methods, this paper first proposes an intelligent information security risk assessment method based on decision tree. Compared with other classification algorithms such as support vector machine, the decision tree classification algorithm has no requirement for data category distribution, and has good classification effect and fast speed. Finally, this paper introduces the security measures in network data communication for reference only.

Keywords: Network communication; Cloud computing; Decision tree; Information security risk analysis; Preventive technology

1. Introduction

In the traditional computing mode, users have complete control over data; In the cloud computing mode, the user's management of data and machines will completely depend on various cloud service providers, and the user only reserves the control authority over virtual machines [1]. Therefore, from the user's point of view, how to ensure the security and privacy of stored data and calculation results is particularly important [2].

Nowadays, the openness of network communication is constantly increasing, which will promote the rapid growth of network communication risks, such as a series of network communication security incidents such as information theft and network attacks, the increasingly profitable characteristics of some network malicious behaviors, individual network hackers, network underground chains and some network hacker organizations with hostile forces, etc., all of which pose severe challenges to our network communication security, and the whole security form is becoming increasingly severe [3-4]. Therefore, by analyzing the security and risks in cloud computing services, we can better understand the different risks and service advantages in different periods of cloud computing services, make full
use of their advantages, and take necessary measures to transfer and avoid risks, and reduce and avoid losses. In this paper, combining with the existing cloud computing platform architecture, the evaluation method is realized by grey clustering of a new whitening weight function, and then the information security risk evaluation model based on cloud computing is constructed.

2. Risk analysis of network communication information security

2.1. Security risk of network structure

(1) Security risks from cyber attacks
Unauthorized access to network resources attacks the enterprise network, while the enterprise lacks necessary security measures such as discovery, detection, isolation and blocking, and fails to deploy security protection equipment such as physical isolation, logical isolation, intrusion detection, vulnerability scanning, operation and maintenance monitoring, which increases the possibility of attack on the enterprise network system [5].

(2) Network loan risk
The management measures for network data flow are not perfect, and the related technical methods such as bandwidth management are not adopted, which leads to the waste of network bandwidth. However, the network behavior that has been occupying network bandwidth resources is not handled reasonably. Priority should be set according to the importance of business applications to ensure that important and key applications get enough network bandwidth.

(3) Risks in data transmission
Risks of data being deceived, eavesdropped, intercepted and tampered in the process of network transmission: Since most sensitive information is transmitted in clear text, and no effective encryption mechanism and digital signature are adopted, there is a high security risk, which can easily cause the leakage of sensitive information, and it is hidden and not easy to be noticed [6].

2.2. Security risks of operating system
The installation of operating system aims at normal operation, and its security is seldom considered, so the installation is usually set with default options. From the perspective of security, it is characterized by installing many unnecessary service modules and opening many ports that need not be opened, which may imply security risks; There is a lack of necessary monitoring measures for the operation of important application systems, server systems, groupware systems and database systems, which can only be discovered and recovered after the machine is down, and there is a lack of real-time monitoring and alarm measures and reasonable emergency response procedures, etc., or it depends on the manual management of staff.

At the risk of denial-of-service attack, it takes advantage of the weaknesses of network, application and system to launch attacks, resulting in system crash, significant performance degradation and occupation of system resources, thus failing to provide services normally.

2.3. Data confidentiality and integrity risks
If users store data in the "cloud", there is a risk that the confidentiality and integrity of data content will be destroyed. Cloud computing services must ensure the confidentiality and integrity of user data, and ensure that data content is not inadvertently or maliciously accessed and modified by other users, suppliers' operation and maintenance personnel or irrelevant personnel inside users, so as to ensure the security of user data.

2.4. Data privacy risk
When using cloud computing services, user data is usually stored in a shared virtual environment, which may be mastered by irrelevant personnel, saboteurs and even competitors. Suppliers must effectively isolate different user data to ensure the privacy of data. Under the data protection mechanism using encryption, the supplier should ensure that the encryption algorithm is efficient and
reliable, and the encryption mechanism cannot affect the normal use efficiency of data, nor can it destroy the data content.

3. Cloud computing

Cloud computing is a new business computing mode, which integrates computing resources on the network to form a super-large virtual resource pool, and provides users with on-demand computing power, storage capacity and information services. It is the development of parallel computing, distributed computing and grid computing, and integrates utility computing and virtualization technology [7-8]. Cloud computing technology depends on the services provided by various cloud computing platforms. According to the different types of services provided by cloud computing, cloud computing can be divided into three categories: infrastructure as a service, platform as a service and software as a service, thus constituting the cloud computing service model.

![Three-tier architecture diagram of computing service](image)

Figure 1 Three-tier architecture diagram of computing service

As shown in Figure 1. In cloud computing. Different layers provide different services. IaaS covers all infrastructure resources from computer room equipment to hardware platform, which is at the bottom level and is the basic layer of cloud computing services, providing users with basic hardware resources including computing resources, storage resources and network resources; PaaS is located on IaaS, which not only pays attention to the integration of underlying hardware resources, but also provides users with abundant middleware-like resources, and provides users with an open environment as a service, allowing users to develop their own applications on the platform; SaaS is located on the cloud computing service infrastructure, which provides applications as a service to users. Users can obtain the cloud services provided by them through browsers.

4. Information security risk assessment method

Information security risk assessment is to determine the expected loss of the whole system caused by the missing or damaged resources of computer system and network, and it is also an assessment of threats, vulnerabilities and the risks brought by them. Information security risk assessment includes four main factors: asset assignment, threat analysis, vulnerability identification and analysis of existing measures.

Evaluation is always based on certain technical means and evaluation models, and the selection of evaluation methods directly affects every link in the evaluation process, and can even influence the final evaluation results, so it is necessary to select the appropriate risk assessment method according to the specific situation of the system [9].

4.1. Decision tree algorithm

This paper refers to the classification method based on C4.5 decision tree for information security risk assessment [10]. The main idea of C4.5 algorithm is to gradually find out the variable attribute that provides the maximum information gain rate at each level, so as to determine the structure of decision tree from root to branch and then from branch to leaf. The attribute with the largest information gain
rate is taken as the root node of the decision tree.

Information gain rate is used to select variable attributes. Firstly, the entropy of training samples is calculated, and its expression is:

$$\text{inf} o(T) = -\sum_{j=1}^{k} \frac{\text{freq}(C_i, S)}{|S|} \log_2 \frac{\text{freq}(C_i, S)}{|S|}$$ (1)

Where \( \text{freq}(C_i, S) \) represents the number of samples in the set \( S \) that belong to a class \( C_i \) of the \( k \) possible classes, and \( |S| \) represents the number of samples in the set \( S \).

According to the value of non-category attribute \( X \), \( T \) is divided into sets \( \{T_1, \ldots, T_j\} \), and these subsets need to be weighted by entropy, and the calculation formula is

$$\text{inf} o_X(T) = -\sum_{j=1}^{L} \frac{|T_j|}{|T|} \text{inf} o(T_j)$$ (2)

Calculate the difference before and after discrimination to obtain the information gain, and its calculation formula is:

$$Gain(X) = \text{inf} o(T) - \text{inf} o_X(T)$$ (3)

When selecting attributes, information gain tends to choose attributes with more values. In order to make up for this deficiency, information gain rate is defined, which considers the number of sub-nodes and the size of each sub-node generated by each division, and divides the objects to be considered one by one, without considering the amount of information contained in classification.

$$\text{Split}_\text{inf} o_i(X) = -\sum_{j=1}^{L} \left( \frac{|T_j|}{|T|} \right) \log \left( \frac{|T_j|}{|T|} \right)$$ (4)

The information gain rate of attribute \( X \) is defined as:

$$\text{ratio}(X) = \frac{Gain(X)}{\text{Split}_\text{inf} o_i(X)}$$ (5)

C4.5 algorithm has made a great improvement on ID3 algorithm in dealing with the default value of predicted variables, pruning technology and derivation rules. The attribute selection of ID3 is based on entropy measure, that is, the change value of entropy, while C4.5 uses information gain rate, so c4.5 overcomes the defect that ID3 tends to select attributes with more values when selecting attributes with information gain, which is suitable for regression problem and classification problem.

4.2. ISRAD method

Common information security risk assessment methods, whether qualitative, quantitative or a combination of qualitative and quantitative methods, get discrete values. Compared with other machine learning classification algorithms, ISRAD method applies C4.5 decision tree classification method to information security risk assessment, and quantifies the assessment results. When dealing with discrete data, ISRAD method has unique advantages in recognition accuracy and speed.

Use decision tree to evaluate information security risks. The main process is shown in Figure 2.

Analytic hierarchy process is used to decompose the system, establish a hierarchical structure model, give weight to the lowest index in the established hierarchical structure model, and carry out consistency test, which will be used as input data after passing the test; Taking part of the data as training data, the training model is established by C4.5 decision tree; Classify the data with the training model, and get the classification result.
5. The application of network security technology in network communication

5.1. Adopt encryption means
In the process of communication, there are often many contents that involve privacy or have important value, especially some important information between enterprises, which requires higher transmission security. Imagine if the information about the new product is leaked before the product is officially produced, which will make the enterprise very passive and suffer immeasurable losses. At present, many enterprises choose to use encryption means to deal with threats such as network Trojans and hackers. Encryption can be divided into network layer encryption and application layer encryption. Encrypting in the network layer, the data has a guarantee in the transmission process, the data is not easy to be stolen, and the data is like being locked in a safe for transmission; Encryption on the application layer adds a guarantee to the above security. After users get data, they can't open and use the data without identity authentication, just like getting a safe requires a key and password to be useful.

5.2. Strengthen the security of system authentication methods to prevent unauthorized access
Computer terminal identity authentication technology can identify various identities in network activities, and it is the first line of defense of network security system. Once the identity authentication system is breached, all security measures of the system will be ineffective.

At present, the widely used authentication method uses secret information as the authentication method of authentication password, and the system based on this method usually uses "username+password" to identify users. Usually, the user name is public, and the password can be reused, so the attacker has enough time to obtain the password. In order to improve the security of the system, administrators usually formulate corresponding policies to limit the use of passwords. Do not use the same character continuously, and do not use all numbers or letters; Change the password regularly, and change the temporary password when logging in for the first time; Avoid using old passwords or recycling old passwords; Do not share personal user passwords; Avoid recording passwords on paper; When users need to access multiple services or platforms, they should use multiple passwords. Especially in local area network systems with high security requirements, two-factor authentication technology should be adopted.

5.3. Perform intrusion detection
Intrusion detection is mainly applied to the internal network of an organization or enterprise. When the system detects an intrusion, it automatically prevents the intrusion from entering the system, and gives an alarm display to remind the staff. Network communication protocol is the foundation of computer network, which is composed of IP protocol in network layer and TCP protocol in transport layer. Intrusion detection can not only intercept intrusions in simple and regular information systems, but
also distinguish intrusions from complex information systems, and quickly intercept intrusions and manage information systems.

Intrusion detection can be divided into host-based detection, network-based detection and hybrid detection according to object classification. The main function of intrusion detection is to monitor and analyze users' and system activities, audit system structure and weaknesses, identify activity patterns reflecting known attacks and users' behaviors violating security policies, which can effectively improve the information security management of intranet.

5.4. Actively guard against computer viruses

Nowadays, the development trend of computer network viruses is very fast. Nowadays, viruses have become dependent and dependent on network transmission with the previous single mode of transmission. The main methods are email and file transmission, and the generalized network viruses which are integrated with Trojan horses, hackers and other attack means.

The following points must be considered when choosing anti-virus software: First, the anti-virus method of virus killing software needs to be effectively integrated with the Internet, and at the same time, traditional manual file monitoring and killing is needed to monitor the network and mail in real time; Second, virus killing software should have perfect online upgrade service; Third, virus killing software manufacturers should also have a fast-responding virus detection network; Fourth, virus killing software vendors need to be able to provide timely and complete anti-virus consultation.

5.5. Strengthen safety awareness, regular inspection and maintenance

It is necessary to strengthen the safety awareness of communication network managers and users and improve the technical level of operators. The network management personnel should be trained regularly. The network management personnel are the maintainers of network security. They should grasp and understand the new threats encountered in the development of the network in time, master the coping methods skillfully, and improve the technical level at all times. Hidden dangers often lurk in small things, so it is necessary to detect and maintain the communication network regularly, patch the discovered loopholes in time, and deal with the emerging threats in time, so as to nip in the bud.

6. Conclusion

At present, cloud computing technology is sought after by more and more countries because of its advantages, and its application is also very extensive, and the related research of cloud computing has become a hot spot. With the continuous development of China's communication technology, data communication has occupied a mainstream position in China's communication development, and more information and resources have been shared. But in the process of development, people pay more and more attention to the stability and security of communication. Therefore, the stability and security of data communication can be strengthened by improving the management of network security and strengthening the maintenance means. Classification algorithm based on CA.5 decision tree has no requirement for data distribution, so the information security risk assessment method based on C4.5 decision tree has a good development prospect and high practical value, and can be widely used in actual risk assessment work.

References

[1] Song Jianheng. E-government information security risk analysis and prevention strategy. Digital Communication World, no. 03, pp. 264-265, 2017.
[2] Lu dong. Analysis of personal information security risks and prevention and control technologies from the perspective of big data. Think tank times, vol. 141, no. 25, pp. 286-288, 2018.
[3] Duan Jun, Liu Yajong, Huang Dian. E-government Information Security Risk Analysis and Prevention Strategies. Software (Education Modernization) (Electronic Edition), vol. 000, no. 005, pp. 149, 2018.
[4] Fu Saiping. Risk and prevention of enterprise accounting information security under cloud
7

accounting environment. Journal of Taiyuan City Vocational and Technical College, vol. 207, no. 10, pp. 188-189, 2018.
[5] Xu Huina. Analysis of network information security risks and preventive measures in public libraries. File, vol. 009, no. 018, pp. 36, 2019.
[6] Gao Wu. Analysis of computer network information security risks and protective measures under the background of big data. Computer knowledge and technology, vol. 014, no. 007, pp. 29-30, 36, 2018.
[7] Wu Bo. Research on Information Security Risk Prevention under the Mode of "internet plus Finance". China Strategic Emerging Industries, vol. 000, no. 12X, pp. 85-85, 2017.
[8] He sijiang. Information security risks and prevention of computerized accounting. youth, vol. 000, no. 006, pp. 290-291, 2018.
[9] Kang Yang. Risk Analysis and Prevention in Credit Information Security Management of People's Bank. Financial and Economic Monthly, 2017:148.
[10] Luo Tao. Research on information security risk prevention under the mode of "internet plus finance". Information and computer (theoretical edition), vol. 406, no. 12, pp. 212-213, 2018.