Development of Computer Network Security Based on Cloud Computing

Yizhi Li*  
College of Internet of Things, Jiangxi Teachers College, Yingtan, Jiangxi, China  
*Corresponding author e-mail: 2002018003@jxsfgz.com

Abstract. Cloud computing not only provides convenience for users, but also brings certain information security threats to users. How to effectively protect the user's information security has become one of the core issues of network security. This paper analyzes the problems and reasons of network security in cloud computing environment, and points out the main ways to improve network security. This paper analyzes the network security problems in the cloud computing environment, and discusses the information security technology in the network. This paper studies the definition, characteristics, classification and core technology of cloud computing security, analyzes the security risk of cloud computing network, and puts forward the cloud computing network security model and security level evaluation method from different angles. Level experiment results show that the network security model in cloud environment is feasible, computing can fully meet the development requirements of the current network information age, and effectively standardize the network security operation environment. The results show that: in 2016, the number of articles related to cloud computing is at least 2653, and in 2020, the number of articles related to cloud computing is at most 6438.

Keywords: Cloud Computing, Computer Network Security, Vitalization, Hierarchical Protection

1. Introduction
Cloud computing has become the real trend of computer IT service mode, which provides cost-effective and scalable processing. At the same time, software defined network (SDN) has been widely used in computer network for its advantages of flexible network management services and reducing operating costs. When providing enterprise IT services, there seems to be a trend that these two technologies go hand in hand. Cloud computing brings us the convenience of sharing network resources, but the potential network security risks can not be underestimated.

With the continuous development of information technology, many experts have studied computer network security. For example, some domestic teams have studied secure network coding technology, introduced the concept, characteristics, network security meaning and security status of cloud computing, and proposed the application of data center cluster technology to improve performance and capability by reducing the number of cloud database clicks. This paper discusses the network security
problems in the cloud computing environment, and puts forward some suggestions and suggestions to strengthen the network security. This paper proposes a storage security framework, including encrypted storage scheme and data structure. In this framework, the encrusted server can not understand any plain text information and can complete dynamic operation in a short time. The encryption algorithm and data storage structure are simple and easy to maintain. In order to prevent unauthorized data access, a distributed cloud data security scheme is proposed. This paper summarizes some important work in intrusion detection system, and focuses on the research of intrusion detection system, in order to protect intrusion detection system from the impact of threat environment. In order to protect users effectively, we should maintain the expansion ability, increase the number, and quickly reduce the number. Depending on the amount of resources, access to the system level and / or its purposes and characteristics can be isolated. In the intrusion detection system based on virtual machine, the migration between different tsnd implementations across multiple platforms is used, which makes it a better alternative to intrusion detection. Cloud computing and network security are combined to study the "cloud" firewall technology. This paper compares the "cloud" firewall with the traditional firewall, and further studies the cloud computing, architecture and vitalization technology in the "cloud" firewall [1]. Some experts have studied the departmentalization of improved AES encryption algorithm in cloud computing, selected neural network as the research object, put forward the concept and concept of computer network system security domain, to maintain economic development and social stability. This paper proposes a design method of network chat system based on socket and cloud computing technology. Java socket is customized by sun for Java language, which is used to develop network applications. This paper introduces the important concepts of socket interface and cloud computing technology, analyzes socket communication mechanism in principle, and studies the application of java socket. In order to improve the security and efficiency of data storage in communication network chat, an improved method of cloud computing technology is added based on the application of socket technology [2]. Some experts have studied the design and implementation of cloud platform vitalization security test system, and proposed a new privacy protection computing technology, that is, using implicit security model in cloud computing. In the proposed technology, data is divided into multiple partitions and stored on an independent cloud server. When the user wants to perform the calculation on the data, he sends a signal to the server, and the server performs the required calculation. This paper first summarizes the security problems of virtual machine, and then discusses and analyzes the security problems existing in the virtual network based on Xen platform. Finally, a new virtual network framework is proposed to control the communication between virtual machines deployed on physical machines, which has high security. It is proved that the privacy of user data can be maintained when the master data storage server does not collude. This can be guaranteed by using an independent cloud provider. This technology eliminates the requirement of key management and has high efficiency and practicability [3]. Although the research results of computer network security are quite abundant, there are still some deficiencies in the development of computer network security under the background of cloud computing.

In order to study the development of computer network security based on cloud computing, this paper establishes a network model through the research of computer network security, and the results show that computer network security is very important.

2. Method

2.1. Computer Network Security

2.1.1. Security Ontology. Ontology in the field of security is called security ontology, which is "based on the security aspect of information system, and can be used as a container to extract information system security requirements from information sources" [4]. At present, the research of security ontology is still in its infancy at home and abroad [5]. At present, the main research direction of security ontology is the security ontology of trust relationship and risk assessment in information
system, as well as the security ontology related to e-commerce [6]. While cloud computing brings convenience to users and improves the efficiency of resource utilization, due to the complex architecture of cloud system, its dynamic management mode, powerful computing power and storage scale will also face new security problems [7]. Cloud computing security is an important branch of system reliability, and also the main attribute of the actual system operation [8]. The data storage mode of cloud computing belongs to cloud storage [9]. This outsourcing storage and computing mode is implicit for third-party customers, because the data will not be stored on the customer's local server, which increases more unacceptability [10]. Safety requirements include three aspects: first, similar security requirements, mainly including usability, confidentiality and integrity requirements; second, similar system threats, such as the source, mode and intensity of threats; third, similar asset values, such as the separation of important assets and other non important assets.

2.1.2. Access Security. Compared with ordinary network access, cloud system is faced with more user access, which makes access authentication and authorization audit become the key to deploy security policy. Managers need to customize reasonable configuration to meet the relevant access requirements. However, due to the imperfection of the management mechanism, the system internal managers can access the virtual machine management system through malicious software, and then steal illegal resources. For physical access security, common threats include cold start attack and hardware tampering. These attacks can maliciously delete specific kernel modules, such as virus monitoring system, firewall and so on, so that the protection ability of the system is reduced. Therefore, it is necessary to reasonably supervise and control the special authority of administrators to prevent the occurrence of such security incidents. The common method is to force the configuration of external security access control list.

2.1.3. Cloud Computing Security Status Assessment. The key of cloud computing security state assessment is to determine the security indicators in the cloud system, so as to reasonably integrate different types of index information, and finally get the evaluation value that can fully reflect the security state of the cloud system. For complex system state evaluation, there are hidden Markov evaluation method, service stability evaluation method, fuzzy composition operator evaluation method, probability density trust relationship evaluation method, fuzzy comprehensive hierarchy evaluation method, system availability evaluation method and so on.

2.2. Network Model
Random linear network coding is mainly divided into two stages: coding and decoding. In the coding stage, the system randomly combines the information sent by the source, and randomly selects all the coefficients from the finite field. In the decoding stage, the Gauss elimination method is used to solve the linear equations, and then the original message sent by the source node is restored to the destination node. Suppose that the original message to be sent by the source node is m. before sending the message, the source node first divides the message M into L generations, each generation has m messages, and each message is represented by a vector of length n. then the original message M can be expressed as, as shown in formula (1):

\[ M_i = (a_{i1}, a_{i2}, ..., a_{in}), (i = 1, ..., m), a_{in} \in G_p \]

(1)

Isomorphic: Metamorphism can be divided into multiplicative isomorphic and additive isomorphic. Suppose there is a function K, given two variables t1 and t2, there is a function at the same time. If equation (1) holds \( \psi \), then the function K is said to satisfy multiplication, as shown in equation (2-3):

\[ K(t_1 \times t_2) = \psi(K(t_1) \cdot K(t_2)) \]  

(2)

\[ K(t_1 + t_2) = \psi(K(t_1) + K(t_2)) \]  

(3)
If the message is contaminated, it will be discarded. If it is not polluted, it will be saved. After receiving m linearly independent messages, the destination node decodes and restores the messages sent by the source node by Gaussian elimination method, and obtains the original messages sent by the source node to the destination node. Finally, the first m columns of the generated matrix are expressed as s, and the last n columns are expressed as Z. According to equation (2-3), m original messages sent by the source node can be decoded, as shown in equation (4):

\[(M_1, M_2, ..., M_m) = S^{-1}Z\]  

(4)

3. Experience

3.1. Experimental Object Extraction

The research objectives include three aspects: one is to analyze the changes of information service mode, process and service organization form of digital academic resources in the cloud environment, and make clear the security requirements of digital academic resources information service in the cloud environment; the other is to establish the digital academic information resources cloud service by using the relevant theories and management methods of service chain and combining with the characteristics of digital academic resources information cloud service. On this basis, the guarantee scheduling method of digital academic resources cloud service chain in cloud environment is established. Third, set the key quality indicators of cloud services, and ensure the security of digital academic resources information services by establishing service monitoring.

3.2. Experimental Analysis

When evaluating the security status of the actual cloud system, due to the complex working environment, vulnerable to external attacks, the data fluctuates greatly in the process of monitoring data collection. Considering the working state and external environment of the cloud system, the fluctuation of monitoring indicators mainly comes from two aspects: on the one hand, the external attack on the cloud system is random, and in the process of system operation, the attack on the cloud system is random; on the other hand, in the process of obtaining the monitoring indicators of the cloud system, the quality of the monitor will change with the growth of time, and its tracking ability will also increase. In the actual work process, the monitoring data will be affected by environmental noise and other factors, so the monitoring data will have a certain volatility, and the reliability of the data will be reduced. In the process of cloud system security assessment, the fluctuation of its monitoring indicators will not affect the assessment accuracy of the security assessment model, and the accuracy error of the security assessment model mainly comes from the influence of external environmental noise and other factors. Therefore, it is necessary to calculate the reliability of monitoring indicators.

4. Discussion

4.1. Cloud Computing Security

Security is the most concerned problem in business and academic circles. According to the National Institute of standards and Technology (NIST) cloud computing research report, security is one of the most important obstacles in cloud computing research. As shown in Table 1.

| Table 1. Research popularity of cloud computing security articles |
|------------------|----------------|----------------|----------------|----------------|
| particular year  | 2016           | 2017           | 2018           | 2019           | 2020           |
| numerical value  | 2653           | 3875           | 4687           | 5343           | 6438           |

As can be seen from the above, there are 2653 articles related to cloud computing in 2016, 3875 articles related to cloud computing in 2017, 4687 articles related to cloud computing in 2018, 5343 articles related to cloud computing in 2019 and 6438 articles related to cloud computing in 2020. The
results are shown in Figure 1.

![Graph showing research popularity of cloud computing security articles]

**Figure 1.** Research popularity of cloud computing security articles

It can be seen from the above that in 2016, the number of articles related to cloud computing was at least 2653, and in 2020, the number of articles related to cloud computing was at most 6438.

### 4.2. Performance Testing

The purpose of this test is to compare and analyze the time-consuming of opencast ordinary cloud and open stack Security Cloud in the login process. Because the network transmission speed has a great influence on the test results, in order to make the test results scientific and reasonable, this test adopts the LAN environment with the maximum transmission speed of 100Mbps, and there is no irrelevant data interaction in the test process. In this test, the time recording function is set at the beginning and end of the system login processing to record the login processing time, which does not include the user input time. A total of three single tests were carried out, and the specific results are shown in Table 2.

**Table 2.** Cloud LAAS layer trusted access protocol performance test

|                     | first test | Second test | third test |
|---------------------|------------|-------------|------------|
| Opencast general cloud | 0.23       | 1.32        | 0.28       |
| Open stack Security Cloud | 0.17       | 0.13        | 0.16       |

It can be seen from the above that the average time for the first trial landing of opencast ordinary cloud is 0.23s, the average time for the second trial landing of opencast ordinary cloud is 1.32s, and the average time for the third trial landing of opencast ordinary cloud is 0.28s; the average time for the first trial landing of open stack security cloud is 0.17s, the average time for the second trial landing of open stack security cloud is 0.13s, and the average time for the third trial landing of open stack security cloud is 0.28s. The average landing time of the third test of stack security cloud is 0.16s. The results are shown in Figure 2.
5. Conclusion
The adoption and promotion of cloud computing is threatened by the unsolved security problems of cloud providers and cloud users. In this article, we will show how vitalization can improve the security of cloud computing by protecting the integrity of client virtual machines and cloud infrastructure components. In particular, we propose a new architecture, advanced cloud protection systems (ACPs), to ensure the security of cloud resources. This paper analyzes the key technologies and characteristics of cloud computing, and expounds the main aspects of cloud computing security. This paper analyzes the security technology of cloud computing, and puts forward the corresponding countermeasures to solve the security problems of cloud computing. Cloud computing security is a relatively new field. Due to the rapid development of cloud computing technology, its application is more and more extensive and in-depth. Therefore, many enterprises are engaged in the research of cloud computing.

References
[1] Stergiou C, Psannis K E. Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey. International Journal of Network Management, 2017, 27(3):1-12.
[2] Huang B, Cheng X, Huang C, et al. Meet-Cloud for Secure and Accurate Distribution of Negative Messages in Vehicular Ad hoc Network. Tsinghua Science and Technology, 2018, 23(4):377-388.
[3] Shila D M, Shen W, Cheng Y, et al. AMCloud: Toward a Secure Autonomic Mobile Ad Hoc Cloud Computing System. IEEE Wireless Communications, 2017, 24(2):74-81.
[4] Khan A U, Bagchi S. Software architecture and algorithm for reliable RPC for geo-distributed mobile computing systems. Future Generation Computer Systems, 2018, 86(SEP.):185-198.
[5] Hasan R, Hossain M, Khan R. Aura: An incentive-driven ad-hoc IoT cloud framework for proximal mobile computation offloading. Future Generation Computer Systems, 2017, 86(SEP.):821-835.
[6] Sotelo Monge M A, Maestre Vidal J, Martinez Perez G. Detection of economic denial of sustainability (EDoS) threats in self-organizing networks. Computer Communications, 2019, 145(SEP.):284-308.
[7] Hu Z, Qiao Y, Luo J. ATME: Accurate Traffic Matrix Estimation in both Public and Private Datacenter Networks. IEEE Transactions on Cloud Computing, 2018, 6(1):60-73.
[8] Deshpande P, Sharma S C, Peddoju S K, et al. HIDS: A host based intrusion detection system for cloud computing environment. International journal of systems assurance engineering and management, 2018, 9(3):567-576.

[9] Zhang Y, Deng R H, Han G, et al. Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things. Journal of Network and Computer Applications, 2018, 123(DEC.):89-100.

[10] Lou J, Jiang Y, Shen Q, et al. Failure Prediction by Relevance Vector Regression with Improved Quantum-inspired Gravitational Search. Journal of Network and Computer Applications, 2017, 103(FEB.):171-177.