Research on Innovation of Network Information Security Technology Based on Cloud Computing

Jianshi Zhang1,*

1Changchun Polytechnic Information Institute, China, 130033

*Corresponding author e-mail: 23746978@qq.com

Abstract. Cloud computing has become a new network service mode, which can provide a series of resources for many users and carry out intelligent computing according to their needs and daily habits. While technology development brings positive effect, it will also have negative effects. More and more hackers and viruses are trying to invade computers, endangering network security to provide users with storage and data processing services. Based on the widely used environment of cloud computing, this paper studies the innovation of network information security technology with the development of science and technology.

Keywords: Cloud Computing, Network Information, Security Technology

1. Introduction

Information technology is used in state secret scientific research and people's daily life study. Information technology can be expected to develop in the direction of high quality, high level and high efficiency, looking forward to bringing people a better life [1]. Cloud computing technology has the advantages of simple operation, large scale of processing information and high accuracy of information data processing, and has been widely used at home and abroad. Compared with other technologies, the cost of information data processing is relatively low, and the resource allocation can be completed dynamically, and the application value is relatively high. However, in the cloud computing environment, the problem of network information security has gradually been exposed, and network information security technology has become the focus of public attention. In order to explore the technology in depth, researchers should first clarify the structure of cloud computing architecture and lay a good theoretical foundation for further research. While enjoying the convenience of information technology, life will also encounter with the negative impact of information technology, such as enterprises, individuals will occasionally be hacked, stolen private information and so on [2-3]. Therefore, it is imperative to establish a secure network environment, strengthen the network information security technology, and ensure the basic interests of people in the network environment.
2. Cloud computing architecture

The cloud computing architecture shown in figure 1 is mainly divided into physical layer, application layer, development platform layer, core layer and resource architecture layer.

![Cloud computing architecture](image)

**Figure 1.** Cloud computing architecture

2.1. Application layer

Based on different development environments and development platforms, distributed applications are used to develop. This layer structure is mainly responsible for user service quality assurance and software development, operation and so on.

2.2. Development platform

Based on the resource architecture layer, the platform layer will use API applications to provide cloud computing programming environment and distributed services, which can effectively improve the deployment efficiency of application services. And can provide the corresponding support for the application service expansion.

2.3. Resource architecture

It will build the resource service architecture system based on the core layer, which can ensure the flexibility and efficiency of distributed computing services, and can realize distributed communication with high reliability and large capacity distributed storage.

2.4. Core layer

This layer is mainly responsible for physical resource management, which can provide the corresponding application environment for the upper layer, and can abstract the services by using the system virtual machine monitor, kernel and middle layer.

2.5. Physical layer

As a cloud computing infrastructure, this layer will collect global related resources according to geographical distribution, provide backbone resources for cloud computing, such as storage resources, computing resources and network resources, can provide local data support for upper management, operation and maintenance, and can provide good hardware support and services for large IT enterprises.

3. The necessity of enhancing network information security in cloud computing environment

In the cloud computing environment, the enhancement of network information security is very important for the development of information technology. The concrete function and value are as
follows: the enhancement of network information security can effectively improve the degree of information confidentiality, can carry out scientific protection of important information, will make the whole cloud computing platform more secure and reliable, users can safely store and use information data in the platform, and can fundamentally guarantee the data information security; After improving the level of network information security, it can effectively meet the requirements of customers, directly protect and monitor the corresponding information data, and effectively avoid the problem of data loss or damage. For example, the user client and software system can be supervised and controlled.

4. New factors affecting network information security in cloud computing environment

4.1. Inadequate estimation of network information security in cloud computing environment

The managers of some network sites do not have a deep understanding of information security, do not work hard on the information security configuration of network sites, and do not limit the scope of use of information resources of network sites. In some cases, users are often provided with too much authority. Not paying enough attention to the security problems of these systems often makes some network lawbreakers take advantage of invade network sites, steal resources, release viruses and so on.

4.2. Network security information system weaknesses

In addition to network communication protocols and communication systems, some computers themselves also have certain system vulnerabilities, especially their own operating systems, which are very vulnerable to hackers, and their intrusion traces are very easy to remove [5]. It is difficult to track the hacker's location under certain circumstances, and these intruders can access all the information of the whole system by some means. In addition, the vulnerability of the database is also a point of concern. There are some problems in the confidentiality, sustainability, integrity and self-limitation of the traditional database. It is very easy to be cracked by others and steal the important data and resources of the user.

4.3. The network information environment is more complex

In the convenient environment of cloud computing, people benefit from its benefits and become network users one after another. Lawbreakers will naturally find ways to gain improper benefits from it and bring many security risks to the network environment. Many lawbreakers will release viruses on the Internet, transfer data resources from computers directly to their own computers with the help of viruses, and even some hackers will directly invade personal computers. Even a lot of network swindlers carry out network fraud [6].

4.4. Network system is not sustainable and stable

At present, because of its long design time, many network sites are very backward in their own security configuration. This leads to the lack of stability of the network system, often network errors or crashes, seriously affecting the user's sense of use and experience. Of course, some network site managers have also carried out the corresponding maintenance, but because the security and hardware settings are not deeply considered in the maintenance phase, the site is easily affected by external factors [7]. Some network data fluctuations easily affect the normal operation of the site data transmission is prone to fluctuations and distortion.
5. Research on innovation of network information security technology in cloud computing environment

5.1. Super smart firewall technology
The network intelligent firewall is different from the traditional firewall. On the basis of the accurate database, the traditional firewall intercepts and blocks some specified accurate data sources and filters the information. In order to limit the access of some users, and then protect our network system. The network intelligent firewall is based on fuzzy database and uses fuzzy recognition technology to prevent most illegal elements from accessing. This new firewall can analyze and deconstruct the data source of the visitor with the help of intelligent data analysis technology, and refer to the characteristic value of the network behavior of the other party, so as to accurately distinguish the access purpose of the target user and carry on the corresponding control processing.

5.2. Advanced information encryption technology
Encryption technology is one of the most frequently used information security technologies in the world. In the network environment of cloud computing, encryption technology is widely used in today's network environment. We know that the basic principle of encryption technology is to encrypt information. In short, it is to use the prescribed code table to convert the information that the original user can read into the information that cannot be read. Only the recipient can use the code table to restore the information and read the required information. Figure 2 is a demonstration diagram of public key cipher algorithm of information encryption technology.

![Diagram of Public Key Cryptography Algorithm for Information Encryption Technology](image)

**Figure 2.** Presentation of Public Key Cryptography Algorithm for Information Encryption Technology

5.3. Sharp anti-virus technology
We all know that Internet virus has always been a serious threat to the existence of network information security, and with the research and development of network security technology, antiviral technology has also been born. At present, two kinds of antiviral techniques are more common on the network. One is dynamic real-time antiviral technology, to some extent its antiviral technology is the
best, mainly to control and limit the underlying data resources of the system, and immediately alarm when the virus invades, and timely remove the virus, repair data. The other is static antiviral technology, which is more traditional and is a single system defense technology, which cannot judge whether the system is invaded by virus according to the dynamic changes of the system itself. Its application effect is getting worse and worse, with the development of time has begun to be replaced by other antiviral technology.

5.4. Strict identity technology
Identity authentication technology is mainly divided into two parts: identity authentication and identity identification. In specific use, identity authentication technology will be used to authenticate the identity legitimacy of users according to authorization protocols and authentication protocols. Then the user specific authority and personal data are clear. The whole identification and authentication process can effectively prevent the appearance of user identity impersonation and illegal login, and can effectively protect the whole system, which is the basis and premise of authorization control means. In the single machine state, the body card is mainly divided into hardware equipment authentication, physiological characteristics and password authentication. When using password for authentication, information security may be affected because of network monitoring, so it is usually recommended to use high-intensity cryptographic technology for authentication. Along with the traditional static password authentication, fingerprint authentication, dynamic password authentication and one C card authentication are widely used.

6. Conclusion
Under the current conditions, the development of society and the country needs the high-speed transmission of network information. Network information security issues are closely related to national security, national economy and people's livelihood. In the era of cloud computing, network attack means change many ends, tend to be complicated and sophisticated, our information security technology should also be updated in time, from all-round defense against network attacks, constantly improve our network security system, Establish a comprehensive and stable network security protection system to eliminate network intrusion.

References
[1] Liu Min. Computer Network Information Security Technology Research [J].From Cloud Computing Perspective Journal of Heihe University, v.9;No.60(06): 213-214.,2018

[2] Zhou Zhiyong. Development of Network Information Security Technology in Cloud Computing Environment [J].Research China's high-tech enterprises 2014000(017):40-41.

[3] Wu Weiqiang. A study and practice of omni-directional multi-angle information security technology in cloud computing and big data environment [J]. World of Communication ,2017,000(014):45-46.

[4] Cheng Yuzhen. Research on Cloud Service Information Security Risk Assessment Index and Method [D]. Beijing Jiaotong University, 2013.

[5] Wang Mengjie. Research on Saas ERP service migration based on risk control perspective [D]. Xi'an University of Technology, 2018.
[6] Liu Aiyun, Qi Zhi, Wang Xiaoqiang. A Study on the User Information Security Strategy in Cloud Computing Environment [J]. China Electronic Commerce: Science and Technology Innovation, 2014.

[7] Liu Liming, Li Qunying, Liu Hongbo, Research on the Development of Network Information Security Technology etal [C]. Cloud Computing Environment Proceedings of the third Smart Grid Conference. 2018.