

Research on the Problems and Countermeasures of Computer Security under Cloud Computing Background

Zhang Dujuan

Xi'an Medical University, Xi'an, Shaanxi, China

Keywords: Cloud computing; Computer security; Problems and countermeasures

Abstract: Cloud computing is a network-based modern computer technology, it is a new computing service model. The application of cloud computing has brought great changes to computers in many aspects, and also brought many new directions and opportunities. However, the development of cloud computing has also brought a certain impact on computer security. Based on above, the paper expounds the cloud computing features and computer security firstly, then explores computer security issues and measures under cloud computing in details, to solve practical security problems through research on computer security issues.

1. Introduction

With the continuous improvement of science and technology, computer technology has been popularized in People's Daily life. Facing the needs of economic development and people's material life, it is of great significance to accelerate the development of computer technology. With the development of the big data era, we will face increasingly large data. Therefore, our effective data management is the inevitable requirement of The Times development. The cloud computing has effectively solved the current problem of increasing data freedom. We need to strengthen the cloud computing data security protection work, we must use advanced technology to ensure the security of data operation environment.

2. The cloud computing working principle and characteristics

2.1 The cloud computing working principle

In the cloud environment, Map/Reduce is often adopted for data processing. It divides a large-scale data processing problem into several small-scale ones, and then processes each node in parallel. In this way, we can improve data completion efficiency and reduce execution time. The cloud computing working principle is shown as the figure 1. During the process of data and information processing, some illegal or unauthorized users steal or destroy the system information. Computer information security in the context of cloud computing has many problems.

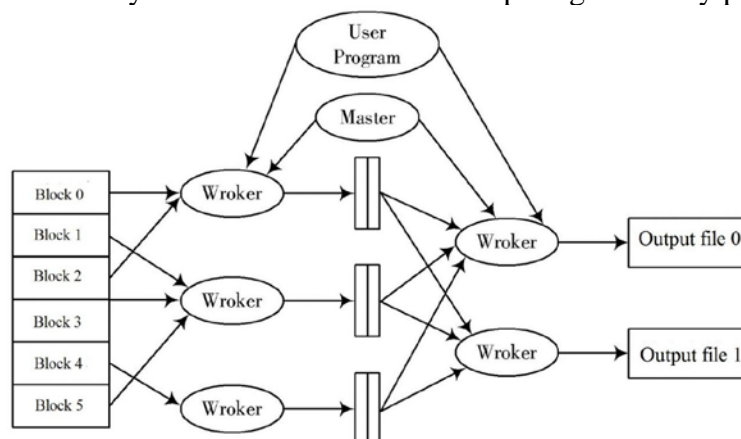


Figure 1: The cloud computing working principle

2.2 The cloud computing working principle and characteristics

2.2.1 Resource sharing

Cloud computing is about gathering and centralizing resources. In this way, a pattern is achieved to provide services for each user. It can redistribute and utilize the collected resources according to users' own requirements. In this way, cloud computing meets the needs of customers.

2.2.2 High scalability and shrinkage

While providing services for users, cloud computing has the characteristics of scalability and shrinkage. When users experience cloud computing security, they can redistribute flexibly and autonomously according to their own needs. This pattern improves the efficiency of cloud computing resources allocation.

2.2.3 Diversified access modes

In recent years, with the increasing importance of e-commerce to user experience mode. Users can access cloud computing not only from desktop computers, but also from mobile phones, tablets and laptops.

2.2.4 Pay according needed

The emergence of cloud computing reduces the cost for customers. The customers can select the required resources and pay for them according their own needs when they query the resources. This paid behavior can not only bring benefits to resource providers, but also refine the access process of resource searchers.

3. The problems of computer security under cloud computing background

3.1 Computer data security

In addition to the large amount of resource storage and fast sharing speed, customers are also very concerned about the security and privacy of resource data when they experience cloud computing. They believe that cloud computing is based on the Internet and can be easily attacked and utilized by hackers or viruses during the resource data transmission. This situation greatly increases the risk for customers in downloading and using resources.

3.2 Computer storage security

Cloud computing stores resources through virtualization and sharing. If the customer stores the resource data on the virtual storage system, then the customer will have the risk of data backup, destruction and access right. If the customer stores the resource data on the Shared storage system, then the customer will face the risk of data leakage and loss. Because most cloud computing businesses operate cloud computing programs through cooperation with foreign enterprises, they cannot achieve zero risk for storage security.

3.3 User access management

User access is a critical issue not only for computers, but also for cloud computing. Users can only access and log on to the cloud application if it is legal. Only after logging in, users can create, update, download, copy and paste when retrieving and browsing the software. However, not every user who enters the cloud program has these permissions, but any restrictions on permissions will undoubtedly bring great temptation to hackers. Hackers often exploit vulnerabilities to attack and modify existing data in transit. So that these modified with virus data can achieve some kind of destruction through the user's download and access.

4. The Countermeasures of Computer security under cloud computing background

4.1 Data security management

Data security threats mainly come from two aspects. On the one hand is the user, on the other hand is the cloud. In order to ensure data security, we must do a good job in data security management. Users should avoid using computers in public places when viewing data. At the same time, the user should secure anti-virus software in the computer system to ensure the security of the computer system. Cloud technology personnel must strengthen the cloud management, set up data encryption program, and strengthen data management. For example, when the user is viewing the data, the technician should set the password and ask the user to input the correct password to complete the operation. Through these two ways, data security can be improved and risks can be reduced.

4.2 Attach importance to the management of user rights

User permissions are important credentials to access data and information in the cloud, and also one of the effective measures to ensure data security. In order to ensure computer security, it is necessary to strengthen the management of user rights. First, technicians should establish scientific permissions according to the user characteristics. Second, technical personnel must also strengthen the user rights management. When using the cloud, we should set up multiple authentication to prevent hackers from entering the computer.

4.3 Implement dynamic password

In recent years, people use the network for various data storage and business access. The key of cloud computing data security is data security and privacy protection. Using dynamic encryption to encrypt data can ensure the data security of cloud computing. We need to encrypt the transmitted data and store it in the cloud, which can effectively improve the data security and prevent data from being stolen. If the data is stolen by hackers, there is no corresponding dynamic password, and the stolen data will not be opened. At the same time, the cloud encryption operation effectively avoids the efficiency problem when the encrypted data is operated compared with the traditional operation. If you need to operate the ordinary encryption scheme, you must return the encrypted data to the cloud after decryption.

4.4 Enhance monitoring measures

People use the cloud for data manipulation. After the user transfers the data to the cloud, the user must take some necessary monitoring measures and reach an agreement with the cloud. Cloud computing configuration and network environment must be effectively monitored and managed through the third-party platform. As soon as we find that there is something wrong with our data, we should call the police immediately to prevent the data from being stolen.

5. Conclusion

Nowadays, computer security is a hot topic. Ensuring the security of the computer is also a more difficult work, computer security under cloud computing background is becoming more and more important. This needs to strengthen the security measure from many aspects, enhances the computer security management level. This paper probes into the problems related to computer security, hoping to help solve practical problems.

References

- [1] Wang Lili, Li Ping, Li Lihong. Discussion on computer security issues and countermeasures under the background of cloud computing [J]. Science and technology outlook. 2016(05):19.
- [2] Du Pu. Computer security problems and countermeasures in the context of cloud computing [J].

Heilongjiang science and technology information. 2016(07):154.

[3] Wang Yuanpeng, Computer security problems and countermeasures in the context of cloud computing [J]. China Informatization. 2017(9):65-67.

[4] Zhang Chaocheng, Zhang Song. Computer network information security attack and prevention [J]. Network security technology and application. 2018(06):5-6.