Journal of Electronics and Information Science (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2023.080210
ISSN 2371-9524 Vol. 8 Num. 2

Network information security technology based on cloud computing environment

Li Ke[*]

Shandong Rongyue Financial Holdings Co., Ltd, Jinan, Shandong, China
[*]Corresponding author: like@royojr.com

Keywords: Cloud computing; Network information; Safe practice

Abstract: With the rapid development of cloud computing technology, the problem of network information security has become increasingly prominent. This paper aims to study the network information security technology based on cloud computing environment, in order to improve the security and reliability of the network system. Firstly, the challenges and problems faced by network information security in cloud computing environment are analyzed, including data privacy protection, identity authentication, access control and so on. Then, the common network information security technologies, such as encryption algorithm, firewall and intrusion detection system, are introduced, and their applications in the cloud computing environment are discussed. Then, a network information security technology framework based on cloud computing is proposed, which comprehensively considers the characteristics of cloud computing and the requirements of network information security, and can effectively protect the network system in the cloud computing environment. The research results of this paper are of great significance for improving the level of network information security technology in cloud computing environment, and also have certain reference value for promoting the development and application of cloud computing technology.

1. Introduction

1.1 Network information security issues in the cloud computing environment

In the cloud computing environment, the problem of network information security becomes more complicated and severe. In the cloud computing environment, users' data are stored on the servers of cloud service providers, so data privacy protection has become an important issue. Users need to ensure that their data is not accessed and stolen by unauthorized personnel during transmission and storage. In addition, users also need to pay attention to whether the cloud service provider encrypts and controls the data reasonably. Users need to be authenticated to access cloud services. However, the security of identity authentication mechanism directly affects the overall security of cloud computing environment. If the authentication mechanism is flawed or attacked, the attacker may impersonate a legitimate user to perform illegal operations. Therefore, designing a secure and reliable identity authentication and access control mechanism is an important task in the cloud computing environment.

In the cloud computing environment, the network system is facing various types of network attacks, such as DDoS attacks and SQL injection attacks. These attacks may lead to serious consequences such as unavailability of system services and data leakage. In order to detect and stop these attacks in time, it is necessary to deploy an efficient intrusion detection system in the cloud computing environment. Data backup and recovery is an important means to ensure data reliability and availability. However, there may be security risks such as data leakage and data integrity problems in the process of data backup and recovery. Therefore, the data backup and recovery mechanism in cloud computing environment needs to have high security.[1]

The above issues are important for the network information security in the cloud computing environment. To solve these problems, it is necessary to comprehensively consider the characteristics of cloud computing and the requirements of network information security, and put forward corresponding solutions and technical measures.

1.2 Research purpose and significance

In the cloud computing environment, the problem of network information security has become increasingly serious, which has become one of the important bottlenecks in the development of cloud computing. The purpose of this paper is to explore the network information security technology based on cloud computing environment, so as to improve the security and reliability of the network system. Analyze the challenges and problems faced by network information security in cloud computing environment; Research and evaluate the application effect of common network information security technologies in cloud computing environment; A technical framework of network information security based on cloud computing is proposed to solve the network information security problem in the cloud computing environment.

As a new computing mode, cloud computing has a wide range of applications, but the security of network information has always been the bottleneck of its development. The research results of this paper are helpful to improve the technical level of network information security in cloud computing environment and promote the development and application of cloud computing technology. The network system in the cloud computing environment is facing various security threats and attacks, such as data leakage and identity forgery. The research results of this paper will help to provide effective network information security protection measures and improve the security and reliability of the network system. Users usually rely on third-party cloud service providers for data storage and processing. The research results of this paper will help to protect users' data privacy and rights, and prevent data from being maliciously tampered with, abused or leaked. This paper will introduce and evaluate the application effect of common network information security technologies in cloud computing environment, and provide reference for research and practice in related fields. At the same time, the technical framework of network information security based on cloud computing proposed in this paper will also provide an effective solution for relevant researchers and practitioners. [2]

To sum up, the purpose of this paper is to improve the technical level of network information security in cloud computing environment, and its research results have important theoretical and practical significance. Through the research of this paper, it will provide strong support for the development and application of cloud computing technology, improve the security and reliability of network systems, protect users' data privacy and rights, and promote the research and application of network information security technology.

2. Network information security challenges in the cloud computing environment

2.1 Identity Authentication and Access Control

In the cloud computing environment, identity authentication and access control are key technologies to protect network information security. Authentication is the process of verifying the identity of users, ensuring that only legitimate users can access cloud computing resources. Access control is to control users' access rights to resources to prevent unauthorized access and data leakage.

In the traditional authentication method, the user authenticates by providing the user name and password. However, this method is vulnerable to password guessing, password leakage and other attacks. Combine multiple authentication factors, such as passwords, fingerprints, smart cards, etc., to improve the security of identity authentication. Two-factor authentication can effectively prevent the risk of password theft. Use biometric information, such as fingerprint, iris, voiceprint, etc. for identity authentication. Biometrics are unique and difficult to forge, so they have high security.

Assign users to different roles, each role has different rights, and control users' access rights to resources through roles. RBAC can improve the flexibility and manageability of the system. Access rights are controlled according to users' attributes and environmental conditions. ABAC can dynamically adjust the access control strategy according to the specific situation, and provide more detailed access control. Control users' access rights to resources based on system security policies and labels. MAC can provide a high degree of protection, but it usually needs to be configured and managed by administrators. Allow owners of resources to decide for themselves who can access their resources. DAC provides flexibility, but it also easily leads to confusion in rights management. [3]

Cloud computing is usually multi-tenant, and data and resources of different users need to be isolated and protected from each other. Therefore, identity authentication and access control need to take into account the characteristics of multi-tenant. There may be a large number of users in cloud computing environment, which puts forward higher requirements for the performance of identity authentication and access control. Efficient authentication and access control mechanisms are needed to meet the needs of large-scale user management. There may be different cloud service providers and different authentication systems in the cloud computing environment. Need to solve the integration and interoperability problems between different systems.

2.2 Data backup and recovery

In the cloud computing environment, data backup and recovery is an important part of network information security. Due to the large-scale data storage and processing in cloud computing, the security and reliability of data are very important for protecting users' privacy and business continuity.

In the cloud computing environment, data backup technology can determine the frequency, scope and storage location of backup. According to the change of data, choose incremental backup or full backup to reduce the consumption of backup time and storage space. The backup data is compressed and encrypted to reduce storage space and improve data security. Ensure the consistency and integrity of the backup data and the original data, so that the data can be restored correctly when restoring.

In the cloud computing environment, data recovery technology can determine the priority and steps of recovery to ensure the timely recovery of key data. During the recovery process, check the consistency and integrity of the backup data to ensure that the recovered data is correct. In the process of data recovery, disaster recovery and failover strategies need to be considered to ensure business continuity and availability. By optimizing the data recovery algorithm and technology, the speed and efficiency of data recovery are improved.

2.3 Security of data backup and recovery

In the cloud computing environment, the security of data backup and recovery is very important.

Encrypt the backup data and the data in the recovery process to protect the confidentiality of the data. Restrict access to backup data and recovery operations, and only allow authorized users to operate. Log backup and recovery operations for tracking and auditing operation behavior. Improve the reliability and fault tolerance of data backup by means of multiple backup copies. Reasonable selection and application of data backup and recovery technology can effectively improve the data security and reliability of network system in cloud computing environment, and ensure the confidentiality, integrity and availability of user data. However, there are still some challenges and problems in data backup and recovery technology, such as the efficiency of backup and recovery and the guarantee of data consistency, which need further research and improvement.

3. Existing network information security technology

In the cloud computing environment, security authentication and access control technology are important means to protect network information security. Security authentication technology is used to verify the identity and authority of users and ensure that only legitimate users can access cloud computing resources. Common security authentication technologies include password authentication, two-factor authentication and biometric authentication. In the cloud computing environment, due to the large number and wide distribution of users, security authentication technology needs to be efficient and scalable. Therefore, some emerging security authentication technologies, such as attribute-based authentication and multi-factor authentication, have been widely studied and applied.

Access control technology is used to limit users' access rights to cloud computing resources and ensure that only authorized users can operate accordingly. Common access control technologies include role-based access control (RBAC), policy-based access control (PBAC) and attribute-based access control (ABAC). In the cloud computing environment, access control technology needs to be efficient and flexible because of the huge scale and dynamic changes of resources. Therefore, some emerging access control technologies, such as attribute-based access control and context-based access control, have been widely studied and applied. [4]

Security authentication and access control technology in cloud computing environment need to consider the following characteristics: multi-tenant environment, dynamic resource allocation, cross-organizational collaboration and so on. Therefore, the traditional security authentication and access control technology needs to be improved and adapted. Some research work has proposed security authentication and access control schemes based on cloud computing environment, such as attribute-based authentication and access control, role-based access control and access control in multi-tenant environment. These schemes have made some achievements in improving the security and reliability in the cloud computing environment.

Although the existing security authentication and access control technologies have made some achievements in the cloud computing environment, they still face some challenges. For example, how to achieve efficient identity authentication and access control, and how to solve the rights management problem in multi-tenant environment. Future research should pay attention to these challenges and propose innovative solutions to improve the security and reliability in the cloud computing environment. At the same time, with the development of technology, new security authentication and access control technologies will continue to emerge, such as authentication and access control technology based on blockchain, authentication and access control technology based on machine learning, etc. These technologies are expected to further improve the network information security in the cloud computing environment.

4. The technical framework of network information security based on cloud computing

The design of the framework should take the security of the network system as the primary goal. This includes the protection of confidentiality, integrity and availability of data, as well as the prevention of unauthorized access and network attacks. The framework should have good scalability to adapt to the ever-changing cloud computing environment and network information security requirements. It should be able to flexibly integrate new security technologies and tools to deal with emerging threats and attack methods. Considering the characteristics of cloud computing and the requirements of network information security, various security measures and technologies are integrated to form a complete security solution. This includes identity authentication, access control, encryption algorithm, intrusion detection system and so on. Considering the high efficiency requirements of cloud computing environment, the impact of security measures on system performance should be minimized. It should have efficient encryption algorithm and access control mechanism to ensure the normal operation and high performance of the network system. [5]

The framework should be able to provide comprehensive network information security protection, including data privacy protection, identity authentication, access control, intrusion detection and so on. Through the comprehensive application of various security technologies and measures, the overall security of the network system is ensured. It has flexible security policy configuration function to meet the security requirements of different users and applications. According to the actual situation, users can customize the security policy and make dynamic adjustments to adapt to different security threats and attacks. Efficient data encryption algorithm and access control mechanism are adopted to ensure the confidentiality and integrity of data. At the same time, the efficiency of access control should be ensured so as not to affect the performance and response speed of the network system. It has a reliable intrusion detection and response mechanism, which can detect and stop network attacks in time. When a security incident occurs, the framework should be able to respond quickly and take corresponding measures to minimize security vulnerabilities and losses.

5. Discussion and prospect

Although there are some methods and technologies for data privacy protection at present, with the continuous growth of data scale and types, data privacy protection is facing greater challenges. Future research can explore more efficient and flexible data encryption and privacy protection algorithms to improve data security and privacy.

In the cloud computing environment, identity authentication and access control are the key links to protect the security of the network system. Future research can focus on developing more intelligent and adaptive identity authentication and access control mechanisms to cope with the ever-changing network environment and threats. With the continuous evolution and complexity of network attack means, the traditional intrusion detection system may not be able to find and respond to new attacks in time. Future research can explore intrusion detection technology based on machine learning and artificial intelligence to improve the recognition and response ability of network system to unknown attacks. Data backup and recovery is an important means to ensure data reliability and availability. Future research can focus on the efficiency and scalability of data backup and recovery, and put forward a more efficient and reliable data backup and recovery mechanism to deal with data disasters and failures.

Blockchain technology provides new ideas and solutions for network information security because of its decentralized and tamper-proof characteristics. Future research can explore the combination of blockchain technology and network information security technology in cloud computing environment to build a more secure and credible network system.

The rapid development of cloud computing has brought more security threats and challenges. By providing an effective technical framework for network information security, this study can improve the security and reliability of network systems in the cloud computing environment and protect users' data and privacy. In the cloud computing environment, network information security is one of the important considerations for users to choose cloud services. The results of this study can provide a safer and more reliable foundation for cloud computing, enhance users' trust in cloud computing technology, and further promote the development and application of cloud computing. Network information security is an important concern of enterprises and organizations, especially in the cloud computing environment. The results of this study can provide an effective technical framework for network information security for enterprises and organizations, help them better protect their own data and privacy, and reduce security risks. [6]

In the future, the network information security technology based on cloud computing environment will continue to receive extensive attention and research. With the popularization of cloud computing and the continuous expansion of application scenarios, the demand for network information security will continue to increase. The results of this study provide a good foundation for future research and application. At the same time, with the continuous progress and development of technology, we can further improve and perfect the existing technical framework of network information security, improve its efficiency and reliability, and meet the ever-changing security needs.

6. Conclusion

In this paper, the network information security technology in cloud computing environment is deeply studied. By analyzing the challenges and problems faced by network information security in the cloud computing environment, we realize the importance of identity authentication and access control, network attack and intrusion detection, and data backup and recovery. In order to solve these problems, the common network information security technologies are investigated and their applications in cloud computing environment are discussed. Based on the research and analysis of the existing technology, a technical framework of network information security based on cloud computing is proposed. The research results of this paper are of great significance to improve the level of network information security technology in cloud computing environment. It provides an effective solution for the network system in the cloud computing environment, which can ensure the security of identity authentication and access control, prevent network attacks and intrusions, and provide support for data backup and recovery. At the same time, the research results of this paper also have certain reference value for promoting the development and application of cloud computing technology.

In the future research, we can further explore and optimize the technical framework of network information security based on cloud computing, and strengthen the research on emerging technologies, such as artificial intelligence and blockchain, to cope with the ever-changing network threats. In addition, we can expand the research scope and explore other aspects of network information security issues in the cloud computing environment, such as cloud storage security and cloud computing platform security. Through continuous efforts and research, I believe that the network information security technology in the cloud computing environment will be further promoted and developed.

References

[1] Wei Yuhao. Discussion on network information security technology in cloud computing environment [J]. China New Communication, 2019, 21(05):123.

[2] Angelababy. Analysis of information security protection technology in cloud computing environment [J]. Software, 2021, 42(04):163-165.

[3] Liu Wenjun. Research on the development of network information security technology in cloud computing environment [J]. China New Communication, 2020, 22(17):33-36.

[4] Tang Rongxiu. Research on the development of network information security technology in cloud computing environment [J]. Wireless Internet Technology, 2021, 18(03):19-20.

[5] Li Minglei. Research on the development of network information security technology in cloud computing environment [J]. Science and Technology Innovation and Application, 2022, 12(36):170-173.

[6] Chen Xiao. Research and Implementation of Network Security Technology and Intrusion Prevention Technology in Cloud Computing Environment [J]. Information and Computer (Theoretical Edition), 2020, 32(11):184-186.