On the Application of Cloud Computing Technology in Computer Security Storage

Honglin Wang
School of Information Engineering, Yancheng Teachers University, Yancheng 224002, China.

Abstract: With the widespread adoption of the Internet and the growing volume of data storage, cloud computing has emerged as the predominant method for storing information. It offers users convenient and efficient storage processes, along with remarkable flexibility and scalability. By dynamically allocating computing resources and storage space according to user needs, cloud computing ensures secure storage of information data. In light of this, this paper provides a comprehensive overview of the specific application of cloud computing technology in the field of computer security storage.

Keywords: Computer; Secure Storage; Cloud Computing Technology

Introduction

In practical applications, the use of cloud computing technology introduces certain potential security risks in network storage. Such security issues can lead to the leakage of users' private data and business information, and even result in losses to corporate trade secrets. To ensure the reliability of network security storage, a series of security measures must be implemented to protect users' data.

1. Overview of Cloud Computing Technology

With the rapid development and widespread adoption of cloud computing technology, cloud-based network storage services have found increasing applications across various sectors of society. This storage approach offers users a superior data storage experience compared to traditional methods that relied on local servers or databases. Resource virtualization, a crucial network storage technology in cloud computing, consolidates previously dispersed storage resources into a virtual resource pool. This integration enhances the efficiency of storage resource utilization and simplifies user access to these resources. Through virtualization technology, users can swiftly create, modify, and delete virtual storage devices without the need for physical device manipulation, thereby ensuring robust storage capabilities and high stability. Cloud computing not only amplifies the efficiency of storage resource utilization but also facilitates the quick and secure storage of the colossal volume of data generated in the digital realm. In the era of big data, cloud computing emerges as a highly promising technology. By leveraging cloud computing, users can expeditiously store, manage, and analyze vast amounts of data, providing more precise support for enterprise decision-making. Cloud-based network storage services have become an indispensable component of prominent enterprises and organizations in today's society. As cloud computing technology continues to advance and innovate, network storage services will become more intelligent, efficient, and secure, delivering enhanced convenience and productivity to people's work and daily lives. Cloud computing technology has three service models: infrastructure services, software services and platform services. Infrastructure services provide scalability services that allow users to use computing resources as needed without having to purchase and maintain their own hardware and software. Software services, on the other hand, are based on virtual desktops, applications and resource management, allowing users to use software on cloud platforms without having to install and maintain their own software. Platform services, on the other hand, provide working platforms, such as databases, development tools and Web services, that allow users to easily develop and deploy their own applications.

2. Application Analysis of Cloud Computing Technology in Computer Security Storage

2.1 Identity Authentication

Identity authentication technology plays a crucial role in network security storage. Ensuring the authenticity and legality of user identities is essential for maintaining network security. Currently, there are three main types of identity authentication technologies based on cloud computing: password authentication, smart IC card authentication, and PKI identity authentication. Password authentication is the most common method, requiring users to input the correct user ID and password to verify their identity. While this method is simple and convenient, it also poses security risks, such as users choosing weak passwords or the risk of password theft. Smart IC card authentication requires users to prepare an IC card in advance and use it for authentication. Users store their personal information on the IC card, which is transmitted through a card reader for identity verification. This method offers strong security and reliability but requires the prior preparation of an IC card, making it relatively cumbersome to use. PKI identity authentication is the most complex yet highly secure method of authentication. It uses public keys as verification facilities and ensures secure network storage through encryption and decryption using matching keys. This method offers the highest level of security but also requires a higher level of technical proficiency to use effectively. Overall, each identity authentication method has its own advantages and disadvantages, and the most suitable method should be selected based on the specific circumstances. The importance of identity authentication technology in network security storage is self-evident. To ensure the security of user identities, it is crucial to ensure that user authentication is valid and reliable.

2.2 Data Encryption Technology

With the development of information technology, the amount of data stored on the internet is increasing, and many people choose to store it in the cloud. Although this storage method provides convenience for people's work and life, it also poses significant risks to data security. Plain data is susceptible to attacks from hackers and malicious software, leading to information leaks and losses. To protect data security, cryptographic data encryption techniques have been proposed. Data encryption refers to transforming plaintext into unrecognizable ciphertext according to specific cryptographic rules. Currently, symmetric and asymmetric encryption techniques are widely used. Symmetric encryption uses the same key for encrypting and decrypting plaintext, so the security of the key must be ensured during transmission and processing to prevent risks of hacking and key leakage. In contrast, asymmetric encryption provides higher security for cryptographic systems while improving the efficiency of information transmission and management. It utilizes a pair of public and private keys, where the public key can be distributed freely, and the private key is held only by the user, ensuring the security and convenience of key transmission. However, the complexity of asymmetric encryption technology limits its widespread adoption to some extent. Therefore, in practical applications, it is necessary to choose the appropriate encryption technique for data encryption and decryption based on the security requirements and transmission efficiency of the data. In conclusion, data encryption technology plays a crucial role in network security storage systems. By using encryption techniques to protect information security, it is possible to prevent intrusion and theft and ensure the integrity and reliability of information. In the future development of digitalization, data encryption technology will continue to play an important role.

2.3 Data Recovery and Backup

Data recovery and backup technologies play a crucial role in information data storage services. With the development of information technology and the increasing richness of information resources, the security and integrity of information resources have become increasingly important. In this context, there are two main types of cloud-based data recovery and backup systems. Firstly, by connecting clients' local networks to the cloud, key information stored in the local network is regularly uploaded to the cloud for updates and backups, ensuring the security of clients' information. The benefit of this approach is that users can access their data at any time without worrying about data loss. Additionally, due to the vast storage space in the cloud, users can confidently store their data without worrying about storage issues. Secondly, in cloud

computing, all information submitted to the cloud can be stored in the cloud. The advantage of this approach is that users do not need to manually back up their data, and since the backups occur in the cloud, users do not need to worry about the security of backup files. Moreover, if users need to recover data, they can directly perform operations in the cloud, which is very convenient. Of course, in practical applications, various reasons such as erroneous deletion or storage resource failure may occur. In such cases, we can use the data stored in the backup server for restoration, ensuring the integrity and security of data. Overall, cloud computing-based data recovery and backup systems can provide comprehensive data protection for users and are indispensable tools in the modern era of digitalization.

3. Conclusion

In conclusion, the application of cloud computing technology has brought great convenience and development opportunities to information storage and management. However, we must also recognize the security risks and vulnerabilities that exist within it. Only through the joint efforts and effective collaboration of all parties can we ensure the reliability and stability of network security storage.

References

[1] Wang HJ. Jun X. Zhu Y. Application Analysis of Cloud Computing Technology in Computer Network Security Storage. Electronic Technology and Software Engineering, 2020(12).

[2] Yuan GL. Li JJ. Liu HJ. Analysis and Reflection on Computer Network Security Issues in Cloud Computing Environment. Digital World, 2018(34).

[3] Ling YT. Guang LP. Zhang HW. Computer Network Security Storage System in the Context of Cloud Computing Technology. Electronic Technology and Engineering, 2021(76).

About the author: HongLin Wang, Sex:Male, Han, Birth Place: Xinghua, Jiangsu, Date of birth: March 26, 1971, School of Information Engineering, Yancheng Teachers University, Yancheng, Jiangsu, China, 224002, Associate Professor, M.E., Research direction: Computer Network Security