Innovation of Network Information Security Technology under the Background of Cloud Computing Technology

Ding Gaohu

Sichuan Vocational and Technical College, Suining, Sichuan, 629000, China

Keywords: Cloud computing, information security, network.

Abstract: Cloud computing is an emerging application of computer technology based on the internet, which plays an important role in the development of the information industry. It provides internet users with secure and reliable services and computing capabilities. Its information security is not only the primary problem to be solved by cloud computing, but also the key factor to determine the development prospects of cloud computing. This paper mainly analyzes the overview of cloud computing, cloud computing security risks and cloud computing information security.

1. Introduction

Cloud computing is a business computing model, but also a convenient, on-demand, network access to a customizable computing resource pool model, it will be computing tasks distributed in many computers resources pool, so that users can access computing power, storage space and information services on demand, is regarded as a global IT. The third revolution in the industrial revolution. Users can dynamically apply for some resources to support the operation of various applications, which is conducive to improving efficiency, reducing costs and technological innovation. Through cloud computing technology, network service providers can process tens of millions or even billions of information in seconds to achieve the same powerful network services as "supercomputers". The goal of cloud computing system is to transfer the original independent and personalized computing running on PC or single server to a huge number of server "cloud", which is responsible for processing user requests and outputting results. It is a data computing and processing system at the core[1].

2. Overview of cloud computing

2.1 The concept of cloud computing

Cloud computing in a narrow sense refers to the mode of delivery and use of IT infrastructure. It refers to the acquisition of required resources through the network in an on-demand and scalable manner. Generalized cloud computing refers to the delivery and use of services, refers to the network to obtain the required services in an on-demand, easy-to-expand manner. Deployment on demand is the core of cloud computing. To solve the problem of on-demand deployment, we must solve the dynamic reconfiguration, monitoring and automatic deployment of resources, and these

Published by CSP © 2018 the Authors
DOI: 10.23977/iceccs.2018.027

need to be based on virtualization technology, high-performance storage technology, processor technology, high-speed Internet technology. Therefore, besides carefully studying its architecture, cloud computing should pay special attention to the dynamic reconfiguration of resources, automatic deployment, resource monitoring, virtualization technology, high-performance storage technology, processor technology and so on[2].

2.2 Cloud computing architecture

The architecture of cloud computing is illustrated in Figure 1, including the basic management layer, the application interface layer and the access layer. The basic management layer solves the problem of sharing computing resources, the application interface layer solves how to provide services to the outside world, and the access layer uses cloud computing to solve some practical problems.

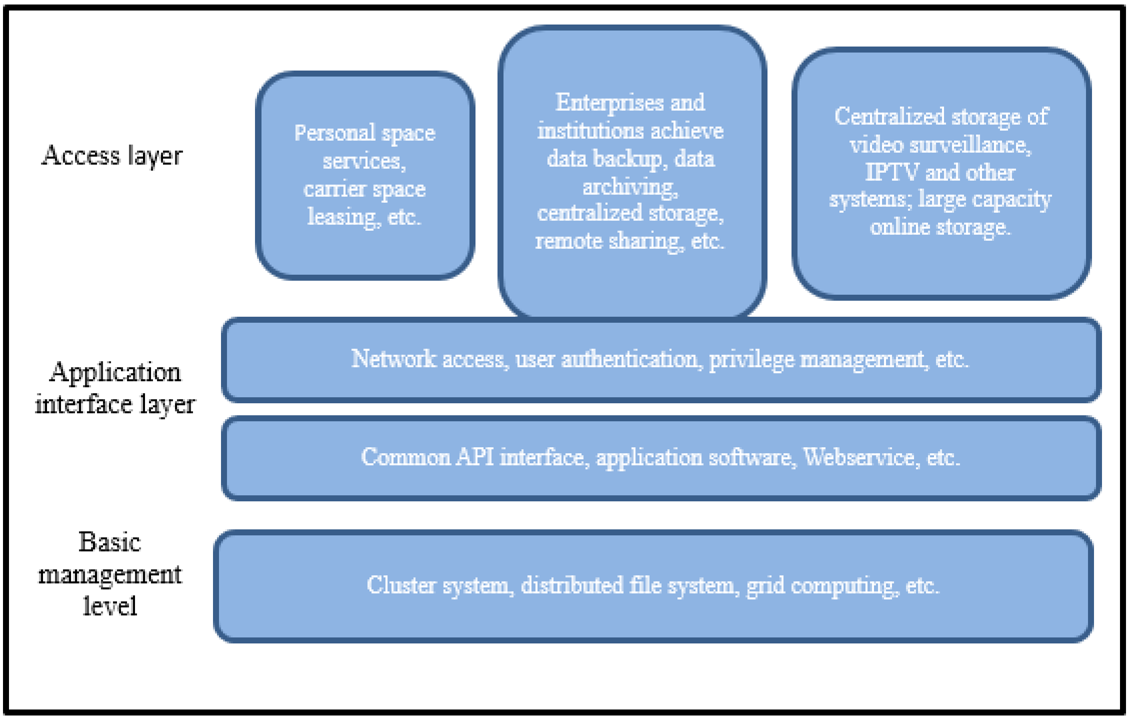
Access layer
Personal space services, carrier space leasing, etc.
Enterprises and institutions achieve data backup, data archiving, centralized storage, remote sharing, etc.
Centralized storage of video surveillance, IPTV and other systems; large capacity online storage.
Application interface layer
Network access, user authentication, privilege management, etc.
Common API interface, application software, Webservice, etc.
Basic management level
Cluster system, distributed file system, grid computing, etc.

Figure 1 Cloud computing architecture

2.3 Characteristics of cloud computing

First, higher reliability: Cloud computing uses branches such as compute node isomorphism interchangeability, data multi-copy fault tolerance, and so on, so it is more reliable than local computers.

Second, the large-scale nature: consisting of several nodes with a certain scale, the scale of the system can be unlimited.

Third, a high degree of scalability: Plug and play is available to facilitate, quickly increase and reduce resources, scalability and resilience is relatively high.

Fourth, resource sharing: Provides one or more forms of computing or storage capability resource pools, such as physical servers, virtual machines, things and file processing capabilities or task processes[3].

Fifth, dynamic allocation: to achieve automatic allocation and management of resources, including real-time monitoring and automatic scheduling of resources, and can provide monitoring and management of usage.

Sixth, cross-regional: can be distributed in several physical locations to integrate resources, provide a unified sharing of resources, and can achieve load balancing between physical locations.

3. Risk analysis of cloud computing information security

Although many research institutes believe that cloud computing provides the most reliable and secure data storage centre, security is one of the main problems in cloud computing. Although each cloud computing solution provider emphasizes the use of encryption technology (such as SSL) to protect user data, even if the data is encrypted using SSL technology, it is only exponential data encrypted over the network transmission, data processing and storage protection is still not resolved. There are mainly the following security risks:

3.1 Security risks caused by the blurring of network boundaries

In the traditional network boundary protection, the area is generally divided according to the importance of resources in the network. The boundary between each area is clear, and then the corresponding boundary protection measures are taken in different areas according to different security requirements. However, in the cloud computing environment, due to the massive use of virtualization technology, resource pooling technology leads to a high degree of integration of hardware infrastructure such as servers, storage devices and network devices in the cloud computing environment, multiple systems running on the same physical device at the same time, the traditional network boundaries are being broken, the traditional sense of the network. Border protection measures also need to be adjusted to adapt to new technological changes[4].

3.2 Security risks faced by remote transmission of information

In the cloud computing environment, all data processing and storage are completed in the cloud, and the user only has less computing power. This means that the user's raw data, the processing requests sent, the content displayed by the client and other data need to be transmitted through the network, cloud computing environment will be heavily dependent on the network. How to ensure the confidentiality and integrity of data transmission between cloud and client is a problem to be solved in the open Internet.

3.3 Security risks faced by centralized information storage

If a user migrates to a cloud environment, all the user's data will be in the cloud. What technology does the cloud service provider use to ensure that the user's data is properly preserved in the cloud without unintentional or malicious disclosure? How can the user ensure that the data he or she stores is legitimate and accessed by authorized users? However, whether the security mechanisms, such as identity authentication, authentication management and access control, meet the needs of users in cloud computing environment has become an urgent problem to be solved[5].

3.4 Security risks faced by cloud servers

In the cloud computing environment, due to the large concentration of data and resources, cloud servers need to undertake more onerous tasks than traditional network architecture servers. Cloud computing environment to provide external application services, data processing needs of users, etc. need to be completed by the cloud server. But at the same time, the open network environment and multi-user application scenarios bring more hidden dangers to the security of cloud servers.

4. Information security strategy in cloud computing environment

4.1 Data transmission security

Data transmission in a cloud computing environment includes two types, one is remote data transmission across the Internet between users and the cloud, and the other is data transmission within the cloud between different virtual machines. To ensure the security of data transmission in the cloud, it is necessary to implement end-to-end transmission encryption in the process of information transmission. Specific technical means can adopt protocol security socket layer or transport layer security protocol (SSL/TLS) or IPSec to implement data between cloud terminals and cloud servers, and between cloud application servers based on SSL protocol. Transmission encryption.

Homomorphic encryption mechanism should be adopted as much as possible to improve the security of user terminal communication in some high security application scenarios. Homomorphic encryption refers to the cloud computing platform can directly process the user's ciphertext data without decrypting user data and return the correct ciphertext results. Homomorphic encryption technology can further improve the security and reliability of user data transmission in cloud computing environment, but this technology is still in the research stage, cannot be put into commercial applications.

4.2 Data storage security

One of the most effective solutions to secure data storage in cloud computing is to encrypt data. Encryption in cloud environment can be divided into two ways: one is using object storage encryption; the other is using volume label storage encryption.

Object storage is a file / object library in a cloud computing environment that can be understood as a file server or hard disk drive. To realize data storage encryption, the object storage system can be configured as an encrypted state, that is, the system encrypts all data by default. However, if the object storage is a shared resource, that is, when multiple users share the object storage system, in addition to setting the object storage to an encrypted state, a single user needs to use the "virtual private storage" technology to further improve the security of private data storage. "Virtual Private Storage" is that the user encrypts the data first and then transfers it to the cloud environment. The key of data encryption is in the hands of the user. Even the administrator in the cloud computing environment is not entitled to the key, which can ensure the security of the user's private data storage.

Another solution to data storage security is volume label storage encryption. In the cloud computing environment, the volume label is simulated as a common hardware volume label. There are two ways to encrypt the volume label data: one is to encrypt the actual physical volume label data, and the user volume label is not encrypted by the encrypted physical volume label instance, that is, the user volume label is adopted in the process of instantiation. The encryption and decryption process are completed in a transparent manner; another is to use a special encryption proxy device, which is serially deployed between a computing instance and a storage volume label or file server. These encryption proxy devices are also the virtual devices in the cloud computing environment. The transparent data encryption and decryption between the computing instances and the physical storage devices are realized by serial way. Its working principle is that when a computing instance writes data to a physical storage device, the data of the computing instance is encrypted and stored in the physical storage device by the encryption agent device; when the computing instance reads the data of the physical storage device, the data in the physical storage device is decrypted by the encryption agent and the plaintext is handed over to the computing reality. Example.

5. Concluding

Cloud computing is the trend of the development of Internet industry in the future. This is the research hotspot this year. With the further development and application of cloud computing, information security is bound to become a key technology in the development of cloud computing, whether for cloud service users or cloud service providers. This paper mainly summarizes the related knowledge of cloud computing and discusses the information security issues in the cloud environment.

References

[1] Wang Xiaoni, Han Jiangang. Research on Information Security Threats and Defense Strategies Faced by Cloud Computing [J]. Aeronautical Computing Technology, 2018,48(02): 113-117+121.

[2] plateau, Wu Changan, cloud computing, information security research [J]. information science, 2015,33 (11): 48-52.

[3] Song Hao. Research on Key Technologies of Information Security Level Protection and Evaluation of Cloud Computing Information System [J]. Information Network Security, 2015 (09): 167-169.

[4] Hui Zhibin. Research on the Theory and Countermeasure of Cloud Computing Information Security in China [J].Science and Technology Management Research, 2013, 33 (16): 171-174 + 180.

[5] Tong Detian, Liu Xudong, Guo Taofeng, Liang Jiewen. Cloud computing information security analysis and practice [J].Telecommunications Science, 2013, 29 (02): 135-141.