Research on Data Security Storage Strategy in Cloud Environment

He Qian

Chongqing College of Electronic Engineering, Chongqing 401331, China

11047225@qq.com

Keywords: Data Security, Storage Strategy, Cloud Environment

Abstract: As a new network computing model, cloud computing has remarkable features such as large scale, highly virtualization and high scalability. It can provide users with high-quality, low-cost and on-demand data storage services, namely cloud storage. The emergence of cloud storage meets the needs of massive data on the storage space, but a series of cloud storage security incidents frequently occur in the most convenient cloud storage services to users, which is hardly to protect the user's information and asset safety belt with huge threats and challenges. So data security issues cannot be ignored. Studying how to protect users' data storage in complex cloud environments is of great theoretical and practical significance for promoting the deep development of cloud computing and its applications.

1. Introduction

With the widespread application and continuous development of Internet technology, the data has exploded which has higher requirements for storage system capacity, performance and scalability, and also drives the rapid development of network storage technology at this stage. As an emerging network computing model, Cloud Computing is a product of the integration of computer technology and network technology in the traditional sense. With the core of resource renting, application hosting and service outsourcing, cloud computing rapidly becomes a hot spot in the development of computer technology. Specifically, it uses computer technologies such as virtualization, distributed processing, Web services and online software to converge various types of resources such as computing and storage and provide them to users in a service manner, which makes the traditional storage on the client side Data and information are all sent to the huge cloud computing data center, and the daily management and maintenance of data and information are all undertaken by cloud service providers.

In cloud computing, data storage is the focus, but also the foundation. Data storage in the cloud environment, that is, cloud storage, refers to technologies such as converged cluster applications, grid computing, distributed computing, and Web online. The application software integrates a large number of different types of storage devices in a network into a powerful virtual resource pool and make them work together to jointly provide data storage and business access functions of a system is a new cloud-based technology. Compared with the traditional data storage technology, cloud storage has the unique advantages of large capacity, high scalability, high versatility and high reliability. Its most prominent feature is Storage as a Service (SaaS). Users can by requesting services, on-demand metering, using storage resources in cloud storage anytime, anywhere and solving the problems of insufficient local hardware and software resources, inconvenience of movement, destruction or loss of storage devices, etc. at a small cost.

As an important part of user's assets, data information occupies the core position in people's daily work, study and life. In the cloud storage service mode, the user's data and information are all stored on the cloud server. As the legal owner of the data, the user still has the right to perform various maintenance and operations on the data. In addition, as the cloud storage service is network-based, the data storage server may be illegally attacked due to software defects, and some human factors or hardware failures may also pose a security threat to the user's data. In the case of lack of necessary Protection measures, the consequences will be disastrous. Coupled with the

frequent occurrence of a series of cloud storage data security incidents, it is enough to show that current Cloud Storage Providers (CSPs) do not provide effective security guarantees. For example, Amazon clearly stated in the official document of EC2 that it cannot to ensure the safety of user data, and suggested that users use additional security technologies, such as encryption, access control and other technologies.

Often, most users do not tend to outsource the storage of their data to CSPs for security reasons. Frequent emergence of various security incidents by famous cloud service providers such as Amazon and Google has further exacerbated the concerns of people. In 2012, the cloud server of Chinese grand cloud service provider failed, resulting in a loss of user data. In addition, a survey of more than 500 executives from around the world found that the primary reason they refuse to use cloud storage is their data security and privacy concerns. This shows that cloud storage services to bring great convenience for users, but also for the realization of user information assets security and privacy protection has brought great challenges. Whether it is important data for private users, or valuable information for business users, must have storage security protection. The data security of cloud storage needs to be solved urgently. Studying the data storage security technology in cloud computing environment has great theoretical and practical significance for promoting the deep development of cloud computing and its applications.

2. The Cloud Computing Service Model

Since the birth of cloud computing, experts and scholars in relevant fields have different understandings of its concept. Generally speaking, cloud computing can be understood as a technology, a service, or a business model. It is a cluster of computing capabilities will be pooled, including computing power, storage capacity through the Internet to provide all kinds of users on demand Internet technology, new services and new business is the traditional IT areas of progress and commercial. The result of the common promotion of pattern transformation. Because of its remarkable features such as large scale, highly virtualization, high scalability, ease of use, universality, high reliability, on-demand use and automation management, cloud computing has not only received extensive academic attention, but also gained the real rapid development of industry.

Typically, cloud computing can provide users with three levels of service models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service, SaaS). These three service modes, also known as "SPI mode," are three types of functions that are based on the cloud physical infrastructure and are layered hierarchies that are independent of each other. Among them, IaaS is the foundation of all cloud services, PaaS is based on IaaS, and SaaS is based on PaaS.

Cloud storage can serve as an important form of IaaS service model. It is not only a new type of network storage technology based on cloud computing, but also a cloud computing system capable of providing online storage services to users in essence. This is because when the core function provided by a cloud computing system is the centralized storage and management of large amounts of data, the system must intensively and uniformly configure and manage a large number of storage devices, and at this moment, it is transformed into a typical cloud Storage System.

Data Storage Layer: The data storage layer at the bottom, to provide the most basic physical facilities. It connects various types of storage devices (such as SCSI, SAS, NAS, etc.) over the network, and builds a unified and intensive storage management system based on this, so as to realize the centralized management and maintenance of storage data.

Basic Management: Utilize technologies such as grid computing, cluster technology and distributed processing so that multiple storage devices can be coordinated and synchronized to ensure the stability of the storage device management system and provide users with unified and efficient services.

Application Interface Layer: Cloud storage service providers design and develop various application interface APIs according to their actual business needs and provide different types of application services to users through various application interfaces.

User Access Layer: Users use the cloud storage service according to their actual needs and

through a common API interface. However, users must be authenticated and authorized by the cloud storage server before starting to use the cloud storage service.

3. The Necessity of Cloud Storage Data Security

While cloud computing is gaining momentum, a series of security incidents have emerged, posing a huge challenge to the development of cloud computing and its applications. For example, Azure, the Microsoft cloud computing platform that took place back in 2009, crashed out of service for 22 hours due to a platform-centric processing and storage device failure. The downtime event on the Azure platform exposed a major cloud computing hurdle and caused Microsoft Company users worried about Azure platform security. Amazon suffered the worst security incident in its history in 2011 with massive downtime of its cloud data center servers, raising fears about the migration of its infrastructure to the cloud and its incomplete trust of third-party agencies. In addition, cloud storage service provider Dropbox made it clear that some users 'Dropbox accounts were hacked from third-party sites, causing the user's account and password to be compromised, threatening the users' most fundamental interests. Cloud computing security issues cannot be ignored, its own security is the core factor restricting its in-depth development, many well-known domestic experts to carry out research.

Feng Dengguo and others focused on the risks and challenges brought by cloud computing in the field of information security in the literature and set up a comprehensive and comprehensive evaluation system from three aspects of cloud user security objectives, cloud computing security service system and cloud computing security support service system Cloud computing security reference framework, summarizes the key technologies of cloud computing security protection and key research content, which points out the direction for future research work. Lin Chuang et al. analyzed the key issues in cloud computing security from three aspects of cloud computing security architecture, cloud computing security mechanism and cloud computing model evaluation, and proposed a manageable, controllable and measurable cloud computing security architecture, which laid the foundation for further research.

In cloud computing, data storage is not only the focus, but also the basis for data security is also the top priority cloud computing security. Therefore, data information as an important part of corporate and personal user assets, the data stored in the cloud information is the user's most concerned about the security issues.

4. Cloud Data Storage Security Related Technologies

4.1 The Cipher-text Access Control Technology.

Data confidentiality means that only the data owner and the authorized user can access or receive the data in plain text, and no other user can access or receive the data in plain text. Currently, the most commonly used method of data confidentiality protection is encryption. Often, users encrypt data before transmitting their data to the cloud. Access control is to protect the legitimacy of the use of information, network security, system resources, one of the important strategies. Since the data stored in the cloud is in the ciphertext state, the user's access changes to an access control problem of ciphertext. Ciphertext access control technology is to encrypt the key information, and then control access to key information by controlling access to the user. It is an important means to ensure the confidentiality of user data in the untrustworthy cloud environment. It cannot only effectively improve the confidentiality and privacy of user data, but also greatly reduce the risk of user data from being illegally disclosed.

4.2 Integrity Verification.

The integrity of technical data is an important basis for reflecting the authenticity and reliability of data, including the integrity of the storage and the integrity of the use. Generally, the data integrity in the cloud storage environment refers to that the cloud storage service provider stores the data intact on the cloud server according to the user's needs, that is, the integrity when storing. The

integrity verification of data in the cloud storage environment, also called provable storage, is to allow the user to prove by some knowledge protocol by retrieving a small amount of stored data or to judge whether the data stored in the cloud is highly probable Complete. In the traditional sense, there are mainly two kinds of data integrity verification methods in storage system: one is based on access and the other is based on challenge-response. In contrast, the latter is more suitable for distributed cloud storage environment. Challenge-response-based integrity verification models include verifiers and respondents. The verifier is usually the data owner or the trusted third party, the responder is the cloud server. The working principle is as follows: first, the verifier sends a challenge message to the cloud server; then, the cloud server generates and returns the corresponding response message according to the content of the challenge message; finally, the verifier performs the integrity verification and judgment according to the received response message. The main technologies used include Provable Data Possession (PDP) technology and Proof of Retrievability (POR) technology.

5. Conclusion

In recent years, cloud computing has drawn wide attention from industry and academia due to its convenience and ubiquity. It can flexibly configure computing resources (such as network, storage and service, Servers, etc.), all services are provided to the users on demand and these resources can quickly be provisioned and released with minimal administrative costs and service provider interactions. As a new Internet-based IT service model, cloud computing has revolutionized traditional computing and storage businesses.

References

[1] Feng Zhaosheng, Qin Zhiguang, Yuan Ding. Technology for Secure Storage of Cloud Data [J]. Computer Science. 2015 (01)

[2] Zhang Kai, PAN Xiaozhong. Access Control Model Based on User Behavior Trust under Cloud Computing [J]. Journal of Computer Applications. 2014 (04)

[3] Feng Dengguo, Zhang Min, Li Hao. Big Data Security and Privacy Protection [J]. Computer Journal. 2014 (01)

[4] Zhou Wenqiong, Li Qingzhong, Fan Luqiao, Zheng Shuzhao. Research and Implementation of SaaS Multi-Tenancy Data Storage Model [J]. Computer Science. 2013 (10)

[5] Zhao Weidong, Bi Xiaoqing, Lu Xinming. Design and implementation of role-based fine-grained access control model [J]. Computer Engineering and Design.2013 (02)

[6] Zhang Xiao-hua, Miao Yu-qing, Su Jie, Wu Kong-ling. Privacy Protection Association Rules Mining with Vertical Distribution [J]. Computer Engineering and Design.2012 (05)