Study on Data Security Policy Based On Cloud Storage

DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan
University of International Relations,
Beijing, China

***Abstract*—Along with the growing popularisation of Cloud Computing. Cloud storage technology has been paid more and more attention as an emerging network storage technology which is extended and developed by cloud computing concepts. Cloud computing environment depends on user services such as high-speed storage and retrieval provided by cloud computing system. Meanwhile， data security is an important problem to solve urgently for cloud storage technology. In recent years, There are more and more malicious attacks on cloud storage systems, and cloud storage system of data leaking also frequently occurred. Cloud storage security concerns the user's data security. The purpose of this paper is to achieve data security of cloud storage and to formulate corresponding cloud storage security policy. Those were combined with the results of existing academic research by analyzing the security risks of user data in cloud storage and approach a subject of the relevant security technology, which based on the structural characteristics of cloud storage system.**

Keywords—cloud computing; cloud storage; security policy; data security

I. INTRODUCTION

A. Research background

As the development and progress of computer technology, the Internet has been becoming an integral part of one's life. The user-demands of internet use have not only limited to browse the portal but also to the development of Internet application services resulting in explosive growth of internet data. Facing massive data, the ISPs needs more processing units and storage devices to ensure the regular operation of the corresponding system functions. However, it is still an urgent issue to solve for ISPs that the high cost of memory devices, personnel management, and equipment maintenance. To reduce these problems, cloud computing came into existence. Compared to the traditional computing model, the cloud computing model distributes computing tasks on a large number of computers due to the explosive growth of internet data today. This model allows users to allocate resources to the required on demand and access the computer and storage systems on demand, providing fast, efficient, and inexpensive computing power that maximises users' storage service needs. As a result, the data computing model has changed from the traditional computing model to the large data cloud computing model.

At present, as an emerging network storage technology extended and developed by cloud computing concepts, cloud storage technology is essential with the widespread popularisation of Cloud Computing. Cloud storage technology uses cluster applications, network technology or distributed file systems, etc. Cloud storage technology makes full use of the existing different storage devices in the system to provide users with data storage, data retrieval, data backup and other functions through application software ran by a user terminal.

B. The purpose and significance of the study

More and more individual and business users focus on cloud storage and transfer data to cloud storage with the development of cloud storage. Using cloud storage services requires users to store the data in the cloud storage device, instead of storing data on a PC as traditional computing model does. There must be a outsize risk because users do not know the boundaries of the cloud storage system, do not know whether the storage devices were shared, and can not ensure the availability and reliability of storage devices. The data of the user may be stored in a shared cloud storage system instead of storing in devices of cloud service provider. So users cannot control data security to ensure the confidentiality and integrity.

978-1-5090-6296-6/17 $31.00 © 2017 IEEE
DOI 10.1109/BigDataSecurity.2017.12

Cloud storage technology has no standardised, normalised security policy as an emerging network storage technology, notwithstanding cloud service providers have put forward many specific cloud storage safety measures. Moreover, previous research results lacked enough systemic and in-depth analysis and discussion about the security risks and cloud management leaks of cloud storage users. To attract more Internet users and promote cloud computing and cloud storage systems successfully, this paper summarises a perfect security policy that applied to cloud service providers and users which aiming at ensuring the safety and reliability of the data and the benefits of cloud service providers and users.

II. RELATED KNOWLEDGE AND RESEARCH STATUS

A. Basic concepts

i） Cloud computing

In recent years, the data of network application is showing the scale of explosive growth. Some traditional server devices are too difficult to load a huge amount of data processing. Meanwhile, the costs of server operation and maintenance are also increasing. As a result of distributed processing, parallel processing and grid computing, cloud computing will split a huge calculate processing tasks into some subroutines through the network automatically. And then return the result to a user after calculated and analysed by a system composed of many servers. Service providers' net service can deal with tens of millions or even billions of information in a few seconds using cloud computing technology, which is as powerful as "supercomputer". Furthermore, the service is multi-functional such as a model of computer and software, Internet-related, etc.

The architecture models of cloud computing system consist of three layers:

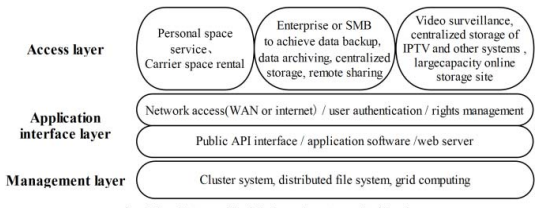

figure1:The architecture models of cloud computing system consist of three layers

Characteristics and advantages of cloud computing:

a） Virtualization

Users can use variety kinds of terminals to obtain application services regardless of whatever his location is and do not need to care about where the application runs.

b） High reliability

Cloud computing ensures high reliability of service using multiple copies of data for fault tolerance and node isomorphism interchangeable.

c） Very Large Scale

At present, cloud computing has a considerable scale, superior business such as Google, IBM, Yahoo has hundreds of thousands to millions of servers.

d） On-demand service

Cloud computing allows users to purchase anytime, anywhere according to their needs.

e） Low-cost

Automated centralised management of cloud computing allows many companies do not need to burden the high cost of data centre management. The versatility of cloud computing is a huge improvement of resources utility compared with a traditional system.

ii）Cloud storage

Cloud storage has become one of the hotspots of information storage recently with the rise of cloud computing. Cloud storage refers to a system that provides data storage and service access functions for users through cluster application, network technology and distributed file system, which collects a large number of different types of storage devices in the network through application software to work together.

In summary, cloud storage is a service, which is not referred to a device, but rather an aggregation of many storage devices and servers for users. For those who use cloud storage, they use the data access service provided by entire cloud storage system instead of using merely a storage device. Storage service stores the local data over the network in the online storage space provided by the Storage Service Provider (SSP). Users who need to store services only need to apply for storage services to the SSP rather than to build their data centres. Therefore, users avoid the duplicated construction of the storage platforms and save expensive investment of hardware and software infrastructures.

The structure of the cloud storage system consists of four layers:

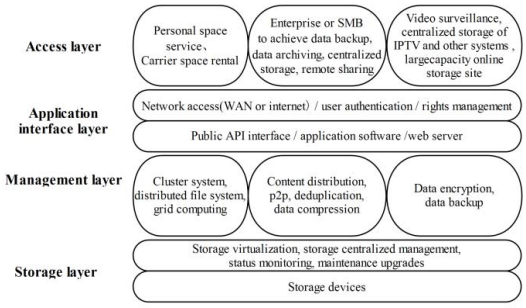

figure2:The structure of the cloud storage system consists of four layers.

a) Storage layer

The storage layer is the most fundamental part of cloud storage. The storage device can be an FC Fiber Channel storage device. It also can be an IP storage device such as NAS and iSCSI, or a DAS storage device such as SCSI or SAS. Cloud storage system often consists of numerous storage devices which distributed in different regions. They were connected to each other through WAN, Internet or FC fibre channel network. Over storage devices, the unified storage device management system will achieve logic virtualization management, multi-link redundancy management of storage devices and status monitoring and fault maintenance of hardware devices.

b) Management layer

Management layer is the core of cloud storage and the part most difficult to achieve. Management layer implements the collaboration between multiple storage devices in the cloud storage through the cluster, distributed file system and grid computing technology so that multiple storage devices can provide the same service and greater and better data access performance.

CDN content delivery system and data encryption ensure that cloud storage data will not be accessed by a unauthorised user. Meanwhile, to keep the security and stability of cloud storage, taking measures such as data backup and disaster recovery can prevent cloud storage data from being lost.

c) Application interface layer

Application interface layer is the most flexible part of cloud storage. According to the actual business type, different cloud storage operators can develop different application service interface, providing a series of services. For example, video surveillance application platform, IPTV and video-on-demand (VOD) application platform, network hard disk application platform, remote data backup application platform, etc.

d) Access layer

Any authorised user can access the cloud storage system through the standard public application interface and enjoy cloud storage service. Access types and access methods provided by cloud storage are the different results from the difference of operating units.

B. Current situation

i) Development of cloud storage

a) Dropbox

Dropbox is an online storage service product launched by Dropbox in 2007. The free space of the product is 2 GB, and it can be paid for expansion, up to 100 GB for $ 199. Due to the excellent characteristics, product strategy and Word-of-mouth Marketing of Dropbox, the number of users increases very quickly. The number of registered users had been broken 100 million. Dropbox has a considerable number of fans in China.

b) SkyDrive

SkyDrive is an online storage service product launched by Microsoft in 2007 with free space of 25 GB by April 22, 2012, followed by 7 GB. SkyDrive can also be paid for expansion. The current number of registered users is about 40 million.

c) Google Drive

Google Drive is a cloud storage service launched by Google on April 24, 2012, officially with free space of 5GB. Google Drive can also be paid for expansion. Pay $ 60 upgrade to 60 GB, and $ 25 for 25 GB. The current number of registered users is nearly 100 million.

Furthermore, Amazon, Apple and other companies have been competing to launch their free cloud storage products. China Telecom, Lenovo, Alibaba, Xiaomi and other vendors cloud mobile phone and cloud services were also unveiled. Cloud storage has become a trend.

III. SECURITY RISK ANALYSIS OF USER DATA STORAGE IN CLOUD STORAGE

Although more and more users start using cloud storage services, there is no security mechanism in the process of data transmission and storage in the cloud storage system. The following parts will analyse the security risks of data storage from four aspects.

A. Data transmission risk

Data transmission depends absolutely on the network in cloud storage mode. Therefore, the threat of network attacks

on data security is badly big. Hackers can take advantage of the vulnerabilities and technical errors of the network. They intercept information, modify access rights, obtain or modify data, to compromise the benefits of cloud storage providers and users. In the physical layer, the data of cloud storage system may not only be leaked in the form of electromagnetic waves but also be intercepted in the process of network communication. In the Data Link, Network and Transport Layer, in the case of improper use of Technology, data will be at risk even though there are SSL, SSH, IPSEC and other VPN technology for data transmission to establish a trusted secure connection. In the Application layer, the DDoS and other network attacks will take up most of the network bandwidth, resulting in network equipment downtime. Service can't respond to user requests, resulting in user data in the transmission process damaged or lost, affecting the availability and Integrity of data.

B. Data storage risk

Some valued data and resources, related programs and applications of users are stored in the cloud using cloud storage service. Current cloud storage service providers take measures of centralised storage, unified management, real-time monitoring of users' data, to ensure system and data security. However, the cloud storage system is a huge and complex system with a structure of four layers, which involves the integrity, confidentiality and availability issues of data. Different cloud service providers have their security policies and technical solutions to ensure the safety of the user's data. This section will briefly describe the risk of data storage from two aspects of the hardware application strategy and cloud storage service providers' management.

i) Cloud storage hardware device and application strategy

Management layer is closely related to the security of data refer to the four-tier structure. Management Layer is the core part of the cloud storage, assumed the encryption, disaster recovery and data backup tasks. However, in the complex environment of multi-user coexistence, the user's data is stored in different storage space, and there is no backup of user data. User's data is highly possible to be intercepted, damaged or lost once the cloud service provider does not provide data encryption, disaster recovery, backup and other functions.

ii) Cloud storage service provider management

Compared to traditional storage systems, the biggest difference is that these cloud storage devices are managed and maintained by a third party. Users are not aware of how cloud service providers store data. Cloud service providers possess data control after upload massive data to cloud storage service provider. How the cloud service providers will not be driven by the interests to collect users' habits. How to ensure that the user's data would not be further integrated and analyzed. How to ensure the effective destruction of back-up user data under recovery mechanism when transmit data between different cloud storage service providers. Cloud storage service providers have the responsibility to provide trusted services to maintain the interests and the security of data privacy of different users.

C. Cloud terminal risk

Cloud terminal software provides users with a friendly interface, which greatly enhance the performance when user access to cloud services resources. With the rapid development of modern information technology, cloud terminal gradually transform into diversified and intelligent devices such as smart phones, tablet PCs, in addition to traditional personal computers. Current common terminals have different loopholes due to technical defects. There are still new loopholes were found even though the system is constantly updated. These loopholes are a serious threat to the stability of the cloud terminal, and increase the risk of cloud terminal infection or attack by the virus.

IV. RESEARCH ON SECURITY STRATEGY OF USER DATA STORAGE IN CLOUD STORAGE

According to the characteristics of the cloud storage system and the security problems, we carried out this kind of cloud storage as the core of the online distributed storage system.

A. Research on data security architecture strategy

i) Application interface layer to the Access layer

We need to use identity authentication, access control, encrypt transmission technology to protect the security of cloud storage system. First step is to confirm the identity of the user. That is to use the identity authentication mechanism in the cloud terminal to achieve mutual authentication between the cloud storage server and the user. Second step is to achieve end-to-end data transmission using data transmission encryption. This protects data from security threats in transmission process. The third is to use access control to ensure that user data will not be accessed by others illegally, aiming at protecting the benefits of users. These technologies protect the confidentiality and availability of data to keep the illegal users out.

ii) Management layer

In the management layer design, the first need is to encrypt data, so that illegal users can not read. Even if they get the user data, the encrypted content will not be leaked. This protects the confidentiality. Check user data regularly to ensure that the data in the cloud storage is consistent with the data uploaded by the user, so that illegal users "can not change" data. This protects the availability and integrity of legitimate users' data. Meanwhile, disaster recovery, backup processing of user data is necessary. The user data information is fragmented using Shamir's threshold secret sharing program to transform the complete data to a data fragment. Even if the data is lost, it can be restored to ensure the availability and integrity of the information.

iii) Storage layer

In order to ensure the security of data storage, Data scattered storage technology is used effectively to satisfied massive storage data requirements of user. Because the storage data error rate increases as the storage system capacity increases. And data scattered storage technology can effectively ensure the reliability and availability of cloud storage data as a result of the devices in the storage layer based on data-dispersed storage technology are distributed. These devices are redundant, which can effectively improve the storage utilization and fault tolerance. At the same time, by monitoring the operation of the user in the process of data access, the system ensures that illegal users can not escape after invade system.

iv) Data access for online distributed cloud storage

When the user stores the data, the cloud storage system uses the chip to process the data which is accessed, and then transfers the data to the storage medium distributed in different places. When the user read the data, they complete the read operation after passing client identity verification, by the virtual view provided by the storage manager distributed in different places.

V. CONCLUDING REMARKS

Cloud storage technology develops very fast, and cloud storage security technology is facing unprecedented challenges. However, cloud storage security is not just a technical issue. It also involves the standardization, management, laws and regulations and other problems. In this paper, a few some technical problems of cloud storage security are analyzed from the technical point of view. To achieve the security of cloud storage completely, academia, industry and government departments need to work together.

VI. ACKNOWLEDGMENT

This work was supported by the Beijing Municipal Science and Technology Commission(No.XX2014B052).

VII. REFERENCES

[1] AtenieseG,BurnsR,CurtmolaR,etal.Provable data possession at untrusted stores[A].In Proceedings of CCS'07[C],ACM Press,New York,2007:598-609.

[2] Aaram Yun,Shi Chun-hui,Yongdae Kim.On protecting integrityand configentiality of cryptographic file system for outsourced storage[c].In CCSW'09:Proceedings of the 2009 ACM Workshopon Cloud Computing Security,Chicago,Illinois,USA,2009:67-75.

[3] Feng Deng-Guo,Zhang Min,Zhang Yan.Study on cloud computing security.Journal of Software,2011,22(1):71-83(in Chinese)

[4] Bai Xin .Research on Key Technology of Safety Monitoring Mechanism in Cloud Environment[D].Beijing industry university.2015(in Chinese)

[5] Hai JiaJia.Research on User Data Storage Security in Cloud Environment[D].Heilongjiang University.2015(in Chinese)

[6] Feng Chao-Sheng,Qin Zhi-Guang,Yuan Ding.Cloud data secure storage technology[J].Journal of Computer Science,2015,(01):150-163.(in Chinese)

[7] Q.Wang,C.Wang,J.Li,K.Ren,W.Lou.Enabling public verifiability and data dynamics forstorage security in cloud computing [C]// 14th European Symposium on Research in Computer Security,Springer Berlin/Heidelberg,2009:355-370

[8] Wenhong Tian, Yong Zhao.An Introduction to Cloud Computing[J].Cloud Resource Management and Scheduling,2015:1-15.

[9] Deyan Chen,Hong Zhao.Data Security and Privacy Protection Issues in Cloud Computing[C].2012 International Conference on Computer Science and Electronics Engineering(ICCSEE),PP.647-651

[10] Wang C,Wang Q,Pen K,etal.Privacy-preserving public auditing for data storage security in cloud computing[C].In Proceeding s of IEEE INFO.COM'10,2010:14-19

[11] Behl A,Behel K.An analysis of cloud computing security issuses[C].//World Congress on Information & Communication Technologies.IEEE,2012:109-114

[12] Wei J,Zhang X,Ammons G,Managing Security og Virtual Machine Images in a Cloud Environment[J]. Proceedingd of the Acm Workshop on Cloud Computing Security Ser Ccsw' , 2009:91--96

[13] Shaikh F B, Haider S.Security threals in cloud computing[J] . International Conference for Internet Technology & Secured Transations. 2011:214-219