Data Security Issues in the Process of Applying Cloud Computing

Kai Wang
Equipment Department
Tianjin Bohai Vocational Technology College
TianJin, P.R.China
wangkaieiei@163.com

Xia Yang
Electrical Engineering Department
Tianjin Bohai Vocational Technology College
TianJin, P.R.China
yangxiaei@163.com

***Abstract*—in recent years after the cloud computing architecture through the fast development period, inevitably exposed in terms of data security problems. The calculated data safety platform in the cloud through several occurred recently, more to deepen some questions about cloud computing. This article from the cloud data security problem of cloud computing, to improve data security measures.**

Keywords- cloud computing, data security, authentication mechanism, storage architecture, security strategy

I. BACKGROUND

Computer network with its huge scale and almost unlimited data resources, in a short period of time more than 20 years of profound influence and change our lives. People gradually understand and accept the new things, and with great application prospect in the. In the face of immeasurable huge economic interests, strong power of technology progress, cloud computing technology has been rapid development. Cloud computing has been an important source of most IT enterprise manager and the industry as the core architecture of next generation network application technology. In the cloud computing environment, people can easily get rid of the traditional architecture is very difficult to break through the technical bottleneck, and at a lower cost investment, in a more convenient way to master far exceed the computing resources and huge storage capacity of the past. Worldwide, many enterprises and research institutions have begun in-depth study for cloud computing, cloud computing data centers have also been around the world is based on the construction, including Google, Amazon, IBM here, some enterprises have already established a cloud computing service platform, the platform can provide large-scale global computing services. According to the forecast, the independent research group Forrester to 2020, global cloud computing market scale will reach $241000000000.

With the rapid development of the market for cloud computing, security issues of cloud computing is found, especially data security issues, has become an important factor in the rapid development and popularization of the influence and restriction of cloud computing. In recent years, according to the survey, more than 80% of respondents think the current cloud computing service providers have no way to solve the security problem, the absolute guarantee completely solve the safety hidden trouble and implementing reliability, most users will not give up the use of internal current system. In recent years occurred in the accident, Dropbox Google, Alibaba Cloud, accidents not only cause the individual user data loss, but also to the enterprise users caused great loss of data. Important data loss can lead to unacceptable losses to the enterprise, data security and let many users of cloud computing brings great challenge.

II. WHAT IS CLOUD COMPUTING ?

Cloud computing is a developing concept, in a variety of interpretation, a common definition is: cloud computing is a virtual resource dynamic expansion through the Internet to provide services to the calculation model of the user, the user does not need to know how to manage the infrastructure that supports the cloud computing. USA national technology and standard research center (National Institute of standards and technology, NIST) five key features defined as cloud computing: self-help service on demand (on-demand self-service), high bandwidth network (broad network access), virtual resource pool (resource pooling), high speed flexible architecture (rapid elasticity), which can measure the service (measured service). According to the service model of cloud computing, cloud computing platform can provide the infrastructure virtualization and virtual application of different levels of service to users.

III. DATA SECURITY THREATS FACING THE CLOUD COMPUTING

The rapid development of cloud computing makes many users are attracted by its advantages, and focus on the development of its future. Many institutions and researchers began to notice, all sorts of problems after the explosive growth of cloud computing are exposed.

Cloud computing is huge, with openness and complexity of hitherto unknown. Based on virtualization technology, the physical infrastructure in cloud computing on the application and the data of a large number of users, not only each user computing tasks are intertwined, the data itself is so. Users, applications and data concentration has brought the security problem is very complex, and the problem itself has gone far beyond the category of traditional security technology of information system.

According to the results of Gartner company, in the current cloud computing security risks exist in the seven: priority access right of investigation and risk, management risk, risk, data access location data isolating risk, data recovery risk, risk, risk to support long-term survival, most

of the risk event, the inevitable will directly or indirectly endanger the user data security.

The security problem of user data can be summarized as follows:

A. *The lack of suitable for identity authentication mechanism in cloud computing architecture.*

In the data storage conditions for the application of virtualization and virtual, weak identity authentication mechanism of traditional network architecture, will give hackers, resulting in the user data is false. Establishing bidirectional authentication strictly between the user and the cloud, the cloud is an important prerequisite for users to access data and services. Otherwise, the legitimate user's data security will not be able to obtain the effective protection.

B. *The lack of effective monitoring mechanism of cloud services.*

Application and data users are outsourced to cloud service provider management, user cannot realistically on the application and data of absolute control, cloud service providers have priority access and control actually for data and application. The cloud service provider behavior is difficult to effectively monitor the credibility, service providers are also difficult to assess. Users in the totally unaware of the circumstances, the data may have been stolen, or been hacked, or is in the wrong maintenance process destroyed. The confidentiality, integrity, privacy, reliability and other aspects of the data is not protected effectively.

C. *The lack of effective isolation applications and data between users, resource management mechanisms of virtualization to cloud computing platform of highly concentrated.*

Many users are using public service program for data access permissions initiated, convergence is the inevitable result of the carrier is shared access. If the virtualization technology vulnerabilities are malicious programs using the virtual privilege, then the attacker. Illegal users make use of such a security breach, can easily get on the same physical host adjacent user data.

D. *The lack of security mechanism of virtual platform.*

May use the data security mechanism provided households or cloud service providers are malicious destruction, can not play the role of malicious code may use the data security mechanism for households or cloud service settings cannot be performed or bypassed, so that security mechanisms such as together, can not play a role in.

IV. THE MAIN WAY TO SOLVE THE PROBLEM OF DATA SECURITY IN CLOUD COMPUTING

A. *The establishment of a more reliable user authentication mechanism*

For the user, password based scheme is relatively simple and easy to implement. However, the user password is often associated with the user information, and is easy to memory string. Information entropy is low, it is easy to be a dictionary attack against. Therefore, the key problems must be solved for the password protection.

Three party key exchange protocol based on password (3-Party Password-Authenticated Key Exchange, 3PAKE) certification system. In the three party password key exchange authentication scheme, three party users, private and public cloud corresponds to the 3PAKE protocol. Private cloud is already established system of user identity information management, user and public cloud with private cloud to help achieve the certification process of both sides.

In order to improve the security of password authentication, you can use 3PAKE authentication protocol based on elliptic curve. Under the agreement, users and public cloud in the private cloud does not store the password explicitly, but stored password authentication element, to protect the security of password. In addition, the protocol can resist guessing attack, anti validation element stealing attacks with the session key forward security in the random oracle model.

At present, researchers have proposed a variety of 3PAKE protocol, RSA or based on discrete logarithm (Discrete Logarithm, DL) method, although it has high security, but in the verification process of the large computational overhead, service response time, low efficiency, is not suitable for use. Another direct method is the discrete logarithm based protocol for proper transformation, so that it can be used for elliptic curve (Elliptic Curve, EC) environment, because of the elliptic curve is essentially a special case of the discrete logarithm. The elliptic curve based protocol has low computation and storage overhead, the most suitable for use in the cloud computing environment to meet the response time requirements of the cloud service provider to the user commitment to SLA

B. *Data storage framework can be authenticated user is trusted*

In the cloud computing environment there are a lot of storage at the main purpose of the static data, users hope that cloud service providers provide massive, safe, reliable storage service. But in the current service mode can not be on cloud service provider credibility assessment, so that the user can't believe the data safe and effective. In order to establish a cloud storage service can be trusted to the user, need trusted cloud storage scheme of a support to verify the cloud data at the user end can be. With a support dynamic update and publicly verifiable multiple copies of data integrity verification scheme, provides data to the remote data integrity verification and recovery data protection. The

user through the means of verification, can timely know the integrity status of cloud data, and when the data is damaged to repair, in the occurrence of safety accidents when all the data retrieved cloud.

The basic idea of multi copy integrity verification scheme to support dynamic updating of data and public verification is:

Firstly, based on the extension of the file copy mechanism is then distributed to each storage server.

Then, a "challenge response protocol based on the back," in less data, deterministic verification method based on judgment of remote data is complete.

The validation process the user can timely know the integrity status of the cloud data, and when the data is less than a certain degree of damage, all data can be retrieved cloud.

From the distributed file system GFS (Google File System) framework, can deploy cloud storage architecture for privacy preserving data integrity verification scheme, storage architecture consists of three types of entities: the client (Client), a trusted third party server (Trusted Third-party Server, TTS) and the cloud storage server (Cloud Storage Servers, CSS).

Client represents huge amounts of data can be stored in the cloud users, rely on service providers to maintain data and provide a variety of services, is also the cloud data integrity program verifier Verifier. Client can be an individual user can also be organized by the user. TTS is a trusted medium Client and CSS communication, Storage Cloud user identity information, to carry out the authentication. CSS is used to store the user key data, a prover is data integrity scheme in Prover.

The mechanism is the protection of user data, can not effectively determine the existence of illegal data service providers to leak, or there are serious problems in data management failures. Therefore, but also needs to be based on database watermarking data leakage accountability scheme, users in the suspected data leakage, as judged by analysis the Disclosure Act process.

Data in the cloud data stored in database, the watermarking technology based on the methods of signal processing in the database is not easy to detect embedded markers which are difficult to remove without damaging the premise, the content and usability of database, to achieve the aim of protecting the database security. Based on the LSB (Least Significant Bits) watermark carrier channel algorithm is one of the most simple and commonly used. The essence of watermarking channel LSB is redundant space through the tiny distortion numerical vector data to access database. As chaotic sequence is sensitive to initial conditions, equalization, iterative and non periodic sequence properties, better able to meet the requirements of embedded locations were randomly selected, the replacement algorithm based on chaotic sequences of LSB, the watermark is embedded into the user database.

The suspected leak or stolen data, relying on the proposed watermarking algorithm to extract the data, using the robust human identification, method can also use the machine recognition of watermark, the extracted watermark is compared with the original watermark, judging by the owner of the database.

C. Establish division and protection mechanism of multi regional security for cloud applications.

Cloud computing based on virtual resource management way, so the calculation model is not like the traditional, can divide the physical host boundary very good security domain. In the resource pool pattern, not physical boundary exists between applications, resources and authority application will overlap, calculation of safety protection strategy in traditional cloud pattern is difficult to play a role in.

Therefore, the need for the application of cloud computing and data environment, a multi-level, multi-level, micronized security domain settings. Virtual application, for each user's virtual machine to use a protection system for dynamic data security, sensitive data at any time to track the user's security policy, in strict accordance with the secure domain user belongs to the set of control data flow.

In order to realize the user isolation more accurate, current cloud computing system must be able to perform fine-grained labeling and tracking the object level of program data, even if the process address space in different tenants data can be effective tracing and isolation. For each application is implemented to the programming language level information flow control, sensitive data for each of the application code to the operation of the user, to the least privilege principle is given a specific subject based permissions, judging labeling and strategies, in accordance with security policy can be performed for sensitive data operation. In addition, the virtual machine operating system level security enhancement is necessary. The user isolation can accurate and fine-grained effectively avoid application vulnerabilities are exploited, not illegal data read and write operations and inter process communication.

V. PROBLEM SUMMARY

This paper briefly discusses the security problems in four aspects of security mechanism, isolated storage, verification, cloud computing, and from strengthening the verification, data storage framework can be authenticated user is trusted, the establishment of three division and protection mechanism of multi regional security for Cloud Applications of cloud computing solutions safety issues.

There are all kinds of problems inevitably cloud computing architecture in the development process, solve the problem of data security is the key condition for services for more users in the future. Believe that after solves many problems of cloud computing, cloud computing will usher in the development of space more great.

REFERENCES

[1] Wayne Jansen, Timothy Grance.Guidelines on Security and Privacy in Public Cloud Computing.NIST.January, 2011

[2] NIST. Challenging Security Requirements for US Government Cloud Computing Adoption (Draft).November, 2011

[3] Vivek Kundra. Federal Cloud Computing Strategy. U.S.Chief Information Officer.February, 2011

[4]J. K. Resch, J. S. Plank. AONT-RS: blending security and performance in dispersed storage systems[C]. In 9th USENIX FAST, 2011

[5]Jianxin Li, Bo Li, Tianyu Wo, Chunming Hu, etc. CyberGuarder: A Virtualization Security Assurance Architecture for Green Cloud Computing[J]. In: Future Generation Computer Systems, 2012, 28:379-390.