Research on security threats and Countermeasures for Cloud Computing

Qing Mi, Zhen-tao Ni and Xiao-duan Wang

Informatization Department, Hebei Academy Of Governance, Shijiazhuang, 050000, China

Keywords: Cloud computing; Safe strategy; Information security

Abstract. This paper introduces the concept and architecture of cloud computing, discuss the security problems facing the current cloud computing.The security problem of cloud computing is very important and it can prevent the rapid development of cloud computing. This paper introduces some cloud computing systems and analyzes cloud computing security problem and its strategy according to the cloud computing concepts and characters. The data privacy and service availability in cloud computing are the key security problem. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system.

Introduction

Cloud computing is a new technology brought business and work the way change, provides convenience to people's work study and life.% in cloud computing user data are stored in the "cloud", leakage loss and data privacy of all users will bring great loss, this makes people more and the security issues more attention.

Cloud computing has many benefits from economies of scale to the usability, the absolute can bring some positive factors to the application environment. Nowadays, respected computing providers and supporters in the vast cloud, many enterprise users have begun to itch to try. However, cloud computing brings some new security problems, due to the large number of the users shared IT infrastructure, seriously the importance of safety.

Cloud computing is grid computing, distributed computing, parallel computing, utility computing, virtualization, network storage, load balanced development of traditional products such as computer technology and network technology fusion, it aims to integrate a plurality of network computing entity relatively low cost into a perfect system has powerful computing ability, and by means of SaaS, PaaS, IaaS, MSP advanced business model is the distribution of the powerful computation ability to end users.

Cloud computing architecture is divided into 4 layers: physical resources layer, resource pool management layer, middleware layer and SOA to construct the layer, as shown in Figure 1, the physical resource layer includes a computer, memory, network infrastructure, database and software; resource pool layer is a lot of the same type of resources structure isomorphism or nearly isomorphic pool of resources, such as computing resource pool, data resource pool; management management middleware is responsible for cloud computing resources, and scheduling of numerous application tasks, so that resources can be highly efficient, security services to applications; SOA build layer will cloud computing power package into the standard Web Service services, and incorporated into the SOA system management and use, including the service registration, search, access and build service workflow. Management middleware and resource pool layer are respectively corresponding to 3 layer cloud computing service system in the PaaS layer and IaaS layer, which is the key part of the.SOA cloud computing technology to construct the layer corresponds to the SaaS layer, the function of it to rely more on external facilities provide.

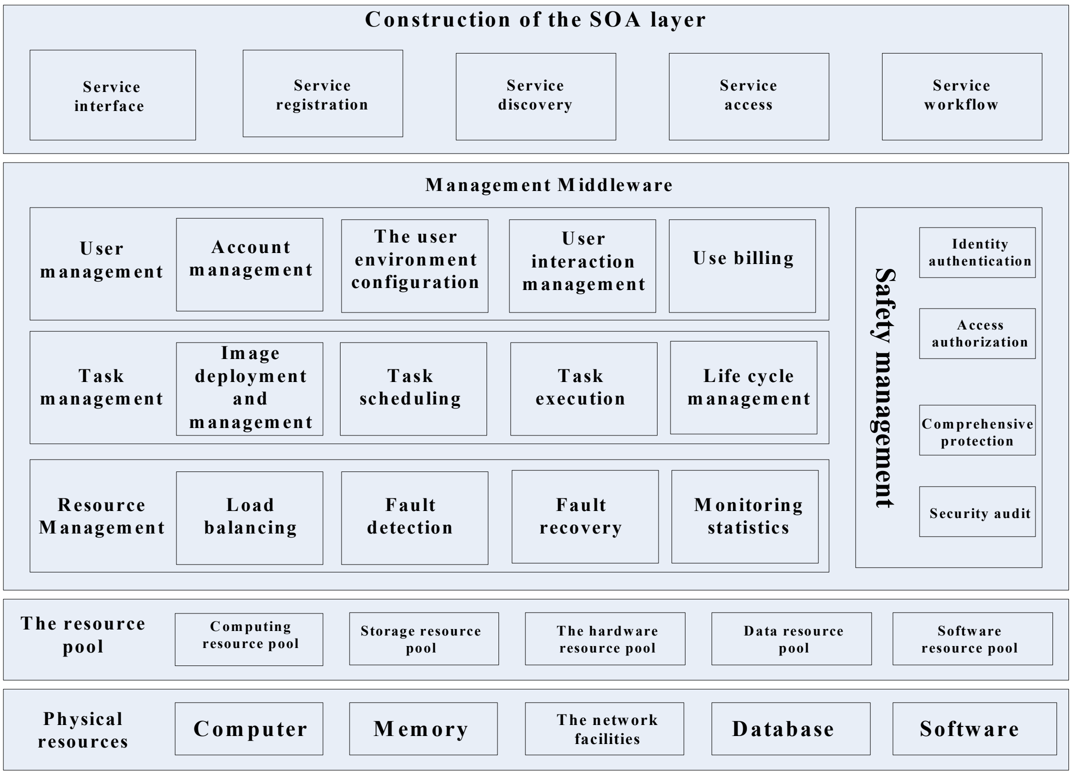

Figure 1.Cloud computing architecture

Multi level cloud computing security mechanism

Cloud computing security requirements including:

① Data access control
② The confidentiality of data storage
③ Runtime data privacy
④ The confidentiality of data transmission
⑤ Data integrity
⑥ Data persistence availability
⑦ The speed of data access

According to the requirements of the security of cloud computing, draw lessons from the traditional network security techniques (including SSL, VPN, PKI, RBAC, RAID etc.), this paper proposes the multi-level security mechanism in the construction of cloud computing model.

Cloud computing security assessment

Cloud computing system operation needs to establish a set of safety standards and assessment system, safety target validation, safety service level evaluation, measure the cloud user security goals and a cloud service provider security service ability and safety verification of cloud computing platform system; short board for the cloud computing platform and reinforcement, to further improve the safety assessment system scientific and cloud resource pool platform, provides the important reference to the service providers to construct a security service; in addition, according to the detection and evaluation of scientific testing methods, the safety accident occurs during rapid implementation of accountability, to avoid the buck.

In practice, the traditional sense of service providers the ability of the security risk assessment is through a comprehensive identification and analysis system under the framework of threat and vulnerability and its potential impact on the assets to determine the level of safety and resistance risk ability. But in the cloud computing environment, multiple service providers to buy cloud service providers may hire to provide other services infrastructure services or software services, according to the system status of dynamic selection. Therefore, according to the characteristics of dynamic and multi participation in cloud computing, cloud computing security standards should support the safety assessment on cloud service process flexible and complex, need the calculation and evaluation methods of providing cloud services security capacity of the corresponding.

The security mechanism of cloud data access

In the use of public cloud, for the transmission of data in the biggest threat is not use encryption algorithm, data transfer via Internet, the protocol is to ensure the integrity of the data. If the encrypted data and method of using non secure transmission protocol can also achieve the purpose of confidentiality, but can not guarantee the integrity of the data.

Cloud computing system operation needs to establish a set of safety standards and assessment system, safety target validation, safety service level evaluation, measure the cloud user security goals and a cloud service provider security service ability, safety verification of cloud computing platform system; short board for cloud computing platform and reinforcement, to further improve the safety assessment system scientific and cloud resource pool platform, provides the important reference to the service providers to construct a security service; the other on the basis of the detection and evaluation of scientific testing methods, the safety accident occurs during rapid implementation of accountability, to avoid the buck.

Specifically, the security level of cloud files on the server and related resources are defined as top secret, secret, secret and ordinary several levels, access to the resources to implement strict access control. User access process as shown in Figure 2.

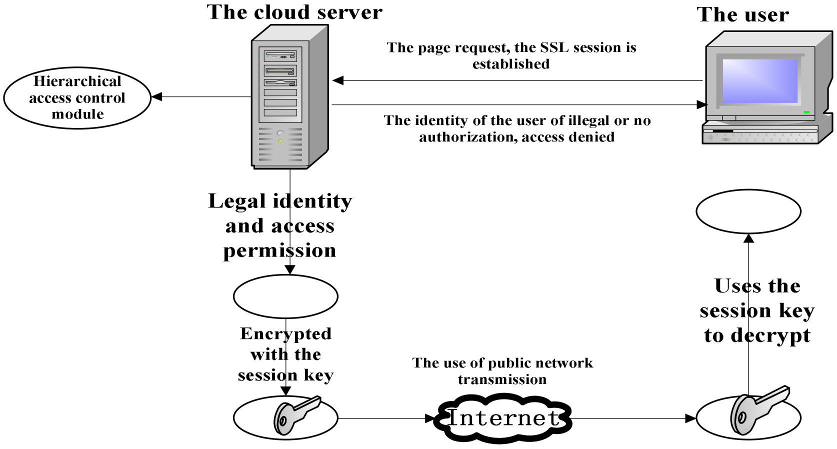
The cloud server
The user
The page request, the SSL session is established
Hierarchical access control module
The identity of the user of illegal or no authorization, access denied
Legal identity and access permission
Uses the session key to decrypt
Encrypted with the session key
The use of public network transmission
Internet

Figure 2.Hierarchical control access data access

Cloud data transmission security mechanism

In a typical cloud computing online document management environment, the realization of sensitive data online editing, save the encryption decryption, ensure that the network transmission process security. Even if the half-way information is intercepted, but also because it is encrypted and cannot get the real information.

In addition, with the help of VLAN, VPN and other data isolation mechanism can enhance the security of.VLAN data transmission is mainly used inside the data center, used to isolate different user and client, ensure that the network data a user can not obtain other user. VPN will be multiple distributed computer with a private encrypted network connected, forming a user private network. Using this method can effectively ensure the safety of the user data transmission.

Cloud data storage sharing security mechanism

The cloud must first ensure the safety platform. First through the specific removal mechanisms of operating system threat, fill the loopholes in the system; and then the corresponding function and service disabled. At the same time to solve the remote management, certificate and DNS protocol quality and improper implementation problems. Most importantly, all stored in the cloud must use public key sensitive information / private key asymmetric encryption technique processing, the user must use their private key to carry (best for use in electronic equipment dedicated to store the private key, such as online banking use now U shield) can access the cloud information. In this way, no matter where the user is, no matter who he authorized, other people are unable to obtain the document information. Even if the other party master the user account Google or Microsoft live account, sensitive information still will not leak out, even can prevent the cloud service provider IT and technical personnel of the malicious attack. Cloud data encryption storage sharing diagram as shown in Figure 3.

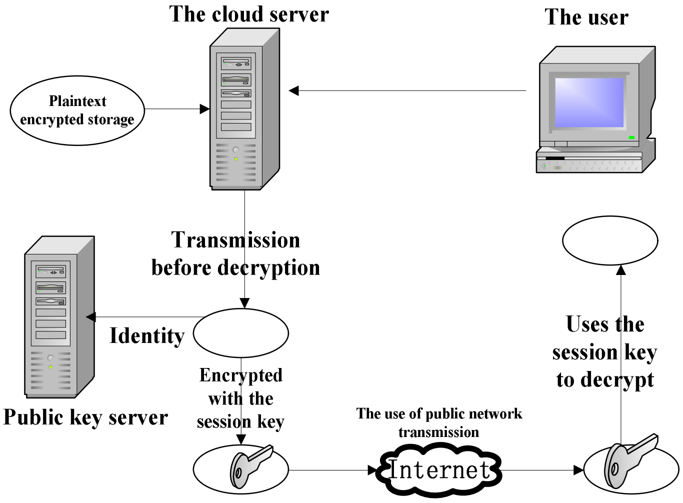
The cloud server
The user
Plaintext encrypted storage
Transmission before decryption
Identity
Public key server
Encrypted with the session key
The use of public network transmission
Internet
Uses the session key to decrypt

Figure 3.Cloud storage encryption sharing

Cloud computing security protection technology

Technical protection of cloud data security is mainly for data encryption, data protection, data backup, storage isolation platform and the application of the terminal operation and virtual host data backup / recovery etc.. With the increase in the number of business platform pooling and virtualization, security risks also will gradually increase. Aiming at the security of cloud computing, we first need to build trusted cloud computing environment, the security level in the data and application security level and safety level virtualization deployment of security protection measures.

Data security level:

Data transmission security

In the use of public cloud, if you do not use encryption algorithm for data in transit will pose a great threat. Through the Internet to transmit data, the protocol is to ensure data integrity. So the need to adopt the encrypted data and the use of security protocol to ensure data transmission security in cloud computing.

Data isolation

The core technology of cloud computing is virtual, which means that different user data may be stored in a shared physical storage. For shared memory, the need to achieve to isolate untrusted applications using the virtual resources to limit the malicious behavior of untrusted applications.

Data encryption

Objective data encryption is the original files to prevent others to get the data after data theft. Data encryption application forms in cloud computing: data using the private key is encrypted on the user side, and then uploaded to the cloud computing environment, when used real-time decryption, avoid the decrypted data stored in any physical media. There are many kinds of mature data encryption algorithm, such as symmetric encryption, public key encryption.

In the cloud computing environment, with the use of methods and data segmentation and data encryption, data on the client side is to scatter the encrypted and then dispersed in several different cloud services above, so for any one service provider, are unable to get to the data complete, even through brute force also cannot obtain the data content.

Application security level:

End user security

For the use of cloud service users, need to keep your computer safe. The deployment of security software on the user's terminal, including anti malware, anti virus, personal firewall and IPS types of software, and to take the necessary measures to ensure the implementation of end-to-end security in cloud environment.

Cloud Application Security

Cloud application security including cloud technology platform for their safety and security two levels of customers deploy computing platform application in the cloud. In the cloud environment, customers usually only responsible for security function operation layer, including the user and access management, which need a cloud computing service providers to ensure maximum available to client applications and components such as security.

Cloud providers will the application client deployment in virtual machine as a black box, provider didn't know customer application management and maintenance. So the application and operation of engine customer whether operation in what platform, are in need of management in cloud computing platform. Therefore need in cloud computing application layer equipment for abnormal traffic monitoring, flow cleaning system and flow tracing system and other safety product deployment, implementation of cloud computing security.

Virtual security level

Virtualization software security

Virtualization software is important to ensure the implementation of virtual machine customer mutual isolation in a multi tenant environment, can make the customer on a computer security at the same time to run multiple operating system, so we must strictly limit any unauthorized access to the virtualization software layer. A cloud service provider shall establish safety control measures are necessary, such as password authentication and access control mode restriction for virtualization level of physical and logical access control.

7.3.2 The virtual server security

Safety protection virtual server system need regular reinforcement and prevention, similar to other server loading system patches, patches, open application is allowed to run the service and port etc.. At the same time, strictly control the physical host running virtual service quantity, run the other network services in the physical host banned, and the way to use encrypted for transmission between the virtual machines, and carries on the strict monitoring of the virtual machine. In addition, through the installation of virtual firewall, security strategies and other methods of protection and isolation of the virtual machine.

Conclusion

Cloud computing is essentially a kind of new method is more flexible, efficient, low cost, energy saving operation of information, since the Internet revolution since the IT industry the most profound change, is also the long-term development of the information technology and the accumulation of synthesizer. Multi level security mechanism is proposed in this paper can effectively avoid the security threats from other users, but to be technically to completely eliminate the security threat from the service provider is difficult, need to use third party certification, corporate reputation, the contract restriction and other non technological methods to supplement, improve service quality in order to supervise the service provider, ensure the security services.

References

[1] S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, AutonomIc and Secure Computing, Chengdu, China, 2009.

[2]J Brodkin. (2008). Gartner Seven cloud-computing security risks.Available: http://www.networkworld.com/news/200S!07020Scloud.html

[3] D. L. Ponemon, "Security of Cloud Computing Users," 2010.

[4] S. K. Tim Mather, and Shahed Latif, Cloud Security and Privacy:O'Reilly Media, Inc , 2009.

[5] C. Almond, "A Practical Guide to Cloud Computing Security," 27August 2009 2009.

[6] N. Mead, et ai, "Security quality requirements engineering(SQUARE) methodolgy," Carnegie Mellon Softare Engineering Institute.

[7] J. W.Rittinghouse and J. F.Ransome, Cloud Computing: Taylor and Francis Group, LLC, 2010.

[8] Dean,J.and Ghemawat,S.2008.MapReduce:simplified data processing on large clusters. Communication of ACM 51, 1 (Jan. 2008),107-113.

[9] Trelea LC. The particle swarm optimization algorithm: convergence analysis and parameter selection. Information Processing Letters, 2003: 317-325.