Research on Security Issues in the Application of Cloud Computing

Honggang Wang

Xi'an Siyuan University, Xi'an, Shaanxi, China

Keywords: Cloud computing; Service; Security; Management; System

Abstract: Cloud computing has become a new Internet service mode, which has attracted wide attention from both industrial and governmental services. However, related security issues are imminent. This study analyzes these issues and proposes a standard system of public cloud management service, which can be used as a reference and basis for enterprises and organizations to strengthen security protection, for users to choose cloud computing service on demand and for any need to establish a third-party cloud computing security assessment, monitoring and management platform. The system is expected to help promote safe and orderly development of cloud computing industry.

1. Introduction

The concept of "cloud computing" was proposed by IBM in October 2007. Due to the characteristics of dynamic deployment, on-demand use and elastic growth, cloud computing has rapidly become a new Internet service mode after distributed computing, parallel computing and grid computing, which has attracted wide attention from both industrial and governmental services. Under this service mode, users do not need to purchase system software, servers and other hardware and software devices at one time while they only need to submit computing and storage tasks to cloud computing providers through the Internet. Cloud computing providers use distributed computer clusters to complete tasks, and then feed back the results to users through the Internet. Cloud computing provides users with basic IT resources (including computing, storage, network, software, etc.) by the Internet that can be hired on demand, which will reduce the cost of IT operation and maintenance of users and enable them to focus on their own business. [1]

Cloud computing has been developing rapidly since its birth and various cloud computing applications have sprung up in social life, such as Amazon's cloud computing service Amazon Web Service (AWS), Google's Google App Engine, IBM's Blue Cloud, Microsoft's Azure have gained popularity abroad and Aliyun Cloud, Tencent Cloud, Huawei Cloud at home, etc. However, cloud computing, as a new Internet service model, has brought as many security problems as benefits at the same time. [2]

2. Major Cloud Computing Services

According to the typical characteristics of cloud computing proposed in the previous section, combined with commercial cloud computing services, this paper draws up the scope of cloud computing service as follows.

(1) Cloud host service: It is an IaaS model that provides flexible hosting rental services, usually provided by IDC companies or telecom operators. For example, Alibaba and Wan-Net jointly develop an IaaS service Aliyun similar to Amazon EC2.

(2) Cloud storage service: It is an IaaS model that provides network storage service on demand, i.e. "network disk". Cloud storage service generally provides more than 1G network hard disk space, and charging users can get more space and storage function upgrade (e.g. total number of files, single file size limit, etc.).

(3) Platform as a service: PaaS model provides Web application development and hosting platform. Sina App Engine is a domestic PaaS platform, which combines with Sina Weibo to provide services for users of Weibo.

  DOI: 10.25236/isrme.2019.071

(4) Software as a service: SaaS mode provides online software leasing for small and medium-sized enterprises, such as OA, ERP, CRM, etc. [3]

3. An Analysis of Cloud Computing Security

3.1 Cloud Host Service Security

Cloud hosting services provide very convenient and fast self-service, making it easier for users to access host resources than before. The on-demand payment mechanism allows users to access computing resources at low cost. However, there may be security issues as follows:

(1) Lack of real-name authentication for cloud computing users. Users need to fill in real names, ID cards and telephones when registering, but the authenticity of these information may not be verified. If users use forged ID cards and post bad information after applying for cloud host resources, or engage in network attacks, it will be difficult to trace their real identity to the cloud.

(2) Lack of control over the default computing resource privileges obtained by computing users. Users only need to recharge their accounts to obtain the function of dynamically applying for cloud hosts. The cloud hosts that users apply for can be used to do any Internet business. Although the archival number is listed in the security and archiving option list that users need to provide if they want to start a website, actually, the system does not impose port restrictions on the newly acquired hostsby default. Their users can use cloud hosts to open any information services (such as Web sites, proxies, etc.).

(3) Vulnerabilities of cloud computing hosts. Generally, the rental services of cloud hosts provide free anti-virus and Trojan Horse removal software for cloud hosts. However, the choice of installation depends on users, and most of these protections are only for Windows hosts. Cloud hosts face the same risk of being attacked as hosts on the Internet. [4]

3.2 Cloud Storage Service Security

Microdisks generally provide users with more than 1 GB of space by default. Some microdisks also provide web pages and desktop clients to facilitate users to synchronize files stored in computers and clouds. The main security problem is the freedom to use microdisks to publish information. At present, the user identity of microdisks hardly needs authentication, and the way to share and distribute to other platforms is becoming simpler and more convenient. This makes the dissemination of micro-disk information fast and wide-ranging, may face the network malicious programs, garbage or a large number of bad information dissemination security issues.

3.3 Cloud Computing Security

The highly centralized resources of cloud computing make the traditional network security problems more serious. At the same time, its virtualization, multi-tenancy and dynamic also introduce new security issues. After the above analysis, the security issues of Cloud Computing mainly involve three levels:

(1) Data and applications of cloud computing service users. User data and application hosting in cloud computing platforms face double risks of security and privacy, including unauthorized access, data access control, privacy protection, content security management, user authentication and identity management from cloud computing service providers and other users in a multi-tenant environment.

(2) Cloud computing service platform itself. With the expansion of business scale and the increase of users of cloud computing services, cloud computing platform itself is easy to become the target of hackers' attacks. The technical architecture of virtualization computing and storage mode makes the security of cloud platform itself particularly prominent, but at present there is no cloud computing security risk assessment system and third-party cloud platform security assessment mechanism.

(3) Abuse of service provided by cloud computing platforms. Flexible and scalable resources provided by cloud computing may be used as malicious network attack tools or as a channel for the

dissemination of garbage and bad information, but there is no regulatory mechanism for the level and legitimacy of cloud computing services. [5]

4. Design of Service and Management System for of Public Cloud Security

Based on the above analysis, this paper puts forward the standard system of public cloud security management service: establishing a third-party cloud security management service platform according to the standard system of public cloud security management service, providing cloud computing resources network security assessment and monitoring services, cloud computing data transmission and security management services and cloud computing service main body authentication and quality monitoring services to achieve network security and number According to the three layers of security evaluation, monitoring and management functions of security and platform operation.

4.1 Assessment and Monitoring of Resource Security

The cloud computing resource network security assessment and monitoring service evaluates the network security of the data center infrastructure running cloud computing services and the cloud computing resources and interface samples provided to users (such as cloud computing virtual machine, programming interface of PaaS platform).

(1) Network security protection: including firewall, DDoS detection, vulnerability scanning, intrusion detection equipment, etc.

(2) Host and terminal security: For IaaS services, including virtual machine image security, user-defined image, virtual machine to physical machine penetration vulnerability testing; for PaaS services, security permission penetration and pressure testing of the provided PaaS service interface. This service can provide common network security monitoring service to cloud computing service providers through API interface. [4]

4.2 Management of Data Transmission and Security

Cloud computing data transmission and security management service evaluates the data encryption and protection measures provided by cloud computing service providers, including disaster preparedness for data storage, privacy protection of communication behavior, key level and encryption algorithm used.

(1) Data access control: logical boundary security access control strategy settings in virtual environment, data access control between virtual machines and virtual units. Data transmission security: whether to support the use of data encryption, VPN and other technologies to ensure the privacy of communication behavior. Data storage security: whether to support encryption storage services.

(2) Remaining information protection: whether the data has been erased thoroughly after data deletion and before storage resource redistribution. Data backup and recovery: whether to support data integrity and incremental backup, whether to support image recovery and data recovery. [5]

4.3 Service Subject Authentication and Quality Monitoring

Cloud computing service subject authentication and quality monitoring services evaluate the platform’s operation and quality of service, including: whether to achieve centralized management of platform user accounts, access control, authorization and audit functions; whether to establish a unified and centralized authentication and authorization system for access authentication; whether to establish a security audit system, with the ability of ex post review of irregularities traceability; and whether it conforms to SLA service level specification, etc.

In the aspect of cloud computing service main body authentication service, it provides public authentication service to the main body involved in cloud computing service (cloud computing service provider, cloud computing user). The identity authentication service for cloud computing user identity verification: public service for the authenticity of the identity of cloud computing user or enterprise, and enterprise qualification verification. The service can be proposed by API interface.

Provide cloud computing service providers with specific ways, including: identity information audit, mobile phone audit, enterprise license audit, etc. According to the qualification of service providers, that is, to evaluate the qualification of cloud computing service providers, to issue business licenses to qualified service providers. In terms of technical standards evaluation, according to cloud computing service types, according to common technical standards. And the technical standards provided by the suppliers are evaluated to confirm whether the services provided by cloud computing service providers are in line with the SLA expected by users. [6]

5. Summary

This paper focuses on the current situation of cloud computing applications and its security issues. In terms of these security problems, a standard system of public cloud security management service is put forward, which includes three levels: network security, data security and platform operation management. This system can be used as a reference and basis for enterprises and organizations to strengthen security protection, for users to choose cloud computing services on demand, and for any need to establish a third-party cloud computing security assessment, monitoring and management platform.

Acknowledgement

The study is financially sponsored by Natural Science Research Project of Shaanxi Education Department in 2018 (No. 18JK1100).

References

[1] P. F. You, Y. X. Peng, W. D. Liu, et al, Security issues and solutions in cloud computing, International Conference on Distributed Computing Systems Workshops, 1 (2012) 573-577.

[2] C. L. Tsai, U. C. Lin, A. Y. Chang, et al, Information security issue of enterprises adopting the application of cloud computing, Sixth International Conference on Networked Computing & Advanced Information Management,(2010) 645-649.

[3] J. Shi, H. Li, L. D. Zhou, The technical security issues in cloud computing, International Journal of Information & Communication Technology,5,3/4 (2013)109-116.

[4] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing[J]. Journal of Network & Computer Applications, 34, 1 (2011)1-11.

[5] N. Vurukonda, B. T. Rao, A Study on data storage security issues in cloud computing, Procedia Computer Science, 92 (2016) 128-135.

[6] Shaikh R, Sasikumar M. Security issues in cloud computing: A survey, International Journal of Advanced Computer Research, 2012, 2(3):1-11.