The Cloud Data Security and Access Control Model in the Study

Jing Dong
Qujing normal college, yunnan qujing 655001

Keywords: Cloud computing; Utility security; Access control; Strategy optimization and security analysis

Abstract. Cloud computing is a kind of based on the calculation of the Internet, through the cloud computing, to other computers and other devices to share information and resources. Although it can bring convenience, operated and managed in a cloud computing infrastructure services in the security problem of nots allow to ignore. After the cloud security problem analysis, put forward the safety of the infrastructure services is the foundation of cloud computing security. Then, on the basis of the traditional access control model to take into consideration the characteristics of cloud computing infrastructure services, design a set of access control model. The model well enhanced the security of cloud computing infrastructure services.

Cloud computing is a kind of new IT services based on Internet, use and delivery mode, cloud computing can through the Internet provides a variety of resources, dynamic easy extension and these resources can be virtualized. It means that the computing power can become a circulation of commodities in the Internet.

The Safety Situation of the Cloud Computing Environment

In the cloud security problems mainly include the following two aspects: one is unique to cloud computing environment safety, traditional users cannot recognize myself uncontrolled environment can provide better security for information or resources, meaning that the resource or information stored in a controlled environment is safer than in an unfamiliar place. Secondly, the traditional IT is under a state of closed, only need to external access interface and firewall protection, internal deployment of anti-virus software to ensure safety. But in the use of cloud computing, cloud computing has changed the software system of the safety protection of the existing model. Because all access to the public in the cloud computing exposed in the network, and the user's operation also need to be done after the remote login. At present, in view of the cloud computing application security problems while no form the relevant international standards, but there have been three types of organization for the study, the first kind is cloud computing service providers, they mainly through the identity authentication, the system redundancy, data encryption, security and other means to solve the security problem of cloud computing, so as to improve the robustness of cloud computing service platform and the security of user data, including Google via a two-step authentication mechanism to control access to information so as to improve the security of cloud computing is a typical example. The second type is engaged in the security organization, such as rising, jinshan, etc; the third class some non-profit institutions, as a cloud security alliance.

Second, the Cloud Computing Security Challenges

Now, it seems, in the era of cloud computing due to the large number of application virtualization technology makes the traditional information security under the age of security isolation method is facing enormous challenges, such as when a customer to buy the cloud service provider of virtual servers, it already has a cloud service provider's network address and the public, which means the user also has the trust of the cloud service provider domain address and untrusted domain, and the results will make some malicious users to use virtual server for users to buy cloud service provider network address in the network of large quantities of fake Intranet address and MAC address, which produces a large amount of ARP traffic makes the network congestion or interrupt. In addition, security challenges associated with cloud service types and then born, such as

ali cloud open ODPS data processing services, it is based on the data driven multistage water flow parallel computing framework, direct use of ODPS SQL statements can be offline analysis was carried out on the huge amounts of data. Divided the huge amounts of data through the data of its spread to the interior of the whole cluster, such not only can make the calculation, internal pressure evenly to the cluster computing performance problems, but also solved the problem of the user's data capacity. But in this mode allows the user to by random programming on the cluster of ODPS mission, this allows a malicious user can be achieved by some action to the invasion of ODPS cluster, thus achieve the purpose of theft of user data. In the era of cloud virtualization security mainly includes strengthening, isolation of the virtual server and destroyed, according to these security issues, although cannot solve by purchasing a security device class, but can still be by means of a series of software and the security isolation and access control

Three, Summary of Access Control Model

Access control model is to stand in the Angle of the access control to describe the security system, to establish a method of security model, mainly in the main body of the system to control access to the object and its safety. This model mainly includes the subject, object and the reference monitor. The role of the reference monitor is to identify validation entity subsystem and control access between entities. In the access control model defines the subject, object and access is how to represent and manipulate, it determines the expression ability and flexibility of authorization policies, and the core of the access control is the authorization policy. The authorization policy is a set of can determine the main body of the object access rules. Under the unified authorization policy, authorized user is legitimate users, otherwise it is illegal users. From the authorization policy, access control model can be divided into the traditional access control models, role-based access control model, and workflow access control model based on task, task and role based access control model, etc.

With the continuous development of security requirements and change, people put forward a new access control model, called usage control model, also known as the ABC model. UCON model contains three basic elements: subject, object, permissions, and the other three elements related to the authorization. In UCON model, authorization rules, conditions and obligations associated with the authorization process, which is to determine whether a subject can have certain permissions to access the object of the decision factors. UCON model covers the security and privacy in the modern business and information systems needs these two important questions. UCON model for the study of the next generation of access control, therefore, provides a feasible method, known as the next generation of access control model, will be an important direction of the development of the access control model.

Fourth, To Improve Cloud Environment Data Security and Access Control Strategy

As mentioned earlier, data security and access control in cloud environment problems mainly strengthening, isolation of the virtual server and destroyed. In virtual server consolidation, can through the establishment of security reinforcement process to test the virtual server, remove unsafe service, protocol, port and other factors may lead to invasion, ensure the safety of users a virtual server. In view of the isolated virtual server, to the isolation requirements of different users to buy cloud server, cloud server production system automatically tag cloud server for each user, so you can through the security group for different users in isolation. Aimed at the destruction of the virtual server, cloud server production system can automatically eliminate the original physical disk and memory on the server on a regular basis data, makes the virtual server. If the cloud platform for development of other reference software security development cycles of different to establish a corresponding security development process.

References

[1] Xiao-long xu; Xiong Jing reduced; Chun-ling cheng. Based on the cloud computing architecture of malicious code joint defense mechanism [J]. Journal of southeast university (natural science edition), 2011, 02.

[2] Willow; Tang Zhuo; Ren-fa li; Zong-li zhang. Cloud computing environment based on the role of user access requirements lookup algorithm [J]. Journal of communications, 2011, '07.

[3] Lin orchard; He Shan; Kropp; Ji-yi wu; Chen wei. Cloud computing access control security model based on behavior [J]. Journal of communications, 2012, 03