IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

Research and Design of Cloud Computing Security Framework

Priyank Sunil Lale
Student, MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Master of Computer Application, Mumbai, India

Abstract: *As a new technique, cloud computing has a rapid development in recent years. However, the security problems have caused great influences to the development and popularization of cloud computing, the importance and urgency has not to be ignored. This paper introduces cloud computing and security situation, studies the main security problems of cloud computing, and comes up with a cloud computing security framework which can effectively solve these security problems, and points out that only to solve the security problems, cloud computing can unceasingly expanded, and the application will be more and more widely.*

Keywords: Cloud computing security, Firewall, Data security

I. INTRODUCTION

Cloud computing is a new technology based on distributed processing, parallel computing and grid computing, and is one of the hottest topics in the field of information technology. Academic circles, industrial circles and governments have also paid close attention to it.

Cloud computing has three main aspects: SaaS (software as a service), PaaS (platform as a service) and IaaS (infrastructure as a service). As shown in Figure 1.A SaaS provider typically hosts and manages a given application in their own data center and makes it available to multiple tenants and users over the Web. Some SaaS providers run on another cloud provider's PaaS or IaaS service offerings. Oracles CRM on Demand ➢ Salesforce.com are some of the well-known SaaS examples. PaaS is an application development and deployment platform delivered as a service to developers over the Web. It facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure, providing all of the facilities required to support the complete life cycleof building and delivering web applications and services entirely available from the Internet. This platform consists of infrastructure software, and typically includes a database, middleware and development tools. Well-known PaaS service providers include Google App Engine, Engine Yard. IaaS is the delivery of hardware and associated software as a service. It is an evolution of traditional hosting that does not require any long term commitment and allows users to provision resources on demand. Amazon Web Services Elastic Compute Cloud (EC2) and Secure Storage Service (S3) are examples of IaaS services.

Cloud computing faces a lot of different challenges. Security is one of the key challenges, and has become the key of popularization cloud computing and restrictive factor. In recent years, the cloud services appear many security accidents. For example, in March 2009, Google leaked a large number of documents. Microsoft Azure platform stopped working for about 22 hours. In April 2011, Amazon's EC2 service disruptions, influences the service of Quora, Reddit etc. When happened, these security problems caused a great loss, even devastating blow. Therefore, to make the enterprise and the organization accept cloud computing services, it is necessary to solve the security problems.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

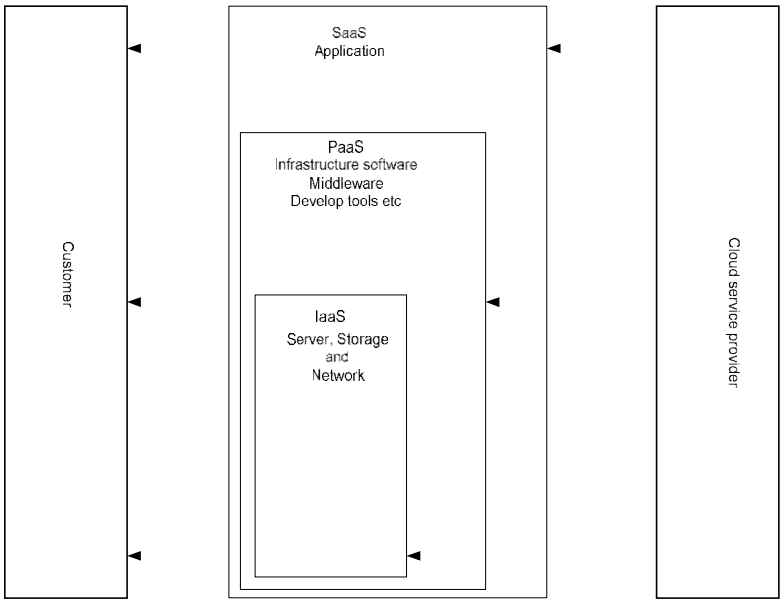

Fig. 1. The three main aspects of cloud computing

II. CLOUD COMPUTING SECURITY PROBLEMS

2.1 Cloud Computing Lacks Uniform Standards of Security

At present, the cloud computing security standards are in the initial stage, yet haven't a complete set of security standards. There are more and more standard organization set out to make cloud computing security standards to increase interoperability and security, reduce repeated investment or repeat invention. For example, Cloud Security Alliance (CSA), Distributed Management Task Force (DMTF) have already launched Cloud computing standard work, and made progress. Cloud computing security standards are the measure of clouds user security goals and the ability of cloud service providers. With the uniform standard, the user can choose through the cloud service standard authentication, establishing trust, and once accident happens, also can quickly realize that responsibility.

2.2 Security Problems of Cloud Computing Network Layer

- Traditional network attacks: Cloud computing is based on the network structure, so there exist great menace for the traditional network attacks. Basically they are the following kinds: distributed denial of service (DDOS) attack, utilization type attack, information collection type attack and the false news attack. Cloud computing has the characteristics of its own: huge user information resources, highly centralize, complicated management, so are also more likely to become the target of hackers, hackers probably attack the whole cloud computing services via a user, and the damage and loss will be obvious more than the traditional enterprise nets application environment.
- Priority access control: Generally speaking, the cloud services has the priority rightto access data but not the users, so the user's data may be leaked out by the administrative staff and other employees, unable to guarantee the user's important andconfidential data security.
- SSL attack: Secure Sockets Layer (SSL) is the encryption method to provide security for network communication; a lot of cloud providers employ SSL to guarantee cloud security. Now many hackers and communities are studying the SSL, different from the general way of network attack, at present the SSL attacks are rare, but SSL has become a worry to cloud computing security.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

2.3 Data Security of Computing Clouds

- Data Location: When use cloud computing services, customers don't know where the data are placed on the servers, even don't know which country these servers are placed in. When these countries need to investigate these data, due to the different law, providers may be forced to submit data and be unable to guarantee the security of userdata.
- Data separation: In the cloud computing services, a large amount of user data are in a shared environment. In order to reduce spending, providers usually reuse the IP address, the IP address of one user may be reused to another, so often leads to the abuse of the data, there is no guarantee to data privacy. The data encryption is the wayto ensure the data security in one way, but encryption does not always guarantee the security of the data, the fail of decryption may cause damage to the data. To users and cloud services the data can't use, this reduces efficiency of data, causes waste of resources.
- Data backup: To the important and confidential data, if cloud services dose not backup the data, when data lost by the server problems, or users accidentally delete data, important data can't be restored

III. CLOUD COMPUTING SECURITY FRAMEWORK

Cloud computing are currently having many security problems, and also become block to the development and popularization of cloud computing, so there need to build a cloud computing security framework, and actively carry out its cloud security key technology research. Here we proposes a cloud computing security framework, as shown in Figure 2, it has several aspects:

3.1 Firewall

For cloud computing, it can greatly increase the security in the configuration of a firewall. The method is to limit the form of open port. Among them, the Web server group opens port 80 (HTTP port) and 443 (HTTPS port) to the world, application server group only open port 8000 (special application service ports) for the Web server group, database server group only open port 3306 (MySQL port) for application server group. At the same time, the three groups of network server open port 22 (SSH port) for customers, and default refuse other network connection. By this mechanism, the security will be greatly improved.

3.2 Security Measures of SaaS

In cloud computing, SaaS providers offer users full application and components, and should guarantee program and components security. The proposing security functions have two main aspects:

Priority access control strategy: SaaS providers offer identity authentication and access control function, usually the user name and password verification mechanism. Users should know enough to the provider they have chosen, in order to eliminate the threat to the security of the cloud applications internal factors. At the same time cloud providers should provide high strength, change the password on time, make password length base on the data of the sensitive degree, and shouldn't use the function such as old password to strengthen the security of the user account.

Common network attack prevention: Rely on the exiting mature network attack defensive measures, for DDOS attack, based on its attack means, providers can use several methods: for example, configuring a firewall, blocking the ICMP and any unknown protocol; shutting down unnecessary TCP/IP services, configuring firewall to refuse any request from Internet. For utilization type attack, providers can monitor the service of TCP regularly, update software patches in time. The traditional network attack has been studied for a long time, and there are very mature products can be employed, cloud providers can make full use of these products to ensure the computing clouds security

3.3 Security Measures of PaaS Layer

In cloud computing, PaaS is the middle layer, the security measures are two aspects:

- Virtual machine technology application: Using the advantages of virtual machine technology, providers can set up virtual machine in existing operating system. At the same time, set access restrictions, common users can operate computer hardware only through promoting operating permissions. This is good distinguished between the ordinary users and administrators, even if the user has been attacked, there will be no damage to the server.
- SSL attack defending: For the possible existence of SSL attack, the user must strengthen prevent method. Providers should provide the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

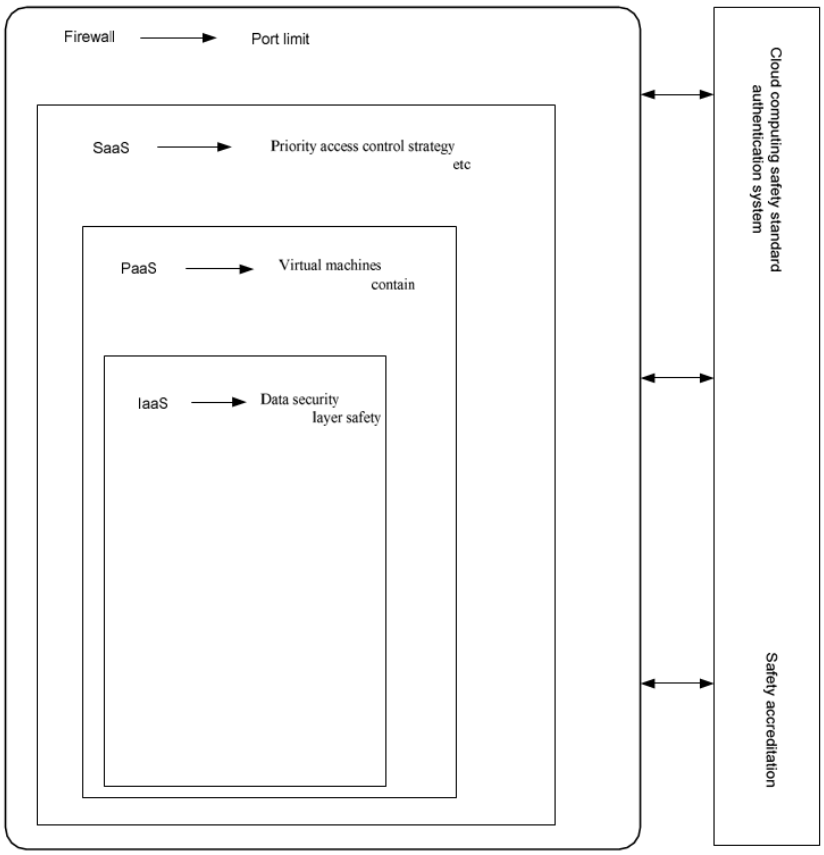

Fig. 2. Cloud computing security framework

corresponding patch and measures, so the user can patch in the first time, and make sure the SSL patch can quickly work. At the same time, using the firewall to close some port to prevent common HTTPS attacks, strengthening management authority, making security certificate not easy to get are good defending methods.

3.4 Security Measures of IaaS Layer

Generally, IaaS is not visible for ordinary users, management and maintenance also entirely rely on cloud providers, and the most important part is the security of data storage. Cloud providers should tell users the information of the country where server locates, and it isn't a problem to operate these data without conflicting with the local law. For the combination of different user data, the data encryption is not just reliable, but also reducing the efficiency of data, providers need to separate user data stored in different data server. Separating the user data storage can prevent data separation chaos. For data backup, important and confidential data should be backed up, at the same time, even if there is certain hardware failure, data can be easily recovered and the recovery time also needs a guarantee.

3.5 Cloud Computing Security Standard Authentication

Cloud computing currently lacks of unified security standard authentication system, but there has been much organization established to set the standards, a complete set of cloud computing security framework need to have a reference standards, the integrity, function, security of a framework can be measured according to the standards. The system depends on the improvement of the unified cloud computing security standard, which as stated before, a set of complete security authentication standard is to solve a cloud computing all kinds of security problems existing in the first thing to do.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

IV. CONCLUSION

In recent years, cloud computing is a technology of rapid development, however, the security problems have become obstacles to make the cloud computing more popular which must be solved. This paper analyzed the present situation of the development of cloud computing, and the security problems, and proposed a cloud computing security reference model. The model put forward a series of solutions for the present security problems cloud computing meet, but technology realization needs more organizations and individuals to join into the cloud computing security research. At the same time, cloud computing security is not just a technical problem, it also involves standardization, supervising mode, laws and regulations, and many other aspects, cloud computing is accompanied by development opportunities and challenges, along with the security problem be solved step by step, cloud computing will grow, the application will also become more and more widely.

REFERENCES

[1]. Dikaiakos, M.D., Katsaros, D., Mehra, P., et al.: Cloud Computing: Distributed Internet Computing for IT and Scientific Research 13, 10–13 (2009)

[2]. Amazon Web Services. Amazon Virtual private Cloud, http://aws.amazon.com/vpc/

[3]. Catteddu, D.: Cloud Computing: Benefits, Risks and Recommendations for Information Security. CCIS, vol. 72, pp. 50–56 (2010)

[4]. Amazon Web Services. Overview of Security Processes, http://aws.amazon.com/ec2/

[5]. Bikram, B.: Safe on the Cloud. A Perspective into the Security Concerns of Cloud Computing 4, 34–35 (2009)

[6]. Boss, G., Malladi, P., Quan, D., et al.: IBM Cloud Computing White Book,

[7]. http://www-01.ibm.com/software/cn/Tivoli/ao/reg.html

[8]. Jamil, D., Zaki, H.: Cloud Computing Security. International Journal of Engineering Science and Technology 3(4), 3478–3483 (2011)

[9]. Somani, U., Lakhani, K., Mundra, M.: Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In: 1st International Conference on Parallel Distributed and Grid Computing (PDGC 2010), p. 211 (2010)