ISSN : 0974 - 7435 Volume 10 Issue 13

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(13), 2014 [7382-7388]

Research on the model of network security risk assessment for cloud computing

Shi Qiao

Computer School of China West Normal University, Nanchong 637000, (CHINA)

ABSTRACT

This study describes the definition, the highlights and the development status in domestic and overseas of cloud computing. It simply analyzes the network security risk caused by cloud computing, division of the three modes in cloud computing platform architecture and the relationship among them. Starting from the definition and the framework, the paper analyzes the nine elements (asset, threat, vulnerability, security precaution, risk, residual risk, standardization, laws and regulations) of the security risk assessment of cloud computing and the relationship of them. Based on the relationship of the nine elements and the method of traditional information security risk assessment, it worked out a formal model for the risk assessment of cloud computing. This model has some similarities with the method of traditional information security risk assessment and also it has the particularity owned by cloud computing. It can predict the information security of users in cloud computing service well, so as to protect the users' assets.

KEYWORDS

Cloud computing; Network security; Risk assessment; Particularity.

INTRODUCTION

With the development of computer technology and the innovation of communication technology, great changes have taken place in Internet technology. In 2006, the chief executive officer of Google put forward the "cloud computing" in the search engine conference. From then on, cloud computing came into our life gradually. Cloud computing is a kind of computer resource which is fast, can be accessed through the network, shared and configurable. It provides the IT resources, data and applications through the network for users as a service, which is the new direction of the service mode and the change of the shared data model[1]. However, with the rapid development of Internet, the network security risk of cloud computing come up. The unique features of cloud computing, such as data storage transmission mode, service outsourcing, resource virtualization, have brought great challenges to network security. As shown in TABLE 1, several major cloud service providers both at home and abroad had all kinds of safety accidents. More and more researchers carried out researches for cloud computing security issues. Ponemon Institute, the security consulting agency, published a cloud computing security research report, made a detailed description of cloud computing security issues that may arise, as well as the source distribution of these security issues[2]. Albeshri A. and other researchers studied the cloud platform service sharing and collaboration and put forward a cloud service resource management method[3]. Roschke S. and his colleagues researched the intrusion detection method under the cloud environment and made certain achievements[4]. Starting from the management direction of cloud computing service, Brandic I. and other researchers proposed a method of self-management of cloud service [5]. Professor Feng Dengguo also carried on the thorough research in the safe direction of cloud computing and proposed the security service framework of cloud computing[6]. For the issues of cloud platform business and performance, Dr. Mi Haibo came up with the diagnostic method for the hierarchical performance problems of cloud computing platform[7]. The research results of these documents offer a certain data support and research idea for the network security of cloud computing.

The study starts from the network security of cloud computing and analyzes the security risk that may be encountered in the environment of cloud computing. On the basis of full analysis of the structure, combined with the method of traditional network security risk assessment, it draw a set of models for the network security risk assessment of cloud computing.

TABLE 1 : Security events summary of cloud service providers at home and abroad

time	Service provider	description of event
February 15, 2008	Amazon	There was a network service downtime in Amazon. Many network which relied on Amazon's EC2 cloud computing and S3 cloud storage were influenced.
February 24, 2009	Google	Gmail broke out global fault, causing service disruption.
September, 2009	Google	It occurred downtime twice in Gmail service, resulting in the user can not access the mail system.
October, 2009	Microsoft	Microsoft server broke down, causing the loss of the users' data and the users' personal data in the backup server.
April-May, 2011	Sony	PSN public cloud suffered three successive attacks by hackers, causing a lot of customer information stolen.
March, 2011	Google	Google mailbox occurred the event that users' data lost massively. About 0.08% Gmail users' (about 150,000) all messages and data records were deleted and parts of the users' accounts were reset.
October, 2011	Aliyun	Aliyun server carried out restart operations in the process of wrong disk maintenance. It led to the data loss of TeamCola Company and caused serious losses to the company.
August, 2012	Grand Cloud	Individual user's data was lost because a physical server disk of Grand Cloud was damaged.

CLOUD COMPUTING

Definition of cloud computing

There are many kinds of definitions for cloud computing. The definition in Baidu encyclopedia is: based on the increase, use and delivery models of the Internet related service, usually, they are the virtualized resources which involve providing dynamic scalability through the Internet[8]. NIST defined it as: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and service) that can be rapidly provisioned and released with minimal management effort or service provider interaction[9]. In fact, cloud is a metaphor of network.

Highlights of cloud computing

As a new technology, cloud computing has many definitions. However, no matter how many explanations for it, all these explanations reflect the following highlights[10]

(1)Cloud computing mainly provides service for users. It offers the resources to users through the Internet.

(2)According to the needs of users, cloud computing could carry out dynamic scalability and configuration to provide resources for the users.

(3)The users in cloud can share the virtualized resources. Resources exist in the way of share in physics and present in a form of single overall in logic.

(4)The users, who use cloud resources, are charged according to the actual use. They need not bear the cost of idle computing resources.

Development status of cloud computing in domestic and overseas

Development status of cloud computing in overseas

In 2006, Eric Emerson Schmidt, the chief executive officer of Google, put forward the concept of cloud computing in the search engine conference. From 2010, the U.S. government put the cloud computing into the government plan and funded a lot of pilot projects to strengthen the arrangements for cloud computing. In Japan, the government introduced a number of policies to support the development of cloud computing. But, with the wide application of cloud computing, security problems of it has come out. In March 2010, some European legal experts of network proposed to make a global agreement to protect data and to solve the possible security problems with it.

Development status of cloud computing in domestic

The development of cloud computing is late in China. But it has made considerable headway since it was introduced into China. Since 2008, we have had several cloud computing centers established by famous IT enterprises. As the largest search engine company in domestic, Baidu also joined the ranks of cloud computing service. It has provided a series of service, such as network disk, photo albums and pictures. The users can get a lot of data and information through Baidu search within one second, which totally depend on the mass storage capabilities and high-speed data computation capabilities of cloud computing.

NETWORK SECURITY RISK OF CLOUD COMPUTING

In the process of construction of cloud computing, every part may cause security problem. Because cloud computing system has a large scale, most of the users' privacy data is concentrated in it and cloud computing is open and complex, so the security of it faces great challenge. With the development of cloud computing, the security of the data has become the significant reference for users to choose service. Figure 1 is the survey report of Forrester Consulting in 2011. It shows that concern about security has become the second major factor to influence the choice of the users. The followings are the potential security risks of cloud computing:

Leakage or loss of users' data. When users' data is transported and stored in the environment of cloud computing, there is no control ability for itself actually. Data security completely depends on the control of the service providers. If service providers fail to control data security or lack of management, it will result in data leakage. The impact on the users is extremely bad.

Users don't have plenipotentiary power to use the applications in cloud computing. In the process of operation and maintenance, the service providers of cloud computing need to operate and manage all the resources in the cloud computing center, such as server, storage and network. In this process, any problems in operation and management may cause great damage to the application of users.

There are loopholes in shared technology. Cloud computing is a large shared data center. The greater the shared degree is, the more potential loopholes exist in it.

The insiders of supplier steal data. The storage of users' data in the cloud requires the management and audit of the administrator. If the inside of service provider has management loophole, the insiders will make use of it to steal users' data and cause damage to them.

The security mechanism of users' authentication is weak. Cloud computing service is a multi-user operating environment. Different users have different accounts and codes. If the authentication mechanism of cloud computing is weak, it will be easy for the invaders to get users' account information and steal their data.

There are some vague and unknown threats. When providing cloud computing service, the providers only emphasize the benefits of users if they put information and data into cloud, but the service providers would not tell them the danger.

Figure 1 : Survey of service concerns on choosing cloud computing

INTRODUCTION TO CLOUD COMPUTING FRAMEWORK

Figure 2 is the general structure of cloud computing framework. Figure 2 shows that the core of cloud computing is service. SaaS means software as a service, SaaS means platform as a service, Iaas means infrastructure as a service. These three models build the platform framework of cloud computing. Understanding the roles and relationship of the three modes in platform framework of cloud computing is the basis for understanding the security risks of cloud computing, The IaaS is the basis of cloud computing service. It mainly provides the basic framework service, such as computing service, storage service and network service. PaaS is built on the framework of IaaS, which mainly provides the public platform services, such as unified operating system, including the operating platform, the backstage support (unified billing, unified distribution, unified report etc.) and general technology (distributed caching, distributed database etc.). SaaS is built on the top of the platform, which primarily provides specific services for users, such as cloud search, online sharing and SNS community. The three models play different roles in cloud service. From the platform framework of cloud computing, we can see that in cloud service, the lower of the framework level offered by service providers, the lower of the security and management duty born by users.

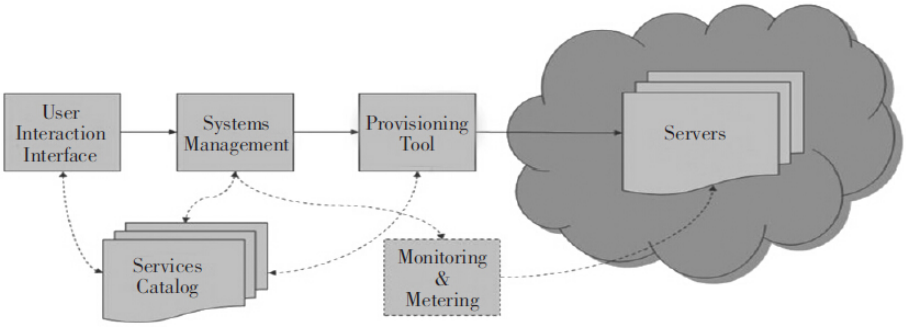

Figure 2 : General structure of cloud computing framework

ANALYSIS OF ELEMENTS OF NETWORK SECURITY RISK ASSESSMENT FOR CLOUD COMPUTING

As a new technology, the business models and ways of working are different from the traditional ones. It brings a more convenient living environment for users. In the course of construction of cloud computing, there are great changes in the aspects of business model or server virtualization. However, essentially, the application system of cloud computing and the user access behavior haven't been changed. Based on the analysis for the security problems of cloud computing and the method of traditional information security risk assessment, the study discusses the security risk assessment of cloud computing from the followed nine elements: asset, threat, vulnerability, security precautions, risk, residual risk, standardization, laws and regulations[11]. The relationship of these nine elements is shown in Figure 3. Squares represent the basic elements of evaluation. As a part of the assessment elements, ovals represent the attribute of elements.

The followings are the analysis of the nine elements which influence the network security risk assessment of cloud computing.

Asset refers to all kinds of resources in the cloud computing. As we all know, when one possesses more things, he should adopt greater strategies to deal with them and the risk will be higher than others. In fact, the resources in cloud computing have the same situation with this.

Vulnerability refers to every asset in cloud computing is likely to have loophole, and cloud computing system has vulnerability.

Threat refers to the structure, technology and management in cloud computing are likely to cause problems and these problem can lead to security problems.

Security precautions refer to the technology and management methods aiming at the reasons of safety accidents in cloud computing.

Risk refers to the probability of having security accidents in cloud computing.

Residual risk refers to the probability of having security accidents in cloud computing after taking safety precautions.

Security requirement refers to the requirement to information security of cloud computing system. This requirement is proposed in order to achieve the strategic target of business.

Standardization refers to the establishment of a unified calculation standard aiming to solve the compatibility of cloud products in interoperation. This makes products' switchover and data transfer among different cloud become more convenient, fast and safe. Also, it cannot be subject to the service providers' lock to the users and it can make data acquisition and responsibilities division when there is a security accident.

Laws and regulations refer to the users' data in the cloud should be protected by law. However, due to the data storage in the cloud is not subject to the limitation of countries and regions and different countries have different legal systems, it will cause potential legal risks.

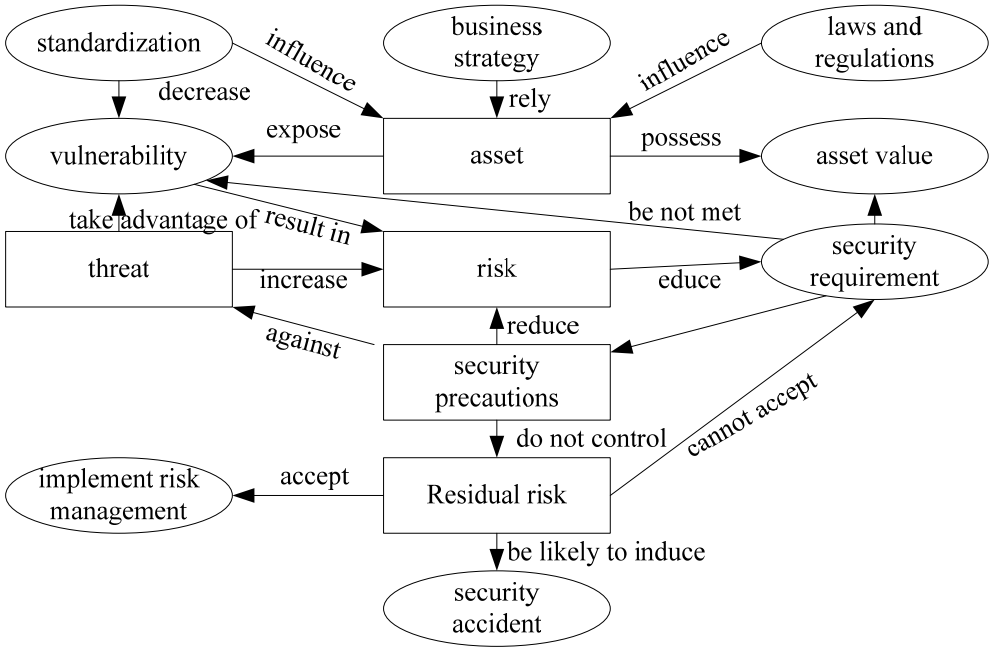

Figure 4 : Relationship of various elements in security risk assessment of cloud computing

MODEL OF NETWORK SECURITY RISK ASSESSMENT FOR CLOUD COMPUTING

Security risk assessment process for cloud computing

Based on the relationship of the elements of cloud computing and the method of traditional network security risk assessment, the study designs a security risk assessment process for cloud computing as shown in Figure 5. In this process, according to the importance of the assets and the regulations of laws and standardization, the users, the owners of the assets, can require the protection degree for one of the assets. Then, on the basis of the vulnerability of assets and the potential threats, the users should make an assessment for the risk level and work out appropriate precautions to deal with these risks to make up the vulnerability of assets and reduce the possibility of the occurrence of security accidents. However, if the residual risk cannot meet the requirement of the protection degree, you need to continue to assess the assets and amend the safety precautions accordingly, until the protection level can meet the requirements for the protection of assets.

Formal model for the risk assessment of cloud computing

Cloud computing system has some unique features which are different from the traditional information system. So, though the risk assessment method of cloud computing has some similarities with the method of traditional information system assessment, it has its unique characteristics and different cloud has different characteristic. Therefore, the methods and requirements are different in the aspects of risks' quality and quantity when setting a model of risk assessment for cloud computing. Based on the model of traditional network security risk assessment and according to unique features of cloud computing, the study designs a formal model for the risk assessment of cloud computing. In the model, R refers to risk, A

refers to asset, V refers to vulnerability, T refers to threat, I refers to importance, S refers to standardization, L refers to laws and regulations, P refers to security precautions.

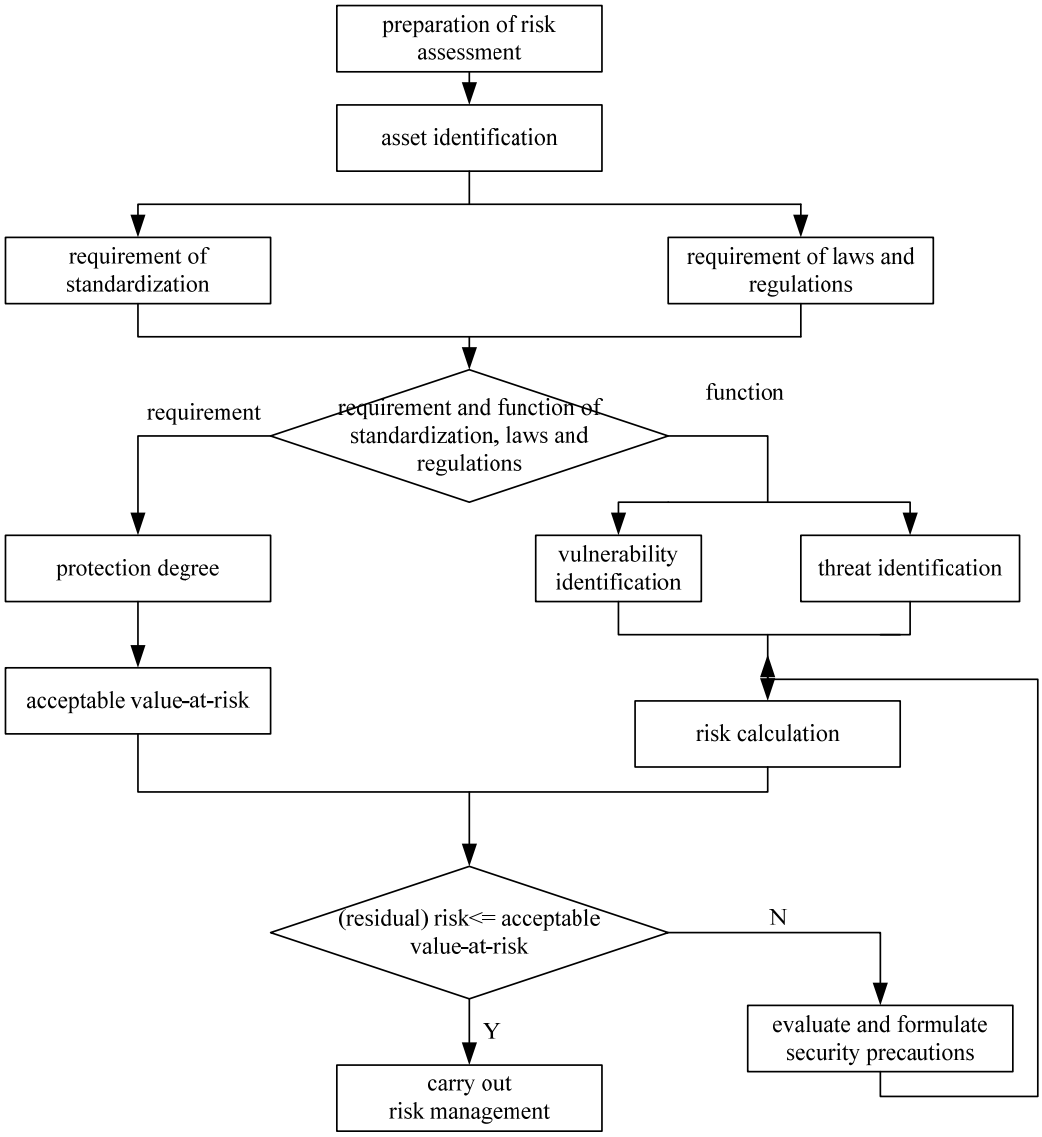

Figure 5 : Security risk assessment process for cloud computing

The formal model for the risk assessment of cloud computing is shown in formula (1).

$$R = F(A,V,T,S,L,P) \quad \textbf{(1)}$$

The residual risk of each asset is shown in formula (2). N refers to the number of assets in the cloud system.

$$R_i = F(A_i,V_i,T_i,S_i,L_i,P_i) = F_1(A_i,V_i,T_i) - F_2(A_i,S_i,L_i,P_i), \quad i \in N \quad \textbf{(2)}$$

In formula (2), $F_1(A_i, V_i, T_i)$ refers to the breakdown strength caused by all the vulnerability of i asset. F_2 (A_i, S_i, L_i, P_i) refers to the protective capability to i asset after i asset is regulated by the requirement of standardization, laws and regulations and takes security precautions.

The acceptable value-at-risk of asset is shown in formula (3).

$$RR_I = F_3(A_i,S_i,L_i,P_i), \quad i \in N \quad \textbf{(3)}$$

In formula (2), RR_i refers to the acceptable value-at-risk of i asset according to the requirement of the importance, standardization, laws and regulations of asset.

$Ri \leq RR_i$ shows that the residual risk of i asset is safe. $Ri > RR_i$ shows that the residual risk of i asset is not safe. You should continue to assess the assets to strengthen security precautions and reduce the risk-at-value.

The overall residual risk of cloud computing system is shown in formula (4).

$$R = \sum_{i-1}^{n} R_i = \sum_{i-1}^{n} [F_1(A_i, V_i, T_i) - F_2(A_i, S_i, L_i, P_i)] = \sum_{i-1}^{n} F_1(A_i, V_i, T_i) - \sum_{i-1}^{n} F_2(A_i, S_i, L_i, P_i) \text{ n、 } i \in N \quad \textbf{(4)}$$

It requires that the risk-at-value of each asset must meet $Ri \leq RR_i$ in formula (4) to guarantee the safety of the asset.

CONCLUSION

With the development of society and the progress of science, Internet technology is also undergoing great changes. The emergence of cloud computing technology allows a large number of data and information to be stored in the cloud server. Also, it reduces the pressure of the client through putting the data into the cloud which should be put into client. However, the confidentiality, availability and uncertainty of the network make the data security in the cloud become an unavoidable problem. The study starts from the definition and framework of cloud computing, quotes the nine elements which influence the network security risk assessment of cloud computing: asset, threat, vulnerability, security precautions, risk, residual risk, security requirement, standardization, laws and regulations and explains the relationship of them. Based on the relationship of the nine elements, the method of traditional information security risk assessment and the characteristic of cloud computing, it worked out a formal model for the risk assessment of cloud computing. This can predict the risks and take appropriate security precautions to protect the security of customers' information in cloud computing services. With the development of science and technology, cloud computing technology will continue improving and new threats will appear. Maybe, introducing a dynamic strategy is a direction for the development of network security risk assessment method of cloud computing.

REFERENCES

[1] M.Armbrust, A.Fox, R.Griffith, et al; Above the clouds: A berkeley view of cloud computing, Technical Report No.UCB/EECS-2009-28[J], Berkeley, USA:University of California at Berkeley,**(2009)**.

[2] CAS. SecaaS (Security as-a Service).Defined Categories of Service **(2011)**.

[3] A.Albeshri, W.Caelli; Mutual Protection in a Cloud Computing Environment. High Performance Computing and Communi cations (HPCC), 641-646 **(2010)**.

[4] S.Roschke, Feng Cheng, C.Meinel; Intrusion Detection in the Cloud. Dependable, Autonomic and Secure Computing, 729-734 **(2009)**.

[5] I.Brandic; Towards Self-Manageable Cloud Services. Computer Software and Applications Conference, 128-133 **(2009)**.

[6] Feng Dengguo, Zhang Ming, Zhang Yan, Xu Zhen; Study on Cloud Computing Security [J], Journal of Software, **22(1)**, 71-83 **(2011)**.

[7] Mi Haibo, Wang Huaimin, Cai Hua; The Diagnostic Method for the Hierarchical Performance Problems of Cloud Computing Platform [J], Journal on Communications, **32(7)**, 114-124 **(2011)**.

[8] Cloud Computing- Baidu Encyclopedia [EB/OL].http://baike.baidu.com, **(2014)**.

[9] P.Mell, T.Grance; The NIST Definition of Cloud Computing[R/OL], http://c src. nist. gov/groups/SNS/cloud-computing/cloud-def-v 15.doc, **(2010-02-11)**.

[10] Shen Changxiang; Cloud Computing Security and Ranked Protection [J], Financial Electronic, **5,** 12-14 **(2012)**.

[11] Xiang Hong; Information Security Evaluation and Risk Assessment [M], Publishing House of Electronics Industry, **1**, **(2009)**.