Advances in Engineering Research (AER), volume 82
2016 International Conference on Engineering and Advanced Technology (ICEAT-16)

Study on risk assessment of information security based on cloud computing model

Guo-Hua WU[1],Yu-Cheng LIU[1],Kai-Kai QI[1],Peng WANG[1] and Jian-Da Xu[2]

[1]China Electric Power Research Institute

[2]Beijing hualian electrical engineering supervision company

KEYWORDS: Cloud computing; Information security; Risk assessment

ABSTRACT: First of all, this paper analysis the risks on the cloud calculation briefly, and then according to its own characteristics and traditional assessment method for risks lying in information security of cloud computing, it studies the of risk assessment on information security based on cloud computing model, focusing on the process of assessment for information assets, stressing the importance of the evaluation index of evaluation system.

1 Overview of cloud computing

1.1 Definition of cloud computing

The definition of cloud computing was proposed by Google in 2007. At that period of time the cloud computing has been known in the world of the Internet, even be named as an important information technology revolution hailed in computer and Internet revolution in human history by the people in the field. Cloud computing brings earth shaking changes to the traditional Internet model, and then to our life, work and business where it has import aspects.

In the narrow sense, cloud computing refers to the new business models for the end customer to provide its amazing computing services through SaaS, PaaS, MSP and so on. Cloud computing integrates the traditional computer technology and modern Internet technology including grid computing, parallel computing, utility computing, network storage and Virtualization. More broadly speaking, cloud computing is a new way of service using by which users (such as individuals, companies and other institutions) can obtain the appropriate service based on their own needs only through the Internet.

With cloud computing, users can enjoy amazing computing service and all kinds of network resources only with networked hardware devices, such as mobile phones, tablet computers, computer and so on. In essence, cloud computing is a kind of service with its powerful cloud computing power, which reduces the computing burden of hardware terminals for its users. Simple said, this is also similar to that used in our daily life, such as water, electricity, natural gas and other resources, and in order to use these resources, users do not need to build their own water plant, power station or digging for oil, but pay it on time. Similarly, the user can directly buy this kind of product called cloud computing, and they don’t need to upgrade the hardware device or software based on the required services to solve the problems.

1.2 Advantages of cloud computing

For the public cloud, cloud computing can greatly reduce business investment in software and hardware and related staff and operation maintenance, and because the cloud computing has characteristics including rapid deployment, on-demand service and pay data on demand making it’s

more convenient for enterprise developing application amount. However, compared to the public cloud,development and construction of private cloud requires greater investment. It is expected that in the future, with the continuous promotion of the use of cloud computing, the size of the world market for cloud computing will quickly expand. The development of cloud computing will have a major impact on the world's information industry, while creating opportunities of good development for many countries and companies. For example,the enterprises in China may use the information revolution wave launching the introduction of new products, new modes of work and new services, so as to catch up with the international level. And in the future there will emerge more and more small and medium-sized enterprises in China, and the in the process of development, small and medium-sized enterprises may can not keep up with growth rate of business because of its size, investment in the establishment of private computer center with large investment and low rate of return. The promotion current of the cloud computing, because of its savings in terms of computing resources, it is also in line with the policies for domestic industrial transformation and upgrading about reducing discharge.

2 Security challenges faced by cloud computing

Cloud security is different from cloud computing security, because cloud security mainly refers to the newly introduced anti virus architecture based on cloud computing, while cloud computing security includes terminal’s access control, encrypting data and virtual machine protection. In addition, the cloud security also includes the prevention of network security provided by the cloud service, such as hacking. Because cloud computing has a large number of information of users, trade secrets and other data, so the use of cloud computing will bring the following security risks to the users.

2.1 Sustainability of services

When faced with natural or non natural factors causing damage for hardware equipment which can not be operated normally, cloud service providers can guarantee the continuity of service. In addition, the user's data and other information can not be affected by the cloud service providing company which have changes which need to be noticed.

2.2 Issues for user’s privacy

Cloud service providers may exist problems such as unauthorized access or using customer’s information. And if cloud service providers can carry out investigation for user’s privacy violations.

2.3 Isolation problem of data caused by multi-person’s renting

While if there is the case of multi-person’s renting, the user needs to share the basic equipment, services and applications, then how the user's data and information can achieve mutual isolation greatly. In addition, it is necessary to prevent some users from using the program that runs in the data center shared, which infringe the privacy of other users’data.

2.4 Risks on Sovereignty of National Information

Because the data of users of cloud computing may be distributed on the server in different countries or regions, the information security has risen to the level of national security currently. For example, because cloud computing service providers are mainly concentrated in the western developed countries led by the United States, so these countries often manipulated the flow, storage and operation of information in the whole world, having the absolute monopoly of information in world,

controlling Internet technology and information resources. The original intention of creating cloud computing is to allow users to enjoy more convenient Internet resources and services. However, the Internet resources and basic services needed by users are controlled by these developed countries as a country's natural resources are contained by other countries which will bring a great threat to the information security of this country. Privacy disclosure problem of Google users and Amazon downtime events have sounded the alarm, which means it needs to beware of cloud service providers or its host countries using cloud computing leading to the damage of information security for other country.

2.5 Laws and regulations have not kept pace with the progress

Firstly, the law can protect the user's information in the computer from infringement, but for information stored in the cloud, there is still no relevant laws and regulations about the service providers and the government can not access to this type of information without allow by the user.

Secondly, in the agreement of service level, cloud service providers even don't need to undertake legal obligation for any kind of data leakage or damage to avoid a lot of risk problems. This kind of unreasonable clauses lead to the rights and interests of the users under serious threat. For example, in the Amazon outages, Amazon Company should not bear any responsibility.

Thirdly, the current global information technology is also making the global cloud computing be more complex. Country A uses country B's service providing by cloud service providers, while the data is stored in Country C's server, which means once users' data is destroyed in Country A, how the users maintain their own rights and interests in Country A where lies a big problem, because the relevant laws and regulations in different countries are not unified, the situation will be very difficult. Therefore, it is necessary to establish a bilateral or multilateral agreement on cloud computing in different countries, of course, the best way is to achieve a unified global legal agreement.

2.6 Black box for cloud computing service providers

The cloud service providers such as Google, Microsoft, Amazon and so on, have different standards about cloud services and each other are not compatible. Because the cloud computing service for user data processing and storage process provided by above companies look like "black box", and users only know the results,so there is a certain kind of risk for users' data.

2.7 The issues of traditional information security become more serious

Cloud computing is still facing a lot of traditional information security issues, such as malicious network attacks, network transmission security, access control, data loss and so on.

Although there are a variety of cloud computing security issues, while with the continuous development of cloud computing, these issues will become more and more prominent. But as a user, it is not possible to stop using the cloud computing because of the issues. And it is more important to strengthen their own security awareness for the process of using cloud computing and to take certain precautions. Therefore, it is very meaningful to study a kind of method for assessment of information security risk which is based on the cloud computing model.

3 Overview of information security risk assessment

Information security risk assessment is the necessary work to ensure the security of information. Information security risk assessment mainly refers to three aspects, such as the threat to the information system, the possible influence and the vulnerability of the system, and so on.

Specifically, information security risk assessment is to formulate related security strategy and improve the security of information system through the analysis of all kinds of risks in the current and future, and estimate the impact of risks to the system.

The primary task of establishing a risk assessment model is to analyze the elements of information risk assessment. The basic elements include assets, vulnerabilities and threats. The process of risk assessment should take the risk as the center, and with the evaluation of the three basic elements, it should be related to business strategy, asset value, security event and other factors.

3.1 Assets appraisal

The methods of evaluating assets in the traditional information security risk assessment mainly take business as the main line running through the entire process, the process includes making assignment on recognition of business and assets, classification on assets and security on assets. While the classification of assets lacks of uniform standards. The current draft international standards divide the assets into hardware and software, data, document, services, personnel, equipment and others, and this method can classify information systems according to the forms which is too simple without considering the correlation between assets and the value of the assets that may be influenced by its location and environmental impact. In accordance with this method, the results of the assets evaluation are often incomplete.

For cloud computing, the assessment elements and methods in the traditional information security risk assessment are no longer applicable. Because they are used for often distributed in different locations used in data processing, transmission and storage of the Internet, computing platforms and the corresponding procedures. At this point, we need to improve the relevant risk assessment indicators and methods in the aspects of security facilities, storage devices, service agreements, contracts and service providers as described next:

(1)Determine the cloud data, function and the scope of the asset.

(2)Determine the importance of relevant data and functions.

It needs to assess the importance of applications, functions, processes, and assets, which lie mainly on the confidentiality, integrity and availability of assets and the risk assessment in transferring of assets to the cloud.

(3)Determine the cloud deployment model.

Familiar with the importance of assets, before determining the service provider, it needs to choose the model meeting the requirements of the risk based on a variety of deployment models (public, private, community or mixed).

(4)Valuation of asset

Grades should be Valuated on confidentiality, integrity and availability of asset respectively,and the final choice is the highest value of the three values of this asset.

3.2 Identification of threat

The process of threat identification refers to the classification and assignment of threats. Threat is the external cause of the risk. This threat refers to the risk caused by factors such as people, systems or nature. For cloud computing security risk assessment, there are the following recommendations:

(1)Evaluate the cloud service model or provider.

Cloud computing has characteristics of on-demand service and multi-person’s renting, which often make the traditional audit and evaluation method lose their function, for example,cloud providers limit the user's test evaluation, even not to publish monitoring data where users can replace the

assessment method or find a cloud service provider that meets the requirements of risk management.
(2)Check out the hidden data flow and circle the threat of exposed point.
(3)Assignment made for the possibility of a threat to be matched.

3.3 Vulnerability identification
The process of fragile vulnerability is the identification and assignment of vulnerability. Vulnerability is the internal cause of the risk, and in essence, it's main target is to determine the technical and management defects in the system.

3.4 Risk analysis
Finally, according to the frequency of threats and the the degree of impact of threat assessment to determine the risk of information systems. At the same time, according to the relationship between the threat and vulnerability, to determine the probability of occurrence of security incidents.

CONCLUSION
With the development of cloud computing, a variety of theories and practices related on information security risk assessment will continue to enhance their levels. Cloud computing information security is an important factor to limit the development of cloud computing, and to assess the risk of information security of cloud computing is the necessary way to promote the further development of the cloud computing.

Reference
[1] ginger, Ma Zifei, Li Tong, Zhang Qiujin. Cloud computing security risk factors and coping strategies of modern information mining [J]. 2015 (01).
[2] Zhang Heng, Paul Kay. Building a security inspection and evaluation index system of cloud computing environment [A]. twenty-ninth national computer security academic exchange conference proceedings [C]. 2014