A RISK MANAGEMENT FRAMEWORK FOR CLOUD COMPUTING

Feng Xie[1], Yong Peng[1], Wei Zhao[1], Dongqing Chen[1], Xiaoran Wang[2], Xingmei Huo[1]

[1]China Information Technology Security Evaluation Center, Beijing 100085, China
[2]Beijing Institute of Technology, Beijing 100081, China
xief@itsec.gov.cn, pengy@itsec.gov.cn, zhaow@itsec.gov.cn, chendq@itsec.gov.cn, 1wxr1237@126.com

Abstract: Although cloud computing has the advantages of cost-saving, efficiency and scalability, it also brings about many security issues. Because almost all software, hardware, and application data are deployed and stored in the cloud platforms, there is often the distrust between users and cloud suppliers. To resolve the problem, this paper proposes a risk management framework on the basis of the previous work. The framework consists of five components: user requirement self-assessment, cloud service providers desktop assessment, risk assessment, third-party agencies review, and continuous monitoring. By means of the framework, the cloud service suppliers can better understand the user's requirements, and the trust between the users and the suppliers is more easily acquired.

Keywords: Cloud computing security; Risk management framework; Security assessment; Trust

1 Introduction

In recent years cloud computing has gained wide attentions, but the trust and security issues of cloud computing have prevented the businesses from fully accepting cloud platforms [1, 2]. The security incidents of cloud computing occur frequently in some famous companies such as Google, Microsoft, Amazon and Salesforce.com. For example, Google's gmail failed in global scale on February 24, 2009, and the services were interrupted up to 4 hours. Similarly, the cloud computing center in Amazon's North Virginia was downtime on April 21, 2011 and the service interruptions lasted nearly four days. Through these security incidents, we can conclude that:

Firstly, cloud computing platform is not so strong like that we think about. It has many security issues, such as user privacy, user information security, data center management, etc. Therefore we must pay more attention to it.

Secondly, the cloud computing system is a complex system, which means that the emergency recovery of cloud computing system would become very complex when the incidents occurred.

Thirdly, because mass data of users are stored in cloud computing platform, the risk of data leakage becomes much greater compared with the traditional network platform.

Finally, as we can see from the above incidents, the cloud computing incidents has distinguished global influence and the caused losses are unpredictable.

Traditionally, the security of information system is guaranteed by the users by means of some security policies, best practices, and defensive equipments including firewall as well as IDS. However, the situation is entirely different in cloud computing. All things such as hardware, software, even application data are deployed and stored in the cloud providers. The security procedure becomes intangible and out of control for users. Therefore there is the distrust between users and cloud suppliers [3]. To solve these problems, this paper proposes a risk management framework for cloud computing.

2 Related work

The United States can be regarded as the leader in the cloud computing area. Some development standards and roadmaps of cloud computing have been proposed in recent years [4]. To manage the risk of cloud computing, the U.S. Federal Committee has set up a risk and authorized project team, which consist of the American National Standards Institute (NIST), the General Services Administration (GSA), and other agencies. A draft of security assessment and authorization for government cloud computing is developed [5]. The draft proposes the cloud computing security control baseline, continuous monitoring process, and the method of assessment and authorization. From these literatures we can gain the risk management framework of cloud computing in USA. The framework consists of seven major processes:

- categorization of information systems;
- selection of security controls;
- authorization of request;
- the implementation of security controls;
- assessment of security controls;
- authorization of information system;
- monitoring of security controls.

Zhang et al. propose to manage the information security risk of cloud computing environments by means of Deming cycle [6]. In their methods, the whole procedure includes architect and establish (plan), implement and operate (do), monitor and review (check, act), which is short for PDCA. The framework is very similar with the traditional quality management.

978-1-4673-1857-0/12/$31.00 ©2012 IEEE

Tanimoto et al. look into the various risks when a company uses cloud computing and identify various risk factors from a user's viewpoint [7]. Also the countermeasures are analyzed in detail.

Different from the work above, this paper pays more attention to how to augment the trust between users and service providers. A new risk management framework of cloud computing including the users, the providers, as well as the third-party agencies is proposed.

3 A new cloud computing risk management framework

This framework is composed of five basic processes: user requirement self-assessment, cloud service providers desktop assessment, risk assessment, third-party agencies review, and continuous monitoring, which is shown in Figure 1.

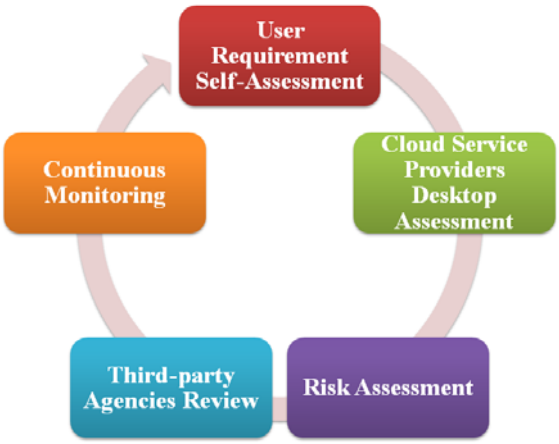

Figure 1 The cloud computing risk management framework proposed in this paper

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

3.1 User requirement self-assessment

At the requirement self-assessment phase, the user should specify the process information of cloud computing service, and determine the needed cloud computing model as well as security level.

Firstly, the security level of cloud computing platform should be determined, which could be divided into several levels. The higher the level is, the more the security is. The security level can be determined from discretionary access control, authentication, data integrity, auditing, and so on.

Secondly, the cloud computing service model should be determined. The models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The user can select one or more service models according to their needs, which is contribute to the selection of cloud service providers.

Thirdly, the deployment model should be determined. NIST proposes the four deployment models: private cloud, public cloud, community cloud, and mixed cloud [8]. The user can select a cloud computing deployment model according to system security request. A system with higher level of security request can choose the private cloud model, in which the whole infrastructure of the cloud service provider is only owned by the user. Otherwise, a system with the low level of security request can choose the public cloud model, in which the infrastructure is shared with other users. It is clear that the private model has the best security and user privacy but spends most costly.

Finally, the user can determine several cloud computing providers as candidates according to previous selection results.

3.2 Cloud service providers desktop assessment

After the candidates of cloud service providers are determined, the desktop assessment begins. The desktop assessment is to evaluate the cloud service plans made by candidates, analyze the historical security status, and furthermore acquire the potential risk of candidates.

The cloud service plans are developed by the candidates according to user requirements, which often include:

- cloud model;
- scope of cloud services;
- data center environment;
- hardware and software facilities;
- security control measures;
- migration process;
- method distinguishing the cloud server which the user is using with other users;
- data backup;
- data processing measures when the cloud service is stopped;
- incident response plan;
- etc.

The historical security status of cloud service providers indicates the underlying risk of cloud service which is based on the cloud provider. We can assess the underlying risk by means of the occurred security incidents from two dimensions, i.e., the likelihood and the adverse impact of the incidents. Generally, the incidents can be divided into two types: adversarial incidents and non-adversarial incidents. The adversarial incidents refer to the incidents that are initiated by the adversary such as hacker, cyber criminal organization, even cyber war, while the non-adversarial incidents refer to the incidents that occur due to the earthquake, flood, system fault, or are initiated by unintentional operators. Whether an incident is adversarial or non-adversarial, we can evaluate its occurrence likelihood. For convenience, this paper divides the occurrence likelihood of incidents into five levels qualitatively, i.e., very low, low, medium, high, and very high, which is reference to [9]. It is noticed that the levels have different meanings for adversarial and non-adversarial incidents. Table 1 shows the levels of occurrence likelihood of adversarial and non-adversarial incidents, in which "A" refers to adversarial incident, while "NA" refers to non-adversarial incident.

Table I The occurrence likelihood levels of cloud security incidents

Levels	Meaning	Types	Description
4	very high	A	The incident is almost certain to be initiated by adversary.
		NA	The incident is almost certain to occur, or occurs more than 100 times a year.
3	high	A	The incident is highly likely to be initiated by adversary.
		NA	The incident is highly likely to occur, or occurs between 10-100 times a year.
2	medium	A	The incident is somewhat likely to be initiated by adversary.
		NA	The incident is somewhat likely to occur, or occurs between 1-10 times a year.
1	low	A	The incident is unlikely to be initiated by adversary.
		NA	The incident is unlikely to occur, or occurs less than once a year, but more than once every 10 years.
0	very low	A	The incident is highly unlikely to be initiated by adversary.
		NA	The incident is highly unlikely to occur, or occurs less than once every 10 years.

Then the total occurrence likelihood is equal to the maximum value of two type's incidents likelihoods, i.e., P=max (P1, P2), in which P denotes the likelihood of incidents, P1 denotes the likelihood of adversarial incidents, P2 denotes the likelihood of non-adversarial incidents.

The adverse impact of incidents is also important to evaluate the incidents risk. Different incident may cause different losses. We can measure the impact due to the caused losses. Table II shows the five levels of impact in this paper.

Table II The impact of cloud security incidents

Levels	Meaning	Description
4	very high	If an incident occurs, it is almost certain to have adverse impacts.
3	high	If an incident occurs, it is highly likely to have adverse impacts.
2	medium	If an incident occurs, it is somewhat likely to have adverse impacts.
1	low	If an incident occurs, it is unlikely to have adverse impacts.
0	very low	If an incident occurs, it is highly unlikely to have adverse impacts.

Therefore we can evaluate the potential risk of cloud service providers according to the likelihood and adverse impact of the occurred incidents. Clearly, the more the likelihood and adverse impact are, the more the potential risk is. Here we define the risk level as a function of the likelihood and caused adverse impact of the incident which is equal to the summarization of the likelihood level and the impact level, i.e., *Level(risk) = Level(likelihood) + Level(impact)*. The resulting risk is measured on a scale of 0 to 8 that can be evaluated against risk acceptance criteria. The risk scale could also be mapped to a simple overall risk rating: low risk of which the level range is from 0 to 2, medium risk of which the level range is from 3 to 5, and high risk of which the level range is from 6 to 8, which is shown in Figure 2.

According to the desktop assessment, we can obtain the basic risk level of candidates and determine the targeting cloud service provider. It is, however, noticed that the risk is only assessed based on the plan and historical incident, while ignores any technological evaluation.

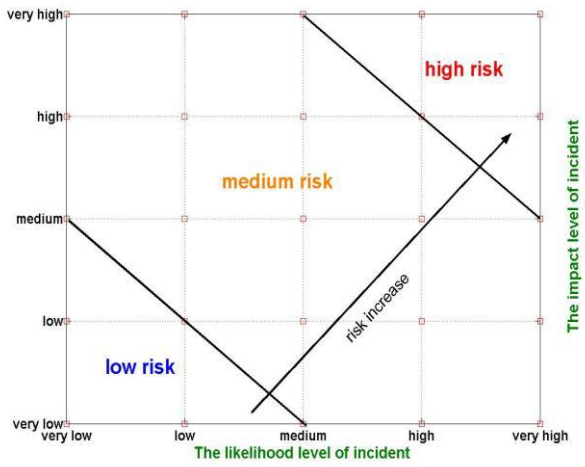

Figure 2 The potential risk resulted from the incidents

3.3 Risk assessment

The security of service is mainly provided by the cloud computing service provider no matter what service types the user selects. Therefore it becomes very important to assess the risk of service provider. The desktop assessment only analyzes the service plan and review the historical incidents, while ignores the assessment of the platform providing the cloud services. Generally the risk assessment is done by the third-party agency.

The risk assessment of cloud provider often includes seven stages: the preparation of risk assessment, asset identification, threat identification, vulnerability identification, existing security measures, risk analysis, and risk assessment documentation. Here we briefly

demonstrate the basic three factors in risk assessment: assets, threats, and vulnerabilities.

1). Assets

There are a lot of assets involved in cloud computing systems. Table 3 shows the classification of assets, asset owners and asset value (very low, low, medium, high, and very high) according to ENISA report [10]. Users can redefine these classifications for their cloud computing security evaluation.

Table III Assets value in cloud computing.

Asset	Owner	Value
Company reputation	Cloud customer	Very high
Customer trust	Cloud customer	Very high
Employee loyalty and experience	Cloud customer	high
Intellectual property	Cloud customer	high
Personal data	Cloud provider / Cloud customer	Very high
HR data	Cloud customer	high
real time services	Cloud provider / Cloud customer	Very high
Access control	Cloud provider / Cloud customer	high
Credentials	Cloud customer	Very high
User directory	Cloud customer	high
Cloud service management interface	Cloud provider / Cloud customer	Very high
Management interface APIs	Cloud provider / Cloud customer	medium
Network	Cloud provider / Cloud customer	high
Physical hardware	Cloud provider / Cloud customer	medium
Physical buildings	Cloud provider / Cloud customer	high
Cloud provider Application (source code)	Cloud provider / Cloud customer	high
Operational logs	Cloud provider / Cloud customer	medium
Security logs	Cloud provider / Cloud customer	medium
Backup or archive data	Cloud provider / Cloud customer	medium

2). Threats

Threats are described as anything that would contribute to the tampering, destruction or interruption of any cloud service or item of value of cloud users as well as cloud providers. In risk assessment the threat analysis is very important and must be looked at in relation to the cloud service environment and what affect they will have on the cloud providers and users.

3). Vulnerability

Vulnerability mainly consists of two types: technical and managemental. Technical vulnerability involves security issues in physical layer, network layer, system layer, application layer and data layer. Managemental vulnerability can be divided into technology management and organizational management, the former is related to the specific technical activities, the latter is related to the management of environment. For cloud computing, some vulnerabilities are usual and not specific to the cloud, such as system or OS vulnerabilities, untrusted software, and so on. While there are some vulnerabilities unique to cloud computing, such as authentication, authorization and accounting vulnerability, user provisioning vulnerability, lack of resource isolation, sensitive data deal, and so on.

3.4 Third-party agencies review

In order to ensure the normal operation and security of cloud services, it is necessary to employ third-party agencies to review the procedure. Of course, the third-party agencies should be authoritative security evaluation institutions, including the review group and expert group. The review process is shown in Figure 3, in which the organizations include cloud service providers, third-party agencies review group, the expert group and users.

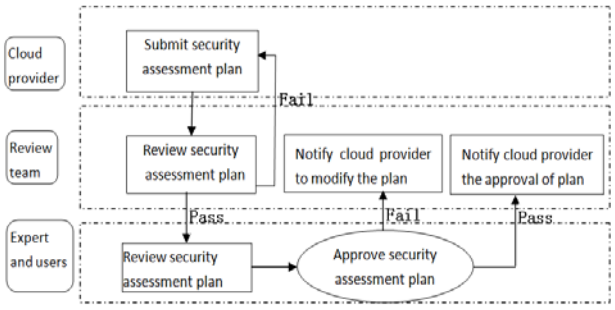

Figure 3 Third-party agencies review process

First, cloud service providers submit security assessment plan of user to the third party review group to review. If the plan is considered as incompetent, it would be returned to the providers for modification. Later, the plan is submitted to the expert group for further assessment. If the plan is approved by expert group, the cooperation relation is established.

3.5 Continuous monitoring

Through the above stages, the providers can provide the cloud services for users. Continuous monitoring process

is to monitor the ongoing risk assessment, and change the risk assessment program along with the environment changes.

4 Conclusions

Cloud computing has the advantages of high efficiency, low costs as well as scalability, which provides better services for the development of organizations or institutions. However the flexibility and openness embedded in cloud computing also bring about some security issues. For example, in cloud computing all data and operation control are transferred from users to the cloud computing providers which perhaps results in the sensitive data leakage. In addition, in the traditional information system the security is guaranteed by users self, while in cloud computing the security process becomes more abstract and users have no way to know the security assurance. Therefore it becomes more important to require the trust between the users and the suppliers. This paper provides a cloud computing security management framework that not only includes the assessments of user and supplier, but also introduces the third-party assessment agency to ensure the effectiveness and safety of cloud computing applications. This framework can help cloud service providers to better understand the enterprise's security condition by risk analysis and assessment, and thus has more effective solutions to resolve security issues in cloud computing applications process.

Acknowledgement

This work is supported by the Next Generation Broadband Wireless Mobile Communication Network under Grant No. 2012ZX03002002.

References

[1] Huiming Yu, Nakia Powell, Dexter Stembirdge, etc. Cloud computing and security challenges. In Proc. Of 50th annual southeast regional conference, 2012.

[2] Deyan Chen, Hong Zhao. Data security and privacy protection issues in cloud computing. In Proc. Of International conference on computer science and electronics engineering, 2012.

[3] Ryan Ko, Markus Kirchberg, Bu S. Lee. From system-cntric to data-centric logging – accountability, trust & security in cloud computing. In Porc. Of defence, science and research confierence, 2011.

[4] Special Publication 500-293. US government cloud computing technology roadmap, 2011.

[5] Proposed security assessment & authorization for U.S. government cloud computing, 2011.

[6] Xuan Zhang, Nattapong Wuwong, Hao Li, etc. Information security risk management framework for the cloud computing environments. In Proc. Of 10th international conference on computer and informaiton technology, 2010.

[7] S. Tanimoto, M. Hiramoto, M. Iwashita, etc. Risk management on the security problem in cloud computing. In Proc. Of ACIS/JNU international conference on computers, networks, systems, and industrial engineering, 2011.

[8] Peter Mell, Tim Grance. The NIST definition of cloud computing, 2009.

[9] Special Publication 800-30. Guide for Conducting Risk Assessments. America: National Institute of Standards and Technology, 2011.

[10] European Network and Information Security Agency (ENISA). Cloud Computing:Benefits, risks and recommendations for information security.2009.