International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.75-84
http://dx.doi.org/10.14257/ijsia.2016.10.2.07

Improvement Framework of Korean Certification System for Cloud Service Focus on Security

Hangoo Jeon[1], Young-Gi Min[2] and Kwang-Kyu Seo[3,*]

[1] Department of Management Engineering, Graduate School, Sangmyung University, 20, Honggimun 2-Gil, Jongno-Gu, Seoul 110-743, Rep. of Korea, {enter1919}@gmail.com

[2] Department of Technology Convergence, Sangmyung University, 31, Sangmyungdea-gil, Dongnam-gu, Cheonam-si, Chungnam 330-720, Republic of Korea, {min}@kcloud.or.kr

[3] Department of Management Engineering, Sangmyung University, 31, Sangmyungdea-gil, Dongnam-gu, Cheonam-si, Chungnam 330-720, Republic of Korea, {kwangkyu}@smu.ac.kr

Abstract

For the purpose of effectively utilizing & managing ICT resources and reducing costs, various companies are using cloud service as their core technological strategy. In spite of such effort, cloud service security, information protection and performance are being considered as areas that need to be considered when implementing cloud service. In Korea, cloud service certification system is being used to ensure user reliability for cloud service and high-quality cloud services are being certified by considering their quality, security and ongoing service capability. Since current certification system is being utilized focusing on management system, however, it lacks the consideration on technical aspects. Accordingly, this study aims to examine information assurance systems such as ISO 20071 and ISMS to propose a framework for enhancing the cloud service certification system of Korea by focusing on security. The findings of this study are expected to help in increasing the use of cloud service by improving user reliability through the increased utilization of cloud service certification system of Korea.

Keywords*: Cloud Service, Security, Certification, Vulnerability Scan*

1. Introduction

Cloud computing, which is provided in the form of service by sharing IT recourses, cannot become activated without solving the issue of information protection. In the case of Korea, cloud computing service is being recognized not only as an IT related business but also as an industry affecting national competitiveness. Accordingly, the cloud computing market size is being increased while expanding the global market share to actively engage in developing core technologies. However, it has not become activated to the level of that in the US and Japan mostly due to lack of trust on information protection. In the case of cloud computing service where multiple users use the same service, one might think that gathering every type of data in one place, namely IDC center to manage it would be safer than users having to directly manage it. However, security issues concerning important data such as personal information could occur and according damage could spread to multiple users. Accordingly, such security issues must be solved first [2].

* Corresponding author: Prof. Kwang-Kyu Seo (e-mail: kwangkyu@smu.ac.kr)

ISSN: 1738-9976 IJSIA

For the purpose of increasing the reliability of cloud service users, this study will analyze the cloud service certification system of Korea for certifying superior cloud services, and present a method of improving the framework of the certification system focusing on the security items being considered as the highest priority in implementing cloud service. Accordingly, it will create items of diagnosing and inspecting threats that could occur in the cloud service virtualization environment to reflect them in the assessment system of cloud service certification system.

As for the flow of the study shown in Fig. 1, it will analyze the assessment system and items of cloud service certification system of Korea, and analyze the security threat factors in virtualization environment. Based on this, this study aims to create security assessment items of cloud service and present an improve framework of cloud service certification system based on the security assessment items that have been created.

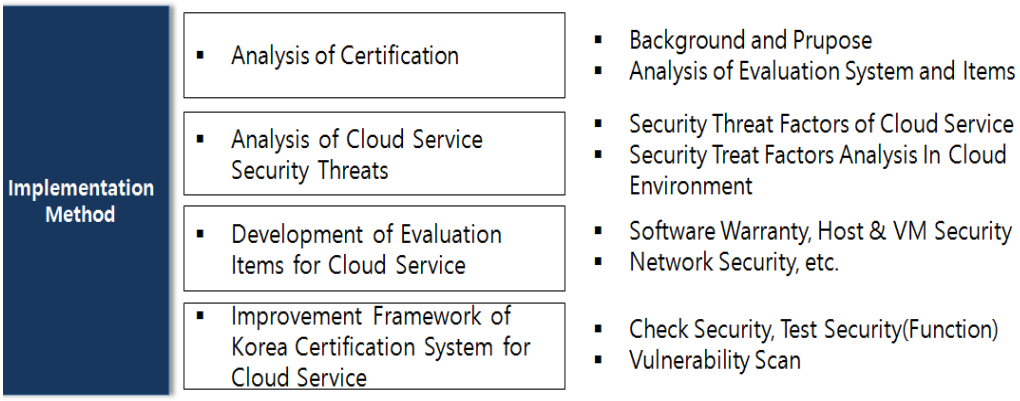

Figure 1. Process

2. Korean Cloud Service Certification System

The "cloud service certification system" of Korea is a system of certifying cloud services of a certain level by checking whether service system (policy, technology, *etc*.) required to guarantee the level of service (quality, stability, *etc*.) provided by cloud service provider. [8]

2.1 Certification Target

The target of "cloud service certification system" is IaaS/SaaS with the services that had been provided for over six months at the time when cloud service certification was requested among the services of connecting to the internet to use IT resources such as hardware & software by utilizing cloud technology (virtualization, distributed processing, *etc*.) and paying according fee, while excluding conventional web hard drives or video streaming services [4].

2.2 Operation System

The operation system of "cloud service certification system" consists of certification committee, assessment group and executive office.

- Certification committee: deliberates main items related to certification such as certification screening, *etc*.
- Assessment group: assesses services according to assessment criteria as the executive office organizes service assessment group upon receiving certification request
- Executive office: a nonprofit corporation involved in cloud services to efficiently perform certification work

2.3 Screening Criteria

The certification screening criteria consist of seven items (availability, expandability, performance/speed, data management security/service continuity, service support) in three main areas (service quality, service information protection, service infrastructure, and IaaS and SaaS respectively consists of 105 items (required items: 39) and 85 items (required items: 33). Specific assessment items of service information protection are as shown in Table 1, through which items for enhancing the security of cloud service certification system can be deduced by comparing them with the analysis result of security threat factors in cloud environment [6].

- Availability: domain of checking service provider's availability policy and present condition to assess the overall environment in which continuous availability can be provided by checking the provider's basic capability to maintain availability such as availability policy status, availability goal & result notification, organization's operational and system maintenance capability
- Expandability: domain of checking service provider's expandability policy and present condition to assess the overall environment in which continuous expandability can be ensured by checking the provider's basic capability to provide expandability such as expandability policy status, expandability standard, organization's operational and system maintenance capability
- Performance: domain of checking service provider's performance policy and present condition to assess the overall environment in which continuous performance can be maintained by checking the provider's basic capability to maintain performance such as performance policy status, performance goal and quality measurement status, organization's operational and system maintenance capability
- Data management: domain of checking service provider's data management policy and present condition to assess the overall environment in which continuous data management capability can be provided by checking the provider's basic data management capability such as data management policy status, data restoration/disposal notification status, organization's operational and system maintenance capability
- Security: domain of checking service provider's information protection policy and present condition to assess the overall environment in which continuous security maintenance can be provided by checking the provider's basic information protection management capability such as information protection plan status, organization's operational and information protection education
- Service continuity: domain of checking service provider's service continuity capability to assess the overall environment in which continuous service operational capability can be provided by checking the provider's basic service support capability such as service policy status, customer support, service provision method and user education

Table 1. Service Information Protection Certification Screening Item

Item	Check Content	Check Method	Note
Data Management	Data management policy establishment	Check	Required
	Organization & responsibility setting	Check	Required
	Backup system & management	Check	General
	Backup implementation and recovery test	Check	Required
	Data restoration & disposal	Check	Required

Item	Check Content	Check Method	Note
Security	Information protection policy establishment	Check	Required
	Organization & responsibility setting	Check	Required
	Information asset management	Check	General
	Certification and access control	Check	Required
	Information protection education	Check	Required
	Internal/external personnel security	Check	Required
	Physical access control	Check	Required
	System development security	Check	General
	Virtualization security	Check	General
	Security accident management	Check	Required

3. Cloud Service Security Threat Factors Survey

Since cloud service is a type of service where external resources are used for some or all of its resources without owning IT resources, analysis will be conducted extract cloud infrastructure system security threat factors. In regards to the security issues that could occur upon using cloud service, as shown in Table 2, the survey result revealed security & data breach, service stability and availability, interoperability with existing application, service provider's stability, laws & regulations (compliance), service use cost, *etc* [3].

Table 2. Security Threat Factors of Cloud Service

Security Threat	Content of Threat
Virtualization vulnerability inheritance (technical threat factor)	o Threat of malicious code infection and dissemination o Service availability infringement * Technical, physical independence damage, account infringement, data seizure, malicious probing and scanning
Threat of information breach from information outsourcing (operational threat factor)	o Information breach from the separation of ownership and management o Information breach by insider * Action against malicious insider, error and incorrect components, encroachment and loss of important log, loss of backup data, forgery and falsification of network traffic
Information breach from variety of terminals used and loss	o Information breach from loss of terminals
Service error from sharing and localization of	o Service interruption for all customers during system error o Vulnerability of easily becoming a target of DDoS

resources	attack during the exposure of central system
Difficulty of security application from distributed processing	o Increasing in the complexity of certification/access control from resource sharing and virtual machine diagram reassignment o Difficulty in the application of batch certification/access control for distributed computing system
Legal and regulatory issue (policy & legal threat factor)	o Unclear responsibility in the case of information breach o Difficulty in audit trail from resource sharing * Governance violation, compliance violation, jurisdictional issues, license issues

4. Security Threat Factors Analysis in Cloud Environment

Because of the characteristics of cloud computing environment, new security requirements are needed as a result of installation and management environment, service installation and operation environment and applicable laws and regulations different from that of current information system. Security threats expected as a result of the cloud computing environment characteristics are as follow [1][5].

4.1 External Attack on Cloud Computing

According to the characteristics of cloud computing environment, user data are managed in one location, namely cloud data center, which can lead to the high possibility of such cloud computing environment becoming a target of hackers. Concentrating data in one location of cloud service center can reduce the scope of protection but the level of damage from a successful attack can become serious. Targeting cloud data center, distributed service denial attack, unauthorized access, attack disguised as rightful cloud user can be expected.

4.2 Attack on Virtualization Technological Vulnerability

Core technologies of cloud computing are virtualization, high volume distributed processing, operation and information protection technology. As for the virtualization technology in particular, various vulnerabilities are being presented, along with attacks taking advantage of such vulnerabilities. When cloud computing become vitalized in the future, attacks taking advantage of the vulnerability of virtualization technology are expected to increase significantly.

4.3 Attack Taking Advantage of Cloud Environment

Taking advantage of the characteristics of cloud computing that can be easily used at low fee, there is a possibility that attacks that have not been attempted thus far due to a significant amount of budget required for attack will be attempted. Namely, there is a possibility that cloud computing environment will be misused as an attack tool. Cyber-attacks such as DDoS might be attempted on a third party by taking advantage of enormous resources of cloud (computing & storage). Another expected scenarios is the attack on other systems than cloud by installing malicious code in rightful cloud user's environment by hackers.

4.4 Threat from Cloud Internal Attack

In cloud computing center, various levels of user data and services are being used. Because of such cloud computing environment, there is a higher possibility of information leakage resulting from insider compared to the case of existing IDC or server management center. Particularly, leakage of important data and personal information is expected and there is a possible of cloud users not being able to use service due to service interruption resulting from data center blackout, software/hardware incompatibility.

4.5 Threat against Network

In terms of security threats against the network between cloud servicer user and cloud service provider, and the network between cloud service providers, wiretapping, alteration and destruction of various data are expected. Although such threats are general threats, they are more exposed to attack threats in the aspect of using cloud service through external network regarding cloud computing environment or transmitting data. In addition, it is expected that illegal access through network will occur frequently and unauthorized access or attack disguised as user is also expected.

4.6 Compliance Threat, *etc*.

Because of multi-tenant environment, one of the main characteristics of cloud computing environment, various user services and data are being stored and operated in the cloud computing center server. During the process of security audit of a particular user, there is a threat of information on other user's data within the same cloud computing environment leaking. It results from a situation of not being able to only provide data of particular users within the same cloud computing environment and it could become a significant threat against cloud computing in the future. It is particularly difficult to find out from outside security compliance level through particular security rules or security management system, which can pose a security threat form physical and managerial standpoint.

5. Development of Cloud Service Security Evaluation Items

In this section, specific assessment items and necessary technologies will be deduced for security diagnosis and check based on the analysis result of security threat factors in cloud environment to develop cloud service security assessment items. Namely, it will analyze to find out which items and indexes will be applicable for specific assessment items for the virtualization security vulnerability checking and monitoring of cloud service infrastructure system. As for the cloud service security assessment items, 19 items of requirements in three areas, as shown in Table 3, were deduced among items applicable for diagnostic and checking purpose regarding technical security measures to allow diagnosis and monitoring by cloud service provider and users [4].

Table 3. Requirements of Cloud Service Security Evaluation Item

Requirement	Content	Check Method	Importance Level
Software Warranty	Verification of forgery/falsification of OS and major software	Agent	High
	Update of security vulnerability patch	Agent	High
	Periodic checking of vulnerabilities	Check	High

Requirement	Content	Check Method	Importance Level
	Installed software management	Agent	Medium
	Checking of web vulnerabilities	Agent	High
Host & VM Security	Application of encryption of VM provided to client	Check	High
	Status of provision of VM applied with patch	Agent	High
	Periodic patch management of VM provided to client	Agent	High
	Status of VM usage of client	Check	Medium
	Provision of VM vulnerability check tool or check items	Check	High
	Security of data sharing between VM and non-VM	Check	Medium
	Provision of network security between VMs of same client	Check	Medium
	Provision of independence from other client's VM	Check	High
	Malicious code detection and blocking function	Agent	High
	System log backup & management function	Agent	High
Network Security	Test & checking of infiltration from outside	Check	High
	Test & checking of infiltration from inside CSP	Check	Medium
	Tracking and management of vulnerabilities	Check	High
	Notification of vulnerabilities to client	Check	High

6. Improvement Framework of Korean Certification System for Cloud Service Focus on Security

In the case of current cloud service certification system, companies assess their internal/external security policies and related technical security measures regarding their security management system, and they need institutional and systematic supplementations to diagnose and assess security management items by applying security diagnostic tools [2].

For the purpose of applying cloud service certification system, it is necessary to ensure stability and reliability of tool by providing security diagnostic tools to allow cloud service providers to diagnose and check their cloud service security level [4][7].

After ensuring the stability and reliability of virtualization security diagnostic tools, it would be necessary to improve and advance in steps current security items of cloud service certification system by checking and diagnosing vulnerabilities in

cloud virtualization environment. The Fig. 2 shows the improvement of assessment method to enhance the security of cloud service certification system.

Additionally, it would be necessary to increase the usability of multi-virtualization security diagnostic tools through additional comparative analysis of the assessment items and methods of the cloud service stability verification system currently being implemented to introduce cloud service in public sectors lead by Ministry of Science, ICT and Future Planning.

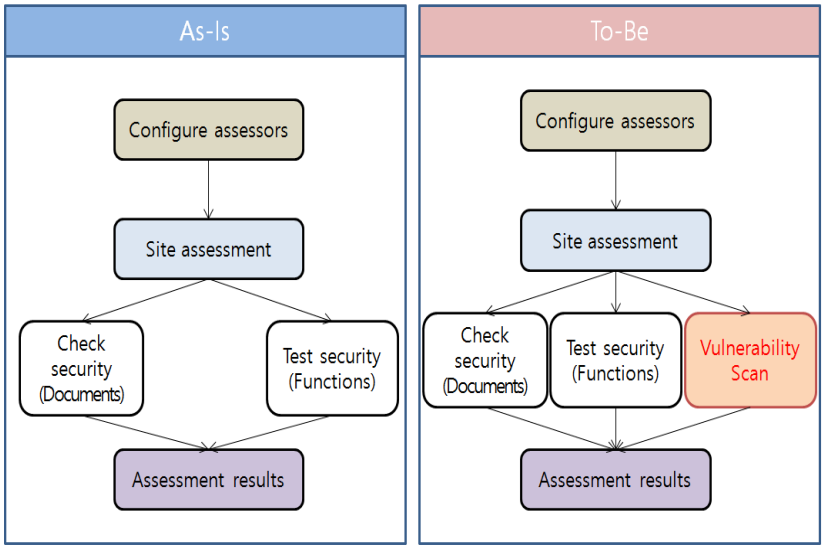

Figure 2. Improvement Framework of Korean Certification System

7. Conclusion

Along with business interest in cloud computing, the interest in the security and legal application of cloud computing is also increasing. For the purpose of enhancing the level of trust of cloud service users and expand the cloud service market, this study examined the Korean cloud service certification system and security stability items and analyzed security threat factors that could occur in cloud environment to develop diagnosis, checking and monitoring items against possible threats in virtualization environment. Based on this, it presented a security enhancement plan by improving the current assessment method of cloud service certification system.

Based on follow-up studies on cloud service security assessment method, it is expected that the security of cloud service certification can be enhanced. It would be also necessary to continuously examine the requirements of security assessment items required as a result of cloud computing technological advancement to develop tools that will allow effective diagnosis, checking and monitoring to incorporate them into the Korean cloud service certification system, which will contribute to the effort of forming a safe cloud service environment.

References

[1] S. J. Jung and Y. M. Bea, “Trend analysis of Treats and Technologies for Cloud Security”, Journal of Security Engineering., vol. 10, no. 2, **(2013)**, pp. 199-212.
[2] K. C. Kim, O. Heo and S. J. Kim, “ A Security Evaluation Criteria for Korea Cloud Computing Service” Journal of Security Engineering, vol. 23, no. 2, **(2013),** pp. 251-265.
[3] K. S. Kou, “A Study on Security-Enhanced Cloud Service Evaluation and Certification Scheme”, Journal of Security Engineering”, vol. 9, no. 6, **(2012)**, pp. 481-494.

[4] H. G. Jeon,Y. G. Min and K. K. Seo, "A Framework of Cloud Service Quality Evaluation System : Focusing on Security Quality Evaluation", International Journal of Software Engineering and Its Applications, vol. 8, no. 2, **(2014)**, pp. 41-46.
[5] J. K. Choi and B. N. No, "Security Technology Research in Cloud Computing Environment", Journal of Security Engineering, vol. 8, no. 3, **(2011)**, pp. 371-384.
[6] H. G. Jeon and K. K. Seo, "A Framework and Improvements of the Korea Cloud Services Certification System", The Scientific World Journal, vol. 2015, Article ID 918075.
[7] K. S. Kou, H. J. Lee, J. I. Shin and C. H. Ryu, " Development of CssT(Cloud Service Security Self-Testing System) for Cloud Service Providers", Journal of Security Engineering, vol. 10, no. 6, **(2013)**, pp. 621-630.
[8] www.kcloud.or.kr

Authors

Hangoo Jeon, He received his B.S in Industrial Information System Engineering at Sangmyung University, Korea, in 2007. He currently is a Ph.D. student in Management Engineering at Sangmyung University, Korea. His recent research interests are in cloud computing, convergence business model, Cloud Service, robot and so on.

Young-Gi Min, He received his master's degree in Business Administration at University of Seoul Graduate School, Korea, in 2009. He currently is a Ph.D. student in Convergence at Sangmyung Unversity, Korea. His recent research interests are in cloud computing, convergence business model, IoT and so on.

Kwang-Kyu Seo, He is a professor of Management Engineering at Sangmyung University. Prof. Seo received his Ph.D. degree in industrial engineering from Korea University. His recent research interests are in cloud computing, management information system, convergence business model and so on.