International Journal of Digital Contents and Applications for Smart Devices
Vol.7, No.1 (2020), pp.1-8
http://dx.doi.org/10.21742/ijdcasd.2020.7.1.01

Prioritizing Cloud Service Threats for Succession to Information Security Management System

Hyun Chul Jung[1] and Kwang-Kyu Seo[2*]

[1] Ph.D Student, Dept. of Management Engineering, Graduate School, Sangmyung Univ., 03016, Seoul, Korea
[2]Professor, Dept. Management Engineering, Sangmyung Univ., Cheonan, Chungnam, 31066, Korea
[1]mujukjay@gmail.com, [2]kwangkyu@smu.ac.kr*

Abstract

With the growth of the cloud computing industry, there is also an increased risk that cloud service providers are stably providing services. Cloud service providers need to identify these threats and be proactive. Because cloud service is a service that requires a high availability rate of at least 99.9%. Therefore, this study presents a framework for collecting and prioritizing potential threats that could compromise the service of a cloud service provider. In addition, a case study was conducted to verify the proposed framework. This framework can be used only when the cloud service provider has a risk management procedure, and has a limitation in that the subjective characteristics of the cloud service provider may be included in the use of the framework. Nevertheless, it can be used in establishing a proactive threat management plan for cloud service delivery and researching cloud security management methodology.

Keywords: *Cloud computing, Security, Cloud service, Job importance, Risk management, Service continuity, Threat evaluation, Threat priority*

1. Introduction

We are living in the era of the 4th Industrial Revolution. The cloud computing industry is growing from the 4th Industrial Revolution to the core that enables convergence between industries. However, as the cloud computing industry grows, security issues of cloud computing services are also continuously raised. It is evolving into a new type of attack technology that is difficult to respond by exploiting the weaknesses of cloud computing. Cloud service providers are obligated to provide reliable services despite these new risks [1]. Therefore, it is necessary to not only identify new threats, but also to grasp the job and connection for cloud service provision and to select which risk to respond first.

In this study, we propose a framework to measure priorities by evaluating threats that can impede service provision so that cloud service providers can provide stable services, and verify the results through case studies.

2. The beginning

Article history:
Received (March 25, 2020), Review Result (April 29, 2020), Accepted (June 3, 2020)

Print ISSN: 2205-8532, eISSN: 2207-4058 IJDCASD

2.1. Motivation

How can cloud service providers overcome the potential threat of emerging cloud computing and provide reliable services? The potential threats are new. Therefore, it is difficult to cope with the management system that cloud service providers already operate. In other words, it is necessary to present a framework that can collect the newly created threats of cloud computing and measure the priority that can act as a real risk in cloud service management tasks and relationships.

2.2. Overview of this study

The framework proposed in this study follows the following procedure. Firstly, in order to prioritize and select potential threats that can impede cloud services, potential threats are first collected and classified. To evaluate the association between the collected threats and the job for providing cloud services, define the job and evaluate the importance of the job. Finally, prioritize the threats that need to be responded to by evaluating the relationship between potential threats and jobs.

The framework proposed in this study will be substituted into the cloud service provider environment for verification.

3. Framework to evaluate threats in cloud service

3.1. Literature review

In the 2019 report released by CSA, “Top Threat to Cloud Computing: Egregious Eleven,” [2], Emphasizing the necessity of preparing for threats in new cloud environments rather than serious threats in cloud computing environments and threats from existing vulnerabilities.

In the 2013 study “Study on cloud computing security vulnerabilities” [3], suggested how to classify and respond to vulnerabilities in classification models for analysis and management of threats of cloud computing, and defined management models through experiments and case study.

In the 2012 study “Information Security Management System for Cloud Computing Service” [4], The potential threats of cloud computing services were classified into origin and derivative, and classified into large, medium, and small classes to define the control area for cloud service security management.

And in the “Cloud security guide” announced by EQST group of SK InfoSec, a security company [5], Defined to include potential threats, importance, response versions, and timing of application recommendations in cloud computing environments using containers.

3.2. Difference

The cloud service can take various forms through convergence with the service model provided by the service and other services, and the job is varied accordingly. Previous studies have focused on “What threats and vulnerabilities exist and how to prepare for them”, however, in this paper, we will study “What threats can pose a real danger to cloud service providers and what are the priorities of the threats to be proactively prepared for?”

3.3. Methodology

In this study, the framework to be presented consists of the following procedures [Figure 1].

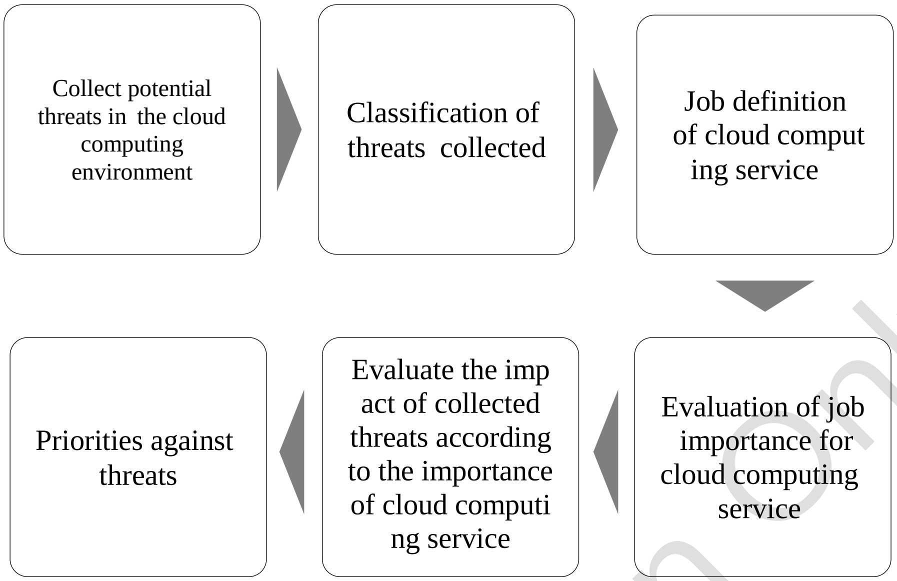
Collect potential threats in the cloud computing environment
Classification of threats collected
Job definition of cloud comput ing service
Evaluation of job importance for cloud computing service
Evaluate the imp act of collected threats according to the importance of cloud computi ng service
Priorities against threats

Figure 1. The procedure of this study

3.3.1. Collecting

The methods of collecting potential threats in the cloud environment are divided into “external data collection” and “internal data collection”. External data collection is collected through the latest reports published by trusted organizations, or through academic data and papers. Use the collected data by identifying the source. Internal data collection can be done through vulnerability inspection results, or through past problem occurrence or action history. When using the collected internal data, specify the data collection environment.

3.3.2. Classifying

Threats collected from external organizations, papers, etc. are referred to as trend factors, internal vulnerability checks, threats collected from past history are attributed, and common factors are classified from trend factors and attribution factors. Each trend, attribution, and common factors are subdivided into external, internal, and environmental factors depending on where threats act on cloud service management and operation. External factors include invasion of attacks from outside. Defects are examples of environmental factors. Examples of internal factors are insider intentions, negligence, and abuse.

3.3.3. Job definition

It defines by enumerating the jobs required to provide cloud services. It includes not only direct jobs but also indirect jobs such as sales and finance in providing services such as operation and development of cloud services.

3.3.4. Job importance

Job importance refers to the importance for providers to stably provide cloud services. The job importance calculation is performed when the defined job is stopped, the degree of damage that is imparted by the service provider, and the degree of urgency that the job should be restored urgently.

3.3.5. Evaluation

"Evaluation" is a step to quantify how much of the collected potential threats can affect a cloud provider's job. We calculate with below formula.

$$\mathit{Formula} = (\mathit{Job\ Importance\ x\ threat\ Importance})\ x\ \mathit{Job\ Weight} \qquad (1)$$

Job importance is a measure of how important the job is to cloud service management, and is calculated as a relative value for each job as a product of business evaluation items. Threat importance identifies business continuity risks and evaluates them as high, medium, and low according to three factors: financial impact (CAP), non-financial impact (N-CAP), and recovery requirements (R-R). Job Weigh is determined based on the value of the assessed job through relative assessment with other jobs.

3.3.6. Priorities

According to the calculation result, the priority of potential threats is arranged in the order of highest score.

3.4. Results

Case study was conducted with the environment of the IaaS provider.

3.4.1. Collecting

The following data were collected from the following for external data: CSA's report in 2019, "Top Threat to Cloud Computing: Egregious Eleven" [2], Korea Internet & Security Agency's "Detailed Guide to Analyzing Technical Vulnerability Infrastructure Technical Vulnerability" [6], Cyber Research Group's "Cyber threat Defense Report" in 2019 [7], and for internal data: Physical threats to the IaaS cloud service environment, Inspection for Common Configuration Enumeration (CCE). Inspection for Common Vulnerabilities Exposures (CVE), Inspection for Common Weakness Enumeration (CWE)

3.4.2. Classifying

Classification based on the method defined by the methodology of framework by referring to the collected threats

3.4.3. Job definition

IaaS provider's service management Jobs are defined / as the following five [Table 1].

Table 1. IaaS provider's Job definition

Job title	Identifier	description
Infrastructure management	C-INF	Facility and equipment management, import and export control, virtual infrastructure management

Technical operation	C-SYS	Architecture, security, access control, operations management
Development	C-DEV	Platform and function development, database and configuration management
Sales and consulting	C-SAL	Service attraction, contract management
Administration support	C-ADM	Administration, HR, accounting and secretary

3.4.4. Job importance

The job defined as suggested in the framework is summed up by measures of financial, non-financial, and recovery urgency due to suspension, and then a “job score” and “Job value grade” is obtained. Then multiply the values of “job score” and “Job value grade” to get the “value score” of the job.

3.4.5. Evaluation

When job importance is determined, the collected threats are assigned to the job and evaluated [Table 2].

Table 2. Treats evaluation against relating job

Ra	Threat	THV	TCL		REJ	TPE	JOI
			CME	OLO			
1	Threat 1	48.6	Trend	External	C-SYS	Service	27
2	Threat 3	14.4	Trend	External	C-INF	Service	8
2	Threat 4	14.4	Trend	External	C-DEV	Job	8

Ra = Rank, THV = Threat evaluation, TCL = Threat classification, CME = Collection method, OLO = Occurring location, REJ = Related job, TPE = Threatening permanence effect, JOI = Job importance

3.4.6. Priorities

The order of the threats with the highest evaluation scores is listed in order of priorities. The table lists only the top priorities [Table 3].

Table 3. Threats with the highest evaluation scores

Priority	Threat factors	TEP	TCL		REJ	TPE	JOI
			WOC	OLO			
1	Data Breaches	48.6	COM	EXT	C-SYS	SER	27
	Lack of security architecture and strategy	48.6	COM	ENV	C-SYS	JOB	27
	Insufficient identity, credential, access and key management	48.6	COM	ENV	C-SYS	SER	27

	Insider threat	48.6	COM	INT	C-SYS	SER	27
	Abuse and nefarious use	48.6	COM	INT	C-SYS	SER	27
	Weak control plane	48.6	COM	ENV	C-SYS	SER	27
	Account hijacking	48.6	COM	EXT	C-SYS	JOB	27

TEP = Threat Evaluation Point, WOC = Way of collection, OLO = Occurring location, COM = Common, EXT = External, SER = Service, ENV = Environment, INT = Internal, BEL = Belonging

3.5. Discussion

In this study, we proposed a framework that collects potential threats in a new cloud computing environment and derives the priority of threats that need to be proactive in response to related service management tasks. The results of case study conducted to verify the suggested framework are interesting. The fact that the collection classification of threats ranked in the first priorities are common factors those are the intersection of external and internal threats In general, threats are easy to be mistaken for the influence of external influences on the internal environment, but it can be seen that environmental factors and internal factors are included in addition to external factors. Finally, it is confirmed that the system management job of the IaaS provider is most affected by the potential threat of cloud computing, and the impact is related to the continuity management of services and operations.

4. Conclusion

With the growth of the cloud industry, new risks are emerging that threaten the cloud service environment. Cloud service providers need to identify these threats and prepare for them proactively in order to provide stable services. Therefore, this study presents a framework that prioritizes threats that cloud service providers need to prepare in advance through collecting and classifying threats that may pose a potential risk to the service environment and evaluating them through operations that provide cloud services. And conducted a case study to verify this framework.

The cloud service provider’s subjectivity can be reflected in the threat collection, classification and task assessment. In order to identify and proactively prepare for the identified threats and the evaluated priorities, the cloud service provider must have internal risk management regulations and decision-making procedures.

Priorities derived through the framework of this study should be able to be continuously managed by succeeding to an information security management system with life cycles of “PLAN”, “DO”, “CHECK” and “ACT” [8]. Furthermore, research and development of a cloud security management methodology that can stably operate cloud services from constantly occurring cloud threats is required.

References

[1] Sungpil Jo, “A study on threats and countermeasures of information security in the era of the 4th Industrial Revolution,” Security Research, pp.9-35, **(2017)**

[2] https://cloudsecurityalliance.org/press-releases/, Aug 9 **(2019)**

[3] Jeong-hoon Jeon, “A study on the vulnerability of the Cloud computing security,” Journal of The Korea Institute of Information Security and Cryptology, vol.23, no.6, vol.23, no.6, pp.1239-1246, **(2013)**

[4] Kyoung-a Shin and Sang-Jin Lee, “Information security management system on cloud computing service,” Journal of The Korea Institute of Information Security and Cryptology, vol.22, no.1, pp.155-167, **(2012)**

[5] http://www.skinfosec.com/newsRoom/eqstInsight/eqstInsightList.do, Jun 21 **(2019)**
[6] https://www.kisa.or.kr/public/laws/laws3.jsp, Dec, **(2017)**
[7] https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf, Mar, **(2019)**
[8] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, **(2013)**

Authors

Hyun Cchul, Jung
Ph.D Student, 03016 Dept. of Management Engineering, Graduate School, Sangmyung Univ., Seoul, Korea
Director, Korea Server Hosting Inc., Seoul, Korea

Kwang-kyu, Seo
Professor, 31066 Dept. Management Engineering, Sangmyung Univ., Cheonan, Chungnam, Korea

This page is empty by intention.