**ISSN** 1816-6075 (Print), 1818-0523 (Online)
**Journal of System and Management Sciences**
Vol. 10 (2020) No. 4, pp. 45-61
DOI:10.33168/JSMS.2020.0404

# Jobs and Potential Threat Assessment for Continuous Provision of Cloud Computing Services

Hyun-Chul Jung and Kwang-Kyu Seo*
Department of Management Engineering, Graduate School, Sangmyung University, Korea
*mujukjay@gmail.com, kwangkyu@smu.ac.kr (Corresponding author)*

**Abstract.** Cloud service threats are on the increase as the cloud computing (CC) industry grows with the fourth industrial revolution, cloud service threats continue to rise. Job permanence for CC services must be ensured to guarantee service provider's continuous provision obligated by service level agreements. Hence, cloud service providers (CSPs) should collect, classify threats that could potentially affect services to understand the impacts on cloud-related jobs and provide countermeasures. In this study, we presented methods and procedures for collecting and evaluating potential threats that may inhibit the job permanence of CSPs. In addition, we selected one CC service model and examined it via a case analysis. We expect this study to affect evaluation results when a CSP has an information security management system and a risk response system. However, as there are several CC service models and providers, it is difficult to apply the proposed methods and procedures on a consistent standard for all CSPs. Nevertheless, they can be employed to develop management plans against threats that influence CC service permanence and to study cloud security management methodology.

**Keywords:** Cloud computing, cloud computing industry, cloud computing threats, cloud computing service, cloud computing service continuity, job importance, threat evaluation, threat response system.

## 1. Introduction

Cloud computing (CC) is leading to the fourth industrial revolution as a convergence medium between technologies and between industries. However, security issues the threaten cloud computing service (CCS) are on the increases as CC technologies are combined and utilized in various forms. These security threats are emerging in several areas, such as traditional application vulnerabilities, structural problems in CC and possible loopholes in cloud service operations. Cloud service providers (CSPs) are obliged to continue providing services under the service level agreement (Sungpil, 2017). In other words, it is necessary to identify and respond to threats that may inhibit the provision of stable services.

Potential threats that could affect cloud services continue to emerge. However, CSPs cannot analyze and respond to all threats. Hence, this study can be used appropriately by CSPs to actively handle potential threats. In this study, we propose methods and procedures to assess the effects of potential threats on CSPs' primary tasks for continuous services provision and how much these effects inhibit the services. By doing so, recognition of factors that threaten CCS and preparation of response plans against threats for stable service provision is possible. Fig. 1 illustrates an overview of this study.

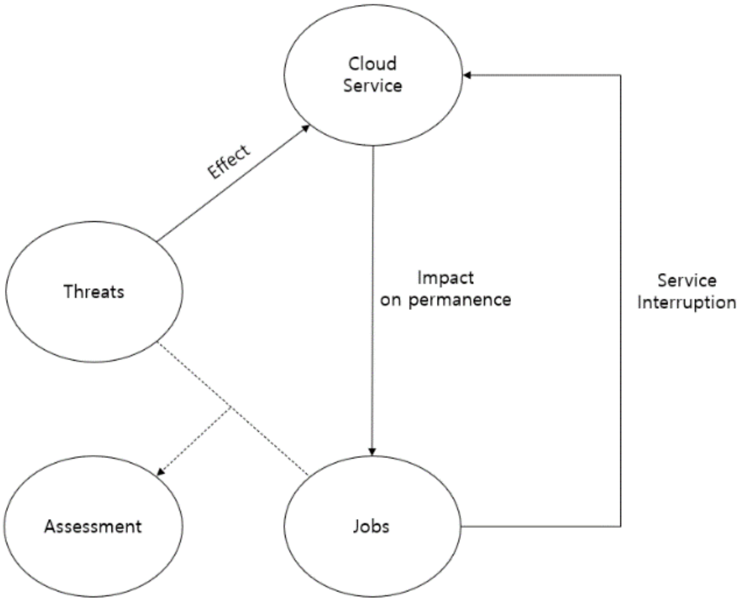

Fig. 1: Overview of this study.

This paper consists of four chapters. Chapter 1 describes the background and purpose of this study; Chapter 2 describes literature review and the differences between this study and previous studies; Chapter 3 deals with assessment methods and procedures based on threat definition. CSP's job analysis and definition are also presented. Finally, Chapter 4 summarizes the study results and draws conclusions, also it presents future works.

## 2. Literature Review

There are some studies dealt with IT job analysis and potential threats and risks assessment of security in IT industry including CC and so on.

Chang *et al.* predicted potential threats of a particular target by using machine learning; they described methods to predict possible threats via machine-learning the definition and classification of threats (Chang and Lee, 2020).

Jung and Seo discussed succession to an information security system through prioritizing threats; they included internal procedures for collecting and prioritizing risks that could be potential threats (Jung and Seo, 2020).

Jing and Lim presented the effect of management service quality of high-rise apartments on relative situations; their study include an impact analysis of the effects of one factor on another on the occurrence of new results (Jing and Lim, 2020).

Kim’s study on job and creativity, “An Analysis of Convergence Core Competency Affecting Team Creativity of Industrial Workers” measured how job performance changes due to factors that affect it ( Kim, 2020).

Park and Seo analyzed the optimal cloud platform based software marketing strategy for domestic and global cloud market changes (Park, 2020).

A 2019 report, "High Threats to Cloud Computing: Egregious Eleven", published by Cloud Security Alliance (CSA) analyzed serious threats posed CC environments. The report listed new threats that may arise in a CC environment with a severity degree, including threats from internal flaws in the cloud service environment, as well as threats from abuse and misuse by internal management personnel.

A guideline published by SK InfoSec’s security company EQST Group, “Cloud Security Guide", listed potential threats in the CC environment using containers and presented the importance, response plans, and recommended application timing of threat response .

Yang and Jang (2018) presented criteria and methods for categorizing factors while explaining machine running methods and time series models.

Yang and Yang (2018) described changes in the role of psychological capital related to job performance, emotional exhaustion, etc.; they also emphasized the need to analyze job performance influence according to changes in external threats.

Jeon (2013) proposed a model that can analyze and classify CC threats and derived a management model that can respond to vulnerabilities through experiments and case studies.

Shin and Lee (2012) defined the control area of cloud service security management by separating factors of potential threats from CCS into "ORIGIN" and "DERIVATIVE" factors; they classified these threat factors into large, medium and small.

CCS can be provided in a variety of service models through convergence with various technologies and industries. While previous studies focused on identifying potential threats and preparing threat responses, this study explores evaluation methods and procedures of how many potential threats can become real threats based on the CSP's jobs.

# 3. Assessment Methods and Procedures Based on Threat Definitions and Jobs

In this chapter, we review existing works related to the analysis and management of CC threats. In addition, we present the differences between this study and previous studies, and describe the detailed procedures for the research methodology of this study. Further, we applied the presented methods and procedures to a particular CSP environment to review the verified results.

## 3.1. Procedure and Methodology

In this section, we present procedures for assessing the impact of potential threats on CSPs based on their job. We also present the criteria and methods for detailed implementation.

A. PROCEDURE OF THIS STUDY

We conducted this study in three phases, as shown in Fig. 2. First, we defined threat factors through grouping by collecting threats and analyzing common elements of those threats. Second, we defined CSP's jobs and then calculated the importance of the jobs to the permanence of the cloud service. Third, we assessed how many threats influence CSP's job performance using to an equation that considers threat factors and job importance.

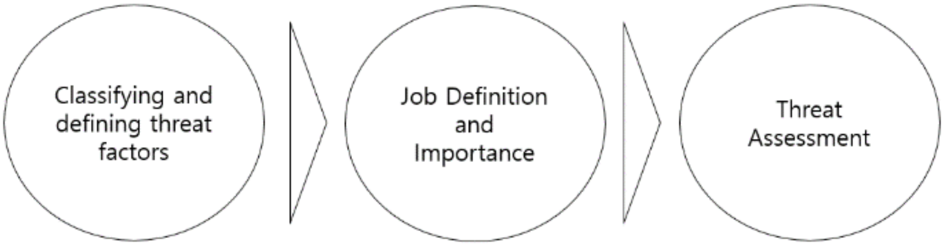
Classifying and defining threat factors
Job Definition and Importance
Threat Assessment

Fig. 2: Procedure for assessment of threats based on threat factors and job definitions.

We verified the methods and procedures proposed in this study by sampling cloud service provider and service models.

B. METHODOLOGY OF THIS STUDY

Each phase includes criteria and methods for collecting threats, classification of threat factors, job definition, job importance assessment, and threat impact assessment.

### 3.1.1. Classifying and Defining of Treat Factors:

We can define the methods for gathering a list of potential threats to assess the impact of CCS based on CCP's job as follows. First, we can collect external data from the latest reports, academic materials and papers published by trusted authorities; this is defined as external data collection. Second, we can collect internal data from past service history and results of cloud system/application vulnerability test; this is defined as internal data collection.

We classified list of threats collected from external and internal data as trend, attributed, and common threats. Trend threats are threats collected from external data, attributed threats are threats collected from internal data, and common threats are threats commonly identified in both trend and attributed threats.

We can subdivide trend, attributed, and common threats into external, internal, and environmental threats depending on where they function in a cloud service environment, as illustrated in Fig. 3. Examples of external threats include intrusions of external attackers into CC service environments or service applications, and examples of internal threats include internal negligence and abuse by CCS operators, developers, and managers. Examples of environmental threats include flaws inherent in CC systems or service applications.

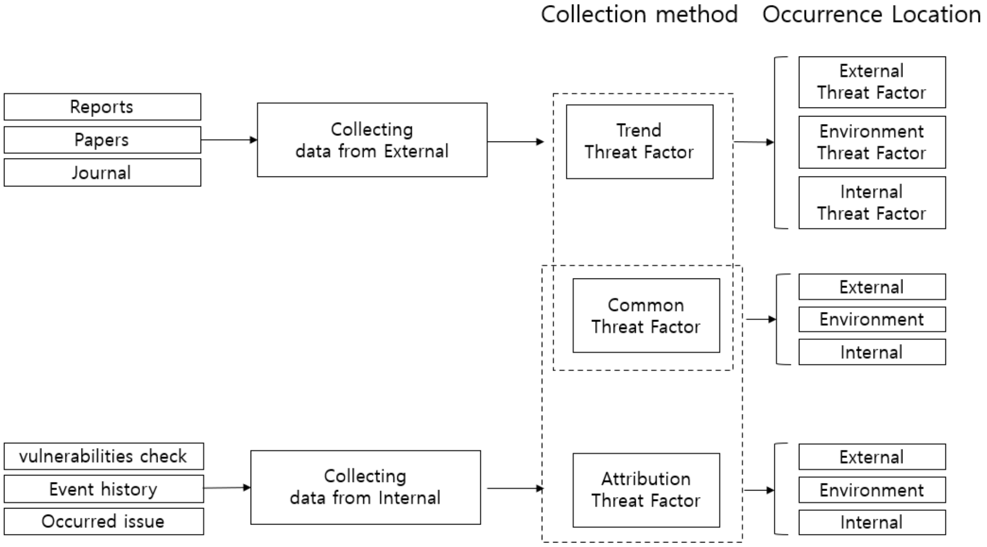

Fig. 3: Defining threat classification criteria.

Classifying threat factors is to easily recognize where threats occurred, whether they occurred in the past, and threat categories when the CSP prepares a counterplan based on evaluation results.

### 3.1.2. Job Definition and Importance:

Definition of jobs required to provide CCS is governed by the “IT sectoral qualification framework (ITSQF)" (Kim, 2019) of Korea Software Industry Alliance (KOSA), a tool that establishes and recognizes the competency criteria of technicians in the IT industry by linking qualifications, field experience, vocational training completion results, and degrees. Table 1 lists job definition according to ITSQF.

Table 1: Definition of ITSQF

| NO | JOB | ALIAS | DEFINITION |
|---|---|---|---|
| 1 | Information Technology Planning | IT Planner | A person who plans IT strategies to achieve the organization's management goals and establishes strategies for each area such as governance, investment, performance analysis, operational policy, R&D, process, architecture, etc. |
| 2 | Information Technology Consulting | IT Consultant | A person who understands the organizational management environment from an objective point of view and analyzes the target business and information system to help achieve the organization's objectives |
| 3 | Information Protection Consulting | Information Protection Consultant | A person who verifies and advises the objective fulfillment of security requirements and pre-defined processes in administrative, physical, and technical domains to protect key information assets |
| 4 | Business Analysis | Business Analyst | A person who draws and analyzes business requirements based on the organization's vision and understanding of goals, structures, and policies to establish a response strategy that meets the objectives |
| 5 | Data Analysis | Data Analyst | A person who performs data analysis planning, data analysis, and data visualization based on basic knowledge of data understanding and processing technology and supports scientific decision-making such as process innovation and marketing strategy decision |
| 6 | IT Project Management | IT PM | A person who plans and integrates the project to comply with the delivery date of IT projects |

| | | | |
|---|---|---|---|
| 7 | IT Project Business Management | IT PMO | A person who provides indicators, project management guidelines and standardization measures to enable clear decision-making and direction setting, and supports project execution through management of key issues, risks, resources, schedules, documents, and scope |
| 8 | SW Architecture | SW Architect | A person who guarantees the quality of functions, performance, security, etc. of SW, and analyzes and designs elements and relationships that make up the SW to systematize the overall SW structure |
| 9 | Infrastructure Architecture | Infrastructure Architect | A person who designs and configures infrastructure including hardware, middleware, network, and cloud, and organizes them to provide appropriate and reliable services for all resources |
| 10 | Data Architecture | Data Architect | A person who designs, creates, manages, and organizes data from a structural point of view so that data can be stored, consumed, integrated, and managed by applications that process data and various data entities |
| 11 | UI/UX Development | UI/UX Developer | A person who develops effective UI/UX through the process of prototyping, design, and implementation, and implements user interface planning and architecture by analyzing the user's usage form and technical environment |
| 12 | Application SW development | Application SW Developer | A person who develops and improves the functions of the product through analysis, design, implementation, testing, and distribution of application software in a computer programming language |
| 13 | System SW Development | System SW Developer | A person who performs analysis, design, implementation, and distribution of system platform requirements for the operation of software and application programs that control and manage system resources in the operating system environment |
| 14 | Embedded SW | Embedded SW | A person who develops software such as porting of operating systems for each platform, firmware, |

| | | | |
|---|---|---|---|
| | Development | Developer | device drivers and applications, and performs hardware platform optimization based on understanding of the hardware platform |
| 15 | Database Management | Database Operator | A person who designs, builds, and converts a database from requirements for data and performs tasks such as modifying, improving, and backing up the database through trend analysis to ensure optimal performance and quality |
| 16 | NW Engineering | NW Engineer | A person who analyzes the network environment and designs and configures topology, resource management, and quality management for the network |
| 17 | IT System Management | IT System Operator | A person who is in charge of stable computing infrastructure and information system operation by analyzing system requirements and establishing, operating, and managing HW and SW service platforms for cloud and virtualization, system and network, and storage resources |
| 18 | IT system technical support | IT system technical supporter | A person who supports the composition and failure handling of systems using IT resources such as computer hardware, storage, cloud and virtualization, and network based on the understanding of information technology infrastructure, and supports stable computing infrastructure operation through system improvement and regular inspection |
| 19 | SW product Planning | SW Product Planner | A person who establishes a product strategy by analyzing the company's internal/external environment, required technology, and marketability in the SW application field based on the company's management strategy, and develops and supports SW product development, support, sales, and marketing plans |
| 20 | IT Service Planning | IT Service Planner | A person who discovers IT services that meet customer and market needs through information technology environment analysis, and plans new services through product and solution convergence |

| | | | |
|---|---|---|---|
| 21 | IT Technology Sales | IT Technology Salesman | A person who performs IT sales such as negotiation, contract, sales, and post-management by establishing customer management and sales strategies based on knowledge of information technology, creating business opportunities, and suggesting solutions that meet the requirements |
| 22 | IT Quality Management | IT Quality Manager | A person who establishes an enterprise-wide quality policy and management system to achieve IT quality goals, conducts training and management activities to improve quality, and performs quality assurance activities at the project level |
| 23 | IT Test | IT Tester | A person who performs and manages planning, diagnosis consulting, planning, environment construction, execution, defect management, and documentation necessary to effectively perform tests |
| 24 | IT Supervision | IT Supervisor | A person independent from the interests of the supervisor and the supervisory authority who comprehensively checks information on the planning, construction, and operation of the information system from a third party's point of view to improve the efficiency and safety of the information system, and checks corrective actions to handle problems |
| 25 | IT Audit | IT Auditor | A person who performs tasks comprehensively by checking, evaluating, advising and recommending relevant people on a given system audit basis from an independent perspective to ensure the validity, efficiency, reliability and stability of the computer system |
| 26 | Information Protection Management | Information Protection Manager | A person who establishes the security policies necessary to stably operate information assets to perform the organization's vision and mission, complies with relevant legal systems, performs protection management activities, and draws and manages information protection measures based on risk management |
| 27 | Security Incident | Security Incident | A person who responds promptly by detecting threat information to prevent the spread of |

| | | | |
|---|---|---|---|
| | Response | Response Expert | infringement accidents, establishing a system recovery and prevention strategy, and obtaining and analyzing evidence that has affected business and services |
| 28 | IT Technology Education | IT Technology Educator | A person who performs performance improvement through establishing the direction of IT technology education, creating the environment for IT technology education, subject development and data development, and IT technology education performance evaluation to systematically and effectively carry out technical education in the IT field |

Job importance refers to the relative importance of jobs that CSPs provide to manage their service. Job importance quantitatively calculates the degree of financial damage transferred to CCS and CSPs, the degree of non-monetary damage, and the urgency of job recovery.

The calculation method as follows. First, it assigns each assessment item for a particular task from one point to three points, as summarized in Table 2, and then adds up the points to calculate "Job score". Job score is sorted as "Job value class" as shown in Table 3. We calculate "Job value store" in accordance with "Job value class". We calculate “Job importance” by multiplying "Job score" and "Job value score".

Table 2: Calculation of job score.

| **JOT** | **CAP** | **N-CAP** | **R-R** | **JOS** |
|---|---|---|---|---|
| Job A | 3 | 3 | 3 | 9 |

JOT = Job title, CAP = Capital Damage, N-CAP = Non-capital damage, R-R = Recovery urgency, JOS = Job score

Table 3: Job value class and job value score

| **JOS** | **JVC** | **JVS** |
|---|---|---|
| 8~9 pts | A | 3 |
| 5~7 pts | B | 2 |
| 4 pts or less | C | 1 |

JOS = Job score, JVC = Job vale class, JVS = Job value score

- JOI = JOS x JVS
- JOI = Job importance

### 3.1.3. Threat Assessment:

Threat assessment may also leverage OWASP's "Top 10 Web Application Security Disks", a standard for developer, and web application security. However, the purpose of this study is to assess the impact of potential threats on the CSP’s job. This is why assessment such as quantitative calculation of digital object identifier (DOI) or identification of threat impact should be designed to measure job permanence of CC. Therefore, this study applies JOI evaluation factors for threat evaluation as shown in Table 4.

Table 4: Threat assessment for cloud service continuity

| **THS** | **THI** | | | **TVS** |
|---|---|---|---|---|
| | **CAP.** | **N-CAP.** | **R-R** | |
| Loss of data | H(3) | M(2) | M(2) | 8 |
| Software flaw | L(1) | M(1) | M(2) | 4 |
| Unauthorized access | H(3) | M(2) | H(3) | 8 |
| No security policy | M(2) | M(2) | M(2) | 6 |
| ...... | ...... | ...... | ...... | ...... |

*THS=Threats, THI=Threat impact, TVS=Threat value score*

We derived JOI from multiplying JOS and JVS; we derived TVS, as shown in Table 4. The assessment of this study quantifies how many potential threats of CC can affect the job and service permanence of CSPs. Therefore, we can calculate evaluation scores by multiplying DOI and TVS.

In addition, in calculating the final evaluation score, if a job is biased due to the cloud service model of the CSP, or if there is a disparity in JOI score, we set the job weight as A=60%, B=30%, and C=10% according to JVC, and include it in the calculation.

- ASSESSMENT CALCULATION = JOI x TVS x Job weight
- JOB WEIGHT: A = 60%, B = 30%, C = 10%

## 3.2. Assessment Results

A. PRIORITIES

Threat priority can be listed according to quantitative scores that calculate CC service permanence and performance threat factors.

B. CASE STUDY

To verify threat assessment procedures and methods presented in this study, we conducted a case study by sampling an Infrastructure-as-a-service (IaaS) model among CSPs.

Table 5: Classification of collected threats

| NO | THS | CLF | |
|---|---|---|---|
| | | CME | OCL |
| 1 | Data breach | TRE | EXT |
| 2 | Incorrect configuration and improper change management | COM | ENV |
| 3 | Insufficient cloud security architecture and strategy | COM | INT |
| 4 | Insufficient identity, credential, access, and key management | COM | ENV |
| 5 | Insider threat | COM | INT |
| 6 | Insecure interface and API | COM | ENV |
| 7 | Weak control area | COM | EXT |
| 8 | Apply the latest patches and recommendations | COM | INT |
| 9 | Cloud visibility limitations | COM | ENV |
| 10 | Account hijacking | TRE | EXT |
| 11 | Meta-structure and Apple List Failure | TRE | ENV |
| 12 | Physical disasters such as fire, power outage, flooding, and water leakage | ATT | ENV |
| 13 | Breakdown of computerized equipment | ATT | ENV |
| 14 | Core personnel disease or absence | ATT | INT |

CLF = Classifying, CME = Collection method, OCL = Occurrence location, TRE = Trend, COM = Common, ATT = Attribution, EXT = External, ENV = Environment, INT = Internal

We collected external data was collected from the 2019 CSA report “Top Threat to Cloud Computing: Egregious Eleven” , Korea Internet & Security Agency report “Detailed Guide to Analyzing Technical Vulnerability Infrastructure Technical Vulnerability”, and a 2019 Cyber Research Group report “Cyberthreat Defense Report”. We collected internal data through “Physical threats to the IaaS cloud service environment”, “Inspection for Common Configuration Enumeration”, “Inspection for Common Vulnerabilities Exposures”, and “Inspection for Common Weakness Enumeration”.

We classified threats collected externally and internally as shown in Table 5 according to methods presented in Section 3.3.1.

We classified jobs of the IaaS model CSP into five types that are directly or indirectly related to cloud service delivery, as listed in Table 6. We measured and calculated JOT as quantitative indicators, as in Table 7.

Table 6: Job definition of IaaS provider

| JOT | IDF | DES |
|---|---|---|
| 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 |
| Administratio n support | C-ADM | Administration, HR, accounting, and secretary |

IDF = Identification, DES = Description

Table 7: IaaS provider's job importance

| INF | THI | | | JOS | JVC (JVS) | JOI |
|---|---|---|---|---|---|---|
| | CAP | N-CAP | R-R | | | |
| C-INF | H(3) | M(2) | M(3) | 8 | A(3) | 24 |
| C-SYS | H(3) | H(3) | H(3) | 9 | A(3) | 27 |
| C-DEV | M(2) | M(2) | H(3) | 7 | B(2) | 14 |
| C-SAL | M(2) | M(2) | L(1) | 5 | B(2) | 10 |
| C-ADM | M(2) | L(1) | L(1) | 4 | B(1) | 4 |

We accessed threats classified in Table 5 using the method presented in Table 4. Table 8 shows the TVS results.

Table 8: IaaS Provider's threats value score

| NO | THS | CLF | | TVS |
|---|---|---|---|---|
| | | CME | OCL | |
| 1 | Data breach | TRE | EXT | A(3) |
| 2 | Incorrect configuration and improper change management | COM | ENV | A(3) |
| 3 | Insufficient cloud security architecture and strategy | COM | INT | A(3) |
| 4 | Insufficient identity, credential, access, and key management | COM | ENV | A(3) |
| 5 | Insider threat | COM | INT | A(3) |
| 6 | Insecure interface and API | COM | ENV | A(3) |
| 7 | Weak control area | COM | EXT | A(3) |
| 8 | Apply the latest patches and recommendations | COM | INT | B(2) |
| 9 | Cloud visibility limitations | COM | ENV | A(3) |
| 10 | Account hijacking | TRE | EXT | A(3) |
| 11 | Metastructure and Apple List Failure | TRE | ENV | A(3) |
| 12 | Physical disasters such as fire, power outage, flooding, and water leakage | ATT | ENV | A(3) |
| 13 | Breakdown of computerized equipment | ATT | ENV | B(2) |
| 14 | Core personnel disease or absence | ATT | INT | B(2) |

We measured the extent of the impact of potential threats on CSP's job by multiplying TOI and TVS. We organized the results in the order of priority, as shown in Table 9.

Table 9 shows some threats with the highest evaluation score.

We set job weight as A = 60%, B = 30%, and C = 10%, depending on JVC.

Table 9: Threats assessment with IaaS provider's job

| PRI | THS | TAP | TCL | | INF |
|---|---|---|---|---|---|
| | | | CME | OCL | |
| 1 | Data Breaches | 48.6 | COM | EXT | C-SYS |
| | Lack of security architecture and strategy | 48.6 | COM | ENV | C-SYS |
| | Insufficient identity, credential, access and key management | 48.6 | COM | ENV | C-SYS |
| | Insider threat | 48.6 | COM | INT | C-SYS |
| | Abuse and nefarious use | 48.6 | COM | INT | C-SYS |
| | Weak control plane | 48.6 | COM | ENV | C-SYS |
| | Account hijacking | 48.6 | COM | EXT | C-SYS |

PRI = Priority, TAP = Threat assessment point

### 3.3. Discussion

This study suggests a method to provide stable services against evolving threats for CSPs. To provide and verify methods and procedures for evaluating the effects that threats have on the jobs of CSPs, we conducted job studies of cloud services with IaaS. In general, it is easy to conclude that threats originate from external factors, but both internal and external factors become threats. Finally, the system management tasks of IaaS providers are mostly affected by the potential threats of CC, and the threat impacts are related to the continuity management of services and operations.

## 4. Conclusion

CSPs need to identify the CC threats impacts on the CSP's job performance and provide countermeasures in advance for stable service operation.

This study presented a case analysis to propose methods and procedures for collecting and classifying threats that could become potential risks to the service environment and to assess threats impacts on CC service provision. A list of potential threats to evaluate the impact of the job of CCS was collected. Then, the importance of the job was calculated by considering the degree of financial damage transferred to CCS and CSPs, the degree of non-monetary damage, and the urgency of job recovery quantitatively. The proposed assessment method in this study quantified how many potential threats of CC affected the job and service permanence of CSPs.

Since CCS can have so many forms of service provision and providers, it is difficult to consistently apply methods and procedures suggested in this study to every CC service environment. Hence, the CSP's job subjectivity can be involved, depending on the cloud model. In addition, CSP should have internal risk management regulations and decision-making procedures to prepare proactive responses to assessed threats.

Nevertheless, threats assessed by methods and procedures proposed in this study should be inherited and continuously managed by the system's information security management system. Furthermore, we need steady research and development on the security management methodology of CC to ensure the stable operation of cloud services under the constant security threats.

## References

Chang, Jaesung. Yoon, Jaeyoung. Lee, Gunho. (2020). Machine Learning Techniques in Structural Fire Risk Prediction. *International Journal of Software Engineering and Its Applications*, 14(1), 25-30.

http://www.skinfosec.com/newsRoom/eqstInsight/eqstInsightList.do, 21 Jun 2019.

https://cloudsecurityalliance.org/press-releases/, 9 Aug 2019.

https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf, March 2019.

https://owasp.org/www-project-top-ten/, 2017.

https://www.kisa.or.kr/public/laws/laws3.jsp, Dec 2017.

Jeon, Jeong-hoon. (2013). A study on the vulnerability of the Cloud computing security. *Journal of The Korea Institute of Information Security and Cryptology*, 23(6), 1239-1246.

Jo, Sungpil. (2017). A study on threats and countermeasures of information security in the era of the 4th Industrial Revolution. *Security Research*, 51(51), 9-35.

Jung, Hyun Chul. Seo, Kwang-Kyu. (2020). Prioritizing Cloud Service Threats for Succession to Information Security Management System. *International Journal of Digital Contents and Applications for Smart Devices*, 7(1), 25-31.

Jing, Feng. Lim, Chae-Kwan. (2020). An Empirical Study on the Effect of Management Service Quality of High-rise Apartment on Residential Satisfaction: Focused on High-rise Apartment in China. *International Journal of IT-based Management for Smart Business,* 7(1), 23-29.

Kim, Taehyun. (2019). Job description of capacity system in IT field. *A Guide to ITSQF*, 12-14.

Kim, EunJoo. (2020). An analysis of convergence core competency affecting team creativity of industrial workers. *International Journal of IT-based Management for Smart Business*, 7(1), 31-39.

Park Wonju. Seo,Kwang-Kyu. (2020). Cloud Platform based Software Marketing Strategy Using SWOT and Case Analysis. *International Journal of Software Engineering and Its Applications*, 14(1), 27-32.

Shin, Kyoung-a. Lee, Sang-Jin. (2012). Information security Management System on Cloud Computing Service. *Journal of The Korea Institute of Information Security and Cryptology,* 22(1), 155-167.

Yang, Su Jin. Jang, SeYoon. (2018). Demand Forecasts in Fashion Trends: Applying the Time Series Model and the Deep Learning Method. *International Journal of IT-based Business Strategy and Management*, 4(1), 35-40.

Yang, Woo-Ryeong. Yang, Hoe-Chang. (2018). The Role of Positive Psychological Capital in Relation to Authentic Leadership, Job Performance and Job Burnout. *International Journal of IT-based Business Strategy and Management*, 4(1), 29-34.