A methodology of Assessing Security Risk of Cloud Computing in User Perspective for Security-Service-Level Agreements

Sang-Ho Na
Computer Engineering
Kyung Hee University, Global Campus
Yongin, Korea
shna@khu.ac.kr

Eui-Nam Huh
Computer Engineering
Kyung Hee University, Global Campus
Yongin, Korea
johnhuh@khu.ac.kr

***Abstract*— underlying cloud computing feature, outsourcing of resources, makes the Service Level Agreement (SLA) is a critical factor for Quality of Service (QoS), and many researchers have addressed the question of how a SLA can be evaluated. Lately, security-SLAs have also received much attention with the Security-as-a-Service mode in cloud computing. The quantitative measurement of security metrics is a considerably difficult problem and might be considered the multi-dimensional aspects of security threats and user requirements. To address these issues, we provide a novel a methodology of security risk assessment for security-service-level agreements in the cloud service based on a multi-dimensional approach depending on services type, probabilities of threats, and network environments to reach a security-SLA evaluation.**

Keywords-component:* *Security-SLA; Security Risk Assessment in User Perspective; Personal Cloud Service

I. Introduction

Explosive growth in information systems is shifting to the cloud computing, which has five typical features: multi-tenancy, scalability, elasticity, pay as you go, and self-provisioning of resources. These attributes allow customers to manage their computing capability as needed. In the 1980s, personal computers (PCs) were "hooked up" [1] to a set of devices in order to input and output information, while after the paradigm shift, personal devices, i.e., mobile devices are "hooked up" [1] via a personal cloud that is registered with and has permission to use a network, e.g., the Internet. Cloud services delivered over the Internet, such as web-based applications, to meet users' ‘4S’ needs: storing and synchronizing personal data, and sharing and streaming stored personal data via a personal cloud. The personal cloud, or the Personal Cloud [2], is a hybrid cloud in which the public cloud and private cloud are combined in a user-centric cloud computing model to facilitate access to and manage personal data. In this way, emerging cloud collaboration services based on mobile devices seem to be very efficient and effective solutions for managing and accessing data in cloud. However, we must bear in mind that along with these benefits, security vulnerability and risk have been increasing, especially regarding privacy, data loss and breaches.

For the outsourcing of virtual resources, the guarantee of availability and the capability of resources become a more important consideration, and accordingly providing Service-Level Agreements (SLAs) have become critical factors. An SLA is a kind of contract negotiated between a service provider and a user that establishes service levels, which are enforced by penalties and compensation if the conditions are violated by the cloud service provider [3]. The traditional SLA, also cloud computing, are enforceable contract performance clauses that do not cover conventional security aspects; such as availability, integrity and confidentiality; and emerging security issues in cloud computing. In terms of availability and reliability, though, security assurance is essential conditions for Quality of Service (QoS).

In particular, cloud-based access to data and services like personal cloud service and enterprise solutions brings with it some threats regarding privacy and data security. Increasing service complexity has been growing a need for Service-Level Agreements (SLAs) that cover emerging security issues as well as traditional aspects of security such as availability, integrity and confidentiality.

The Consumerization of IT, has grown out of consumers’ increasing integration with their personal mobile devices with BYOD policy to embrace a flexible workspace for the productivity benefits it provides, requires more complex and specified security solution as a service to manage service and data delivery to end users. In cloud computing environments, the Security as a Service (SECaaS) model seems to satisfy these expectation. The purpose of security as a service provides customized three legged stool (i.e. security service) of availability, integrity and confidentiality for the specific cloud service coinciding with SLAs relevant to security. The area of security scope, here, might have the “level of security” in SLAs. The most important thing of these approaches puts a service perspective on security to reflect consumers’ demands and guarantee security. Research on SLAs in security perspective is still in its early stage, since [4] had proposed the need of SLA including security aspects over the past decade. As pointed out previous works [5-11], the security metrics are still quite uncommon for service providers to specify the security-level concerned with their services. To achieve the SECaaS including users’ security requirements with SLA is quantitative evaluation for security metrics in security assessments. A few of previous researches had highlighted the security issue in SLAs; categorized security metrics; and provide some of methodologies of quantitative evaluation of security metrics for SLA. They, however, do not consider the features of security threats and priorities of threats to evaluate risk of security depending on service types of cloud.

978-1-4799-4233-6/14/$31.00 ©2014 IEEE

The security issue in SLAs might address the following fundamental questions: what are the features of security threats; what is the security-level; what are the metrics corresponding the security-level; how it can be assessed quantitatively. Before going on with the questions, let us define the SLAs relevant to security as a security-Service-Level Agreements (security-SLAs).

This paper aim to give convincing answer to the above questions and a methodology of quantitative assessment of security risk for security-SLA considering the features of security threats and purpose of services.

II. Related Works

A. *Security-Service-Level Agreements*

The SLAs is emerging issue in cloud computing. Reference [5] have reviewed recent research concerning SLAs and have identified sensitive issues; the different SLA metrics of users and service providers; and the difficulty in quantifying these metrics. Owing to continued service suspensions in cloud computing environments, [6] provides the refund model with regard to SLA violation.

The security aspects of SLAs are emerging as issues in cloud computing. Security-SLAs for cloud computing have been given considerable attention in recent years, particularly regarding how to reach a unified agreement between users and providers [7–10]. The studies in [9, 10] illuminated the question of how cloud providers could address the user's security needs, such as integrity and confidentiality, from the SLA perspective, and provided a detailed outline of security controls. Cloud security-SLAs are negotiated between the user and cloud providers [10]. An important part of this view is in regard to the current emergence of cloud collaboration services to the worldwide market [11]. Most research has introduced security-SLAs and provided security metrics, rarely focused on how to measure these security aspects. As mentioned above, the metrics s of SLAs, especially those of the security aspects, are very difficult to estimate and calculate. The most researcher, nevertheless, have reached nearly the needs of universal consensus that quantitative evaluation of security metrics is required. In recent years, numerous studies have attempted to address these issue trying diverse approaches [12-18]. Carlos et al. proposed a methodology for management of cloud using security metrics and security agreements to improve security in cloud environments [12]. A quantitative impact and risk assessments framework is presented to analyze and assess the risks in cloud [13]. These researches was carried out to improve security of cloud in management perspective, not security-SLA. Studies on security-SLA [14-19] proposed some of methodologies to benchmark and evaluate security metrics with approaching on security threats and vulnerability. Luna et al. implemented security-SLA benchmark system [14] as defined QUANTS-as-a-Service using quantitative Policy Trees (QPTs) and the reference evaluation methodology (REM [20]). Furthermore, an approach on quantitative security levels and benchmarks considering additional set of metrics are illustrated in [15]. Although those are empirically validated through a real-world case study based on the Cloud Security SLAs found on the CSA's "Security, Trust & Assurance Registry" (STAR [21]), they do not consider the probability of each threats; and network environment, which might influence to security risk; and the types of services, which might require different priorities of security controls relatively.

B. *Security Threats*

The cloud computing provides offering the agility by the on-demand provisioning of computing and the ability to align information technology with business strategies. Even though the cloud computing seams secure, the users are concerned about the risks of cloud computing. The Cloud Security Alliance (CSA) [22] has published documents regarding the top threats and security guidance in cloud computing entitled "Top Threats to Cloud Computing". They propounded the top seven threats to cloud computing by the report and recently issued a report [23], which is a statistical overview of vulnerability incidents with additional 5 more threats categories. The survey results is reasonable to suppose that the degree of influence of each security threat to security concerns of user is difference. It means that assessing security risks requires taking into consideration the possibility of each threats. An open industry standard, Common Vulnerability Scoring System (CVSS) [24], for assessing the severity of computer system security vulnerabilities also has a similar consensus on that. Furthermore, the CVSS consider security controls and environmental factors regarding vulnerabilities to quantify the severity of vulnerability. Although we also addressed that diverse factors–network environments, types of services, and correlation between security threats–are able to influence on security-SLAs [17-19], we did not provide objective security-level and risk assessment for security-SLAs.

III. Security Risk Assessments

A. *Motive and Limitation*

The aim of our approach provide a methodology of security risk assessment that considering probability of each threat based on real world data, feature of services depending on purpose of user, and multi-dimensional measuring of vulnerability in user perspective. As mentioned in [19], we have been focusing on a new angle on security assessment to achieve transparent security "as a service". Transparent security could obtain visibility and controls with respect to security, as a service. Our point of this paper is trying to consider and measure security risk, which a user have concerns with. This approach, even though, have limitations to provide more firm result and prove proposed methodology, it have a value as an approach to assess security risk from a user, not system.

B. *Assessing Model of Security Risk*

A security risk as well known is an intersection of three sets: an asset of service providers, vulnerabilities of those asset, security threats regarding vulnerability on service. We, however, thinks that these kind of risk cannot mitigate user concerns of security threats. Therefore we provide new assessing model of security risk for user related threats T as follow:

$$SR_T = \mathrm{N}_V \times [W]_S \times P_T \times [V]_T \qquad (1)$$

The N_V is network vector to use cloud service. The P_T is probability of security threats, and $[V]_T$ is vulnerability vector associated with security controls of cloud service providers. We add here one more factor, $[W]_S$, which is priority of security controls in accordance with types of cloud service. Before describing how the security risks are evaluated based on the above model, we will briefly examine the security threats and corresponding security controls.

Table I. SECURITY TREATS AND CONTROLS

	Security Controls	DL	ANU	ASH	API	MI
S	Data Isolation	●				
	Data Encryption	●				
	Data Location	●				
	Data Integrity	●				
	Data Back-up	●				
P	Application Isolation			●	●	
	Virtual Firewalls			●	●	
	Application Integrity			●	●	
N	Network Encryption			●	●	
	Traffic Isolation			●	●	
	Integrity Protection			●	●	
A C	Identity Management	●	●	●	●	●
	Access Management	●	●	●	●	●
	Key Management	●	●	●	●	●
A U	Logging	●	●	●	●	●
	Auditing	●	●	●	●	●
	Certification			●	●	
	Customer Privacy	●				

C. Define Security Threats and Corresponding Security Controls

Security threats and vulnerabilities in cloud computing are studied by many researchers and institutes. We considered the five threats related with user risk among the top seven threats [22]: Abuse and Nefarious Use of Cloud Computing (**ANU, denoted to T1**), Insecure Interface and APIs (**API, denoted to T2**), Malicious Insiders (**MI, denoted to T3**), Data Loss or Leakage (**DL, denoted to T4**), Account or Service Hijacking (**ASH, denoted to T5**). We then attempted to match simply these to the corresponding security controls, which is an outlined framework [25] for security mechanisms in SLAs for cloud services. Table 1 categorizes the 5 threats into the corresponding security controls: Secure Resource Pooling (**S**torage, **P**rocessing, and **N**etworking), Access Control (**AC**), Audit, Verification, and Compliance (**AU**) [26].

D. Security Threats Analysis

When we consider threat evaluation, a multi-dimensional approach model is needed. This means that we should consider not only the technical factors and the network environment, but also the service types.

To analyze security threats based on the technical factors and the network environments in cloud, we employed a 2 × 2 thinking matrix (Figure 1), which is used to facilitate better thinking and decisions. The figure 1 is based upon two considerations with above mentioned five threats. The one is technical dependence, the other is uncertainty of threats.

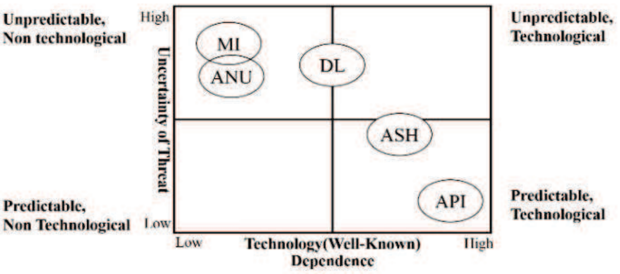


Figure 1. 2 × 2 Thinking Matrix of Threats

The AH, although, is mostly predictable and technical issue in managed network such as internal network in cloud, it has high uncertainty of threats in untrusted network like public wireless network. This makes explicit statements about managing unpredictable aspects, e.g., human resources, natural disasters, untrusted network environments, etc., of security threats are the end of security controls.

In this sense, we have assumed that the personal cloud infrastructure consists of a relatively trustworthy internal network and an untrusted external network (i.e., the Internet), as shown in Figure 2.

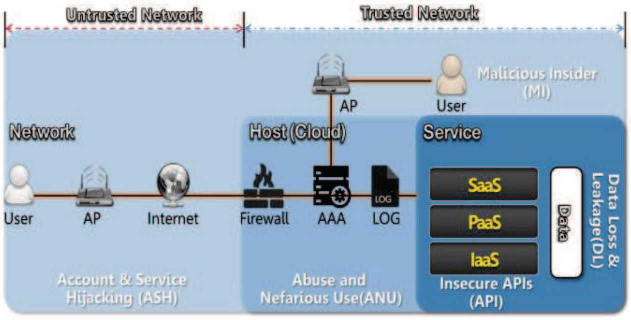


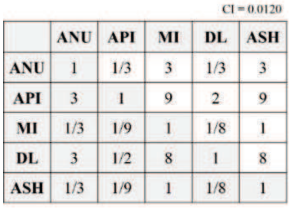
Figure 2. Cloud Infrastructure

E. Network Vector

Security risk are different depending on the network environment, as we noted in Figure 2 All attack start from accessing network to get information. Public network (Untrusted Network in figure 2) such as wireless in public area has more vulnerabilities and easier to overhear network traffics than managed network (Trusted Network in figure 2) such as wireless in private cloud. We define the impact based on the network environments as network vector. A public user might have security concerns of overhearing about their ID and password by attacker in public network, for example. It means that public user could want to check certification of SaaS server (e.g. the sslstrip could get user ID and password in the middle of server and user) and encryption solution about transferred their account information on network. While enterprise user could trusts the connected network, it needs role-based access control and auditing the user action in the system to manage security level to access information. It is very important vector to assess risk, but hard to determine the value. Even we consider access vector for network, drawing the exact value and impact remained for future works. We are figuring out the possibility of applying CVSS metrics to here.

F. *Probabilities of Security Threats*

We define here the probability of each threat employing the Analytic Hierarchical Process (AHP), a mathematics- and psychology based decision-making technique proposed by Saaty [24]. Tian et al. [27] suggested a novel threat evaluation model using the analytic hierarchy process (AHP) to attempt to address privacy and potential threats in Radio Frequency Identification (RFID), employing the AHP model to analyze user preference regarding threats. To establish the probability of each threat, we use statistical data of CSA [23] for a pair comparison matrix as figure 3.



CI = 0.0120

	ANU	API	MI	DL	ASH
ANU	1	1/3	3	1/3	3
API	3	1	9	2	9
MI	1/3	1/9	1	1/8	1
DL	3	1/2	8	1	8
ASH	1/3	1/9	1	1/8	1

Figure 3. A pair comparison Matrix between Threats for the probability

Let $A = (a_{ij})$ be the resulting matrix of the pair comparison on elements a_i, a_j: we use here the five threats (T1-T5). Those matrices have the following characteristics:

$$a_{ii}=1,\ a_{ji} = 1/a_{ij} \tag{2}$$

$$A\omega = \lambda\omega \tag{3}$$

Where λ is eigenvalue of the matrix A and ω is dominant eigenvector. The eigenvector is a priority in Figure 3 and the consistency index (*CI*) value can be acquired by the following equation:

$$CI = (\lambda_{max}\text{-}n)/(n\text{-}1) \tag{4}$$

The *CI* should be lower than 0.1. If that is the case, the result of pair comparison is reliable. Let the initial vector be $u(0)$ to calculate λ and ω.

$$u(0) = (1/n\ 1/n\ \cdots\ 1/n) \tag{5}$$

$$v(k) = A^k u(k-1), k = 1, 2, \cdots, n \tag{6}$$

$$v(k) = (\ v_1(k), v_2(k), \cdots, v_n(k)\ ) \tag{7}$$

$$u(k) = v(k)/t(k) \tag{8}$$

Against a sufficiently large value of k, $v(k)$ and $u(k)$ converged to determined values, i.e., λ_{max} and ω of A, respectively. The result of above pair comparison matrix is probability of each threat as follow:

$$P_T = [\,T1, T2, T3, T4, T5\,]_T \tag{9}$$

$$= [0.129, 0.456, 0.044, 0.328, 0.044]_T$$

It means that impact of probability of threat to security risk might be different and we should consider probability to assess security risk.

G. *Establish Priorities of Security Controls regarding Service Types*

Furthermore, as we mentioned, depending on the personal cloud service type, there are different preferences among the user requirements. In the case of webtop such as virtual desktop infrastructure (VDI) for enterprise, a user may want a strict authentication process with multi-factor and a VPN solution above everything else: usually VDI service is delivered by secure container, it means that we feel more secure about network vulnerabilities. An online storage user, on the other hand, might look for secure data backup, integrity, and encryption. In summary, security threats are closely related with QoS of services, and we should consider the security threats to assess security-SLAs based on underlying service type and property. With these considerations in mind, let us now develop a model that takes a multi-dimensional approach to evaluating security-SLAs.

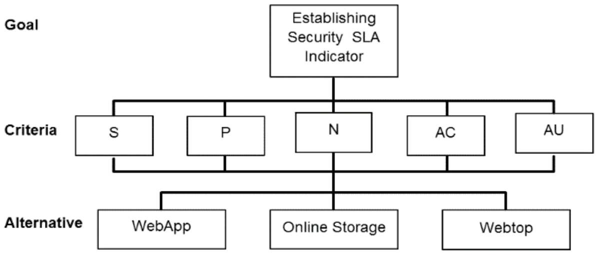
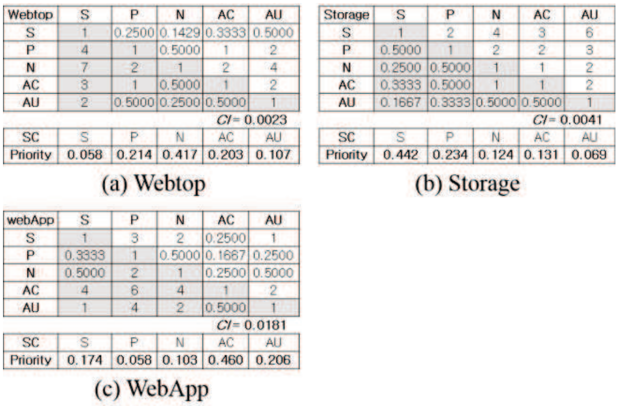


Figure 4. Hierarchy Model for Service Types with Corresponding Security Control

We proposed a methodology for the priorities of security control depending on service types using AHP [19]. The personal cloud services are categorized as webtop, online storage, and webApp [2] and the figure 4 show the hierarchy model for service types with corresponding security control. We used three pair comparison matrix, as shown in figure 5, to evaluate priorities of security controls in [19].



Webtop	S	P	N	AC	AU
S	1	0.2500	0.1429	0.3333	0.5000
P	4	1	0.5000	1	2
N	7	2	1	2	4
AC	3	1	0.5000	1	2
AU	2	0.5000	0.2500	0.5000	1

CI = 0.0023

SC	S	P	N	AC	AU
Priority	0.058	0.214	0.417	0.203	0.107

(a) Webtop

Storage	S	P	N	AC	AU
S	1	2	4	3	6
P	0.5000	1	2	2	3
N	0.2500	0.5000	1	1	2
AC	0.3333	0.5000	1	1	2
AU	0.1667	0.3333	0.5000	0.5000	1

CI = 0.0041

SC	S	P	N	AC	AU
Priority	0.442	0.234	0.124	0.131	0.069

(b) Storage

webApp	S	P	N	AC	AU
S	1	3	2	0.2500	1
P	0.3333	1	0.5000	0.1667	0.2500
N	0.5000	2	1	0.2500	0.5000
AC	4	6	4	1	2
AU	1	4	2	0.5000	1

CI = 0.0181

SC	S	P	N	AC	AU
Priority	0.174	0.058	0.103	0.460	0.206

(c) WebApp

Figure 5. Pair Comparison Matrix for Each Type of Service

The comparison matrix is methodology to present quantitatively relative importance of security controls. It means that services might have different weights of security controls depending on the service-specific feature as discussed in [28]. As well-known saying in security field, the more secure you make something, the less secure it becomes. We, thus, might focus on vulnerability which causes more concerns, when we consider cost, efficiency and usability. The priorities of security controls are express as below:

$$[W]_S = [S, P, N, AC, AU]_S \qquad (10)$$

, where S is service type

The priorities of security controls depending on service types, as shown in figure 6 [19], are as follows:

$$W_{webtop} = [0.058, 0.124, 0.417, 0.203, 0.107]_{webtop}$$

$$W_{Storage} = [0.442, 0.234, 0.124, 0.131, 0.069]_{Storage}$$

$$W_{WebApp} = [0.174, 0.058, 0.103, 0.460, 0.206]_{WebApp}$$

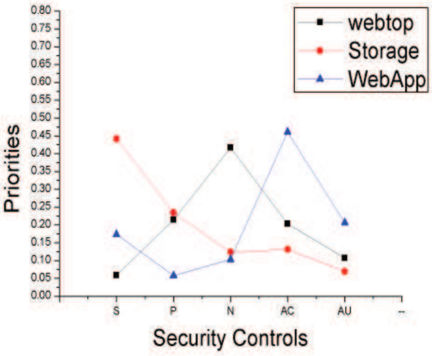


Figure 6. Priority Comparison Depending on the Service Type

Even though each value is result of our simulation of assumed requirements based on the service types, we could reach more practical value involving security expert based on security assessment, analyzing security threats and requirements, by a security service provider of third party. If the third party is a broker for SECaaS, providing quantitative result of security assessment for user, we could reach consensus standard of reasonable weights.

H. Define Security-Level for Measuring Vulnerability

We have described the P_T and W_S for evaluating security risk. To define security-level concerning vulnerability is last step to reach the security-SLA. In our previous works [17-19], we did not security-level of security services or security controls related with vulnerabilities for security-SLA. To provide objective security-level of cloud providers, we apply CVSS metrics and impact as security-level. The vulnerability of cloud providers is related with providing security controls. The security-level is conditioned by combination of Access Vector (**AV**), Access Complexity (**ACP**), Authentication (**Au**), Confidentiality (**C**), Integrity (**I**), Availability (**A**), which are have score from 0 to 1 that means exploitability and impact. In case of AU (i.e. Audit, Verification, and Compliance), it has not defined security-level, so it is 1.

Table Ⅱ. Combiation for Security-Level

Security Controls	Security-Level
Secure Storage (S)	C, I, A
Secure Networking (N)	AV
Access Control (AC)	ACP, Au
Secure Processing (P)	C, I
Audit, Verification, and Compliance (AU)	1

When it comes to the online storage service in public network, for example, *C*, *I*, and *A* are all "*partial*" and the score of "*partial*" is 0.275. Then, ACP is "LOW" (i.e. there are no special conditions for access to the vulnerability, such as when the system is available to large numbers of user, or the vulnerable configuration is ubiquitous, and the score is 0.71) according to CVSS documents.

These security-levels are able to determine $[V]_T$ of specific threats as follow:

$$[V]_T = [S_{<L,T>}, P_{<L,T>}, N_{<L,T>}, AC_{<L,T>}, AU_{<L,T>}]_T \qquad (11)$$

Where $S_{<L,T>}$ is security-level regarding threat T and calculation, refer to CVSS, result of above example is:

$$S_{<L,T>} = 0.6 \times [1 - \{(1 - \mathrm{C})\} \times \{(1 - \mathrm{I})\} \times \{(1 - \mathrm{A})\}] \qquad (12)$$

$$= 0.6 \times [1 - \{1 - (\mathrm{Partial})\} \times \{1 - (\mathrm{Partial})\} \times \{1 - (\mathrm{Partial})\}]$$

$$= 0.6 \times [1 - 0.725 \times 0.725 \times 0.725] = 0.3713$$

Through these security-levels combined multi-factors, types and usage environments of target service are able to feed into security risk assessment. It mean that user requirements on security service can be reflected in a contract of security-SLA. We can calculate, finally, the $[V]_T$ considering security-level. The total security risk (SR_{total}) concerning security threats is:

$$SR_{total} = \mathrm{N}_V \times \textstyle\sum_T^n P_T \times [W]_S \cdot [V]_T \qquad (13)$$

$$= \mathrm{NV} \times \sum_T^n P_T \times [(W_S \times S_{<L,T>}) + (W_P \times P_{<L,T>})$$

$$+(W_N \times N_{<L,T>}) + (W_{AC} \times AC_{<L,T>})$$

$$+(W_{AU} \times AU_{<L,T>})]_T$$

, where T is each threat and n is number of threats

Assessing security risk considering probabilities of threats, weight values (priorities) of security controls depending on service types, and security-level defined by CVSS metrics is possible to provide objective evidence of security-SLA to users. The quantitative methodology, though, for security-SLAs based on numerous researches to reach the general consensus in the future is important thing, the paradigm shift of "security" from just "offered" to "on-demand" in user perspective have to be gained attention with the emerging SECaaS and security-SLAs issues as we mentioned in introduction. Furthermore, we should consider that what should be measured for users' requirements on security service and how the "security" can make provision before it is asked. The contributions of this paper are a) providing probabilities of security threats according to the real statistical data; b) describing approach to assess security risk in user perspective; c) considering security risk in various aspects to measure the vulnerability with security-level.

IV. Conclusion

Great attention has been given to the question that how security-SLA could be assured and how services could be recommended to users based on security-SLAs. Even though many researchers have suggested definitions and evaluation models or processes for security-SLAs, quantitative security risk assessment for a user are rarely studied. A few approaches addressed quantitative model, not considering feature of security threats and services. Assessing security risk for security-SLA might consider service types and usage environments, which influence to risk exposure in a user perspective. In this paper, we propose approach on security risk assessments in view of diverse factors from user, which might impact to the area of security vulnerability. In the future works, we will advance a theory of security-SLA evaluation in a user perspective with measuring user requirements.

Acknowledgment

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014(H0301-14-1020)) supervised by the NIPA (National IT Industry Promotion Agency). A Corresponding author is Eui-Nam Huh.

References

[1] Personal Cloud, http://personal-clouds.org/wiki.

[2] Sang-Ho Na, Jun-Young Park, Eui-Nam Huh, "Personal Cloud Computing Security Framework", Proc. Services Computing Conference (APSCC), IEEE, Dec. 2010, pp.671-675, doi: 10.1109/APSCC.2010.117

[3] A. Sahai, S. Graupner, V. Machiraju, A. Moorsel. "Specifying and Monitoring Guarantees in Commercial Grids through SLA", Proc. Cluster Computing and the Grid, IEEE/ACM, May. 2003, pp.292-300, doi: 10.1109/CCGRID.2003.1199380.

[4] Ronda R. Henning, "Security service level agreements: quantifiable security for the enterprise?", Proc. workshop on New security paradigms (NSPW '99), ACM, Sept. 1999, pp54-60, doi:10.1145/335169.335194.

[5] Chenkang Wu, Yonghua Zhu, Shunhong Pan, "The SLA Evaluation Model for Cloud Computing", Proc. International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013), May, 2013, pp.331-334, doi:10.2991/iccnce.2013.83

[6] Al Amin Hossain, Eui-Nam Huh, "Refundable Service through Cloud Brokerage", Proc. Cloud '13, IEEE press, June, 2013, pp.972-973, doi:10.1109/CLOUD.2013.115.

[7] Mark D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions", Journal of Systems and Software, vol.86, no.9, Sept, 2013, pp.2263-2268, doi:10.1016/j.jss.2012.12.025.

[8] Dimitrios Zissis, Dimitrios Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, vol.28, no.3, Mar, 2012, pp.583-592, doi: 10.1016/j.future.2010.12.006.

[9] Chunming Rong, Son T. Nguyen, Martin Gilje Jaatun, "Beyond lightning: A survey on security challenges in cloud computing", Computers & Electrical Engineering, vol.39, no.1, Jan, 2013, pp.47-54, doi:10.1016/j.compeleceng.2012.04.015.

[10] Bernsmed Karin, Jaatun Martin Gilje, Meland Per Håkon, Undheim Astrid, "Security SLAs for federated cloud services", Proc. Availability, Reliability and Security (ARES), IEEE press, Aug, 2011, pp.202-209, doi: 10.1109/ARES.2011.34

[11] Forrester Research Inc., "Collaboration Services: Deployment Options for The Enterprise", Nov, 2012, pp.1-15.

[12] Carlos Alberto da Silva, Anderson Soares Ferreira, and Paulo Lício de Geus, "A methodology for management of cloud computing using security criteria", Proc. Cloud Computing and Communications (LatinCloud'12), Nov. 2012.

[13] Saripalli, P.; Walters, B., "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security," Proc. Cloud Computing (CLOUD 2010), Jul. 2010, pp.280-288, doi: 10.1109/CLOUD. 2010.22.

[14] Luna, J., Langenberg, R., and Suri, N., "Benchmarking cloud security level agreements using quantitative policy trees", Proc. Cloud computing security workshop (CCSW '12), ACM, Oct. 2012, pp.103-112.

[15] Luna, J., Ghani, H., Vateva, T., and Suri, N., "Quantitative assessment of cloud security level agreements: A case study", Proc. Security and Cryptography, INSTICC, Nov. 2012, pp.64-73.

[16] N. Gonzalez, C. Miers, F. Redigolo, T. Carvalho, M. Simplicio, M. Naslund, and M. Pourzandi, "A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing," Proc. Cloud Computing Technology and Science (CloudCom), Nov. 2011, pp.231-238

[17] Sang-Ho Na, Kyung-Hun Kim and Eui-Nam Huh, "Threats Evaluation for SLAs in Cloud Computing", Proc. Convergence Technology (ICCT 2013), Jul. 2013, pp.1570-1571.

[18] Sang-Ho Na, Kyoung-Hun Kim and Eui-Nam Huh, "A Methodology for Evaluating Cloud Computing Security Service-Level Agreements", International Journal of Advancements in Computing Technology (IJACT), vol.5, no.13, Sept. 2013, pp.235-242.

[19] Sang-Ho Na, Eui-Nam Huh, "A broker-based cooperative security-SLA evaluation methodology for personal cloud computing", Security and Communication networks, 2014 (Accepted).

[20] Valentina Casola, Rosa Preziosi, Massimiliano Rak, Luigi Troiano, "A Reference Model for Security Level Evaluation: Policy and Fuzzy Techniques. Journal of Universal Computer Science", Journal of Universal Computer Science, vol.11, issue.1, 2005, pp.150-174, doi: 10.3217/jucs-011-01-0150

[21] Cloud Security Alliance. "The Security, Trust & Assurance Registry (STAR)", Online: https://cloudsecurityalliance.org/star/, 2011.

[22] Cloud Security Alliance ,"Top Threats to cloud computing", Online : https://cloudsecurityalliance.org/research/top-threats/, 2010.

[23] Cloud Security Alliance , "Cloud computing vulnerability incidents: a statistical overview", Online : https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/, 2013.

[24] FIRST, Common Vulnerability Scoreing System (CVSS), online: http://www.first.org/cvss

[25] Thomas L. Saaty, "How to make a decision: The Analytic Hierarchy Process", European Journal of Operational, vol. 48, pp.9-26, 1990.

[26] K. Bernsmed, M. G. Jaatun, and A. Undheim, "Security in Service Level Agreements for Cloud Computing," in Proceedings of the 1st International Conference on Cloud Computing and Services Science, (CLOSER), 2011.

[27] Yuan Tian, Biao Song, Eui-Nam Huh, "A novel Threat Evaluation method for privacy-aware system in RFID", International Journal of Ad Hoc and Ubiquitous Computing, vol.8, issue 4, pp.230-240, 2011.

[28] Jianyong Chen, Yang Wang, and Xiaomin Wang, "On-Demand Security Architecture for Cloud Computing", Computer, IEEE Computer Society, vol.45, No.7, 2012, pp.73-78.