Integrated Cloud Risk

Yasheng Pang[1], YouJin Song[2] , JangMook Kang[3] and Jae-Kwan Yun[4]

[1,2] Department of Information Management, Dongguk University,
707 Seokjang-dong, Gyeongju, Gyeongsangbuk-do, 780-714, Korea
[3] Electronic Commerce Research Institute, Dongguk University, 707 Seokjang-dong,
Gyeongju, Gyeongsangbuk-do, 780-714, Korea
[4] Real&Emotion Sense Convergence Service Research Section
Smart Green Life Research Department
IT Convergence Technology Research Laboratory
Electronics and Telecommunications Research Instutite(ETRI)

{pangpang7117, mooknc}@gmail.com,{song, redsea}@dongguk.ac.kr, {jkyun}@etri.re.kr

Abstract. Cloud computing become more and more eye-catching these days. What make sense is advantages are inevitably accompanied by disadvantages. Subsequently, risks in cloud are also more and more compelling to people. This paper studies and researches on an array of experienced literature, presents an integrated risks table based on the risk key factors of cloud computing, and gives a comprehensive description for every risk.

Keywords: Risk Assessment, Cloud Computing, Integrated Risks, Security

1 Introduction

"Cloud computing" has ceased to be a unfamiliar vocabulary nowadays but still a newborn business model for IT services. It will be controversial when every fangled turns into our lives. For cloud computing is also without exception. Security problem may be the first hot topic in this controversy. No wonder, delivering your data to a third party provider who owns infrastructure or platform or software that out of your grip is worrying enough.

As so far, a number of organizations established and devote themselves to cloud security. For instance, CSA (Cloud Security Alliance), ENISA, and OWASP are fairly well-know in this area. And each of them published significant literature in cloud risk summary. [1] Of course, each of them has their own specific perspectives, but there also exist a lot of overlaps. Meanwhile, some of them have no classification with these risks; some of them even classified risks into several types, are incomplete or not summary enough due to the premature time or not all-inclusive viewpoint. This paper reduces these redundancies and integrates all existing cloud risks what they mentioned or depicted until now, and classify them with key factors in order to understand the essence of every risk in cloud computing, furthermore, to facilitate the governance in cloud computing risks.

2 A concept of cloud computing and security environment

As NIST defined, we can understand cloud service's architecture in "3,4,5" as figure1:".

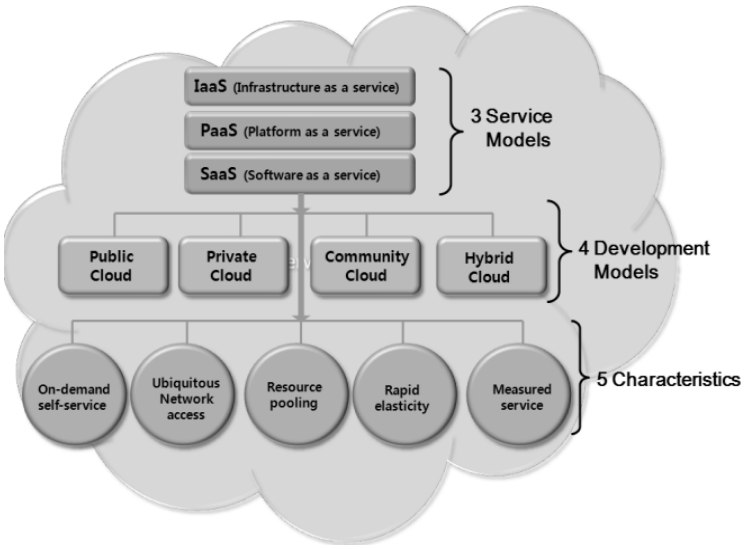

Fig. 1. Architecture of Cloud service [2]

Cloud computing is a growing field, until now, cloud corporation like Amazon, Google and Microsoft are well-known for the public， and all have special focus in their service area. This cloud computing can be easily adapted to reduce transmission costs for the 4D media broadcasting system and open market website that can trade mass of sensory information metadata for real-sense media distribution, 4D media creation, and physical device playback framework [3].

3 Integrated Cloud Risk Table and Risk

We browsed and researched on an array of references in cloud risk area. Amongst these papers, we covered from the well-known authority organizations to individual viewpoints, reclassified the cloud risks into five categories and subdivided into twelve specific risks in detail. Base on the CSA top threat's format, retained the names of their items [4], we made an integrated risk table as below:

Table 1. Integrated cloud risks.

Risk Classification	Specific Risk
Technology Problem	1. Insecure interface & APIs: intrusion[5];API key attack[6]
	2. Shared technology issues: virtual boundary breaks[7] Malicious VM planting; private key recover[8]
	3. Abuse/Nefarious use of cloud computing: DDOS; botnet; SQL injection; backdoor Trojan; SCA, etc.[4]
	4. Account or service hijacking: MITM; phishing or fraud[4]
Trust Problem	5. Malicious insiders: malicious employee or related third party
	6. Composite service's risk: visibility and transparency problems; data migration problems[9]
Data Problem	7. Data leakage: virtual data breaks and physical theft
	8. Data loss(Temporary & Permanent): device failure; power outage[7]; bankruptcy[10]
	9. Lack of update / Patching: virtual and physical level
Compliance Problem	10. Inappropriate SLA/QoS & Lack of standard(security metrics)
	11. Laws & Regulations' regional differences(global-wide laws)
Measurability Problem	12. Metering & Billing Error: manipulation of metering/billing data; billing evasion[11]

Technology problems are mainly about encryption technique, virtualization technology, as well as the technology of access control, ID management and authentication area; Trust problems mainly refer to followed factors: people, contract, organization, governance and the visibility & transparency between provider side and customer side; Data Problems here are more about data availability and timeliness, also the confidentiality; Compliance problems denote the risks relate to regulations, laws and contracts. All of these impact on whether the service and business is going on smoothly; And the measurability problems relate to business profit and business auditing.

4 Conclusion

This paper through an array of review and study on the existed literatures, presents an integrated risks table based on classified key factors in cloud risk, and compare it with SLA requirement. Since the cloud computing area is still at a growth stage, maybe there are still some areas where we untouched.

All in all, only keep the step on the knowledge about risk types and classification is far from these problems. What we need is how to face and solve these risk problems in cloud computing area. Connecting with business model, such as BMIS [12], will be a meaningful work in future.

Acknowledgments. "This work was supported by the MKE (Ministry of Knowledge Economy) [A004700008], Development of realistic sense transmission system with media gateway supporting multi-media and multi-device".

References

1. David Vohradsky, “Cloud Risk—10 Principles and a Framework for Assessment”, ISACA JOURNAL VOLUME 5 (2012)
2. National Institute of Standards and Technology, “The NIST Definition of Cloud Computing Special Publication 800-14” (2011)
3. Jae-Kwan Yun, Jong-Hyun Jang, Kyung-Duk Moon, “Development of the real-sense media broadcasting service system based on the SMMD”, Digest of Technical Papers - IEEE International Conference on Consumer Electronics volume, pp. 435 – 436 (2011)
4. CSA, “Top Threats to Cloud Computing V1.0” (2010)
5. Yashpal Kadam, “Security Issues in Cloud computing A Transparent View” (2011)
6. Robert Lemos, “Insecure API Implementations Threaten” (2012), available at: http://www.darkreading.com/cloud-security/167901092/security/application-security/232900809/insecure-api-implementations-threaten-cloud.html
7. Wayne A. Jansen (NIST),”Cloud Hooks: Security and Privacy Issues in Cloud Computing” (2011)
8. Dan Goodin, “Virtual machine used to steal crypto keys from other VM on same server” (2012), available at : http://arstechnica.com/security/2012/11/crypto-keys-stolen-from-virtual-machine/
9. Dylan Jones, “Some common data migration risks (and how to avoid them)” (2009), available at: http://www.dataroundtable.com/?p=1025
10. David S Caplan, “Bankruptcy in the Cloud: Effects of Bankruptcy by a Cloud Services Provider” (2012)
11. Vadym Mukhin, Artem Volokyta, “Security Risk Analysis for Cloud Computing” (2011)
12. ISACA, “Business Model for Information Security” (2009)