Risk Assessment and Classification of Focusing SLA Requirement in Cloud Computing

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 DepartmentIT Convergence Technology Research Laboratory Electronics and Telecommunications Research Instutite(ETRI)

[1]pangpang7117@gmail.com, [2]song@dongguk.ac.kr, [3]mooknc@gmail.com, [4]jkyun@etri.re.kr

Abstract

Cloud computing become more and more eye-catching these days. Each big company in IT areas hurries to win a chunk of meat which promises to be a whopping market in future. 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. In the meanwhile, it gives a verification and validation for these risks under the comparison with SLA requirements.

Keywords: *Risk assessment, Cloud computing, Integrated Risks, SLA, Security*

1. Introduction

"Cloud computing" has ceased to be a unfamiliar vocabulary nowadays. Put it in the simplest way, you can think it as your experienced and daily used email [1]. Whatever Gmail, Hotmail, Yahoo, Naver and so on, you never need to install it on your physical computer, all you need is just an internet, and you can access it whenever you want, wherever you go. A small variation from your experienced email is: "Cloud computing" charge you fees for this service, and you can pay as you go. It should be point out that cloud computing has never been a new technology, it's a comprehensive product of many kinds of computing and network technologies, such as: Parallel Computing, Distributed Computing, Utility Computing, Network Storage Technologies, Virtualization, Load Balance, *etc*.

The main advanced idea of loud computing is to make a better use of distributed resources, sufficiently integrate various resources to adapt to the changing of clients' requirement. It is a green computing. Nevertheless, it's 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. The most well-known organization focus on this area is CSA (Cloud Security Alliance). Cloud Security Alliance is a not-for-profit organization, which aim at providing security assurance within Cloud Computing, founded in 2008 [2]. Others also related in this area such as ENISA: the European Network and Information Security Agency, to improve network and information security in the European Union, created in 2004 [3]; OWASP: the Open Web Application Security Project, also a worldwide not-for-profit organization focused on improving the security of software [4], and the aim of OWASP is helping people with a useful and clear resource of tools and documents to help understand web application security to better protect themselves online; NIST(National Institute of Standards and Technology); and ISO/IEC; *etc.* In the meanwhile, a good deal of literatures about cloud threats and risks analysis sprang up. For instance, CSA published the widely known "Top Threats to Cloud Computing V1.0"; ENISA produced a document that comparatively comprehensive in cloud risk classification and recommendation; and OWASP summarized a list which describes 10 top cloud risks through the literature review [5].

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

Speaking of the cloud computing, we can trace back to 1960s. John McCarthy, who pointed out that "computation may someday be organized as a public utility" [6], should be a significant opinion in cloud history. And the term "cloud" originates from the telecommunication world, because telecom companies originally started offering Virtual Private Network (VPN) services with comparable quality of service at lower cost [7]. As so far, many concepts of cloud computing were presented, the definition provided by NIST is the most widely recognized amongst them. NIST presented it as below: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models" [8].

As NIST defined, we can understand cloud service's architecture in "3,4,5" as Figure 1 at the top of next page:

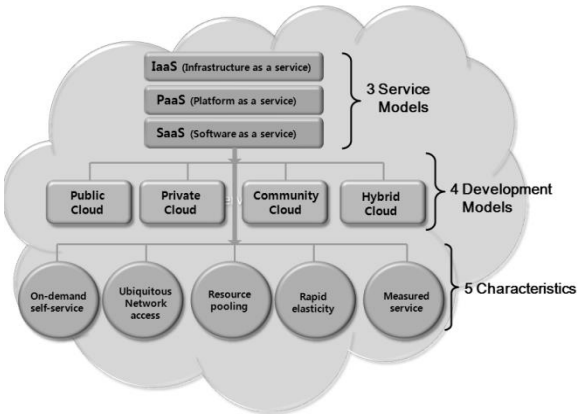

Figure 1. Architecture of Cloud Service [8]

Cloud computing is a growing field, until now, cloud corporation like Amazon, Google and Microsoft are well-known for the public. And they all have special focus in their service area. Such as Amazon, their service include EC2 and S3, it's a typical example for IaaS. For Microsoft, more concentration on PaaS, offering its Azure Service Platform, which are services that allow developers to establish user identities, manage workflows, synchronize data on Microsoft's online computing platform. And Google is well-known with Google Apps, which focuses on SaaS [9]. And, 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 [30].

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, and ultimately made this integrated risk table as a summary. Look at Table 1 at the bottom of this page.

Table 1. Integrated Cloud Risks

Risk Classification	Specific Risk
Technology Problem	1. Insecure interface & APIs
	2. Shared technology issues
	3. Abuse/Nefarious use of cloud computing
	4. Account or service hijacking
Trust Problem	5. Malicious insiders
	6. Composite service's risk
Data Problem	7. Data leakage
	8. Data loss: Temporary & Permanent
	9. Lack of update / Patching
Compliance Problem	10. Inappropriate SLA/QoS & Lack of standard
	11. Laws & Regulations' regional differences
Measurability Problem	12. Metering & Billing Error

Through this analysis, we reclassified the cloud risks into five categories: they include technology problem, trust problem, data problem, compliance problem, and measurability problem. And they can be subdivided into twelve specific risks in detail. We base on the CSA top threat's format, and retain the names of their items. After the research in previous papers, the descriptions of each risk concept are illustrated as below:

3.1. Technology Problems

This kind of problem mainly about encryption technique, virtualization technology, as well as the technology of access control, ID management and authentication area.

1. Insecure interface & APIs: Cloud services allow third-party access by exposing API (application programming interfaces), and especially organizations may be required to relinquish their credentials to third parties in order to enable their agency. Here is a risk relates to anonymous access or improper authentication, which will lead to application security. Through the insecure APIs, intrusion risk are more bigger in cloud environment which adds complexity or blocks visibility to network-based IDS/IPS [10]. These days, a so called API key, which can act as both a unique identifier and a secret token for authentication, are used to track and control how the API is being used [11]. Even then, just if the service providers are not careful, the attacker with access to the key also can produce severe attacks such as DOS or gain profit by pretending the victims [12].

2. Shared technology issues: Using of VMs (virtual machines) to serve for multi-tenants is a typical character for cloud's IaaS provider. There are many kinds of threats in this area. For instance, there are many image repositories distributed in masses of VMs, the information leakage of VM image will take a big toll for cloud customer; Data integrity can be easily maintained in stand-alone system with a single database which can maintain the transactions follow ACID (atomicity, consistency, isolation and durability) whereas it will be more complex in multi-databases and multi-applications [10]; In cloud architecture, a hypervisor or VMM (virtual machine monitor) is designed to run multiple guest VMs, but malicious code can break the virtual boundary of each VMM and intervene in the hypervisor or other guest VMs [13]; Investigation is also a problem in cloud environment since the logging and data for multiple customers may be co-located and ever-changing [14]; What's more, inserting a intended VM in the multi-VM environment can also be terrible: a new tech showed that scientists were able to recover a private encryption key if succeed in running a malicious VM on the same hardware [15]. (See Figure2 as below):

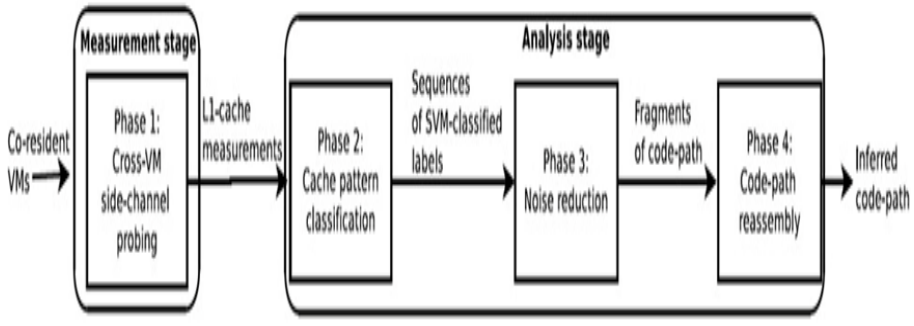

Figure 2. A Side-Channel Attack on a Virtual Machine [15]

3. Abuse/Nefarious use of cloud computing：The on-demanded and elastic cloud service often coupled with “frictionless” registration process [16], thus can bring diversified attacks. This kind of risk can impact the business process, steal confidential information or damage the quality of cloud service even can lead to the interruption of service. All attacks from clients side such as: password and key cracking, DDOS (Distributed Denial Of Service), botnet, hosting malicious data, SQL injection, spyware implantation, keystroke-logging, backdoor trojan, SCA (Side Channel Attacks) and so on.

4. Account or service hijacking: It’s not a special risk in cloud service, all kinds of IT service used to suffer this kind of attack, and cloud’s special value concentration makes it more attractive to attackers. This kind of risk often with stolen credentials and the compromise of confidentiality, integrity and availability of cloud service [16], and may bring financial loss for cloud customers. For this attack, it’s mainly about the problem of ID management, authentication and access control. For example, the most common attack in this area is MITM (man-in-the-middle): A form of active eavesdropping between two victims controlled by the third man, sometimes with unsuspecting tampering of message. [17] Attackers can intercept related information such as account or password once it succeeds. Besides this, phishing, fraud, and exploitation of software vulnerability can also lead to the same consequence [16]. All of these threats obviously relate to ID management problem. Usually we use a “federated identity” to manage this area. It’s a multi-systems, which linking a person's electronic identity and attributes, trusted through one-factor authentication ticket [18]. On the one hand, one-factor authentication is risky itself, for example, XML wrapping attacks may happen in authentication process, which means a malicious replacement body can be manipulative through the embezzlement of original massage body and use its signature. [13] On the other hand, access control also responsible for this kind of threat. A lot of cloud providers use XACML (eXtensible Access Control Markup Language) to control access, but XACML entities are still susceptible to attack by malicious third parties [13].

3.2. Trust Problems

This kind of problem mainly refers to followed factors: people, contract, organization, governance and the visibility & transparency between provider side and customer side.

5. Malicious insiders: To hand out your data or relinquish the direct control to the service providers is a paradigm in cloud computing. And this originally holds a risk of reliability. To CSPs, risks can from not only the attackers outside, but also the inside provider itself. Cloud employees have more convenience to approach the service access, and also the data which is stored in cloud may be seen processed by them. If by any chance there is someone malicious, it can bring various types of fraud, sabotage of information resources, and theft of information [13]. Furthermore, not only the employees but the other parties who somehow have received access to a CSP network, system also may steal data from the system [10]. The impact of this kind of risk, not only unfavorable for customers, but also harmful for cloud providers such as brand damage, financial impact, and productivity losses [16].

6. Composite service risk: This kind of risk can understand simply as "cloud nesting risk", it means that a SaaS provider may use other PaaS provider, and this PaaS provider also may rely on another IaaS provider. It's usually related about contract problem, visibility and transparency. In this case, first of all, trust is often not transitive [13]. SLA (service-level agreement) is one handled method to this situation, but it still lack of visibility and transparency in subcontract. What's more, not just the negotiation of contract (SLA), but more important is the monitoring of their fulfillment. External auditing and performance assessment should be taken on a real-time, but you don't have a clue that cloud computing providers who refuse undergo this scrutiny [14] even whether they have the valid certificates. Secondly, the data migration from one cloud layer to another also can be alarming. Data migration is a key component of data integration and data quality. More intermediate links means more risk in service process. During the migration, problem such as "Lack of data quality management strategy and appropriate tools" and "Target application is constantly changing" [24] may lead to a risk. This kind of risk can be contagious, that means once only one joint error, and then may spread to the whole service chain. Finally, it should be point that, not just composited cloud service but also single outsourced cloud service may exist with these problems, just it's more severe and salient in composited service.

3.3. Data Problems

Situated in the computing environment, data as a carrier of information, every information problem can be ascribed to data problem after all. Mention about information security must relate to CIA (confidentiality, integrity and availability) principles [19]. Data integrity and some kind of confidentiality risks almost included in technology and trust problems we described before, here the data problems more about data availability and timeliness, also the confidentiality.

7. Data leakage: The data compromise can be caused in many different ways. Not just the breaches of electronic data, but also the physical theft could be happen. This kind of risk typically relates to data confidentiality, and may be sort of overlap with encryption technique and malicious insider problems. For example, insecure cryptography, insufficient AAA (authentication, authorization, and audit) controls and operational failures [16], all can lead to data leakage. Numerous of users access the same storage in the cloud environment obviously can make an increase of data leakage possibility. One instance is Microsoft's BPOS (business productivity online suite) has been downloaded by non-authorized users [10]. Further more, recovering data by a previous user [20] or ancillary data's breach [13], both can result in data leakage. Data leakage can damage the brand and reputation for cloud providers, also significantly impact employee, partner, and customer morale and trust [16], and bring client company financial loss.

8. Data loss: temporary & permanent. This kind of risk typically about data availability, can embrace both the temporary and permanent circumstance, and relate to backup & recovery problem and company's BCP (business continuity plan). For temporary data loss, usually owing to company contingencies, has been experienced in many instances before. Temporary outage and performance slowdowns already happened in big company like Amazon and Salesforce.com [13] illustrated this point. Not only data lost from data center virtually but also the physical destruction such as the network device failure or power outage can bring a temporary data loss. Even though big companies may have a fine backup and recovery supply, but the time for enablement of the standby system also should be noteworthy. The other circumstance is permanent data loss. In this case, it always includes 3 kinds of possibility. Firstly, as we mentioned before, large enterprises always are fairly well

covered with DR/BC plans, while smaller company may more concern about economic functions that lack of backup and recovery plan or even completely no backup at all. Thus can obviously lead to a permanent loss if data deletion or alteration of records without a backup of the original content is happened, whatever unintentional or malicious. Secondly, physical theft can lead to not only data leakage but also the permanent data loss if there are no copy materials or straightforward stealing of storage utility. The last one which is most often mentioned by many kinds of literatures is the bankruptcy or complete shutdown of a cloud company. For example, innumerable citizens lost access and the right to use of their e-mail through a bankruptcy happened in San Francisco Bay Area several years ago [31]. The impact of data loss can be devastating, especially for permanent data loss. Loss of core intellectual property not only impact on the competitiveness and finance aspects but also could bring the violations referring to legal questions more evilly [16].

9. Lack of update/patching: This kind of risk relates to CSA's "Unknown Risk Profile" and the maintenance problem. A patch is the software that can update a computer program and fix the problems [21]. Here, the lack of update/patching include not only virtual level but also physical level. For physical level, that means maintenance of hardware, such as the ageing of the cable or server may lead to the data availability problem. For virtual level, this would be more complicated. Not just provider side but also customer side need update/patching. Lack of update or patching may bring vulnerability for system, and nowadays exploit of existing vulnerabilities is more easier through toolkits that allow third parties and people without a great deal of technical expertise to carry out attacks. And that may give rise to all kinds of technology and data problems which described previously in this paper.

3.4. Compliance Problems

In this domain, there are risks relate to regulations, laws and contracts. All of these impact on whether the service and business is going on smoothly.

10. Inappropriate SLA/QoS & Lack of standards: This kind of risk relates to contract dissension problem. Firstly, SLA (service level agreement) sets the natures and requirements about cloud service. There are two kinds of SLAs which can be divided into off-the-shelf (non-negotiable) and negotiable agreement. Non-negotiable SLA always favorable for CSPs and inappropriate quality of service requirements, both of them may bring contract dissension risk to customers. Secondly, the security metrics standards are still vacant in cloud computing area. According to firm Mimecast, the lack of industry-wide security standards is hindering business adoption of cloud services [22]. With the impact at service quality and service progress, the lack of standardization and compliance undoubtedly will bring a risk to cloud users.

11. Laws & Regulations' regional differences: As a cloud customer, you never have a clue that where your data stored since you hand out your data to cloud provider. Thus cloud provider may store or transfer your data or information in a location crossed by national border. This is a risk relates to laws protection problem. It may impact on enterprise rights and interests sometimes. Cloud customers should beware that it may be illegal things while definitely legal in another country under the same situation. For instance, European Union (EU) and US country have a big difference in laws. In EU the policy is the way much more stricter, which means legal affairs in US may be totally illegal in EU [23]. That will be a risk until the global regulatory standards come out.

3.5. Measurability Problems

This is a risk relates to business profit and business auditing.

12. Metering & Billing Error: Cloud as a service for cloud users, you should exchange it at equal values. That means there is a risk not only about the service quality itself but also on business level. Like the mobile phone bill, cloud services also charge you as you use. There can be many parameters to determine this, such as time and traffic. Different companies may have different charging model, but vulnerabilities regarding the manipulation of metering/billing data or billing evasion [20] definitely inflict a serious financial risk. Metering & Billing Error will bring impact both on the cloud customer side and also the provider side. It can cause enormous economic losses to both side of cloud business.

4. Verification and Validation

In the IV part of this paper, we introduced and described the integrated risks table of cloud service, now let's verify and illustrate the meaning of integrated table in this section.

4.1. SLA Verification

A service-level agreement (SLA) is a part of a service contract, which defines the service's formal and origin from telecom operators since late 1980s [25]. SLA can be defined from a variety of disciplines, and different organizations have different definitions for crucial IT parameters. For cloud service, cloud's specific SLA serves as both the blueprint and warranty for cloud computing [26]. Some of articles analyzed SLA requirements in cloud area separately on a different service level (IaaS/PaaS/SaaS), such as "the considerations about cloud computing SLA" [32]. But what we need is the integrated requirements for cloud services.

"Cloud Computing Use Cases Whitepaper" Version 4.0 [27], posted by the Cloud Computing Use Cases Discussion Group, specifically described the SLA's requirements in cloud environment. The "Cases whitepaper" respectively listed 10 considerations and 14 requirements for SLA in cloud service as Table 2, Table 3 below:

Table 2. Considerations Summary

Consideration for SLAs
1 Business level objectives
2 Responsibilities of both parties
3 Business continuity/disaster recovery
4 Redundancy
5 Maintenance
6 Data location
7 Data seizure
8 Provider failure
9 Jurisdiction
10 Brokers and resellers

Table 3. Requirements Summary

Requirements for SLAs
1 Security
2 Data encryption
3 Privacy
4 Data retention, deletion
5 Hardware erasure, destruction
6 Regulatory compliance
7 Transparency
8 Certification
9 Performance definition
10 Monitoring
11 Auditability
12 Metrics
13 Providing a machine-readable SLA
14 Human interaction

Not all of them are related to security and risk problems, for example, some of them purely related to the quality of service. Through the description of each item, we choose the items which related to risk problems as Table 4 below:

Table 4. Selection of Risk Related Items

Risk related items	
Considerations for SLAs	2 Responsibilities of both parties
	3 Business continuity/disaster recovery
	5 Maintenance
	6 Data location
	7 Data seizure
	8 Provider failure
	9 Jurisdiction
	10 Brokers and resellers
Requirements for SLAs	1 Security
	2 Data encryption
	3 Privacy
	4 Data retention, deletion
	5 Hardware erasure, destruction
	6 Regulatory compliance
	7 Transparency
	9 Performance definition
	10 Monitoring
	11 Auditability

And Table 5 illustrates the mapping with the coverage of our integrated risks as below. It distinctly shows that integrated risks covered all risk requirements in SLA.

Table 5. Integrate Risks Mapping with SLA

Risk related items in cloud's SLA	Related integrated risk number
✓ Responsibilities of both parties	Compliance problem: No.10
✓ Business continuity/disaster recovery	Data problem: No.8
✓ Maintenance	Data problem: No.8. No.9
✓ Data location	Compliance problem: No.11
✓ Data seizure	Data problem: No.8
✓ Provider failure	Data problem: No.8; Measurability problem: No.12
✓ Jurisdiction	Compliance problem: No.11
✓ Brokers and resellers	Trust problem: No.6
✓ Security	All Technology problem & Trust problem & Data problem
✓ Data encryption	Technology problem: No.2; Data problem: No.7
✓ Privacy	Technology problem: No.2; Trust problem: No.5; Data problem: No.7, No.8
✓ Data retention, deletion	Data problem: No.7, No.8
✓ Hardware erasure, destruction	Trust problem: No.5; Data problem: No.8
✓ Regulatory compliance	Compliance problem: No.10
✓ Transparency	Trust problem: No.5, No.6
✓ Performance definition	Trust problem: No.5, No.6
✓ Monitoring	Trust problem: No.5, No.6
✓ Auditability	Trust problem: No.5, No.6

4.2. Instance Verification

As we mentioned in the second section, Microsoft is a predominant enterprise in cloud area, and it can be proved by the figure named "cloud computing market penetration" [33]. A study on the connection between Microsoft's cloud problem concerns and the integrated risks table can be a validation for our work. Figure4 illustrate the main control domains in cloud service of Microsoft enterprise [28].

Figure 4. Microsoft Cloud Control Domains [28]

There are 15 domains in Microsoft's cloud control, and they gave the description of every domain. According to these descriptions, we can figure out which kinds of risk refer to each domain as mapping Table 6 below. And through the comparison, not only illustrates that the integrated risks covered all Microsoft cloud control domains, but also figures out that integrated risks is more relevant with instance control domains compared with SLA requirements.

Table 6. Integrated Risks Mapping with Microsoft Cloud Service Control Domains

Microsoft cloud control domains	Related integrated risk number
1 Identity	All technology problems
2 Authentication	All technology problems
3 Authorization	All technology problems
4 Auditing	Technology problem: No.2; Trust problem: No.5, No.6; Measurability problem: No.12
5 Segmentation	Technology problem: No.2; Compliance problem: No.11
6 Data protection	Technology problem: No.2 & All data problems
7 Application security	Technology problem: No.3; Data problem: No.8
8 Security machine health management	Technology problem: No.3; Data problem: No.8, No.9
9 Compliance assessment	Trust problem: No.5, No.6
10 Business continuity/disaster recovery	Data problem: No.8
11 Incident response & Communication	Trust problem: No.6; Data problem: No.8
12 Key management	All technology problems & Data problem: No.7
13 Anomaly detection & Monitoring	All technology problems & Data problem: No.7
14 Physical security	Trust problem: No.5; Data problem: No.8
15 Non-technical	All trust problems & Compliance problem: No.10

5. Conclusion

This paper through an array of review and study on the existed literatures, finds the key factors of every risk in cloud service, classifies the risks based on these key factors and presents an integrated risks table in cloud computing area.

Since the cloud computing area is still at a growth stage, so the problems or risks just can be gleaned from reported experiences of early adopters or researchers. Although we present a integrated risks table, but 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. Cloud service, when you stand on a business level, seeking for the solution or countermeasure of the risk reduction is nothing but for the business profit and business continuity. Connecting with business model, such as BMIS [29], 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] A. Huth and J. Cebula, "The Basics of Cloud Computing" US-CERT, **(2011).**
[2] CSA homepage, available at: https://cloudsecurityalliance.org/about/.
[3] Wikipedia, http://en.wikipedia.org/wiki/European_Network_and_Information_Security_Agency.
[4] OWASP Co., available at: https://www.owasp.org/index.php/Main_Page.
[5] D. Vohradsky, "Cloud Risk—10 Principles and a Framework for Assessment", ISACA Journal, vol. 5, **(2012)**.
[6] Wikipedia, available at: http://en.wikipedia.orgwiki/Cloud_computing.
[7] Y. Jadeja and K. Modi, "Cloud Computing-Concepts, Architecture and Challenges", **(2012)**.
[8] National Institute of Standards and Technology, "The NIST Definition of Cloud Computing- Special Publication 800-14", **(2011)**.
[9] Cloud computing basics, available at: http://www.south.cattelecom.com/Technologies/CloudComputing/0071626948_chap01.pdf.
[10] Y. Kadam, "Security Issues in Cloud computing A Transparent View", **(2011)**.
[11] Wikipedia, available at: http://en.wikipedia.org/wiki/Application_programming_interface_key.
[12] R. 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.
[13] W. A. Jansen (NIST),"Cloud Hooks: Security and Privacy Issues in Cloud Computing", **(2011)**.
[14] J. Brodkin, "Gartner: Seven cloud-computing security risks", available at: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.
[15] D. 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/.
[16] CSA, "Top Threats to Cloud Computing V1.0", **(2010),**
[17] http://en.wikipedia.org/wiki/Man-in-the-middle_attack,
[18] Wikipedia, available at: http://en.wikipedia.org/wiki/Federated_identity,
[19] Wikipedia, available at: http://en.wikipedia.org/wiki/Information_security#cite_note-2,
[20] Vadym Mukhin, Artem Volokyta, "Security Risk Analysis for Cloud Computing", **(2011)**.
[21] Wikipedia, available at: http://en.wikipedia.org/wiki/Patch_(computing).
[22] R. Marshall, "IT industry in vital need of cloud computing security standards", **(2012)**, available at: http://www.v3.co.uk/v3-uk/news/2207958/it-industry-in-vital-need-of-cloud-computing-security-standards.
[23] S. B. Chebrolu, V. Bansal and P. Telang, "Top 10 Cloud Risks That Will Keep You Awake at Night", CSICO, available at: https://www.owasp.org/images/4/47/Cloud-Top10-Security-Risks.pdf.
[24] D. Jones, "Some common data migration risks (and how to avoid them)", available at: http://www.dataroundtable.com/?p=1025, **(2009)**.
[25] Wikipedia, available at http://en.wikipedia.org/wiki/Service-level_agreement#Service_level_agreements_at_different_levels.
[26] A. L. Diaz, "Service Level Agreements in the Cloud: Who cares?" **(2011)**, available at: http://www.wired.com/insights/2011/12/service-level-agreements-in-the-cloud-who-cares/.
[27] Cloud Computing Use Cases Discussion Group, "Cloud Computing Use Cases Whitepaper Version 4.0", **(2010)**.
[28] Y. Li, "Security & Standards in the Cloud. Building trust through openness and interoperability in the Cloud", **(2012)**, available at: http://www.cio-online.com/evenement/documents/document_88.pdf.
[29] ISACA, "Business Model for Information Security", **(2009)**.
[30] J. -K. Yun, J. -H. Jang and K. -D. Moon, "Development of the real-sense media broadcasting service system based on the SMMD", Digest of Technical Papers - IEEE International Conference on Consumer Electronics, **(2011)**, pp. 435-436.
[31] D. S Caplan, "Bankruptcy in the Cloud: Effects of Bankruptcy by a Cloud Services Provider", **(2012)**.
[32] S. -H. Song, "The considerations about cloud computing SLA", **(2012)**.
[33] S. K. B. Tammaiah, "Cloud Computing Data Security Internet and Web System2-Term Paper", **(2012)**.