HAL
archives-ouvertes.fr

In Cloud We Trust: Risk-Assessment-as-a-Service

Marianthi Theoharidou, Nikolaos Tsalis, Dimitris Gritzalis

▶ **To cite this version:**

Marianthi Theoharidou, Nikolaos Tsalis, Dimitris Gritzalis. In Cloud We Trust: Risk-Assessment-as-a-Service. Carmen Fernández-Gago; Fabio Martinelli; Siani Pearson; Isaac Agudo. 7th Trust Management (TM), Jun 2013, Malaga, Spain. Springer, IFIP Advances in Information and Communication Technology, AICT-401, pp.100-110, 2013, Trust Management VII. <10.1007/978-3-642-38323-6_7>. <hal-01468186>

HAL Id: hal-01468186
https://hal.inria.fr/hal-01468186

Submitted on 15 Feb 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

In Cloud we Trust: Risk-Assessment-as-a-Service

Marianthi **Theoharidou**, Nikolaos **Tsalis**, Dimitris **Gritzalis**

Information Security & Critical Infrastructure Protection Research Laboratory
Dept. of Informatics, Athens University of Economics & Business (AUEB)
76 Patission Ave., Athens GR-10434, Greece
{mtheohar, ntsalis, dgrit}@aueb.gr

Abstract. Cloud computing is an emerging paradigm that allows adoption of on-demand services in a cost-effective way. Migrating services to the Cloud also means been exposed to new threats and vulnerabilities, thus, resulting in a modified assessment of risk. Assessing risk in the Cloud remains an open research issue, as it requires a given level of trust of the Cloud service provider for providing assessment data and implementing controls. This paper surveys existing knowledge, regarding risk assessment for the Cloud, and highlights the requirements for the design of a cloud-targeted method that is offered as a service, which is also in compliance with the specific characteristics of the Cloud.

Keywords: Cloud, Risk Assessment, Risk, Threat, Vulnerability, Trust.

1 Introduction

Cloud computing enables cost-effective adoption of on-demand services, coupled with elastic allocation and virtualization of resources (e.g., servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Along with these benefits, the decision to deploy to the Cloud is affected by the security challenges introduced [2-4]. These include the lack of control over security management on a cloud deployment, multi-tenancy and sharing of resources, concerns on data confidentiality and privacy, as well as the lack of trust towards the provider or other co-tenants, who may share unknown risk profiles.

Establishing a level of trust about a cloud service depends on the degree of control on the provider who will provide the required security controls in an effective manner [4]. Note that assessing the effectiveness of security controls may not be feasible. If the level of trust in the service, or in the provider, is low or cannot be assessed, this may affect the adoption of the services or lead to accepting a higher level of risk.

Nowadays, cloud computing still lacks standardized information security frameworks, which applies to risk assessment as well. This is common when new platforms, which require tailor-made methodologies, emerge, e.g. smartphones [5-6]. Thus, although cloud-specific threats and vulnerabilities have already been identified or assessed by numerous sources [2,7-13], it still remains unclear how Information Risk Management frameworks or methods can be applied in the context of the Cloud.

For the purposes of this paper, we will refer to *Risk* as the measure of the extent to which an entity is threatened by a potential circumstance or event. Risk is typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence [14]. *Risk assessment* (ISO27005 standard) consists of: (a) *Risk analysis* comprising of risk identification and risk estimation, and (b) *Risk evaluation* [15]. Similarly the NIST 800-30 (rev.1) [14] describes risk assessment as "the process of identifying, prioritizing, and estimating information security risks". A similar to ISO27005 approach is also recommended by the CSA [16].

Assessing information security risk for cloud deployments requires a thorough analysis of threat and vulnerability information, so as to determine the extent to which circumstances or events could adversely impact an organization and the likelihood of such circumstances occurring [14]. These circumstances may vary or change when we adopt one of the three generic cloud service models (designs) [1]: *Software as a Service* (SaaS), *Platform as a Service* (PaaS), *Infrastructure as a Service* (IaaS). The way that clients deploy data or services into the cloud, as well as the visibility included, separates the cloud into four different deployment models [1]: *Private*, *Community*, *Public*, or *Hybrid*. The level of control on the cloud deployment decreases as we move from private to public clouds, posing obstacles in risk treatment. Also, the level of trust decreases, which makes risk assessment an even more challenging process.

This paper first surveys existing knowledge regarding risk assessment for cloud deployments. Then, it highlights the requirements for a targeted method that complies with the specific characteristics of the cloud and quantifies these security concerns.

The paper is structured as follows: Section 2 presents an extended list of cloud-specific threats, coupled with vulnerabilities (i.e., one of the differentiating elements if we adopt any traditional risk assessment method). Section 3 offers an analysis on the parameters that change when we assess risk on the cloud, and reviews existing approaches and their limitations. Section 4 proposes the deployment of risk assessment on the cloud as a service, and discusses the challenges and applicability of such an endeavor. Section 5 concludes the paper, summarizing the requirements for cloud risk assessment, coupled with a short roadmap for future work.

2 CLOUD COMPUTING: A SECURITY PERSPECTIVE

Cloud faces some of the threats applicable to any type of information systems. At the same time, it faces unique threats and vulnerabilities, which can affect both clients and providers. The Cloud Security Alliance identifies the following potential threats and vulnerabilities as more significant [3]: (1) Abuse and Nefarious Use of Cloud

Computing, (2) Insecure Interfaces and API, (3) Malicious Insiders, (4) Shared Technology Issues, (5) Data Loss or Leakage, (6) Account or Service Hijacking, and (7) Unknown Risk Profile.

These threats and vulnerabilities indicate that when an organization chooses to adopt cloud services, the risk profile of its information systems is modified. Data and services are exposed to new attack scenarios, which can be facilitated by vulnerabilities of the cloud provider (employees, facilities, systems), of the cloud technology (interfaces, API) or even other cloud co-tenants.

In Tables 1-3, we present an improved and combined list of threats applicable to a cloud deployment, based on various sources [2,8,10,17]. Each threat is mapped to indicative examples of vulnerabilities, which - if present - can facilitate its occurrence. We also present the security attribute affected by each threat, i.e., Confidentiality (C), Integrity (I), and Availability (A). The threats are presented grouped in categories according to the components of the information system that is mainly affected. One can observe that there are threats that have business implications as well. In Table 3, we refer to them as 'organizational' threats.

Note that although several of these threats can be applicable to most non-cloud systems, we identify unique vulnerabilities in the cloud, which do not apply to traditional systems, e.g. the loss of physical control, the unknown risk profile of the provider, multi-tenancy, and others. These threats may potentially affect all the available services (SaaS, PaaS, IaaS) and models (Private, Public, Community, Hybrid), but the level of vulnerability may vary accordingly.

Table 1. Network-related Cloud Threats

Threat	Vulnerability	C	I	A
T1. Malicious probes or scans	▪ Open ports ▪ Unavailable or misconfigured IDS	✓		
T2. Cross - VM attack via side channels	▪ Multi-tenancy	✓	✓	✓
T3. Data leakage on up/download, intra-cloud T4. Man-in-the-Middle	▪ Communication encryption vulnerabilities ▪ Weak authentication mechanism ▪ Poor patch management	✓	✓	✓
T5. Denial of Service	▪ Poor system configuration ▪ Inadequate resource filtering ▪ Weak policies for resource capping			✓
T6. Flooding attack via bandwidth starvation T7. Fraudulent resource consumption attack	▪ Bandwidth Under-provisioning ▪ Exploitation of the Cloud Pricing Model			✓
T8. Cross-site scripting	▪ Insertion of unchecked data in restricted system locations ▪ Lack of monitoring mechanism	✓	✓	✓
T9. Cross-site request forgery	▪ Weak authentication or monitoring mechanism ▪ Insertion of unauthorized commands in the browser	✓	✓	✓
T10. Cookie manipulation	▪ Lack of hashes to protect the cookie ▪ Weak encryption mechanism	✓	✓	✓
T11. Cookie replay attack	▪ Insecure system databases ▪ Lack of timestamp	✓	✓	

Table 2. System or Data-oriented Cloud Threats

Threat	Vulnerability	C	I	A
T12. Brute force attacks T13. Dictionary attacks T14. Privilege escalation	▪ Weak password policy ▪ Weak encryption or authentication	✓	✓	✓
T15. Buffer overflows	▪ Application vulnerabilities	✓	✓	✓
T16. Management interface compromise	▪ Remote access ▪ System or OS vulnerabilities ▪ Application vulnerabilities or poor patch management	✓	✓	✓
T17. File system or registry tampering	▪ Poor management of privilege distribution ▪ Weak protection mechanism	✓	✓	✓
T18. Service engine compromise	▪ Hypervisor vulnerabilities ▪ Lack of resource isolation	✓	✓	✓
T19. Dishonest computation in remote servers	▪ Loss of physical control of data and applications		✓	
T20. Connection pooling	▪ Weak authentication	✓	✓	✓
T21. Physical threats (theft, vandalism, etc.)	▪ Unreachable data storage location ▪ Weak physical security measures ▪ Unknown risk profile	✓	✓	✓
T22. Data disclosure/Leakage/Insider threat	▪ Weak encryption or authentication ▪ Insiders on the provider side	✓		
T23. Data loss/Manipulation	▪ Loss of physical control of the data ▪ Poor integrity or backup controls		✓	✓

Table 3. Organizational Cloud Threats

Threat	Vulnerability	C	I	A
T24. Loss of governance	▪ Unclear roles and responsibilities ▪ SLA clauses with conflicting promises to stakeholders ▪ Audit or certification not available to customers ▪ No control on vulnerability assessment process ▪ Certification schemes not adapted to the cloud ▪ Lack of information on jurisdictions ▪ Lack of completeness and transparency in terms of use	✓	✓	✓
T25. Lock-in	▪ Poor provider selection ▪ Lack of supplier redundancy ▪ Lack of completeness and transparency in terms of use			✓
T26. Non-compliance	▪ Audit or certification not available to customers ▪ Lack of standard technologies and solutions ▪ Certification schemes not adapted to the cloud ▪ Lack of information on jurisdictions ▪ Lack of completeness and transparency in terms of use	✓	✓	
T27. Service termination or failure	▪ Poor provider selection ▪ Lack of supplier redundancy			✓
T28. Supply chain failure	▪ Cross-cloud applications creating hidden dependency ▪ Poor provider selection ▪ Lack of supplier redundancy	✓		✓
T29. Conflicts between customer hardening procedures and cloud environment	▪ Lack of completeness and transparency in terms of use ▪ SLA clauses with conflicting promises to stakeholders ▪ Unclear roles and responsibilities	✓		✓

Any traditional risk assessment method requires statistical or real-time data in order to assess the likelihood of these threats. It also requires appropriate tools in order to identify the presence of vulnerabilities or the absence/ineffectiveness of controls. This means that current approaches need to incorporate an extended set of threats and vulnerabilities in their assessments. The question is if this step is sufficient when we assess risk on the cloud.

3 ASSESSING RISK ON THE CLOUD

Before migrating assets to the cloud, the risk of such a business decision needs to be estimated. Existing algorithms treat the project as an outsourcing one, where different services are offered by different providers [18]. From a business perspective, the decision can rely on economic terms. For example, there is an approach which relies on pricing theory in order to identify the optimal rule of migrating to the cloud [19]. Another one quantifies cost, security, and business parameters for different cloud providers [20].

Overall, it seems hard to determine how each of these approaches can be applied in a realistic setting, and whether the required information is available and accurate. The problem is, in its essence, a matter of trust to the data provided by the various cloud providers, regarding the security of their services.

Following the migration to the cloud, an organization will still require to perform risk assessment for its systems, as required by legislation, standards, and best practices. Assessing risk in dynamic, complex and, in some cases, unknown environments [16], such as the cloud, poses additional challenges.

Traditional information risk assessment approaches, such as CRAMM, OCTAVE, etc., can hardly address these challenges. The lack of a novel approach is highlighted by the authors of [21], who stress the need for dynamic (or even real-time) risk management, when we refer to the cloud, and place their focus on SLA and exception management. They also highlight that the proposed method should be cloud-oriented, and accompanied by new modeling languages and tools as well.

In [22], properties of the cloud environment which affect the risk assessment process are presented. These are:

- On-demand-self-service: Cloud environments rely heavily on automated procedures. This also applies to security controls. The effect on risk, when trained personnel are replaced by automated processes, needs to be assessed. Vulnerabilities posed by individuals are now translated into technical ones.
- Broad network access: The available entry points, from an attacker's perspective, create a dynamic collection of end points with different characteristics and properties. Such an alternation poses a challenge to the deployment of a traditionally implemented assessment methodology.
- Resource pooling: The existing dynamic allocation of resources does not allow proactive assessment. So, it only has to be focused on the allocation mechanisms and the qualities of the overall pool. Furthermore, multi-tenancy must also be taken into consideration, as other clients/tenants may co-exist within the same infrastruc-

ture. Finally, the unknown location of the physical resources of the cloud is another element that needs to be addressed during the procedure, as it may lead to legal or regulatory non-compliance.

- Rapid elasticity: The workload of a client can easily migrate to several cloud providers, not specified from the beginning. As a result, the cloud assessment model must consider multiple computing environments, which have different properties and functions, and thus, varying levels of risk.
- Measured service: The property of automatically controlling and optimizing the resource use in the cloud can easily pose as a point of vulnerability. The information that relies on each specific tenant must be well protected from a possible disclosure, while such an observation must be applied in the implementation of the risk assessment framework.

The static nature of risk assessments, which are typically performed on a per-system basis, makes them unsuitable for the cloud environment. The above properties highlight the need for designing new methods for risk assessment, which will not only assess new threat scenarios applicable to the cloud, but will also be able to model and capture its dynamic nature and lack of clearly-defined boundaries [21-23].

Research towards such a direction is still in its infancy; however, some initial attempts, both theoretical and practical, were identified in the literature. An initial attempt to assess various cloud risks, with an approach compliant to ISO27005, is presented by [2]. However, the threat likelihood and impact assessments depend on both expert opinions and a single use case scenario. The report can be viewed as guidance to cloud providers and customers, while the method will require further refinements in order to be applied to a specific system or organization.

A framework that is based on the standard quality management cycle (Plan-Do-Check-Act) of the ISO/IEC 27001 standards is proposed by [24]. It focuses on managing risk via seven individual processes, each assigned to a phase of the management cycle. The proposed model is a risk management framework and includes a risk assessment procedure within its steps.

More specifically, risk assessment is performed on the second phase (DO), which is deployed via the use of the OCTAVE and COBRA models for analyzing and assessing the existing threats of the cloud infrastructure. This framework clearly outlines the majority of the security elements of the cloud, but the traditional tools and methods used, need to be modified according to the new infrastructure that they intend to assess (i.e., the Cloud). Such an observation gives birth to the need of using techniques that are either implemented specifically for cloud computing environments, or existing ones with significant modifications, since there are noticeable differences compared to traditional computing environments.

A model for quantitative risk assessment in the cloud is presented in [17]. The model requires the definition of the cloud environment and then proceeds to assess the value of assets and threat likelihood, vulnerability, and impact, in order to assess risk. To be more specific, it quantifies risk by following the current best practice approach. In contrast, although threats and vulnerabilities are cloud-oriented, the model does not

provide insight on how the assets of the system can be accurately assessed in the cloud, or how statistical data can be acquired, when multiple providers are involved.

In [25] a semi-quantitative risk assessment framework is presented; risk is assessed in terms of impact and probability of an event. The framework relies on statistical data for the assessment of likelihood and on expert opinion for impact assessment. Furthermore, the applicability of the method relies on (a) the availability and accuracy of statistical data collected by cloud providers, and (b) the definition of an extended threat list, as the one presented appears to be limited.

The use of Attack-Defense trees approach is proposed by [26] as a means of threat analysis for cloud computing environments. The Attack-Defense trees depict attack steps and vulnerabilities, as well as defense mechanisms, i.e. countermeasures. The method assesses the required defense cost, based on cost of the attack, probability of success and impact. The applicability of the model relies on both the presence of accurate statistical data (for probability), as well as the selection of a proper defense strategy.

Based on the above, the existing approaches justify the need of integrating the risk assessment method into the cloud computing model [16]. Cloud, as every other deployment infrastructure, needs to be assessed by examining applicable, as well as novel threat and vulnerability scenarios, e.g. the threats posed due to multi-tenancy.

Furthermore, we observe that any risk assessment approach in the cloud not only faces the typical challenges of risk assessment, such as lack of appropriate statistical data and subjectivity of assessments, but additional ones as well. These include (a) the lack of trust to the cloud provider and to the data provided for risk assessment, (b) the absence of a well-defined system topology, (c) the dynamic nature of both the infrastructure and the services provided, and (d) the lack of physical control.

As a result, a holistic approach is needed so as to address the above mentioned challenges. Such a method should include assessment tools, methods and approaches, all equally adjusted to the dynamic structure of the cloud.

4 Risk-Assessment-as-a-Service

Such a risk assessment method can be implemented in the form of a cloud service, which includes methodological assumptions and steps, a framework, tools, and new rules and policies for risk management. An extension to the cloud model is referred to in the literature in the form of two services, i.e. Security-as-a-Service [27-28], and Risk-Assessment-as-a-Service [22].

A theoretical implementation of Security-as-a-Service (SECaaS) can be found in [27]. The idea refers to offering cloud-oriented countermeasures as services by a different cloud provider. This model could be applied on all the deployment models and allow customers and providers to assess and monitor the security of their cloud deployments. The authors suggest services regarding access control, auditing, risk assessment, intrusion detection, etc. In that way, all the necessary services/controls are combined into one service, which is positioned over the cloud infrastructure.

Experimental results of Security-as-a-Service using unified threat management (UTM) for ensuring secured services on the cloud are available in [28]. These results highlight the concern that UTM may not be a feasible approach, as it may prove to be a bottleneck for the application clouds, which is contrary to the requirement for resources-on-demand and high elasticity. These issues can easily be translated into additional cost for the users. Additionally, vulnerabilities found in the cloud deployments will be out of the UTM cloud's control.

In [22], a model is proposed regarding deploying Risk-Assessment-as-a-Service (RAaaS) to either the clients or the provider. Such a model should be deployed on a real-time basis on the tenants, applications, and the entire infrastructure of the cloud. It focuses on providing the assessment service for every consumer and provider in the cloud, where everyone can assess a possible cloud service before migrating personal data and applications onto it. As a result, the party that deploys the assessment procedure can perform an informed decision to trust a specific or several cloud providers.

Similar to the limited SECaaS models found in the literature, [20] remains a theoretical deployment model. The issues discussed focus on the deployment of the service as an autonomic system, the necessary sensors for collecting real-time data, Service-Level Agreements (SLA), a suitable scoring method, existing official standards, as well as how to deploy policies to current cloud deployments.

Based on the above, RAaaS seems to be a suitable way to implement a cloud-tailored method, but the implementation specifics still remain open to research. Risk-Assessment-as-a-Service could be an approach suitable to this particular environment, but it should be implemented in a way that it will not serve as a bottleneck. Furthermore, the requirements of implementing RAaaS are as follows:

- *Dynamic and continuous collection of accurate (trusted), real-time data*, for specific deployments, tenants, and assets.
- Based on comprehensive *qualitative and quantitative metrics*, targeted to a cloud environment.
- Supported by a *knowledge base* (e.g. ontologies [29]) that cumulates the knowledge by public available resources (e.g. for the collection of statistical data) and *modeling tools* in order to mitigate applicable threat or attack scenarios.

The method should allow for the creation of various risk profiles, according to: (a) the services or assets deployed to the cloud, (b) the selected provider, and (c) the specific type of deployment. Of course, such a method could be implemented in a traditional, static way, "off" the cloud.

The benefits of implementing it "as-a-service" lie on the ability to follow the on-demand, automated, and multi-tenant architecture of the cloud, where tenants and providers change constantly. Thus, it offers a continuous and dynamic assessment of the cloud environment, with respect to a given tenant. It also offers a specific application for use by new tenants and applications. Furthermore, the "as-a-Service" approach would be more cost effective, since issues of licensing, deploying and updating the method are adequately facilitated.

5 Conclusions

Cloud computing poses new challenges regarding risk assessment. These include the assessment of a dynamic environment, with loose boundaries, as well as an unknown risk profile that is affected by new threats and adversaries and originates from multiple points (e.g., the provider, the technology itself, other co-tenants, etc.). Such assessments incorporate a level of trust on the notion that several, interchanging third parties will deliver secure services.

In this paper, we have presented the factors that modify risk when mitigating to the Cloud, as well as a list of threats which are cloud-oriented. Such a list can further be expanded in order to cover all domains of information security when we refer to the cloud [30].

We studied the few current approaches that focus on cloud risk assessment. These frameworks could pose as a theoretical starting point for risk assessment on the cloud; yet, they lack implementation and experimental results. Most of these approaches inherit common risk assessment drawbacks, such as the lack of historic or statistic data, the subjectivity or the static nature of results, etc. These flaws are augmented in the cloud environment, which transforms the risk management process towards Security SLA management.

In the future, we plan to build upon our experience and knowhow with critical ICT infrastructures protection, as well as risk management methods [31-35], so as to develop a method suitable for a Risk-Assessment-as-a-Service solution, considering Cloud as a potentially critical ICT infrastructure.

One of the first next steps is to define risk assessment criteria suitable for the cloud client and the cloud provider. We also plan to refine the threat lists presented in this paper, according to the adopted cloud deployment and services, and examine whether some threats are more significant in particular models.

Acknowledgements

This work was performed in the framework of and partially funded by the Hellenic General Secretariat for Research & Technology, under SOLO (56NEW-B-2012) project). M. Theoharidou was supported by a Postdoctoral Fellowship Grant funded by Athens University of Economics and Business, Greece.

References

1. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. NIST SP-800-145 (2011)
2. Catteddu, D., Hogben, G. (Eds.): Cloud Computing: Benefits, risks and recommendations for information security. ENISA (2009)
3. CSA: Top Threats to Cloud Computing v1.0. Cloud Security Alliance (2010)
4. Grance, T., Jansen, W.: Guidelines on Security and Privacy in Public Cloud Computing. NIST SP-800-144 (2011)

5. Theoharidou, M., Mylonas, A., Gritzalis, D.: A risk assessment method for smartphones. In: Proc. of the 27th IFIP International Information Security and Privacy Conference, pp. 428-440, Springer (AICT 267), Greece (2012)
6. Mylonas A., Kastania A., Gritzalis D.: Delegate the smartphone user? Security awareness in smartphone platforms. Computers & Security. 32(3):xx-xx (2013)
7. Dahbur, K., Mohammad, B., Tarakji, A.B.: A survey of risks, threats and vulnerabilities in cloud computing. In: Proc. of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, pp.1-6 (2011)
8. Chhabra, B., Taneja, B.: Cloud Computing: Towards Risk Assessment. In: Mantri A. et al. (Eds.): (HPAGC 2011), CCIS 169, pp. 84–91 (2011)
9. Carroll, M., van der Merwe, A., Kotze, P.: Secure cloud computing: Benefits, risks and controls. In: Information Security South Africa (ISSA) (2011)
10. Xiao, Z., Xiao, Y.: Security and Privacy in Cloud Computing. IEEE Communications Surveys & Tutorials, (to appear) (2013)
11. Tsai, H.Y., Siebenhaar, M., Miede, A., Huang, Y., Steinmetz, R.: Threat as a Service?: Virtualization's impact on Cloud security. IT Professional. 14(1): 32-37 (2012)
12. Luo, X., Yang, L., Ma, L., Chu, S., Dai, H.: Virtualization security risks and solutions of Cloud Computing via divide-conquer strategy. In: Proc. of the 3rd International Conference on Multimedia Information Networking and Security (MINES), pp. 637-641 (2011)
13. Srinivasan, M., Sarukesi, K., Rodrigues, P., Manoj, S., Revathy, A.: State-of-the-art cloud computing security taxonomies: A classification of security challenges in the present cloud computing environment. In: Proc. of the International Conference on Advances in Computing, Communications and Informatics, pp. 470-476 (2012)
14. NIST. Guide for Conducting Risk Assessments. NIST SP-800-30, Rev.1 (2012)
15. ISO/IEC. Information technology - Security techniques - Information security risk management. ISO/IEC27005:2011, 2nd edition (2011)
16. Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing. http://www.cloudsecurityalliance.org/guidance/
17. Wang, H., Liu, F., Liu, H.: A method of the Cloud Computing security management risk assessment. In: Zeng (Ed.) Advances in Computer Science and Engineering, AISC 141, pp. 609-618 (2012)
18. Martens, B., Teuteberg, F.: Decision-making in cloud computing environments: A cost and risk based approach. Information System Frontiers. 14:871-893 (2012)
19. Kantarcioglu, M., Bensoussan, A., SingRu, H.: Impact of security risks on cloud computing adoption. In: Proc. of the 49th Annual Allerton Conference on Communication, Control, and Computing, pp. 670-674 (2011)
20. Johnson, B., Qu, Y.: A Holistic model for making Cloud migration decision: A consideration of security, architecture and business economics. In: Proc. of the IEEE 10th International Symposium on Parallel and Distributed Processing with Applications, pp. 435-441 (2012)
21. Morin, J., Aubert, J., Gateau, B.: Towards Cloud Computing SLA Risk Management: Issues and Challenges. In: Proc. of the 45th Hawaii International Conference on System Science (HICSS), pp. 5509-5514 (2012)
22. Kaliski, B., Pauley, W.: Toward risk assessment as a service in cloud environments. In: Proc. of the 2nd USENIX Conference on Hot Topics in Cloud Computing (2010)
23. Mazur, S., Blasch, E., Chen, Y., Skormin, V.: Mitigating Cloud Computing security risks using a self-monitoring defensive scheme. In: Proc. of the 2011 IEEE National Aerospace and Electronics Conference, pp. 39-45 (2011)

24. Zhang, X., Wuwong, N., Li, H., Zhang, X. Information security risk management framework for the Cloud Computing environments. In: Proc. of the IEEE 10th International Conference on Computer and Information Technology, pp. 1328-1334 (2010)
25. Saripalli, P., Walters, B.: QUIRC: A Quantitative impact and risk assessment framework for Cloud Security. In: Proc. of the IEEE 3rd International Conference on Cloud Computing, pp. 280-288 (2010)
26. Wang, P., Lin, W., Kuo, P., Lin, H., Wang, T.: Threat risk analysis for cloud security based on Attack-Defense Trees. In: Proc. of the 8th International Conference on Computing Technology & Information Management, pp. 106 -111 (2012)
27. Hussain, M., Abdulsalam, H.: SECaaS: Security as a service for cloud-based applications. In: Proc. of the 2nd Kuwait Conference on e-Services and e-Systems, pp. 1-4 (2011)
28. Al-Aqrabi, H., Liu, L., Xu, J., Hill, R., Antonopoulos, N., Zhan, Y.: Investigation of IT security and compliance challenges in Security-as-a-Service for Cloud Computing. In: Proc. of the 15th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops, pp. 124-129 (2012)
29. Dritsas, S., Tsoumas, B., Dritsou, V., Konstantopoulos, P., Gritzalis, D.: OntoSPIT: SPIT Management through Ontologies. Computer Communications. 32(2):203-212 (2009)
30. Theoharidou, M., Gritzalis, D.: A Common Body of Knowledge for Information Security. IEEE Security & Privacy. 5(2):64-67 (2007)
31. Kotzanikolaou P., Theoharidou M., Gritzalis D.: Accessing n-order dependencies between critical infrastructures. In: International Journal of Critical Infrastructure Protection. 9(1-2):93-110 (2013)
32. Theoharidou M., Kotzanikolaou P., Gritzalis D.: Risk assessment methodology for interdependent Critical Infrastructures. In: International Journal of Risk Assessment and Management. 15(2-3):128-148 (2011)
33. Theoharidou M., Kotzanikolaou P., Gritzalis D.: A multi-layer criticality assessment methodology based on interdependencies. In: Computers & Security. 29(6):643-658 (2010)
34. Kotzanikolaou P., Theoharidou M., Gritzalis D.: Cascading effects of common-cause failures on Critical Infrastructures. In: Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection, Springer, USA (2013)
35. Dritsas S., Mallios J., Theoharidou M., Marias G., Gritzalis D.: Threat analysis of the Session Initiation Protocol, regarding spam. In: Proc. of the 3rd IEEE International Workshop on Information Assurance, pp. 426-433, IEEE Press, USA (2007)