Cloud Computing Security Requirements: a Systematic Review

Iliana Iankoulova
University of Twente
School of Management and Governance
Drinerlolaan 5, 7522 AE Enschede, The Netherlands

Maya Daneva
University of Twente
Dept. of Computer Science
Drienerlolaan 5, 7522 AE Enschede, The Netherlands

***Abstract*—Many publications have dealt with various types of security requirements in cloud computing but not all types have been explored in sufficient depth. It is also hard to understand which types of requirements have been under-researched and which are most investigated. This paper's goal is to provide a comprehensive and structured overview of cloud computing security requirements and solutions. We carried out a systematic review and identified security requirements from previous publications that we classified in nine sub-areas: Access Control, Attack/Harm Detection, Non-repudiation, Integrity, Security Auditing, Physical Protection, Privacy, Recovery, and Prosecution. We found that (i) the least researched sub-areas are non-repudiation, physical protection, recovery and prosecution, and that (ii) access control, integrity and auditability are the most researched sub-areas.**

Keywords-sequirity requirements engineering, cloud computing, Software-as-a-Service, empirical study, systematic literature review

I. INTRODUCTION

Cloud computing (CC) is not a specific technology, but a computing concept based on parallel computing, distributed computing and grid computing [1]. The CC business model implies two main actors that will be referred to in this work as a cloud service provider (CSP) and a cloud service user (CSU). The CSPs deliver applications via the internet, which are accessed from web browsers and desktops and mobile apps by the CSUs, while the business software and data are stored on servers at a remote location. Depending on the service level provided, three types of clouds are identifiable: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). For all three, security has been ranked as the greatest challenge [2]. Therefore it is important that more research is done on this topic. The goal of this paper is to provide a structured and systematic overview of the security requirements for cloud computing. Specifically, we intend to get a high level overview that can be used by researchers to quickly assess the current state of research in a given security sub-area and identify gaps for future research. For the purpose of this paper security is defined as the degree to which unauthorized and intentional harm to valuable system assets is detected and prevented [3]. We will investigate which security requirements have been identified and how can they be addressed. The focus will be on SaaS security which due to hierarchical relations also covers to a great extent security issues on the other two levels, IaaS (reviewed in [4] and [5]) and PaaS. The requirements discovered in the literature will be organized and presented in a framework. From the available frameworks (e.g. [3], [6]) we choose the one of Firesmith [3] who provides taxonomy of security sub-factors which can be used as a basis for organizing and identifying different kinds of security requirements. In what follows, Sect. 2 describes our review method. Sect. 3, explains the security requirements model, classifies the literature accordingly and provides a discussion of the findings. Sect. 5 describes the limitations of our work and Sect. 6 gives some concluding remarks.

II. REVIEW METHOD

This study set out to answer the following research questions (RQs): *(1) What cloud security requirements have been treated in the published literature? (2) What solutions are offered to them?* and *(3) Which cloud security requirements have been under-researched ?*

We used these RQs for determining the content and structure of the systematic review (SR), for designing strategies, for locating and selecting primary studies, for critically evaluating the studies, and for analyzing their results. In our SR process we followed some of the guidelines defined by Webster and Watson [7] and of Kitchenham et al [8]. Our literature review is concept-centric as it classifies and presents the publications according to the security area they address. In this section we set the boundaries of our work and the scope of the literature reviewed.

We selected Scopus as initial source because it contains publications from major journals and conference proceedings, which results in a diverse sample that is representative of the current state of the knowledge in the area of cloud computing security. The initial search in Scopus was on '*security AND ({software as a service} OR SaaS)'* in the article title, abstract or keywords. Later the search string was refined to also include materials with '*cloud AND security'* in the article title. This revision was done after manual review of some of the excluded articles by the initial search. Such publications

discuss security challenges for cloud computing in general and sometimes do not refer explicitly to SaaS. We want to underline that the composition of our search string is the result of a learning process including experimentation with a variety of combinations of key words in order to test synonyms used in literature and to cover the variety of cloud security requirements concepts. We have applied the following restrictions to define the boundaries of our study: (i) limit by source type (i.e. conference papers and journal articles), (ii) limit by publication year - before and including the first quarter of 2011, and (iii) limit by Scopus' subject area, i.e. Computer Science, Engineering or Business. The returned records by Scopus were 172 and we have made two interesting observations. First, about 66% of the articles were published in 2010 and 2011, which suggests that this is a fairly new and quickly developing area of research. Second, only 31 articles (approximately 18%) were from conferences on cloud computing or software security which indicates that cloud computing cannot yet be separated from other IS disciplines. The 172 articles were manually reviewed for relevance to our RQs. We consider as relevant all publications that comply with the following criteria:

Inclusion criteria: (1) Cloud computing security or SaaS security must be the major topic or one of the major topics of the publications, (2) Where multiple publications are reporting the same study only the most recent is selected.

Exclusion criteria: (1) Security models for very specific context (e.g. healthcare, national security, etc) are excluded from the study as we are interested in more general security requirements and solutions. (2) Publications that focus on security-as-a-service are excluded since this is a different type of service rather than security for clouds. (3)Journal articles that were not accessible online are excluded. (4) Journal articles that provide a professional perspective and opinions on cloud computing security without scientific references are excluded unless the reliability is ensured by other means e.g. statistical analysis. (5) Publications covering service level agreements (SLA) and multi-tenancy issues but not elaborating on the security clauses and requirements are excluded. (6) Publications focusing on security requirements but not explicitly focusing on cloud computing (e.g. security requirements for SOA, grids, etc) are excluded.

The relevance criteria were applied on the titles and the abstracts of the publications. Where it was not clear enough from the title and the abstract alone if the publication complied with the criteria the whole publication was scanned and then a decision for inclusion/exclusion was made. This process resulted in 55 publications included in the next research steps. Those are classified in a security requirements framework. We make the note that the application of the relevance criteria was done by the first author, while the second author randomly chose 10% of the papers and reviewed them for the purpose of ensuring internal validity. The second author worked in isolation from the first author, however when the second author compared her judgments with those of the first author, it was found that authors had arrived at the same conclusions regarding the inclusion/exclusion of the papers.

III. CLASSIFYING AND USING A MODEL FOR SECURITY REQUIREMENTS

As indicated earlier, we used the security model in [3] to analyze and classify the selected 55 studies. It consists of 9 sub-factors that identify different aspects of system security (Fig 1.). By dividing the security requirements into different groups, it is easy to identify areas that are under-researched and also will guide researchers in the state of the literature on a specific security area in the topic of cloud computing.

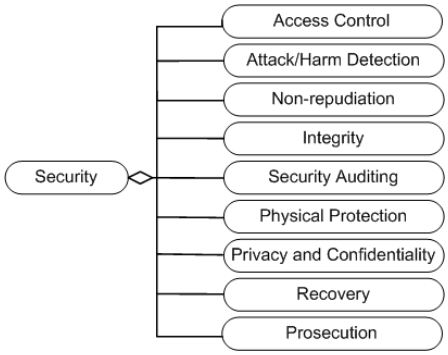

Figure 1. The taxonomy of security quality factors in [3].

Below, the different security sub-factors are explained and the 55 papers selected to be included in the review are classified as addressing requirements for one of the sub-factors. In some cases one paper can address two or more sub-factors. In the cases when 2 sub-factors are discussed the paper is placed in the category with the sub-factor that is the most elaborated upon. On the other hand when 3 or more sub-factors are covered and it is not easy to include in any of the categories, the paper is discussed in sub-section 3.G.

A. Access Control

This is the degree to which the system limits access to its resources only to authorized entities (e.g. human users, programs, processes, devices). Hence, access control security requirements address the need to recognize parties that want to interact with the system, making sure that the parties are who they say they are and giving them access only to the resources they are allowed to access. The various challenges and the current state authentication, and authorization of CSU accessing the cloud along with emerging Identity and Access Management (IAM) protocols and standards are described by Almulla and Yeun [9] and utilized by Sato et al. [10]. IAM are methods that provide an adequate level of protection for organization resources and data through rules and policies which are enforced on CSUs via various techniques such as enforcing login password, assigning privileges to the CSUs and provisioning CSU accounts. When defining the security requirements it could be helpful to use a model-driven approach that transforms the security intentions to enforceable security policies. Such approach is described by Zhou et al.

[11] and allows CSUs to specify the security intentions in system models that enable a simple specification of security requirements. Some of the requirements could be derived by using a 3D model [12] where the value of the data is first assessed and placed accordingly in nested 'protection rings'. An alternative model is the Security Access Control Service (SACS) [13] which includes Access Authorization (for those CSUs who want to request cloud services), Security API (that ensures safe use of the services after accessing the cloud), and Cloud Connection Security. Other approaches to threat mitigation is to use a combination of asymmetric and symmetric cryptography, and capability based access control [14], [15]. For example, in[14], the access to platform services is regulated based on the permissions encoded in cryptographic capability tokens, while [15] addresses security threats and requirements of personal cloud computing through major cloud services such as Amazon EC2 and Azure [15].

When setting the access control requirements, our literature sources indicate three aspects to be taken into consideration: (1) the method of access to the cloud, (2) the architecture of the cloud, and (3) the features of the multi-tenant environment. Below, we summarize our findings regarding these aspects. First, usually cloud environments are accessed by the CSUs through a web application [16] which often is deemed the weakest point of CC. This is because the current browser-based authentication protocols for the cloud are not secure, due to browsers' inability to issue XML based security tokens by itself. In [16, 17]technical solutions to overcome those obstacles are proposed, e.g. by encrypting data, while it is stored under the custody of a cloud service provider or while it is transmitted to a CSU.

Second, regarding the architecture of the cloud, one of biggest challenges is that of virtual machine (VM) instance interconnectivity. A key concern in virtualization is isolation [18], which guarantees that one VM cannot affect another VM running in the same host. When multiple VMs are present on the same hardware (which is common for clouds), one VM could be illegally accessed through another VM. A solution to prevent this is the Virtual Network Framework [18] which consists of three layers (routing layer, firewall and shared network) and aims to control the intercommunication among VMs deployed in physical machines with higher security.

Third, requirements should be aligned to the specific context of the multi-tenant environments in order to avoid the possible problems caused by role name conflicts, cross-level management and the composition of tenants' access control. Solutions that address these requirements are the SaaS Role Based Access Control (S-RBAC) model [19], the reference architecture defined in [20], and the reference architecture encompassing the concept of "interoperable security" [20]. These solutions help one to differentiate between a 'home cloud' and a 'foreign cloud'. The 'home cloud' is a CSP which is unable to meet demand with its current resources and, therefore, forwards federation requests to 'foreign clouds' with the purpose to exploit their virtualization infrastructures.

B. Atach Harm Detection

This refers to the detection, recording, and notification requirements when an attack is attempted and/or succeeds [3]. Currently, four groups of solutions are proposed. The first group includes cloud firewalls as the filtering mechanism for attack prevention. Their essential feature is their dynamic and intelligent technology to take full advantage of the cloud to sample and share threat information dynamically and in real time [1]. Unfortunately the cloud security standards in the cloud firewalls are still in a chaotic state, with vendors fighting each other and each using their own standards.

The second group refers to security-measuring framework suitable to SaaS [21], [22]. For example, the framework in [21] aims to determine the status of user-level applications in guest VMs that have run for a period of time.

The third category of solutions is cloud community watch services that rely on millions of CSUs for constant analysis to detect newly injected malware attacks [23]. The advantage is that community services see more web traffic and can leverage more defenses than any single CSP.

The fourth and last group covers multi-technology based approaches, e.g. for example, the cloud security based intelligent Network-based Intrusion Prevention system (NIPS) [24] that includes four key technologies – active defense technology, linkage technology with firewall, synthesis detecting method, and hardware acceleration system, to block visits under the real-time determination.

C. Integrity

This is about how well various components are protected from intentional and unauthorized corruption. Integrity can be broken down to data integrity, hardware integrity, personal integrity and software integrity. Because of space limitation, we refer readers to [3] for more information on the definitions of these requirements. The current solutions to integrity requirements are: (1) service level agreements (SLA) based, (2) multi-model based, and (3) VM-focused. SLA-based approaches [25–28] postulate that the security requirement for the cloud must be included in the SLA, the document which defines the relationship between the CSP and the CSU.

The multi-model approaches [25], [28] deploy models differently responding to security related features. In [28], five models deal with separation, availability, migration, data tunnel and cryptography, respectively, while in [25], a tunnel and a cryptography models work together to guarantee data security during storage and transmission.

Last, the VM-focused approaches ensure integrity by increasing the requirements for VM security. In systems where multiple VMs are co-located on the same physical server, a malicious user having control of a VM can try to gain control over other VM's resources or utilize all system resources leading to denial of resource attack over other VM users, or steal data located on the server. Jasti et al. [29] explore how such co-existent of VM's can be exploited to gain access over other CSU's data or deny service and propose constructive security measures that can be deployed to avoid such attacks.

Another solution that centralizes guest protection into a security VM and is highly scalable is given by in [30]. Also trusted virtual data center (TVDC) can be deployed which is a technology developed to address the need for strong isolation and integrity in virtualized environments [31].

Integrity challenges in the cloud could arise when SaaS applications in the cloud need to access enterprise on-premises applications for data exchange and on-premises services. Such challenges can be overcome by implementing a Proxy-based firewall/NAT traversal solution which allows SaaS applications to integrate with on-premise applications without firewall reconfiguration, while maintaining the security of on-premise applications [32]. Besides ensuring integrity in the process of data transmission, a mechanism for the CSU or the CSP to check whether the record is modified in the cloud storage is also needed. This could include the use of digital signature and authenticate code [33] which is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks [34].

D. *Security Auditing*

This is about enabling the security personnel to audit the status and use of security mechanisms by analyzing security-related events [3]. This is usually done for the purpose of achieving compliance to laws and regulations or accountability and control. Approaches to security audibility requirements appear to be based on security configuration management and vulnerability assessment [35, 36]. For example, the approach in [38] assesses the vulnerabilities of each VM in an infrastructure and, by using attack graphs, compose these findings into an overall vulnerability assessment of the given multitier infrastructure. A logging framework such as the one proposed in [39] could be very useful for security auditing.

An alternative approach is the data protection scheme with public auditing outlined in [40] that provides a mechanism to allow for data to be encrypted in the cloud without loss of accessibility or functionality for authorized parties. Next to SaaS security auditability, we also found studies that discuss auditability requirements pertaining to IaaS and the PaaS. In [41] a Security Model for IaaS (SMI) is proposed to guide security assessment and enhancement in IaaS layer. On the PaaS layer, [42] presents an infrastructure that combines semantic security risk management tools with dynamic web service policy frameworks to support the mitigation of security threats. The platform addresses the need to model security requirements, dynamically provision and configure security services and link operational security events to vulnerabilities and impact assessments at the business level.

E. *Privacy*

This is about preventing unauthorized parties from obtaining sensitive information. It includes two aspects to privacy – anonymity and confidentiality. For privacy requirements to be well defined, it is vital that meaningful, clear and valuable privacy metrics are identified [43]. Currently, solutions to enhance privacy include the use of cloud-based malware scanners [44] and data fragmentation technology to hide the association between data attributes[45], or the separation of the CSUs' data from the software [46].

F. *Non-repudiation*

This subarea includes requirements about preventing a party to an interaction with the cloud to deny the interaction. We note that only two out of the 55 reviewed papers provided solutions to requirements challenges in the subarea. In [47] the authors use a mechanism to trace the CSUs and get their origin. It enables the recording of visitor's information and makes it very hard for the CSUs to deceive about their identity information [47]. Another solution is the multi-party non-repudiation (MPNR) protocol [48], which provides a fair non-repudiation storage cloud and also prevents roll-back attacks.

G. *Multiple Security Subareas*

Here we present 14 out of the 55 papers which we found hard to fit in one of the above sub-areas of security requirement. This was most often due to the broad range of security subjects tackled by the authors. Table I summarizes the requirements and the solutions addressed in these 14 papers.

TABLE I. SECURITY REQUIREMENTS AND SOLUTIONS IN MULTIPLE SUB-AREAS

Ref.	Requirements	Solutions
[49]	Storage and transmission, integrity, data consistency and availability, data backup and recovery, security tag, key management, remote platform attestation, authentication, access control	A framework from data life cycle perspective
[50]	Workload state integrity, guest OS integrity, zombie protection, denial of service attacks, malicious resource exhaustion, platform attacks, platform attacks	Intrusion prevention and detection framework
[51]	Auditability, non-reputability, access control	4 security mechanisms
[52]	Auditing, attack detection, access control, non-repudiation, privacy and integrity	Intrusion detection framework
[2]	Physical security, data integrity, auditability, privacy	Security management standards
[53]	Trust, privacy	Data handling mechanisms
[54]	Trust, privacy	A wide range of mechanisms
[55]	Individual-stakeholder's security	Not-proposed
[56]	CSU experience and security	Not-proposed
[57]	Privacy, integrity and non-repudiation	Schema for data safety
[58–60]	Most requirements	Survey multiple solutions
[61]	Integrity, access control and attack/harm detection	Generic policy management system

H. Discussion

Overall it was challenging to separate the articles into different security requirements categories. We observe that the access control requirements are often tightly interconnected with the non-repudiation requirements. Also, the attack detection requirements are strongly connected to integrity because once being able to identify an attack the next step it to stop it from harming the integrity and sometimes the two steps are not separated. The areas that were often covered together are: (1) access control, privacy, and non-repudiation; (2) attack detection, integrity, and security auditing; (3) attack detection and non-repudiation; (4) integrity and privacy.

In security areas where multiple sub-areas exist the amount of research coverage was not even. For example, in the access control the majority of the works covered identification and authentication but few addressed authorization requirements. The same situation was in the area of integrity where the most popular subject was data integrity but software, hardware and personal integrity were overlooked. Other complete security areas were rarely mentioned in any of the papers e.g. physical protection. The observation that none of the papers provide a detailed discussion about the physical protection which was surprising as this can be serious threat for cloud computing sites. For example, in 2011 the EC2 data center of Amazon in Ireland was stroke by lightning and some of the CSUs suffered outages up to 48 hours [62]. In order to anticipate and handle such disasters, requirement about the physical storage security and recovery strategy should be defined.

We observe that none of the publications discussed Physical Protection, Recovery or Prosecution. The lack of literature on these cloud security topics can be explained in a few different ways. First, there is a considerable research done in those areas however it is not published as a topic in cloud computing. For example, the system recovery requirement may be researched as part of software engineering or general requirement engineering. Second, it can be argued that recovery and prosecution may not be part of security requirements hence when searching for security topics those will not be retrieved. Third, the topics are not considered as important enough to dedicate complete papers to them and those areas are just mentioned as secondary topics. Most likely the truth is a mixture of the three.

From the classification of the 55 papers some important conclusions could be made about the most heavily and the least researched sub-areas in the cloud security requirements topic. The three most popular subareas are: integrity, access control, and security auditing. According to our reviewed sample, the three least researched subareas are: physical protection, recovery and prosecution. Table II gives a complete overview of the popularity of the various security areas.

An especially surprising area that appeared to be under-researched is privacy and confidentiality with only 7% of the publications. An explanation might be the assumption that private and confidential data should not be moved to the cloud in the first place. However, this contradicts with the trends where more and more business applications with valuable company data are moved to the cloud. Another more likely answer is that the privacy and confidentiality are closely related to access control. By enforcing a strict access control and preventing unauthorized parties to get sensitive data the privacy protection is automatically increased. Therefore many of the issues of the privacy and confidentiality are probably explicitly or implicitly addressed in the publications on access control. For that reason the apparent low level of research on privacy could be misleading.

TABLE II. DISTRIBUTION OF COVERED SECURITY SUB-AREAS

Security sub-area	Count	Percentage
Access Control	12	22%
Attack/Harm Detection	5	9%
Non-repudiation	2	4%
Integrity	10	18%
Security Auditing	8	15%
Physical Protection	0	0%
Privacy and confidentiality	4	7%
Recovery	0	0%
Prosecution	0	0%
Multiple security areas	14	25%
Total	55	100%

IV. LIMITATIONS AND FUTURE RESEARCH

The main limitations in our SR are: (i) bias in the selection of papers to be included, and (ii) categorization. To help to ensure that the process of selection was unbiased, we developed a review protocol, by defining our search strategy and study selection process. We note here that our access to 'relevant' sources depended on the appropriateness of the search strings used. Also, the keywords used to retrieve literature may well be extended to the fields of grid computing, parallel computing, SOA and distributed computing security which are tightly related to cloud computing security. Moreover, our SR might be biased despite our effort to diminish the possibility by selecting a source database that references to a plethora of publications from the most renowned conference proceedings and journals on the subject. The challenges to an unbiased review are that there is no single publications' source, the literature is fragmented and not everything can be accessed online. To reduce the bias further, more literature search could be done throughout publications that are not written in English.

The second limitation is that the literature on cloud computing security is classified in groups of security requirements that are not exclusive and the boundaries are hard to set. Also, the distinction between SaaS, PaaS and IaaS requirements is by far not straightforward. In most cases one publication tackle a number of security requirements and we made the conscious decision to enforce structure in order to provide focus and context for the research. We classified the publications according to the security area that was most elaborated upon; this does not mean that the rest of the security requirements addressed by the same article are not valuable or significant. In order to improve on that limitation,

the cloud computing security requirements could be described by other general security requirements frameworks or methodologies. An excellent starting point for such an alternative classification approach is the work of Mellado et al. [6]. Furthermore, general non-functional requirements frameworks could be deployed if one wants to map the cloud computing security requirements against a broader requirements classification schema, for example, the Non-Functional Requirements Framework (NFR) by Chung et al. [63]. Such a mapping would be indeed beneficial if one would like to clearly see what other non-functional requirements possibly interact with cloud computing security requirements, according to published literature. We think this is a promising line for future research.

V. CONCLUSIONS

With this work we attempted to provide a roadmap for researchers on the subject of cloud computing security requirements and solutions. The discovered literature on the subject was classified in nine groups according to the type of the primary security requirement.

As an answer to RQ1, we found that 6 out of the 9 sub-factors in the Firesmith model [3] have been researched, to varying degrees (Table II). Among those six, access control, integrity and auditability are by far the most researched.

As an answer to RQ2, we found that current solutions in most cases tackle multiple security sub-areas. The solutions vary in terms of cloud layers being covered, technology types involved, and whether they reside on the CSPs' or CSU's sides.

As an answer to RQ3, we found *that the least researched security areas are non-repudiation, physical protection, recovery and prosecution*. We consider this finding our most important one and we plan follow up studies to understand why this is the case.

We evaluated the possible limitations of the review and suggested some ideas for future research.

REFERENCES

[1] W. Huang and J. Yang, "New network security based on cloud computing," in 2nd Int. Workshop on Education Technology and Computer Science, 2010, pp. 604-609.

[2] K. Popović and Z. Hocenski, "Cloud computing security issues and challenges," 33rd Int. Convention on Information and Communication Technology, Electronics and Microelectronics, 2010, pp. 344-349.

[3] D. Firesmith, "Specifying reusable security requirements," J of Object Technology, 3(1), 2004, pp. 61–75.

[4] L. M. Vaquero, L. Rodero-Merino, and D. Morán, "Locking the sky: A survey on IaaS cloud security," Computing 91(1), 2011, pp. 93–118.

[5] B. Hay, K. Nance, and M. Bishop, "Storm clouds rising: Security challenges for IaaS cloud computing," HICSS, 2011, pp. 1-7.

[6] D. Mellado, C. Blanco, L. E. Sánchez, and E. Fernández-Medina, "A systematic review of security requirements engineering," Computer Standards & Interfaces, 32(4), 2010, pp. 153-165.

[7] J. Webster and R. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," MISQ, 26(2) 2002, pp. 13-23.

[8] B. A. Kitchenham, "Procedures for undertaking systematic reviews," CS Dep. Keele University, 2004.

[9] S.A. Almulla and C. Y. Yeun, "Cloud computing security management," ICESMA 2010, pp. 1-7.

[10] H. Sato, A. Kanai, and S. Tanimoto, "Building a security aware cloud by extending internal control to cloud," ISADS 2011, pp. 323–326.

[11] W. Zhou, M. Sherr, W. R. Marczak, Z. Zhang, T. Tao, B. T. Loo, and I. Lee, "Towards a data-centric view of cloud security," Int Conf on Information and Knowledge Management, 2010, pp. 25-32.

[12] P. Prasad, B. Ojha, R. R. Shahi, R. Lal, A. Vaish, and U. Goel, "3 Dimensional security in cloud computing," ICCRD 2011 (3), pp. 198–201.

[13] J. Xue and J. Zhang, "A brief survey on the security model of cloud computing," Int. Symp. on Distributed Computing and Applications to Business, Engineering and Science, 2010, pp. 475-478.

[14] Y. Karabulut and I. Nassi, "Secure enterprise services consumption for SaaS technology platforms," ICDE 2009, pp. 1749-1756.

[15] S.-H. Na, J.-Y. Park, and E.-N. Huh, "Personal cloud computing security framework," IEEE Asia-Pacific Services Computing Conference, 2010, pp. 671-675.

[16] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," CLOUD 2009, pp. 109-116.

[17] M. Townsend, "Managing a security program in a cloud computing environment," IInfoSecCD 2009, pp. 128-133.

[18] H. Wu, Y. Ding, L. Yao, and C. Winer, "Network security for virtual machine in cloud computing," Int Conf on Computer Sciences and Convergence Information Technology, 2010, pp. 18-21.

[19] D. Li, C. Liu, Q. Wei, Z. Liu, and B. Liu, "RBAC-based access control for SaaS systems," ICIECS 2010, pp. 1-4.

[20] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "Security and cloud computing: Intercloud identity management infrastructure," WET ICE 2010, pp. 263-265.

[21] Q. Liu, C. Weng, M. Li, and Y. Luo, "An In-VM measuring framework for increasing virtual machine security in clouds," IEEE Security & Privacy, 8(6), pp. 56-62, 2010.

[22] L. Sumter, "Cloud computing: Security risk," Annual Southeast Conference, 2010.

[23] N. Hawthorn, "Finding security in the cloud," Computer Fraud and Security, 2009(10), pp. 19-20, 2009.

[24] T. Jia and X. Wang, "The construction and realization of the intelligent NIPS based on the cloud security," Int. Conf on Information Science and Engineering, 2009, pp. 1885-1888.

[25] C. Zhong, J. Zhang, Y. Xia, and H. Yu, "Construction of a trusted SaaS platform," SOSE 2010, pp. 244-251.

[26] B. R. Kandukuri, P. V. Ramakrishna, and A. Rakshit, "Cloud security issues," SCC 2009 pp. 517-520.

[27] P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar, H. Medhioub, and D. Zeghlache, "Challenges for cloud networking security," *HP Laboratories Technical Report*, no. 137, 2010, pp. 1-17.

[28] G. Zhao, C. Rong, M. G. Jaatun, and F. E. Sandnes, "Deployment models: Towards eliminating security concerns from cloud computing," HPCS 2010, pp. 189-195.

[29] A. Jasti, P. Shah, R. Nagaraj, and R. Pendse, "Security in multi-tenancy cloud," Int. Carnahan Conference on Security Technology, 2010, pp. 35-41.

[30] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, and D. Zamboni, "Cloud security is not (just) virtualization security: A short paper," ACM CCCS 2009, pp. 97-102.

[31] S. Berger et al., "Security for the cloud infrastructure: Trusted virtual data center implementation," IBM Journal of Research and Development, 53(4), 2009.

[32] F. Liu, W. Guo, Z. Q. Zhao, and W. Chou, "SaaS integration for software cloud," CLOUD 2010, pp. 402-409

[33] J. Feng, Y. Chen, and P. Liu, "Bridging the missing link of cloud data storage security in AWS," Consumer Communications and Networking Conf, 2010 .

[34] P. S. Kumar, R. Subramanian, and D. T. Selvam, "Ensuring data storage security in cloud computing using Sobol sequence," PDGC 2010, pp. 217-222.

[35] H.-C. Li, P. Liang, J. Yang, and S. Chen, "Analysis on cloud-based security vulnerability assessment," ICEBE 2010, pp. 490-494.

[36] F. Lombardi and R. Di Pietro, "Transparent security for cloud," ACM SAC 2010, pp. 414-415.

[37] K. Wood and E. Pereira, "An investigation into cloud configuration and security," ICITST 2010, pp. 1-6.

[38] S. Bleikertz, M. Schunter, C. W. Probst, D. Pendarakis, and K. Eriksson, "Security audits of multi-tier virtual infrastructures in public infrastructure clouds," ACM CCCS 2010, pp. 93-102.
[39] R. Marty, "Cloud application logging for forensics," ACM SAC, 2011, pp. 178–184.
[40] B. Gowrigolla, S. Sivaji, and M. R. Masillamani, "Design and auditing of Cloud computing security," ICIAfS 2010, pp. 292-297.
[41] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions," INFOS 2010, pp.1-8.
[42] S. Bertram, M. Boniface, M. Surridge, N. Briscombe, and M. Hall-May, "On-demand dynamic security for risk-based secure collaboration in clouds," CLOUD 2010, pp. 518-525.
[43] R. M. Savola, A. Juhola, and I. Uusitalo, "Towards wider cloud service applicability by security, privacy and trust measurements," AICT 2010.
[44] I. Muttik and C. Barton, "Cloud security technologies," Information Security Technical Report, 14(1) 2009, pp. 1-6.
[45] Y. Shi, K. Zhang, and Q. Li, "Meta-data driven data chunk based secure data storage for SaaS," *IJ DCTA*, 5(1), 2011pp. 173–185.
[46] Z. Qiang and C. Dong, "Enhance the user data privacy for SAAS by separation of data," Int Conf on Information Management, Innovation Management and Industrial Engineering, ICIII 2009 (3), pp. 130-132.
[47] Z. Shen and Q. Tong, "The security of cloud computing system enabled by trusted computing technology," ICSPS 2010 (2), p. V211-V215
[48] J. Feng, Y. Chen, D. Summerville, W.-S. Ku, and Z. Su, "Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol," CNNC 2011, pp. 521–522.
[49] X. Yu and Q. Wen, "A view about cloud data security from data life cycle," cycle," CiSE 2010.
[50] J. Arshad, P. Townend, and J. Xu, "Quantification of security for compute intensive workloads in clouds," ICPADS, 2009, pp. 479-486.
[51] G. Peterson, "Don't trust. and verify: A security architecture stack for the cloud," IEEE Security & Privacy, 8(5), 2010, pp. 83-86.
[52] C.-L. Tsai and U.-C. Lin, "Information security of cloud computing for enterprises," Advances in ISSS 3(1), 2011, pp. 132–142.
[53] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," CloudCom 2010, pp. 693-702.
[54] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, 8(6), 2010, pp. 24-31.
[55] K. M. Khan, "Security dynamics of cloud computing," Cutter IT Journal, 22(6-7), 2009, pp. 38-43.
[56] N. Oza, K. Karppinen, and R. Savola, "User experience and security in the cloud - An empirical study in the Finnish Cloud Consortium," CloudCom 2010, pp. 621-628.
[57] X. Jing, J. Tang, D. He, and Y. Zhang, "Security scheme for sensitive data in management-type SaaS," Int Conf on Information Management, Innovation Management and Industrial Engineering, ICIII 2009 (4), pp. 47-50
[58] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," ISSA 2010, pp. 1-7.
[59] Z. He and Y. He, "Analysis on the security of cloud computing," SPIE - The International Society for Optical Engineering, 2011, vol. 7752.
[60] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," in HICSS 2011, pp.1-10.
[61] C. Băsescu, C. Leordeanu, A. Costan, A. Carpen-Amarie, and G. Antoniu, "Managing data access on clouds: A generic framework for enforcing security policies," AINA, 2011, pp. 459–466.
[62] P. Wainewright, "Lightning strike zaps EC2 Ireland | ZDNET," 2011. [Online]. Available: http://www.zdnet.com/blog/saas/lightning-strike-zaps-ec2-ireland/1382?tag=search-results-rivers;item0. [Accessed: 24-Sep-2011].
[63] L. Chung, B.A. Nixon, E. Yu, and J. Mylopoulos, Non-functional Requirements in Software Engineering, Springer, 2000.