Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/3954
DOI URL: http://dx.doi.org/10.21474/IJAR01/3954

RESEARCH ARTICLE

AN ANALYSIS OF CLOUD COMPUTING INFORMATION SECURITY CHALLENGES.

Amira Hosni.
Arab Academy for Science and Technology and Maritime Transport Cairo, Egypt.

Manuscript Info

Manuscript History

Received: 18 February 2017
Final Accepted: 15 March 2017
Published: April 2017

Key words:-
Cloud Computing. Challenges, Data, Security, Solutions.

Abstract

Security is one of the biggest obstacles that prevent the adoption of cloud computing [1]. Businesses and research are reluctant in shifting the control of digital assets to the third–party service providers [2].Organizations does not enjoy administrative control of cloud services and infrastructure [3]. The security measures taken by the cloud service providers (CSP) are transparent to the organization [4].The presence of large number of users from different organizations aggravates the situation further [2]; the users might be trusted by the CSP but may not trust each other [4]. The above reasons increase the customers' uncertainty about their digital assets on the cloud resulting in reluctance to adopt cloud computing [2].This paper exploits certain information security risks namely data, user identity and access control and contractual and legal issues. Moreover, the manuscript presents a comprehensive solution in literature to cater for all security risks. A critical evaluation of the solution by comparing it with other solutions that exist in literature is provided. The analysis proves the thoroughness and outperformance of the comprehensive solution compared to the other solutions that exist in literature.

Introduction:-

During the last few years, both organizations and individuals have started to pay attention to the cloud computing services [5]. This paradigm encompasses access to a shared pool of computing resources that can be provisioned and released with minimal management effort [6].In addition, when these kinds of services are aligned with well-defined objectives, they make valuable contributions to an enterprise [7].However, the many benefits provided by cloud computing are accompanied by the appearance of new risks.

Reviews on cloud security issues are presented by the authors in [8, 9]. However, these studies did not discuss security solutions. Ref. [10] reviewed the cloud computing security issues at different levels and provided solutions; however an overview of the cloud technology in addition to the future work were missing. Ref. [11] presented a study on privacy preservation in the cloud in relation to e-health clouds only. Ref. [12] reviewed the security and privacy challenges in cloud computing with regard to the existing vulnerabilities concentrating on confidentiality, integrity, availability, accountability and privacy with little discussion on vulnerability origins. The authors in [13] discussed the security issues in the cloud and the approaches to tackle the vulnerabilities; however future direction was lacking in the survey. The work in [14] discussed the security issues in depth with a brief discussion on current and latest solutions. Ref. [15] conducted a survey of the popular security models of cloud computing. In addition the work discussed the risks of cloud computing from the perspective of different stack holders, but security issues from

Corresponding Author:- Amira Hosni.
Address:- Arab Academy for Science and Technology and Maritime Transport Cairo, Egypt.

the technological and operational point of view were out of the study scope. The strategies to relieve the security issues in terms of the components and processes that should be secured and evaluated were discussed. However the "how" the security objectives are achieved in current research was not discussed. The authors in [16] described the security issues along with the security solutions; however the discussion was focused on the privacy part of the cloud security and the discussion on future research direction was not included. The article [4] was an extensive, comprehensive survey on security issues in cloud computing and includes the latest security solutions presented in literature. In addition it briefly discussed the security issues related to mobile cloud computing and generic solutions strategies.

The remainder of paper is organized as follows. Section two discusses cloud security challenges pertaining to data and information. Section three elaborates on a comprehensive governance framework as a solution in literature. Section four analyzes the governance framework solution and compares it to other solutions existing in literature and section five is the conclusion.

Cloud information security challenges:-

The cloud characteristics and models together with their implementation technologies introduce cloud specific security risks and vulnerabilities in addition to the risks of the conventional IT infrastructure [17].Any compromised service model compromises other layers of the service models [4]. The private cloud deployment model inherits the same set of vulnerabilities as the conventional IT infrastructure [4].The public, community and hybrid clouds posses more vulnerabilities due to the multi tenancy technology and the administrative control of the third party [18].Multi tenancy, virtualization and resource pooling technologies introduces many security concerns [4]; the segregation of multiple tenants and allocated resources is a complex task and requires higher levels of security. Several cloud information security risks exist namely communication, virtualization, data/storage issues, web applications and API issues, identity management and access control and contractual and legal threats with communication, virtualization and web applications and APIs being out of the scope of the study.

Data /Storage issues:-

Distinct to conventional computing model, the cloud permits the CSP to manage servers and data [4]; the user enjoys a limited control over the VMs [19].The lack of control over the data together with the cloud characteristics contrary to conventional computing introduces greater data security risks [4].Below is an overview of the data security challenges in the cloud computing environment.

Data privacy and integrity:-

The data in the cloud is more vulnerable to risks in terms of confidentiality, integrity, and availability compared to conventional computing [20].In the cloud shared environment, the cloud security strength equals the security strength of its weakest entity [21]; a successful attack on a single entity can result in data breach. The multi-tenant nature of the cloud can result in integrity violation [4]. Saas providers having access to information can be a potential risk[14].In addition to stored data, information is susceptible to risks by virtualization that allows malicious users to launch attacks on other users data while being processed[14,22].The absence of secure and standard cryptographic key management techniques for the cloud increases the potential risks to the data [23].

Data recovery:-

Due to cloud characteristics, the resource allocated to a user may be assigned to another user at a later point in time [4]. A malicious user can employ data recovery techniques to obtain the data of previous users [24, 1].This can pose threats to sensitive user data [25].

Media sanitization:-

The need to destruct physical storage is due to a number of reasons: the disks need to be changed, the data no longer need to be there or the termination of service [23].If the CSP does not sanitize the media properly the data can be exposed to risks [26].Sometimes multi-tenancy can prevent media sanitization at the end of a device life cycle as it is in use by other tenants which in turn poses security risks to the other tenants data [1].

Data backup:-

A regular data backup is needed by the CSP to protect the data from intentional and accidental disasters [4].Moreover the data backup needs to be protected against unauthorized access and tampering [9].If data backup is outsourced to a third party by the CSP, risks are broadened [14].

User identity and access control:-
In a cloud environment, authentication is linked to the confidentiality and integrity of data and services [4]. The issue of authentication and access control is more complex as the data is under the control of CSP and the organizations authentication and authorization may not be exported to the cloud in its existing form [23].In addition, the authorizations and authentications may differ for different organizations at the same time and with the same physical resource [27]. The cloud characteristics of being elastic, dynamic, reassigning of IP address, services start and restart over a short period of time and pay-as-you-use demand different authentication systems than traditional IT systems[28]. There is a need for a stricter control by organizations over identity management in the cloud to control unauthorized operations and a need to quickly update access control policies in case of newly joining and leaving employees [9].

SLAs and legal issues:-
The problems of performance assurance, laws compliance, geographical jurisdictions, monitoring of contract enforcement are all a result of adopting the cloud and are related to service level agreements(SLA) and physical location of data[4].The users must be very clear about the security of their assets and all the security requirements must be thoroughly agreed upon in the SLA [4].Ambiguities make it harder to claim the loss at the CSP; if a CSP sub-contracts the service to a sub contractor, then in the case of a problem the sub contractor accountability is often inadequate[29]. Moreover, statistics provided by the CSP on contract performance is unreliable which raises conflicts between the user and the CSP which in turn makes the statistics evaluation and determination of responsibility an issue [30].In addition the SLAs are pre-defined and non-negotiable which makes them CSP bias [29].Furthermore, auditing the security of the CSP is hard to carry out and agree upon in the SLA [4].

The presence of CSP resources in geographically different and sometimes conflicting legal jurisdictions raises certain legal issues [31]. If the data is migrated to a location with different laws, it becomes difficult for the user to configure the policies to comply with the new legal jurisdictions [4]. Moreover the data can be located in more than one location having different security laws and in the case of a dispute the issue of jurisdiction arises as to which laws are applicable [32, 30, 29].E-discovery which happens when a CSP hardware is seized for an investigation claim by a user related to the laws of a geographical location causes in return a risk of privacy breach of other users [33, 30].

A comprehensive cloud security solution:-
The comprehensive security solution proposed in [5] is founded upon two main standards: on the one hand, they implement the core governance principles of the ISO/IEC 38500 governance standard and on the other hand a cloud service lifecycle based on the ISO/IEC 27036 outsourcing security draft. A security governance as part of the corporate governance is the most suitable path to gain control of security processes and guarantee an alignment with business initiatives and objectives [34]. Although there are many technological approaches that can improve cloud security, there are currently no comprehensive solutions [35]. Research shows that existing efforts that attempt to deal with cloud computing security do not detail the governance aspects [36]. Therefore a first approach to a security governance framework that considers the particularities of cloud deployments Information Security Governance framework (ISGcloud) is proposed in [5]. With the use of standards the proposed solution aim to increase the quality and reliability of the results and simplify the governance process while guaranteeing the security of the cloud service and promoting the reuse of resources [37].

To deploy the security governance, the authors in [5] have chosen the model published in the ISO/IEC 38500 standard [38], which states that the directors should perform three main processes: Evaluate, Direct, and Monitor. In addition they propose a fourth process , Communicate, to disseminate security knowledge within the organization as regards to the adoption of new services such as cloud computing is to be performed. In addition to the four core processes a cloud service lifecycle in terms of activities and tasks are performed. The ISO/IEC 27036 standard [39] outlines security controls to be addressed in an outsourcing lifecycle. Taking the ISO/IEC 27036 standard as a basis they propose the following generic cloud computing service lifecycle: Planning / Strategy Definition; Cloud Security Analysis; Cloud Security Design; Cloud Implementation / Migration; Secure Cloud Operation; and Cloud Service Termination.

The four ISG processes constitute one dimension of the ISG framework and the six activities of the cloud computing lifecycle is a second dimension [5]. The four processes traverse the six activities in which successive governance cycles are held [5]. There are several aspects that influence the security governance activities and are considered in

the framework. The internal aspects are: the business pressures and needs, IT infrastructure, Employees/users, and internal threats [5]. The external aspects are: cloud provider, IT advance, regulations and external threats [5]. The activities are performed iteratively. The authors in [5] describe the activities as follows:

Activity 1: Planning/ Strategy Definition: it is constituted of two tasks: Establish Information Security Governance Structure which introduces ISG into the organization culture, identifying the participants, grouping them in teams by affinity and assigning their responsibilities by the directors. The second task is to Define Information Security Program which consists of a series of activities that support the company risk management plan and result in the development of the security strategy and policies. This task must be performed jointly by IT and security managers and senior officers to guarantee that the security program is aligned with the business objectives.

Activity 2: Cloud Security Analysis: Consists of three tasks: Define Information Security Requirements. Ensuring a complete alignment with the organization's mission, the goals are translated into security requirements. When defining these requirements it is important to consider the cloud service the organization plans to implement and its deployment. Task two is the Cost/benefit Analyses, business case, of the available cloud options. The cost includes also the cost of an effective governance to manage risk and ensure regulatory compliance and the value added by the cloud service. The third task is Cloud Risk Analysis which is the cloud security risks analysis together with the management processes for these risks.

Activity 3: Cloud Security Design: The objective of this activity is to provide a comprehensive design of the security governance that will be implemented and the cloud service. It constitutes of three tasks. Task one is Define SLAs and legal contracts. SLAs as part of the iterative governance cycle must be periodically reviewed with the purpose of modifying detected lacks and improving the cloud services security management. The second task is to Establish Information Security Roles and Responsibilities. This task involves the identification of the information assets to define the ownership and responsibility of each one within the organization. Task three is to Specify Cloud Service Monitoring and Auditing which specifies the conditions under which the cloud service will be monitored. In addition the organization defines the processes and metrics to perform security audits based on the SLAs. Task four is to Define Applicable Security Controls, the security controls. Based on the risk analysis, the organization must develop the security measures for the cloud service operation and in cases of incidents or major disasters.

Activity 4: Cloud Implementation / Migration. Once the security design is completed the cloud service implementation takes place. This activity consists of two tasks. Task one is Secure Cloud Implementation, the security during the service implementation and the parallel modification of the organizational security processes. Task two is to Educate and Train Staff. Although the Communicate process should have increased the security awareness in previous activities, it is in this task that a global training plan is developed and each staff member is educated on his/her role in the cloud service.

Activity 5: Secure Cloud Operation: This activity is devoted to the cloud service operation which is of an indefinite duration. This activity is constituted of two tasks: Cloud Security Operation which reflects the successive iteration of the governance cycle in each activity. This may produce modifications to products from previous activities such as security strategies and policies or risk analysis or to revisit previous activities even while the cloud service is in operation. The second task is to Communicate Information Security within the Organization. This task reflects the continuous communication process that takes place within the organization to maintain security awareness and permit the adding of new policies.

Activity 6: Cloud Service Termination or provide the service termination either by moving to another service provider or to discard the cloud securely.

Discussion:-

The comprehensive solution is founded upon two main ISO standards, ISO/IEC 38500 governance standard and the ISO/IEC 27036 outsourcing security draft which increases the quality and reliability of the results. The governance allows the alignment with the business initiatives and objectives. The participants in the security governance and their responsibilities are assigned by the directors and a security strategy and policies are developed and aligned with the business objectives in the first few activities. In developing the business case the available cloud options are considered. ISG defines SLAs and legal contracts that are periodically reviewed as part of the iterative governance cycle. As a result of the governance iterations in an activity, prior activities could be revisited and as a result

previous outputs could be updated. ISG identifies the monitoring and auditing of the cloud service and the security controls. The ISGcloud framework offers secure cloud implementation and provides education and training of staff and a secure termination of service. The communication, virtualization and web applications and APIs risks are dealt with as part of the cloud information security risks analysis task three activity two.

The remaining solutions in literature with regard to data address only certain aspects of information security namely data storage. The solutions range from certain protocols such as SecCloud[19] and the File Assured Deletion protocol FADE[40] based on keys encryption, procedures such as schemes based on sensitivity rating of the user data and 128-bit SSL encryption[41] and the erasure correcting code and homomorphic tokens[20].However ISG offer a comprehensive solution catering for all types of security risks through its Cloud Risk Analysis task in the second activity which provides cloud security risks analysis together with the management processes for these risks. Moreover, the second task carried out in activity one Define Information Security Program consists of a series of activities that support the company risk management plan which result in the development of the security strategy and policies.

The remaining solutions in literature that address identity management and access control in the cloud environment specifies and enforces the access control policies cryptographically such as in Hierarchical Attribute-Set-based Encryption (HASBE) [42]. In HASBE the access control is segregated into a root authority and domain authorities. The access control is defined as a hierarchical tree structure. The root authority is trusted by the domain authorities and users via a certification authority's hierarchy. The trusted authority generates and distributes the group's parameters and the root authority master encryption/decryption keys to its domain authorities. The domain authorities generates encryption/decryption keys to the users which can be of one attribute or group of attributes and with the keys being in a hierarchical structure as in the access control. An expiration time is added to the access control for revocation purposes.

Ref. [43] proposes an anonymous authentication and controlling access to the cloud storage based on Attribute Based Signature (ABS) and Attribute Based Encryption (ABE) respectively. The anonymous authentication allows the user authentication based on a signature that is computed and verified based on user attributes. A trusted third party issues tokens to users that are used by a key distribution center (KDC) that provides the user with the encryption/decryption and signing keys. The user encrypts the data and signs it using the key distribution center (KDC) encryption/decryption and signing keys and transmits it to the cloud. The cloud verifies the signature and stores the data in case of a valid user. The user revocation is dealt with by changing the encryption parameters of all data that has attributes similar to that of the revoked user.

However the authors in [44] propose a Role Based Multi-Tenancy Access Control (RB-MTAC) scheme that combines identity management and role based access control. The user is required to register with the cloud and obtain a unique ID. The user sets the password during the registration process. To enter the cloud, the user uses his registration credentials which he submits to the identity management module to identify him. Next, the user is directed to the role assignment module that connects to the RB-MTAC database that assigns roles to the user based on registered roles information. All the resources are accessed through the role assignment module that maintains the resources access control lists. This scheme resembles much to the roles and access control procedures maintained in the ISGcloud comprehensive solution as each user is assigned a role or responsibility to control which assets to access. In addition, this scheme does not depend on cryptography to access the resources as is the case in the ISG framework. Yet, this scheme is similar to the HASBE in the fact that access to the information in each domain authority is controlled by a certification of trust and a hierarchical public/private encryption keys.

For contractual and legal level solutions the (web-services agreement) ws-agreement [45] defines the syntax and semantics of specifying the competences of the service providers and creates the template based agreements based on quality of service. However risk quantification is not semantically netted in ws-agreement. SecAgreement [46] articulates the security parameters and services to be provided in the SLAs. The SecAgreement extends the template of the ws-agreement to include security constraints and metrics into the SLAs. The extended template includes the risks of using specific cloud services. Based on SecAgreement, the user can quantify the risk of using the CSPs services and choose the CSP services that meet his security requirements. Although the SecAgreement can be a comprehensive solution, it does not allow for alteration or revising of SLAs as in the ISG framework.

Rak et al. [47] delineated the SPECS, an architecture that depends on the SLA-based security as a service and focuses on the three stages of the SLA lifecycle namely, negotiation, enforcement and monitoring and makes use of established work to carry out the phases. In addition the architecture includes security parameters in the SLA to let the end user judge the security offerings and requirements. This resembles much the stages of SLA-based security service provided by ISG namely evaluate, direct and monitor. Ref. [48] built a compliance vocabulary and used ontologies to automate the process of negotiation and selection of better security parameters for the SLA. A similar function is provided in the ISG through the iteration of the governance cycle in activity three task one.

The authors in [49] propose a method to react to the SLA security violations or security services cancelations to reduce the security risks the user assets are exposed to in post violation/cancelations which is also provided by ISG in activity three task four.

Nothing can be done related to legal issues as the user does not know the location of his assets due to location transparency and consequently cannot know his/her legal rights and responsibilities. Yet the user can be given the option during SLA negotiation to mark places that he does not want his/her assets to be migrated to [4]. Consequently compliance with the laws can be managed in an effective manner. Moreover, both the user and the CSP must have mutual understanding of the roles and the responsibility of each other [4].This is implemented in ISG as part of the SLA definition task one activity three.

Conclusion:-

Several research efforts concerning cloud services security have been published together with solutions which concentrated mainly on encryption and auditing. However no existing solutions in literature have made use of security governance. The main contribution of this work is to elaborate on the various information security risks and their corresponding security solutions in literature, present a comprehensive solution in literature, provide a critical evaluation of the solution and prove its comprehensiveness and outperformance.

In order to be able to understand the comprehensive ISGcloud framework solution, a brief description of the framework activities and tasks is provided. Moreover, a discussion which entailed a comparison of the framework security vulnerabilities tackled in the framework and by other security risks solutions in literature is provided. The comparison demonstrates the completeness of the solution especially that it is the only solution in literature that made use of security governance that can be integrated with the enterprise governance and that has a security strategy that aligns with the business objectives.

References:-

1. D.AB. Fernands, L.FB. Soares, J.V. Gomes, M.M. Freire, P. RM Inacio, Security issues in cloud environments: a survey, Int. J. Inform. Sec. 13 (20 (2014) 113-170.
2. R. Latif, H. Abbas, S. Assar, Q. Ali, Cloud computing risk assessment: a systemic literature review, in: Future Information Technology. Springer, Berlin, Heidelberg, 2014, pp. 285-295.
3. A.N. Khan, M.L.M. Kiah, M. Ali, S.A. Madani, S.Shamshirband, BSS: block-based sharing scheme for secure data storage services in mobile cloud environment, J.Supercomput. 70 (2) (2014) 946-976.
4. M. Ali, S.U. Khan, A V. Vasilakos. Security in cloud computing: opportunities and challenges. Information Sciences 305 (2015) 357-383.
5. O. Rebollo, D. Mellado, E. Fernandez-Medina. Introducing a security governance framework for cloud computing, in: Proceedings of the 10th International Workshop on Security of Information Systems WOSIS 2013, Angers, France. July 2013.
6. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. SP 800-145. National Institute of Standards and Technology (NIST) (2011).
7. Gartner: Gartner's Hype Cycle for Cloud Computing. (2012).
8. C. Rong, S.T. Nguyen, M.G. Jaatun, Beyond Lightning: a survey on security challenges in cloud computing. Comput. Electr. Eng. 39 (1) (2013) 47-54.
9. S. Subashini, V. Kavitha,. A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1) (2011) 1-11.
10. C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajarajan, A survey on security issues and solutions at different Layers of Cloud Computing, J. Supercomput. 63 (2) (2013) 561-592.

11. Abbas, S.U. Khan. A review on the state-of-the-art privacy preserving approaches in e-health clouds, IEEE J. Biomed. Health Inform. (2014), http://dx.doi.org/10.1109/BHI.2014.2300846.
12. Z. Xiao, Y. Xiao. Security and privacy in cloud computing, IEEE Commun. Surveys Tutorials 15 (2) (2013) 843-859.
13. Y. Neng-Hai, Z. Hao, J. Xu, W. Zhang, C. Zhang, Review of cloud computing security, Acta Electron. Sinica 41 (2) (2013) 371-381.
14. K. Hashizume, D.G. Rosado, E. Fernndez-Medina, E.B. Fernadez, An analysis of security issues for cloud computing, J. Internet Services Appl. 4 (1) (2013) 1-13.
15. J. Che, Y. Duan, T. Zhang, J. Fan. Study on the security models and strategies of cloud computing, Proc. Eng. 23 (2011) 586-593.
16. Z. Tari, Security and privacy in cloud computing, IEEE Cloud Comput. 1 91) 92014) 54-57.
17. M.D. Ryan, Cloud computing security: the scientific challenge, and a survey of solutions, J. Syst. Softw. 86 (09) (2013) 2263-2268.
18. R. Chandramouli, M. lorga, S. Chokhani, Cryptographic key management issues and challenges in cloud services, in : Secure Cloud Computing, Springer, New York, 2014, pp. 1-30. doi: 10. 1007/978-1-4614-9278-8_1.
19. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing, Inform.Sci.258 (2014) 371-386.
20. C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou,, Toward secure and dependable storage services in cloud computing, IEEE Trans. Services Comput. 5 (2) (2012) 220-232.
21. K. Salah, J.M.A Calero, S. Zeadally, S. Al-Mulla, M. Alzaabi, Using cloud computing to implement a security overlay network, IEEE Sec. Privacy 11 (1) (2013) 44-53.
22. W. Liu, S. Peng, W. Du, W. Wang, G.S. Zeng, Security-aware intermediate data placement strategy in scientific cloud workflows, Knowl. Inform. Syst. 41 (2) (2014) 423-447.
23. W.A. Jansen, Cloud hooks: Security and privacy issues in cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), 2011, pp. 1-10.
24. M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, , A security analysis of amazon's elastic compute cloud service, in : Proceedings of the 27th Annual ACM Symposium on Applied Computing, 2012,pp. 1427-1434.
25. D. Chen, H. Zhao, Data security and privacy protection issues in cloud computing, in: International Conference on Computer Science and Electronics Engineering (ICCSEE, IEEE), vol. 1, 2012, pp. 647-651.
26. V. Vladimir, Cloud adoption issues: interoperability and security, in: Cloud Computing and Big Data, 2013, pp. 53-65.
27. B. Liu, E. Blasch, Y. chen, A.J. Aved, A. Hadiks, D. Shen, G. Chen, Information fusion in a cloud computing era: a systems-level perspective, IEEE Aerospace Electron. Syst.Mag. 29 (10) (2014) 16-24.
28. S. Carlin, K. Curran, Cloud computing security, Int. J. Ambient Comput. Intell. 3 (1) (2011) 14-19.
29. R. Agrawal, Legal issues in cloud computing, in: IndicThreads.com, Conference on Cloud Computing, 2011.
30. N. Gonzalez, C. Miers, F. Redgolo, M. Simplcio, T. Carvalho, M. Nslund, M. Pourzandi, A quantitative analysis of current security concerns and solutions for cloud computing, J.. Cloud Comput. 1 (1) (2012) 1-18.
31. B. Hay, K. Nance, M. Bishop, Storm clouds rising: security challenges for IaaS cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), IEEE, 2011, pp. 1-7.
32. Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for Internet of things, J. Netw. Comput. Appl. 42 (2014) 120-134.
33. E. Schweitzer, Reconciliation of the cloud computing model with US federal electronic health record regulations, J. Am. Med. Inform. Assoc. 19 (2) (2012) 161-165.
34. Mellado, D., Sanchez, L.E., Frenandez-Medina, E., Piattini, M.: IT Security Governance Innovations: Theory and Research. IGI Global, USA (2012).
35. Rong, C.,Nguyen, S.T.,Jaatun, M.G.: Beyond lightning: A survey on security challenges in cloud computing. Computers and Electrical Engineering 39 (2013) 47-54.
36. Rebollo, O., Mellado, D., Fernandez-Medina, E.: A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. Journal of Universal Computer Science 18 (2012) 798-815.
37. Fung, A.R.-W., Farn, K.-J., Lin, A.C.: Paper: a study on the certification of the information security management systems. Computer Standards & Interfaces 25 (2003) 447-461.
38. ISO/IEC: ISO/IEC 38500:2008 Corporate governance of information technology (2008).
39. ISO/IEC: ISO/IEC 27036 – IT Security – Security techniques – Information security for supplier relationships (draft).

40. Y. Tang, P.P. Lee, J.C.S. Lui, R. Perlman, Secure overlay cloud storage with access control and assured deletion, IEEE Trans. Dependable Secure Comput. 9 (6) (2012) 903-916.
41. S. K. Sood, A combined approach to ensure data security in cloud computing, J.Netw. Comput. Appl. 35 (6) (2012) 1831-1838.
42. Z. Wan, J. Liu, R.H. Deng, HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE Trans.Inform.Forensics Sec. 7 (2) (2012) 743-754.
43. S. Ruj, M. Stojmenovic, A. Nayak, Decentralized access control with anonymous authentication of data stored in clouds, IEEE Trans. Parallel Distrib. Syst. 25 (2) (2014) 384-394.
44. S. Yang, P. Lai, J. Lin, Design role-based multi-tenancy access control scheme for cloud services, in :IEEE International Symposium on Biometrics and Security Technologies (ISBAST), 2013, pp. 273-279.
45. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, M. Xu, Web services agreement specification (WS-agreement), <http://www.ogf.org/documents/CFD.107.pdf> (accessed 26.05.14).
46. M.L. Hale, R. Gamble, Secagreement: advancing security risk calculations in cloud services, in : IEEE Eighth World Congress on Services (SERVICES), 2012, pp. 133-140.
47. M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, U. Villano, Security as a service using an SLA-based approach via SPECS, in : IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), vol. 2, 2013, pp. 1-6.
48. M.L. Hale, R. Gamble, Building a compliance vocabulary to embed security controls in cloud SLAs, in: IEEE Ninth World Congress on Services (SERVICES), 2013, pp. 118-125.
49. M.L. Hale, R. Gamble, Risk propagation of security SLAs in the cloud, in: IEEE Globecom Workshops (GC Wkshps),2012,pp. 730-735.