Communications and Network, 2014, 6, 15-21
Published Online February 2014 (http://www.scirp.org/journal/cn)
http://dx.doi.org/10.4236/cn.2014.61003

Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review

Osama Harfoushi[1], Bader Alfawwaz[2], Nazeeh A. Ghatasheh[3], Ruba Obiedat[1], Mua'ad M. Abu-Faraj[4], Hossam Faris[1]
[1]Department of Business Information Technology, King Abdullah II School for Information Technology,
The University of Jordan, Amman, Jordan
[2]Department of Computer Information Systems, Al albayt University, Mafraq, Jordan
[3]Department of Business Information Technology, Faculty of Information Technology and Systems,
The University of Jordan, Aqaba, Jordan
[4]Department of Computer Information Systems, Faculty of Information Technology and Systems,
The University of Jordan, Aqaba, Jordan
Email: o.harfoushi@ju.edu.jo, bm_alfawwaz@aabu.edu.jo, n.ghatasheh@ju.edu.jo,
r.obiedat@ju.edu.jo, m.abufaraj@ju.edu.jo, hossam.faris@ju.edu.jo

Received November 22, 2013; revised December 22, 2013; accepted December 29, 2013

ABSTRACT

Cloud computing is a set of Information Technology services offered to users over the web on a rented base. Such services enable the organizations to scale-up or scale-down their in-house foundations. Generally, cloud services are provided by a third-party supplier who possesses the arrangement. Cloud computing has many advantages such as flexibility, efficiency, scalability, integration, and capital reduction. Moreover, it provides an advanced virtual space for organizations to deploy their applications or run their operations. With disregard to the possible benefits of cloud computing services, the organizations are reluctant to invest in cloud computing mainly due to security concerns. Security is one of the main challenges that hinder the growth of cloud computing. At the same time, service providers strive to reduce the risks over the clouds and increase their reliability in order to build mutual trust between them and the cloud customers. Various security issues and challenges are discussed in this research, and possible opportunities are stated.

KEYWORDS

Cloud Computing; Data Security; Infrastructure; Scalability; Review

1. Introduction

A few years ago, abstract shapes of cloud were used to denote the internet and cyberspace. Afterwards the cloud has been utilized to represent a more specific idea, which is the Cloud Computing. The expansion and evolution of the electronic services requires continuous improvement in terms of infrastructure. Cloud computing offers a relatively low-cost scalable alternative to in-house infrastructure, both in hardware and software [1-5]. NIST [6] defined the term "Cloud Computing" as an ubiquitous on-demand model for accessing common resources over a network. The main idea of cloud computing is to deliver both software and hardware as services. Basically there are three layers of services over the cloud that are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [1]. Individuals and organizations have been considering services over the cloud to cut the costs of expenditure, without any compensation in utilizing recent technologies [7]. Nevertheless, using services over the cloud is accompanied with many doubts mostly about security issues [2,8]. A survey conducted by IDC [9] shows the importance of the challenges for those considering cloud computing as an option. It is shown in **Figure 1** that security is the utmost concern.

Moving essential data over a network to a third-party resource is not an easy decision to be approved. There

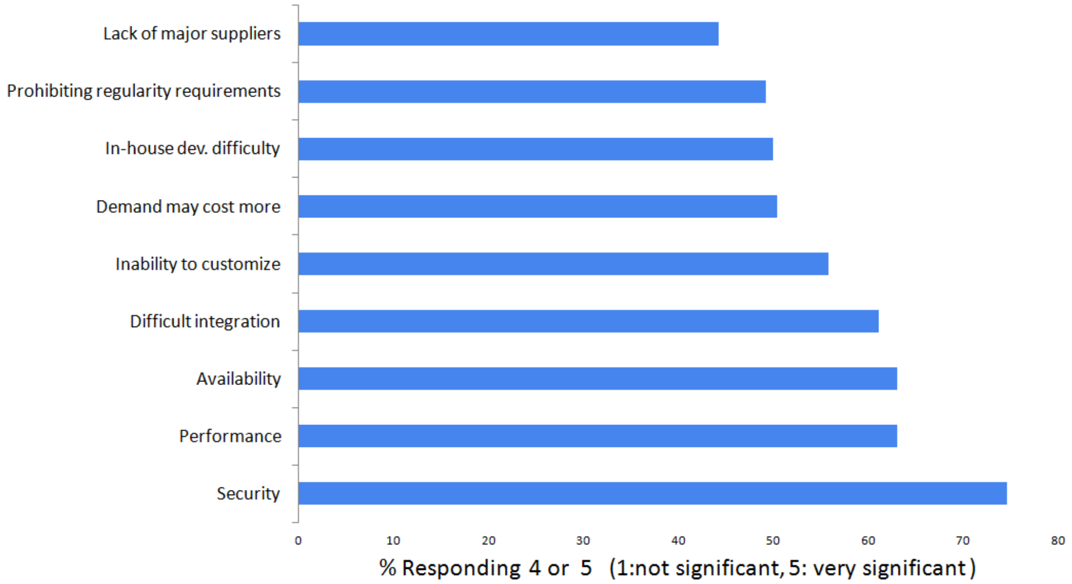

Figure 1. Challenges in considering cloud computing (adapted from [9]).

should be many guarantees as good performance, availability, and mostly secure transmission and storage. Moreover organizations are more reluctant to move essential data when the actual infrastructure, precise cost estimation, privacy level, trust, and many other concerns will be unknown [8,10]. This research presents a conceptual study of the data security issues and challenges in cloud computing. The following section gives a short-term review of literature on security matters in cloud computing. After the consequent sections are arranged as follows: discussing the configurations and security issues in cloud computing while highlighting SaaS, PaaS, and IaaS; presenting related cloud computing challenges; and finally providing the conclusions.

2. Background of the Study

Gartner in [11] recognized seven security risks that are essential to be considered before enterprises make decisions regarding the transformation into a cloud computing model [12]. These problems are as follows: 1) Authorized user access: the potential risk of exposing organizational data over an external processing platform, due to the limited physical, logical and personal controls outside the organizational boundaries. 2) Conformance to regulations: processing data outside the organizational boundaries is still subject to accountability measures, for instance in case of auditing an external third-party space. 3) Storage space: cloud customer has no clue about the exact location of their data that requires service provider commitment to comply with privacy restrictions. 4) Data separation: clouds hold the customers' data over a shared place where data segments are not stored in sequential manner, for that a reliable and well-tested encryption schemes are needed. 5) Recovery: service providers are supposed to make it clear how they will handle disasters and failures. 6) Investigation: breach or intrusion attempts are hard to be tracked and spotted over the cloud due to the dispersion of the data and resources. While in some cases it could be impossible because of the high complexity level. 7) Long-term viability: if a rare case of service provider bankruptcy or acquisition occurs there should be a guarantee of data availability. An organization needs to be sure that it will not lose a huge amount of important data on the long-run.

In [12,13] the authors examined different security and privacy concerns related to cloud computing. They discussed and outlined the risks, their influences, and the opportunities. Adequate levels of reliability, confidentiality, and sensitive data protection are examples of many security concerns [5].

Clouds as a computing model demonstrate a promising future; at the same time they highly require serious acts to cover their weak points. The weaknesses and problems come from unresolved issues in the existing technologies, which are used to build the cloud. Despite the origins or locations of risks and threats, the cloud security as an issue should be handled in a comprehensive manner [14, 15]. Service providers seek fulfilling security requirements over the clouds, but face different challenges to guarantee high level of security. For that, authors in [16] discussed the requirement and challenges, also suggested standardization and management approaches to guide cloud engineers and users. Cloud computing as an approach introduces new risks, influences others, and magnifies some. These risks and their effect on security risks and vulnerabilities were explained in [13]. Standardizing the cloud services security is an important issue that emerged due to the increased demand and importance of clouds [21]. For instance, standardized Security Level Agreement (SLA) guarantees transparent assurance and increases the trust among cloud adopters. These standardized guarantees assist in having mutual trust, reduced risks, and better dissemination of cloud service among organizations as customers, service providers and investors.

3. Security Issues in Cloud Computing

3.1. Security of Cloud Implementation Models

Basically, the deployment of a cloud is managed in-house (Private Cloud) or over a third-party location (Public Cloud). While, for various reasons, it is deployed as an integrated private-public cloud (Hybrid Cloud) [1,8]. A "Community Cloud" is a fourth type of cloud implementation models, where the infrastructure spreads over several organizations and is accessed by a specific community [8]. The different cloud implementation models are shown in Figure 2.

In private cloud configuration an organization may have control over its infrastructure or delegate that to a third-party, being physically on-site or off-site [1,8]. Securing the in-house cloud infrastructure is controllable and requires no need for extra trust mechanisms. While having a third-party service provider running the private cloud is prone to several doubts [8]. Users adopt a private cloud implementation to increase the security level. That decreases the isolation level between the services and the infrastructure. For instance, managing the security of the provided service in conjunction with the existing firewalls and protection services. Furthermore, operating over a secure virtual private network is an option to isolate the private cloud hosted by a third-party. Despite the benefits of a private cloud, several issues need attention as unbalanced resources utilization. An idle infrastructure is a wasted resource for example [17].

Public cloud implementation is a model in which a service provider, third-party, offers public services on pay-per-use manner. Some of the benefits of this model are the economies of scale, ability to have short-term usage and greater resources utilization [1]. Secure use of the shared public cloud is more challenging compared to private clouds. For that, public cloud suits more incidental or less vulnerable applications [17]. In [8] the authors stated that trust is an important issue for public clouds, hence the management is governed by a third-party. A trusted third party auditor (TPA) is proposed in [18] to solve the trust issues in public clouds. A TPA is expected to analyze the public cloud services and provide an adequate report. Public cloud service providers are supposed to prove the credibility of their systems, guarantee service availability, ensure a high level of data protect and handle security breach attempts efficiently [1,8,18].

An organization reluctant to fully trust the public/ community cloud, due to security issues, may think of having a hybrid cloud implementation. Without compromising the security of essential data, they have the possibility of keeping only sensitive data on a relatively small private cloud [1,8,17]. The rest of less-sensitive

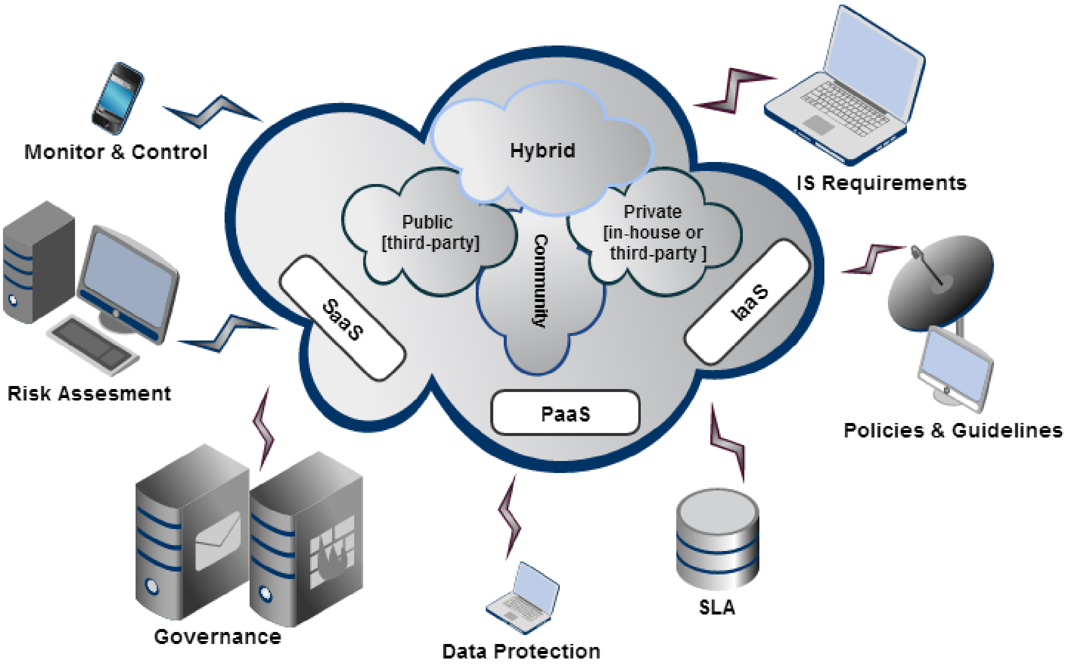

Figure 2. Cloud implementation model (adapted from [8,21]).

data may reside on a public or community cloud to have better utilization of resources. With the hybrid cloud model it is possible to integrate the different implementation models while having an adequate balance and enabling portability of data and services [8]. Though, vulnerabilities are reduced in hybrid clouds, threats still possible over integration points between the different cloud models.

3.2. Security of Service Delivery Models

Cloud service providers mainly offer three delivery models that are the SaaS, PaaS, and IaaS, alternatively called provision and distribution models. **Figure 3** illustrates the delivery models and their basic components. Other delivery models exist, for example in [19] the authors mentioned the Human as a Service (HuaaS), and the Support Services. Here the main security requirements for the three delivery models are exhibited.

IaaS layer provides the primary infrastructure of the cloud as a service to the customers. Infrastructure is the main hardware components and their management software that includes servers, network, storage, file system and operating systems [1,17]. Customers using IaaS have a limited control over the actual infrastructure, as their usage is based on pay-per-use only [3]. Securing the IaaS layer is divided into two main areas, the virtual environment and the physical environment [8,12]. Several security requirements need to be present at the virtual level, which includes controlling the access, data encryption, secure communication channels, and virtual protection [8]. On the other hand in terms of physical components, it is required to ensure the hardware reliability, and preventing physical intrusion [8,12].

PaaS is the application deployment level, where developers are supposed to develop their applications and implement them. Though, some authors [1,8] consider PaaS and IaaS to be at the same layer rather than two. A platform usually enables utilizing development platform, databases and middlewares [17]. Meanwhile, platform providers currently enable a limited number of specific development languages and API’s. For example the limited development languages on Google AppEngine, Facebook Platform, Microsoft Azure and ZohoCreator [19]. The security requirements for PaaS are almost the same as those for the IaaS. Since both share the virtual environment characteristics. The differences in the security measures, if any, are related to the components’ level or the role of the service user, a developer or system administrator for instance [8].

SaaS is usually accessed over the internet by the end users (tenants) as employees, managers, clients and auditors [1,8,17]. It is possible that SaaS may run over an IaaS or PaaS operated by a different provider [17]. This service delivery level encompasses various on-demand applications ranging from automation and productivity to enterprise integration [3]. Being at the higher level of service delivery it requires a relatively different level of security. The main concerns include preserving the privacy, preventing impersonation, availability of services, secure communication and data protection [8,17]. Another important dimension of security to look at is the SaaS provider being a customer to IaaS or PaaS providers [1].

IaaS, PaaS and SaaS service delivery models together are considered the foundations of cloud computing. The complexity of the cloud services as an interrelated system is high, for that managing the security is complex as well. Depending on the service provided by the cloud, the security measurements may vary in application but they still an issue. Another security dimension to consider is the interface channels between the delivery models.

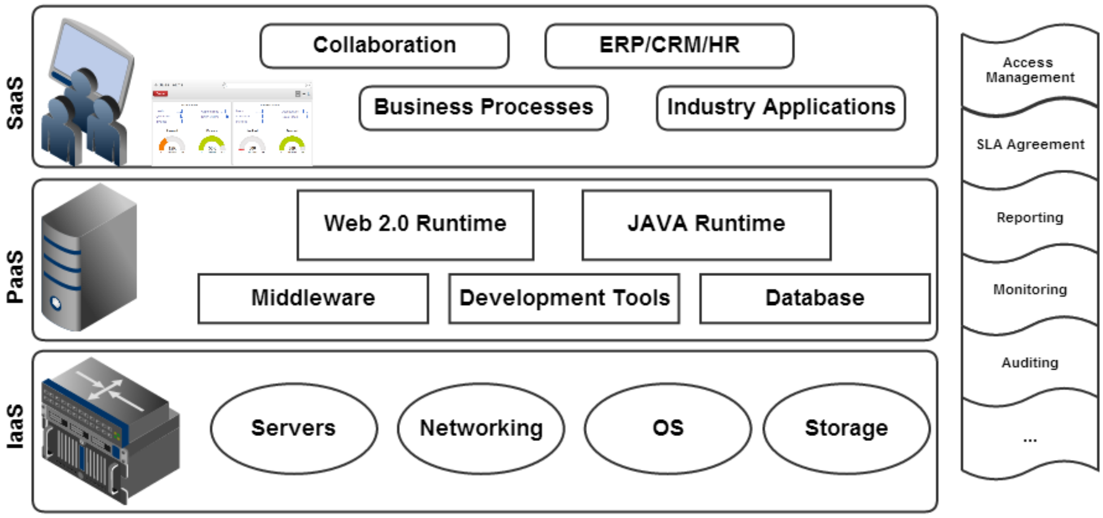

Figure 3. **Cloud computing delivery models (adapted from [8,12,19]).**

Regardless of the delivery model, there are three security levels that are application, virtual and physical level [8, 19]. As the complexity increases, various challenges and issues arise and therefore the need and effort for resolving them increases.

4. Cloud Computing Challenges

Moving towards cloud computing seems to be promising but is has to overcome different challenges. The current state of the services, provided on the cloud, opens the door for many doubts. In [1,3,8,21] the authors present some of the challenges that include security matters, feasibility, interoperability beside many others. Authors suggested alternatives and possible solutions to face the various challenges, while others highlighted the need for further improvements.

Security is a critical issue that worries those considering an external outsource to hold their data and processes [8]. The concerns exceed the potential of data loss and corruption to matters of trust, service availability, and unpredictable issues. Some facts demonstrate the availability challenge as [1] points to instances of Google services interruption ranging from 1.5 to 8 hour periods in 2008. Authors in [1] highlighted ten obstacles to the expansion of cloud computing along with potential opportunities for recovery. Among the obstacles there is the confidentiality of data for which they suggest data encryption as an opportunity for resolution. Moreover, authors in [21] pointed out to the need for serious acts toward improving the security of the clouds. One of the proposals is the assurance given by Service Level Agreement (SLA) that is between the users and the service provider. On the other hand, in [14] one of the proposed possibilities is a “multi-tenancy” support in which customizable security options allow individuals to adapt to their desired context.

It is challenging to justify the costing model in terms of cloud services. Cloud customers need to think of different tradeoffs regarding the cost of security mechanism, communication, computing power, and integration. The infrastructure cost will be replaced by the cost of data transfer and connectivity. Limiting the cost of communication is not an option, due to the high reliance on regular large amounts of data transfer [1]. Taking the special case of hybrid clouds where constant data transfer is required between the private cloud, in-house IT infrastructure, and the public cloud. In [7,21] the authors discussed the managerial decisions of selecting a suitable costing model based on the available alternatives. Also they stated that on-demand services offer reasonable usage-based fees for startups, in contrast to the high cost of in-house infrastructure. Cloud services will replace or integrate with an in-house infrastructure, which requires a serious study of the charge-back model. Cost analysis becomes more complex compared to the establishment of legacy infrastructure. In [20], authors presented three areas for billing customers over the cloud, which are the cost of storage, access, and processing. That increases the analysis dimensions considering a public cloud service. On the other hand, designing a secure architecture will have an overhead of optimization to minimize the public cloud cost. Considering a hybrid cloud is a possible solution to gain a better return on investment [21]. A trade-off between the private or public cloud utilization is needed to maximize the benefits over the costs, taking in consideration the desired security level.

SLA is an important matter when considering public cloud services, as presented in [14]. It is important to have an assurance before conducting serious business operations over third-party resources. The provider is expected to ensure service accessibility, availability, dependability and performance. Potential problems of the agreements include the interpretation of the conditions, as well as the evaluation criteria of the terms. That creates confusion on one hand; on the other hand the terms may omit the customers’ expectations or requirements. Furthermore, the terms vary and increase the SLA complexity for different cloud offerings as for Iaas, Paas, and Saas. For that the SLAs need to be flexible in a way that adapts to customer specific requirements, at the same time clear to both parties. Automated SLAs try to overcome the challenges here, but practically it is difficult as highlighted in [22].

Deciding what to migrate is challenging, customers may hesitate when determining what to put over the cloud. Despite the reduction in the capital and operational expenditures, trust and security concerns limit the migration decisions [7]. The results of an investigation presented in [23] show that security is the most significant concern. Specifically, the respondents are apparently consider data protection and SLA at the top of the requirements for evaluating a service provider, while the security is almost a must when the migration to the cloud is already in place. That indicates the tendency to prohibit the migration of sensitive resources once security is not clear and highly assured. IDC’s [24] survey shows an expected dramatic spending increase to develop public clouds by 2014, to be around 55.5 billion US Dollars. More than half of the spending is going to applications development, while infrastructure, servers and storage follow. Though, migration is expected to be with higher possibility towards SaaS, coming next IaaS and PaaS respectively.

The interoperability of in-house systems and data with cloud services is not straightforward. The lack of common interface raises the issue of data lock-in [1]. Furthermore, expanding the cloud services, possibly utilizing different clouds, is challenging and could be impossible in some cases. Adopting a hybrid cloud approach raises many questions about compatibility of data and operations as well. Public and private clouds integration without common standards prevents a smooth and quick cloud expansion. In [21] the authors pointed to the need of standardizing the security issue, possibly by adopting a well-formulated security standard. Accordingly, a proposed solution in [1] suggests implementing standardized API's, which makes switching between clouds or services easier.

5. Conclusion

Cloud computing has been a surpassing shift so far in terms of utilizing the current technologies. The trend of having cloud services as part of an organization seems to be gaining more importance. Especially in this era the cycle of introducing more technological innovations is getting shorter. For many reasons, including the reduction of capital expenditures, organizations need to consider utilizing cloud services as an essential part of their foundations. Nevertheless, various challenges are prohibiting the attainment of vast deployment and acceptance levels. The main drawback of the existing cloud service implementations is their inability to provide an accredited high security level. Moreover, security assurance needs to cover the transmission channels which might include a third-party. To have better utilization of cloud services many issues need to be enhanced in a way ensuring high level of security, confidentiality, authenticity, integration, agility, scalability and trust. Possibly an automated SLA, third trusted party, or a novel innovation would be an interesting study area to cover the security issues related to cloud computing.

REFERENCES

[1] M. Armbrust, A. Fox, R. Grith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, Vol. 53, No. 4, 2010, pp. 50-58. http://dx.doi.org/10.1145/1721654.1721672

[2] A. M. Andrew, "Cloud Computing: Views on Cybersyn," *Kybernetes*, Vol. 41, No. 9, 2012, pp. 1396-1399. http://dx.doi.org/10.1108/03684921211275450

[3] S. Dhar, "From Outsourcing to Cloud Computing: Evolution of It Services," *Management Research Review*, Vol. 35, No. 8, 2012, pp. 664-675. http://dx.doi.org/10.1108/01409171211247677

[4] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications*, Vol. 34, No. 1, 2011, pp. 1-11. http://www.sciencedirect.com/science/article/pii/S1084804510001281 http://dx.doi.org/10.1016/j.jnca.2010.07.006

[5] B. R. Kandukuri, V. R. Paturi and A. Rakshit, "Cloud Security Issues," *Proceedings of the* 2009 *IEEE International Conference on Services Computing*, Washington DC, 21-25 September 2009, pp. 517-520. http://dx.doi.org/10.1109/SCC.2009.84

[6] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Computer Security Division, IT Laboratory, National Institute of Standards and Technology, Gaithersburg, 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[7] M. Jensen, J. Schwenk, N. Gruschka and L. Iacono, "On Technical Security Issues in Cloud Computing," *IEEE International Conference on Cloud Computing*, Bangalore, 21-25 September 2009, pp. 109-116.

[8] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems*, Vol. 28, No. 3, 2012, pp. 583-592. http://www.sciencedirect.com/science/article/pii/S0167739X10002554 http://dx.doi.org/10.1016/j.future.2010.12.006

[9] F. Gens, "New IDC It Cloud Services Survey: Top Benefits and Challenges," 2009. http://blogs.idc.com/ie/?p=730

[10] C. Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 era," *Journal on Telecommunications and High Technology Law*, Vol. 8, No. 2, 2010, pp. 359-424.

[11] J. Brodkin, "Gartner: Seven Cloud-Computing Security Risks," InfoWorld, 2008. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[12] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," *International Conference on Computer Science and Electronics Engineering*, Vol. 1, Hangzhou, 23-25 March 2012, pp. 647-651.

[13] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security Privacy*, Vol. 9, No. 2, 2011, pp. 50-57. http://dx.doi.org/10.1109/MSP.2010.115

[14] M. Almorsy, J. Grundy and I. Müller, "An Analysis of the Cloud Computing Security Problem," *Proceedings of the* 2010 *Asia Pacific Cloud Workshop*, Australia, 30 November 2010.

[15] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?" *Computer*, Vol. 42, No. 1, 2009, pp. 15-20. http://dx.doi.org/10.1109/MC.2009.20

[16] K. Popović and Z. Hocenski, "Cloud Computing Security Issues and Challenges," *Proceedings of the* 33rd *International Convention in MIPRO*, 2010, pp. 344-349.

[17] D. Jamil and H. Zaki, "Cloud Computing Security," *International Journal of Engineering Science and Technology*, Vol. 3, No. 4, 2011, pp. 3478-3483.

[18] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," *Proceedings IEEE in INFOCOM*, San Diego, 14-19 March 2010, pp. 1-9.

[19] A. Lenk, M. Klems, J. Nimis, S. Tai and T. Sandholm, "What's Inside the Cloud? An Architectural Map of the Cloud Landscape," *Proceedings of the* 2009 *ICSE Workshop on Software Engineering Challenges of Cloud Computing*, Washington DC, 23 May 2009, pp. 23-31. http://dx.doi.org/10.1109/CLOUD.2009.5071529

[20] J. Shamsi, M. Khojaye and M. Qasmi, "Data-Intensive Cloud Computing: Requirements, Expectations, Challenges, and Solutions," *Journal of Grid Computing*, Vol. 11, No. 2, 2013, pp. 281-310. http://dx.doi.org/10.1007/s10723-013-9255-6

[21] S. Ramgovind, M. Elo and E. Smith, "The Management of Security in Cloud Computing," *Information Security for South Africa*, Sandton, 2-4 August 2010, pp. 1-7.

[22] C. Weinhardt, A. Anandasivam, B. Blau and J. Stosser, "Business Models in the Service World," *IT Professional*, Vol. 11, No. 2, 2009, pp. 28-33. http://dx.doi.org/10.1109/MITP.2009.21

[23] A. Aleem and C. R. Sprott, "Let Me in the Cloud: Analysis of the Benet and Risk Assessment of Cloud Platform," *Journal of Financial Crime*, Vol. 20, No. 1, 2013, pp. 6-24. http://dx.doi.org/10.1108/13590791311287337

[24] F. Gens, "IDC's Public IT Cloud Services Forecast: New Numbers, Same Disruptive Story," 2010. http://blogs.idc.com/ie/?p=922