

# ADMINISTRATION SECURITY ISSUES IN CLOUD COMPUTING

Hamoud Alshammari<sup>1</sup> and Christian Bach<sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, University of Bridgeport,  
Bridgeport, Connecticut, USA  
halshamm@bridgeport.edu

<sup>2</sup>Department of Computer Science and Engineering, University of Bridgeport,  
Bridgeport, Connecticut, USA  
cbach@bridgeport.edu

## ABSTRACT

*This paper discover the most administration security issues in Cloud Computing in term of trustworthy and gives the reader a big visualization of the concept of the Service Level Agreement in Cloud Computing and it's some security issues. Finding a model that mostly guarantee that the data be saved secure within setting for factors which are data location, duration of keeping the data in cloud environment, trust between customer and provider, and procedure of formulating the SLA.*

## KEYWORDS

*Cloud Computing, SLA, Service Level Agreement, Trust, Security*

## 1. Introduction

Although new technologies are always emerging to back up the security of the nation, these technologies are also possible roots of the problems that security faces. Having high-tech equipment will indeed counter possible technological threats to security [1]. Cybercrimes in the web community are a major threat that affects a national context. To defend homeland security in the cyber world, it is important to learn how to cope with it. According to Homeland Security News Wire [2], “fighting cybercrime around the world requires strong legal structures to enable prosecutions; a trained corps of investigators to respond to crimes; and the ability to cooperate internationally.”[3].

Security risks are naturally related to all integration technologies. In a time when the Internet is a household commodity, there are certainly new possible threats to securities[4]. Technologies that threaten to bring destruction to security must be countered by technologies as well. The Internet is being viewed as a security endemic, which corporate risks both real and technological. One issue that allows cybercrimes to occur is the weakness in security of the cloud computing security[5,6].

Actually, cloud computing plays an important roles between the new computing concepts and information policies[7]. Cloud computing raises many issues regarding privacy, anonymity, liability, security, and government surveillance and so on, so the existed laws are not really applicable to these new ideas[8]. Because of these weaknesses in the concept of could computing, some information polices that have been developed and improved by the users like creation implementation, and using the technologies, that the law catches up of these activities [9].

## 2. What is the cloud computing?

Cloud computing is defined by the National Institute of Standards and Technology [10] as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Cloud Computing gives a developed paradigm in terms of on-demand (provisioning) of computing infrastructure. That paradigm converts the location of the physical infrastructure to the network to cut off some costs that are associated with the management of software and hardware resources[11].

Cloud is drawing the attention from the Information and Communication Technology (ICT) community, thanks to the appearance of a set of services with common characteristics, provided by important industry players. However, some of the existing technologies the cloud concept draws upon (such as virtualization, utility computing, or distributed computing) are not new[8].

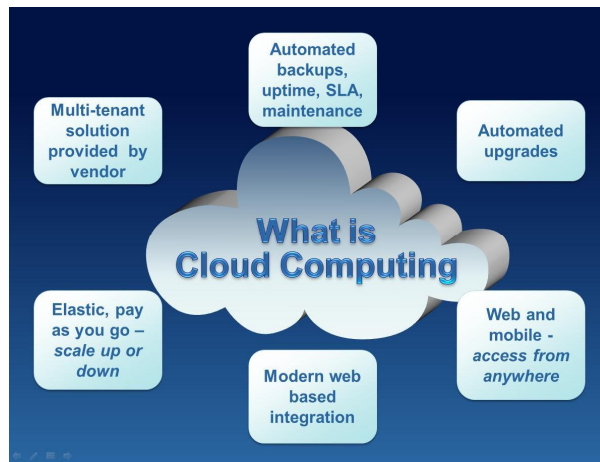


Figure 1. Some of Cloud computing prosperities

Figure.1 [12] shows some concepts that are related to the definition of Cloud Computing. However, other concepts are defined in Cloud Computing environment like DÉJÀ VU, which means to get more benefits from the predication and expectations. Also, the virtual monitoring of the processes in Cloud Computing (VM) which gives the availability of distributing the data among vary servers in the Cloud Computing environment to make the access to the resource more easy and fast [13].

## 3. Using of cloud computing

Seeking more ability to use information widely and reduce the cost of this usage, organizations started using the technology of cloud computing. Some research studies described the cloud as a technology for which one pays per use, which means that the user will pay for the exact tools that he or she uses [14]. Cloud computing gives an ability to pay as using of the computing resources on short-term period of time for example, processing a request for an hour or storage for a day. Also, it releases them when needed or when they are no more useful [2].

Different application could be used via Cloud Computing to meet some security requirements or other requirements like the I-Voting application system. This system provides two of most important conditions of any voting systems which are time of data collection and security of the results [15]. Another using of Cloud Computing is in learning purposes as electronic learning (E-Learning) which is very helpful to save time and cost [16].

#### **4. Service Level Agreement [SLA]**

A third party concept could be used in cloud computing to monitor the data or the whole system that comes in between of the provider and customer. However, there might be some users that there are not comfort with the third party because of the ability to use their information [9]. In this case, the provider and the third party might create the same threat to the client's data.

Usually, the third party works with the service provider and client to control and save the datacenter. In cloud computing, the Private Virtual Infrastructure (PVI) model has been suggested to distribute the responsibility of control and save the datacenter between providers and clients[18]. In this model, users have security over their information in the cloud, and providers would have security over the fabric of the server.

Many enterprises said they were not using the cloud because these services are less secure. But the reality may be the opposite. The hosting companies expanding into the cloud told us that security is one of their core competencies, so it is more a necessary evil for most enterprises. As Greg Papadopoulos, Sun's CTO, put it, "Over time, people will start to view an external service provider as more compliant than internal. They are disinterested third party. Their job is to hold your data but it involves you and me to collude. As a third party provider I would have no motive to muck with your data"[19].

Service level agreement [SLA] between client and provider is critical to defining the roles and responsibilities of all parties involved in using and providing cloud services. The SLA should explicitly call out what security services the provider guarantees and what the client is responsible for providing. As shown in (fig. 2) [20] which explores the methodology of having assured SLA via following some steps that provide the duties and rights that either provider or customer has. Start with defining the service level, designing the service, placing the service, capacity planning, optimizing the resources, and managing and operating the service. The feedback still needed to update the service and the operations.

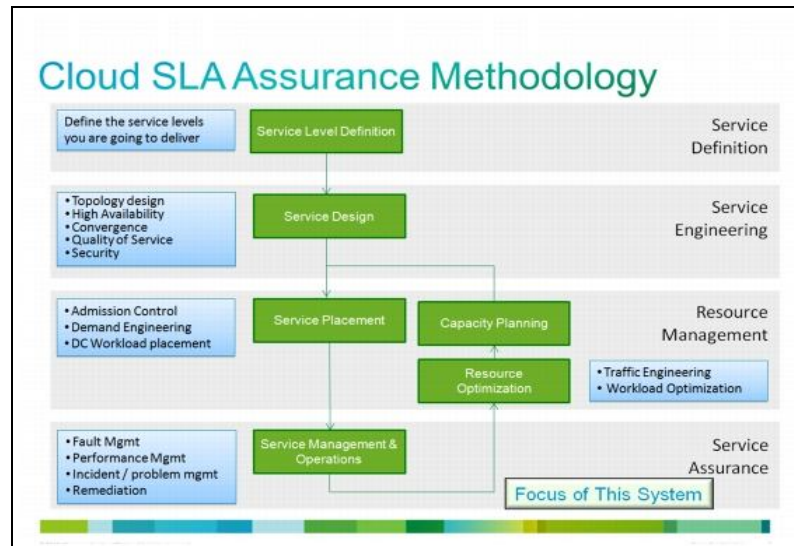


Figure.2 Service Level Agreement Methodology

Web Service Level Agreement (WSLA) framework was developed for SLA monitoring and enforcement in SOA[3]. In the Cloud Computing environment, the monitoring and enforcement tasks are delegated to a third party to solve the problem. However, the third party could use the data illegally or could modify it. On the other hand, one of the weaknesses of using the third party idea is the absence of trust between the provider and the third party or the client and the third party.

## 5. Research Method

Exploring the concept of Cloud Computing and some of its security issues is done by a complete literature review and answering some of questions that has a direct relationship with the research topic. Despite of the fact that the Cloud Computing is one of the hottest topics these days because there is no fully agreement between the vendors and the customers around the world [19].

The Qualitative research methodology is one of the popular methodologies that the researchers follow in many fields like social studies, Human and governments behaviours. The object of this kind of researches is to gather data and analyse it based on the research questions, and then the researcher can present the results and conclusion [21]. The main goal of the Qualitative descriptive studies is to summarize the whole events and data in the terms of the events. Usually researchers stay close to the data meaning that they have got from the words and events [22].

In Qualitative research method, the data is categorized into different forms to report the results and organize them. "Qualitative researchers typically rely on the following methods for gathering information: Participant Observation, Non-participant Observation, Field Notes, Reflexive Journals, Structured Interview, Semi-structured Interview, Unstructured Interview, and Analysis of documents and materials"[23]. Mainly, to observe data from its main sources, the survey methodology is followed in that case. However, the qualitative method could play the same role and give some sort of exact result if it followed by researchers. The main benefits of the following the second method is to reduce the cost whereas the survey method is more efficient in

the terms of the cost. Easley gathering information in the qualitative method might be preferred from the researchers for that reason [24].

### **5.1. Where is the location of the data in the cloud? Is it legal to transfer the data to another data center in another country?**

The service providers usually don't place the location of the application. Most of them don't have geographic coverage [17]. For example, Amazon EC2 doesn't provide the users the exact location of the application neither they couldn't ask for providing the location of these applications. However, some governments' agencies require knowing where the exact location and ask to keep them between the country's borders based on some regulations on these countries[19].

When one uses the cloud, one probably will not know exactly where his or her data are hosted. In fact, he or she might not even know what country it will be stored in. Customers must ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customer [25]. Also, this question leads us to the think about the requirements that the customers have to obey when they want to keep their data away from the providers.

Cloud computing process does not distinguish between government and business information, so the cloud process deals with government data just as it deals with business data. Consequently, the data might be inside the country's borders or outside it. Thus, the data could face different threats of being stolen or used for illegal activities.

### **5.2. How long is the information retain in cloud environment? Who can control the policy of administration the data in the cloud?**

Even if a customers usually don't know where their data are, the service provider should explain them what would happen to the services and the data in case of a disaster[25]. Replicating data and application infrastructure is very important because any offering doesn't apply that replicating across multiple sites is usually vulnerable to some failures. When the service provider go broke the company or the database, the customer must be sure that the data remains available during these changes.

It is important that the data in the cloud environment continue to exist for a period of time that the provider and the customer have agreed about. Consequently, we will examine the Service Level Agreement [SLA] wherein the provider and the customer state their conditions [18]. The SLA is where governments as customers can establish their conditions to make their situations stronger. For example, the government can set conditions about the people who can reach the information and modify it, the time when information should exist or not, and the place where the information should be stored. However, the provider might be one of the weakest points in the SLA.

### **5.3. Could data be copied by cloud service provider (CSP)? Can the data be destroyed, or can he make the data inaccessible? Is the CSP keep the data for his special usage?**

Some issues in cloud computing, such cloud security and data privacy might be in concern because of the absence of the cloud computing standards because each cloud provider takes a different approach and offers different services [26]. Therefore, the provider is the only

one that really has the ability to reach the information and modify it without getting permission. The client cannot control the provider's access to the information.

The only way the client can control his or her information is through the SLA between him or herself and the provider. On the other hand, the third party solution might solve some problems, but not all of them. The third party is someone who works as a broker between the client and the provider to make the information more secure from illegal use [27]. In general, there is no secure procedure the organization or the government can follow to make information secure in the cloud environment, so the data cloud faces these kind of unsecure behaviours like being destroyed rather than secured or being kept longer than necessary and so on.

#### **5.4. Cloud makes huge changes in IT**

IT systems in Cloud Computing have been enabled to be more scalable and elastic, so the end users don't need to determine their requirement of computing resources in advance. Consequently, they request their requirement on demand provisionally [28].

To use Cloud Computing services, the governments don't need to own the infrastructure to serve millions of people. However, using cloud computing is not favoured by government agencies because of some security issues [29].

#### **5.5. Cloud Computing can improve IT in public sector**

Some government agencies accepted the cloud computing in some of their applications to gather some benefits. NASA Nebula gives the researchers ability to access the IT services for small period of time. Without this help, the researchers would take months to procure and configure the IT resources and significant management to control and monitor the systems[29].

Cloud Computing can improve the scalability and elasticity in the IT applications and resources in public sectors. By using of cloud computing on-demand facility, the public sectors don't need to determine their needs in advance [30].

#### **5.6. Resources being in higher-value activities by efficiency improvement**

“Approximately thirty cents of every dollar invested in federal IT was spent on data center infrastructure. Unfortunately, only a fraction of this investment delivers real, measurable impact for American citizens. By using the Cloud Computing model for IT services, we can reduce our data center infrastructure expenditure by approximately 30% (which contributes to the estimated \$20 billion of IT spending that could be migrated to cloud computing solutions)”[2].

The software applications and end-user support systems will improve the efficiency in systems that use Cloud Computing. The capacity and investments in agency missions could be increased using these savings, including citizen-facing services; which are those services in governments that directed to the public, and inventing and deploying new innovations [28].

Cloud computing allows IT organizations to be simplified, since they don't have to maintain complex, mixed technology applications anymore. The focusing on the work will be moved from the technology itself to the mission of the government agency [31].

### **5.7. Duplication of information will be reduced by demand aggregation**

Moving of data, application, and infrastructure into the cloud environment can be improved and helped by using of cloud computing by focusing on the issues that associated with federal organization and funding by increase the efforts on the IT services as utility [32]. However, the aggregation might cause more cost in terms of static and dynamic aggregation methods. "The dynamic aggregation scheme results in 8% to 40% savings over the static aggregation scheme when the degree of aggregation is high"[33].

Management and cost of procurement usually effected by IT services, similar to the current model that is used for utility services and buildings [2]. Data and systems cloud have more flexible environment by using cloud computing. So, by using appropriate standards, many organizations and systems might go to use common services and platforms [34].

## **6. Model: Secure Data Agreement in Cloud Computing**

This model has been developed to formulate the main factors of having secure data agreement in cloud computing, so we will discuss the main four factors:

### **6.1. Location of the data/services**

Usually, services providers don't explain the geographical location of the servers. So, many customers don't trust these services from that provider. Consequently, different users or agencies might ask the provider to locate their data in boarder of the country or in specific location that they trust to avoid the hacking or loosing the data [2, 35].

SLA helps to manage this factor by state the conditions that the provider and the consumer must follow and the penalties that they might get in case of breaking these conditions. So, the location should be explained to the customer if he asks to know that, otherwise the SLA won't help with that [36].

Data Location and Relocation help to reduce some costs in communications or in storage resources in the Internet, based on a study that [37] have done, the results show that importance of Routing Problems and Data Location in the Cloud in case the provider provides the service in efficient manner. So, based on some factors of locations, the services could be costly or not [36]. However, some users might ask for knowing the location because he should be aware about the exact location as what we proposed before.

### **6.2. The period of time that the data is still available in Cloud**

One of main factors that the consumer of Cloud Computing should know is the how long of time that his data be available in cloud. In the other words, when and how has the ability to delete or move the data from the servers. Some of providers/consumers believe that because of less cost of storage the data in cloud, there is no need to move or delete it. In contrary, some of the data owner wants to manage the data by themselves whereas the owner of the servers might believe in the opposite way [38].

Also, SLA could help to manage this factor. In general, the consumer has the rights to manage the data via the third party, so managing the period of time or moving and deleting the data is one of the consumers job. However, the trust is playing a main role here. For example, if the consumer asks to delete some data, which can guarantee that, this data is being deleted?

The [39] Provides essential characteristics that help to determine the availability of data in cloud environment, which are on-demand self services, broad network access, resource pooling, rapid elasticity and measured service.

### **6.3. Trust between services provider and consumer**

You can find the concept of Trust is presented where you read about security between two different involved people. In addition, in Cloud Computing the concept of Trust is stated in the SLA between the provider and the consumer. Consumer and provider should follow the key factor of the agreement, which is the trust [9]. Online relationship is one of the most dangerous relationships between people, so during many activities between the provider and consumer the trust grows exponentially. Creating trust and security is one of the most important factors for the success of cloud computing. Cloud computing are facing a lot of challenges when the trust is absent. So, there is no general form of Trust evaluation models for cloud computing environment [40].

The main Idea of cloud computing that the user can use and operate the services in cloud environment directly which provided by the providers. So, the impact and destruction for resources in cloud computing is worse than the current real Internet environment which also shares the recourses. Therefore, whether or not the behaviour of the cloud users are trusted, the question still exist which is how can evaluate the user behaviour in trustworthy point of view. So, still the process of evaluating the trust of the users has not general template to be followed, so the trust still under practical evaluation process [41].

### **6.4. Service Level Agreement [SLA]**

Users mainly using the main two operations in cloud computing which are upstream and downstream operations in on-demand model, so they can discuss and negotiate some terms and factors to manage some issues as license agreement, using of data, scalability and fundamental breaches [26].

In cloud computing environment, verifying security happens by leading every service to be able to report security facilities in present and verify it. So, these ability means the client needs to have the authority to configure and set the fabric [42]. Although the client is the data owner, sometimes it is not a good idea to give him or her the ability to modify the data or to monitor it because sometime the clients might be lazy about keeping the information secure.

The [42] Proposed a new Reputation System to address the challenging of the process of evaluate the reliability of providers or resources. Also, they proposed a SLA template pool to drive the negotiation between the customers and providers more equitable, convenient and transparent.

## **7. Importance of Cloud Computing**

In cloud computing, there are uncertainties between the policies in public and the capacity in technical demand in terms of developing and provisioning of cloud computing services. The technical solutions could not be adequate or compatible with some policies in some cases, like providing so much security that cloud be guaranteed by providers as a kind of results of data collection processes in some agencies [9, 43].



Developing the cloud environment depends on different factors, as the time that the basic technology completed, the time that the different technologies like computers and telecommunications industries accept the standards, the amount of costing the effects and many different others [7, 43]. Each of these factors can be influenced by government policy. Governments can control the growing of the cloud computing by many ways. Some of them just like and development in the Internet based application system.

### **7.1. The progress would be influenced by some factors [7]:**

- Giving ability to the researchers around the world to access cloud computing services to make science research easier and international;
- Offering an adequate level of security and privacy for the information that is already in the cloud.
- Making access to the cloud easier and affordable for people like researchers and developers.

In general, for governments to operate their operations on cloud infrastructure is more reliable and kind of secure and less costly, than operate the operations and managing hundreds of different systems in traditional network [44]. Also, Cloud Computing support the governments and users to not be locked or stuck with a specific providers or vendors.

## **8. CONCLUSIONS**

Different issues that have been showed over by cloud computing are similar to the issues that the governments have been stuck with form years like privacy, trustworthy, data protection and accessibility. So, to address these issues could cost the cloud as twice as the cost of addressing them in the normal Internet ways because of difficulty and importance.

Because of the Cloud Computing is a many to many applications and medium, it is not that easy to determine the responsible for some issues and the location or the time. Also, government policies should be flexible to meet the quick changes in cloud and technology. The main point of solution to get more secure Cloud Computing environment is to have a strong Service Level Agreement or any trust third party that can control the processing over Cloud Computing. Data location, the period of time that the data must be exist in cloud, trust between provider and customer, and the designing of service level agreement SLA are the main factors that we discussed in this work.

## **ACKNOWLEDGEMENTS**

This work is performed as a requirement from the Department of Technology Management in University of Bridgeport with all thanks to the department of Computer Sciences and Engineering.

## **REFERENCES**

- [1] Regan, P.M., Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly*, 2004. 21(4): p. 481-497.
- [2] Armburst, F., Griffith, Joseph, Katz and Knowinski, A View of Cloud Computing. *Communications of the ACM*, 2010.
- [3] Dawoud, W., Ibrahim Takouna, and Christoph Meinel, Infrastructure as a Service Security:

- Challenges and Solutions. Postdam, Germany: Hasso Platter Institute, 2010.
- [4] Gerber, B.J., et al., On the Front Line American Cities and the Challenge of Homeland Security Preparedness. *Urban Affairs Review*, 2005. 41(2): p. 182-210.
- [5] Paquette, J.a.W., Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly* 2010.
- [6] Braman, S., Change of State: Information, Policy, and Power. RECIIS. *Elect. J. Commun. Inf. Innov. Health*. Rio de Janeiro, 2007.
- [7] Nelson, M.R., The Cloud, the Crowd, and Public Policy. *ISSUES IN SCIENCE AND TECHNOLOGY*, 2009.
- [8] Vaquerol, L.M., A Break in the Clouds: Towards a Cloud Definition. *ACM SIGCOMM Computer Communication Review*, 2009.
- [9] Jaeger, L.a.G., Cloud Computing and Information Policy: Computing in a Policy Cloud? . *Journal of Information Technology and Politics* 2009.
- [10] Wise, C.R. and R. Nader, Organizing the federal system for homeland security: Problems, issues, and dilemmas. *Public Administration Review*, 2002. 62: p. 44-57.
- [11] Brian, H., et al., Cloud computing. *Communications of the ACM*, 2008. 51(7): p. 9-11.
- [12] JConcepts, T.T.M., Cloud ERP Software Company in Los Angeles. <http://abouttmc.com/microsoftdynamicsgp-netsuite-vs-microsoftdynamicsnav/netsuite/what-is-cloud-computing/>, 2012.
- [13] Chen, Y., V. Paxson, and R.H. Katz, What's new about cloud computing security? University of California, Berkeley Report No. UCB/EECS-2010-5 January, 2010. 20(2010): p. 2010-5.
- [14] Xu, W., W. Beizhan, and H. Jing. Cloud computing and its key techniques. in *Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on*. 2011.
- [15] Ramesh, S. and V. MuraliBhaskaran. Internet voting using cloud computing. in *Sustainable Energy and Intelligent Systems (SEISCON 2011), International Conference on*. 2011.
- [16] Kalagiakos, P. and P. Karamelas. Cloud Computing learning. in *Application of Information and Communication Technologies (AICT), 2011 5th International Conference on*. 2011.
- [17] Islam, S.S., et al. Cloud computing for future generation of computing technology. in *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on*. 2012.
- [18] Morin, J., J. Aubert, and B. Gateau. Towards Cloud Computing SLA Risk Management: Issues and Challenges. in *System Science (HICSS), 2012 45th Hawaii International Conference on*. 2012.
- [19] J., S., Is Cloud Computing Ready for the Enterprise. for *Infrastructure & Operations Professionals*, 2008.
- [20] CISCO, Cloud Service Assurance for Virtualized Multi-Services Data Center 2.2. CISCO.
- [21] Franklin, M.I., *Understanding Research: Coping with the Quantitative-Qualitative Divide*. London/New York. Routledge, 2012.
- [22] Sandelowski, M., Focus on Research Methods-Whatever Happened to Qualitative Description? *Research in nursing and health*, 2000. 23(4): p. 334-340.
- [23] Marshall, C., & Rossman, G. B. , *Designing qualitative research*. Sage Publications, Incorporated., 2010.
- [24] Creswell, J.W., *Research design: Qualitative, quantitative, and mixed methods approaches* 2008: SAGE Publications, Incorporated.
- [25] Popović, K., Cloud Computing Security Issues and Challenges. *MIPRO magazine*, Croatia, 2010.
- [26] Kerr, J. and K. Teng. Cloud computing: legal and privacy issues. in *Proceedings of the Academy of Business Disciplines Conference*. 2010.
- [27] Takabi, H., J.B. Joshi, and G.-J. Ahn, Security and privacy challenges in cloud computing environments. *Security & Privacy, IEEE*, 2010. 8(6): p. 24-31.
- [28] Kundra, V., *Federal Cloud Computing Strategy*. The White House Library, 2011.
- [29] Wyld, D.C., *Moving to the cloud: An introduction to cloud computing in government* 2009: IBM Center for the Business of Government.
- [30] Reza, M. Framework on large public sector implementation of cloud computing. in *Cloud Computing and Social Networking (ICCCSN), 2012 International Conference on*. 2012.
- [31] Jun-jie, W. and M. Sen. Security issues and countermeasures in cloud computing. in *Grey Systems and Intelligent Services (GSIS), 2011 IEEE International Conference on*. 2011.
- [32] Hummen, R., et al. A Cloud design for user-controlled storage and processing of sensor data. in *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*. 2012.

- [33] Haiyang, Q., L. Fu, and D. Medhi. On energy-aware aggregation of dynamic temporal demand in cloud computing. in *Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on*. 2012.
- [34] Kaufman, L.M., *Data Security in the World of Cloud Computing*. Security & Privacy, IEEE, 2009. 7(4): p. 61-64.
- [35] Leavitt, N., *Is cloud computing really ready for prime time*. Growth, 2009. 27(5).
- [36] Zaigham, M. *Data Location and Security Issues in Cloud Computing*. in *Emerging Intelligent Data and Web Technologies (EIDWT), 2011 International Conference on*. 2011.
- [37] Larumbe, F. and B. Sans. *Optimal Location of Data Centers and Software Components in Cloud Computing Network Design*. in *Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012)*. 2012. IEEE Computer Society.
- [38] Townsend, M. *Managing a security program in a cloud computing environment*. in *2009 Information Security Curriculum Development Conference*. 2009. ACM.
- [39] Mell, P. and T. Grance, *The NIST definition of cloud computing (draft)*. NIST special publication, 2011. 800: p. 145.
- [40] Qiang, G., et al. *Modeling and evaluation of trust in cloud computing environments*. in *Advanced Computer Control (ICACC), 2011 3rd International Conference on*. 2011.
- [41] Li-qin, T., L. Chuang, and N. Yang. *Evaluation of user behavior trust in cloud computing*. in *Computer Application and System Modeling (ICASM), 2010 International Conference on*. 2010.
- [42] MinChao, W., et al. *A Conceptual Platform of SLA in Cloud Computing*. in *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*. 2011.
- [43] Buyya, R., R. Ranjan, and R.N. Calheiros. *Modeling and simulation of scalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities*. in *High Performance Computing & Simulation, 2009. HPCS '09. International Conference on*. 2009.
- [44] Gibson, J., et al. *Benefits and challenges of three cloud computing service models*. in *Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on*. 2012.