CLOUD COMPUTING TECHNOLOGY: SECURITY AND TRUST CHALLENGES

Sajjad Hashemi[1]

[1]Department of Computer Engineering, Science and Research Branch, Islamic Azad University, West Azarbayjan, Iran

Abstract

A let of exclusive features such as high functionality and low cost have made cloud computing a valuable technology. These remarkable features give users and companies, countless opportunities to reach their goals spending minimum cost and time. Looking at the literature of this technology, it can be claimed that the main concerns of the users of cloud are security issues especially trust. Unfortunately these concerns have not been tackled yet. Therefore we decided to introduce a useful and functioned way to create more trust among consumers to use this technology .In this paper we suggest the foundation of an international certification institute for the service providing companies in order to increase trust and enhance likeliness of using this new and valuable technology among people. Practicality of the technology will improve it and will make its security better by providers.

KEYWORDS

Cloud Computer, Security, Trust.

1. INTRODUCTION

From the point of view of the users, the simplest definition of cloud computing is to access to new functionality rent-based programs [1]. In other words, cloud computing is the next generation of internet-based extended computing systems which in it, the computing resources are provided "as a service" [2]. Cloud computing is an important structure with outstanding potential in decreasing the costs by improving and developing functionality and economic outcome which in turn can increase cooperation, pace and scalability acceptance to comprehensible degree [3]. This technology has provide large organizations and IT companies with lots of opportunities in developed countries but these opportunities face challenges like security which is one of the main concerns in cloud computing field [4]. If the security provisions aren't handled properly and correctly all cloud computing fields like managing private information in a public network can fall into trouble [5, 6]. So it can be claimed that security is the key question in accepting the cloud computing. If the providers can minimize this main hindrance, cloud computing will be the pioneer in it and its acceptance by the companies and people will be eased [6]. Today the main and first concerns in cloud computing are security, trust and the way of creating trust in accepting and sharing applications, hardware and so on in an environment which nobody knows who receives and handles our data in it [4,7]. In this paper we study security questions emphasizing on trust and offering a practical method. We mentioned that it is a need to found an international certificate institute to create accepting cloud computing in order to monitor the work of service providers especially in the field of security and level of services. In this way the users, aware of the credibility of providers can easily and comfortably make benefit of the services of companies which have obtained high and suitable security degree and credibility.

DOI : 10.5121/ijsptm.2013.2501

In section one of this paper, an introduction is provided to the cloud computing and its security. The second section is about the previous works done around the subject. Section three covers the definition of cloud computing its features and different models. In section four we study the problems and challenges about security and trust. Section five covers evaluations and suggestions about improving the security of cloud computing and finally section six contains conclusion and the next works and perspectives of this paper.

2. PREVIOUS WORKS

M. Ahmed et al [8], have observed the security questions related to cloud computing with the aim of discovering and creating a secure canal for communication manner in favor of a single information owner (abbreviated as INO) with the cloud service provider (CPS) while keeping and maintaining trust and privacy of information. Moreover they compared their offered protocol with SSL along with the operations related to the work, together, with a secured and trusted path to guarantee the privacy of data. In [2], the architectural and structural problems and the provided features of cloud, its beneficiaries and from different angels of providing services have been analyzed. Having these evaluations and analyses in hand, they have got accurate characteristics of security questions of cloud and the key features which should be tackled with security solutions. Also in the paper [9], security problems in different levels of structuring cloud computing services have been covered. The security of customer-related information is a necessity in service providing by any model of cloud computing [9]. They study the current security matters in the software as a service (SaaS), platform as a service (PaaS) and Infrastructure as a service (IaaS). This paper is focused on the ways of using cloud and security questions to facilitate cooperation's between internet-connected domains [9].

One main security issue in cloud environment is data-maintenance. To improve the security of information in cloud environment in [10], a dynamic security framework has been provided with different methods. One component of this framework refers to security of information based on saving it and accessing the information is based on meta-data to be recovered in case of the users information failures or malfunctions. Also this paper introduces the concept of cloud security based on the real world's security systems in which the security needed is related to the assets and money of the organizations, so that every organization orders its favored security based on its data importance [9, 11]. Also a new method has been provided for confronting the security challenges and threats in cloud environment in [12]. It is a new model-driven for risk-based security of cloud environment. In this paper a system model based on UML, concepts has been given which is used for automatic analysis and evaluation of risk to control and monitor the cloud environment security. They think the explained idea provides a very complicated method for testing and checking the risk-based security of cloud environments. Firdhous et al [5], have considered the question of trust and managing trust and mentioned various definitions of trust in different sciences. Then they have studied trust in cloud computing a cast an accurate look at the recent change and transitions in this field in order to recognize and categories them [6]. Besides, M.Monsef et al [4], have focused their attempt on the concerns about private and trust in cloud. It is done following the concerns about privacy & trust as a main contribution of cloud. The existing concerns about privacy and trust play an important role in not gaining full supporting and complete acceptance of functionality and efficiency of cloud by companies. In this paper various ideas and structures have been discussed to decrease or prevent these problems, such as the three-layer structure of data-protection based on different needs of users, in order to highlight the relation and position of industry towards it [4, 6].

3. CLOUD COMPUTING

Cloud computing have different shapes causing different understandings of them. For this reason many consider cloud as web-based applications. Others see it as useful and/or parallel computing because cloud is planned for better and improved efficiency in complicated & large scaled processes [13, 14, 15]. Besides different shapes of cloud, the provided services are also highly different & numerous. Cloud computing have various definitions of which some have been brought here. The definition of the national institute of standard and technology of America is as follows [2, 5, 6, 13]:

"Cloud computing is 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."

Following the definition of cloud computing, we should comprehend their developed models, the way of using services and also the way of protecting it, in order to know well and accept it [5]. Development models include the aim and identity of cloud and the way they are settled. NIST definition of the development models are of the following four types [1, 2].

- **Public cloud:** The substructure of public cloud is for the public use and accessible to all in which the resources, applications and web-services are provided through internet and public organizations help to provide and supply the substructures [16]. Indeed a cloud service provider organization owns the public cloud.
- **Private cloud:** Private cloud is for the exclusive use and only for an organization, so everyone in the organization can access data, services and applications but others out of organization can't [16].
- **Community cloud:** Community cloud are provisioned and prepared to make some common facilities and resources available. Its substructure can be shared between one or some organizations but the main point here is that the requested work of them is the same and the demanders follow somehow the same mission, policy, security and soon. In Community cloud a certain group support tasks like security needs. Of course this king of sharing will have consequences for the organization at work [17].
- **Hybrid cloud:** And latest model is hybrid cloud, which is combination of two or more clouds (including public, private and community). It is in fact an environment which uses some internal and external cloud providers [16].

Various services of cloud are presented into three models which are [1, 2]:

- **SaaS.** The services provided by SaaS include using functional programs on the infra-structure of cloud and access through the web browser [18]. in this section the customer doesn't manage the infra-structure of cloud including the net , servers, operational systems , and saving area , except the functional software to limited degree of adjustment at the level of user [17].
- **PaaS.** In this kind of service, the client has the option of putting the purchased functional programs on the infra-structure of cloud [18]. Here also the client dose not mange or control infrastructure of the cloud such as the net, servers, storage. He just has control over the functional program installed or Settled by him [17]. In fact the PaaS is similar to SaaS the difference is that PaaS includes exclusive program environment and computing platform, developing and solution strategies [2].
- **IaaS.** This kind of service providing includes process potential, saving space. Nets and other basic computing re-sources and even operational system and application pro-grams

[17]. The client dose not manage or control in infra-structure but has control over the operational system, saving area, and the established programs. In this service an artificial server is completely available for the client [18].

4. SECURITY IN CLOUD COMPUTING

Data security in IT industry is a key factor to guarantee the success of a system cloud computing which is also in this field can't be excluded from this rule [11]. As the users of this technology do not exactly know where and low their data is saved, so the role and function of providing security seems prominent [6]. Some new security problems in cloud computing by the cloud models and some by the service providing models have been intensified. So he security risks and hazards depend to a large extent on the model of service and development of cloud [19]. It caused the less confidence of users to the provided services by this technology. In provided services by cloud systems still the current and routine protocols and security measures on internet are used. It is true that these protocols and conventions grant and establish the security needs to some extent but they are not context-oriented, so there is a need to a strong set of security policies and protocols for guaranteed and secured transmission of data in clouds [6, 10, 11]. Security issues can be extended into different service models which this technology provides. For more information about the cloud's security problems and issues look at [19, 20, 21] for example.

The security controls and protocols in clouds are those which are used in other IT environments but in cloud environment the security control is performed by the providers instead of the users. An issue which can contain a lot of risks because the security provisions might not be paid enough attention during data-transmission by the CSP or ever the SLAs might not include all necessary rules for security services [19]. So the foundation of an international organization which will supervise and monitor the provided services of cloud providers and awards them a credible rank and security degree seems prominent and important here. Having an organization as such, there can be hope to improve the security level and the quality of the provided services in cloud environment and give the needed and enough trust to the users about them. Also the practical approach which is introduced here will develop the technology and increase the investment of large companies on it.

4.1. Trust

Regarding scientific texts existed in different fields; a widely accepted definition about trust can be mentioned as followers [19, 22]. "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another". However the definition does not include all, its dynamic and various dimensions and capacity [19]. Trust is an expanded concept of security which includes mental and practical criteria. Trust can be divided into hard trust (security-oriented) and soft trust (non-security) oriented trust [19], [23]. The hard trust includes parts and operations such as validity, encoding and security in processes however the soft trust covers dimensions like human psychology, loyalty to trade mark (brand loyalty) and user-friendliness [24]. Fame is an example of soft trust which is part of online trust and can be most valuable asset of a company [25]. A company's brand is liked with trust. If it cannot perform successfully in matters like trust and privacy, it will fail and be defeated. However people still have less confidence to the services provided online in comparison with the offline ones due to the lack of physical cues in digital world [19, 26, 27]. So the infield of online service providing, lack of trust in them can have a negative effect in entering and competitive competence of the firms and old organization which were trust worthy for a longtime into the digital world [24]. Some argue that there is no relation between security and trust. Nissenbaum argues that the security level does not affect trust [19, 28]. On the other hand if for example the people, who have more intention to invest on E-commerce, are assured their credit-card number

and private information is protected through encoding methods, will increase the amount of trust among them [29]. Now, following especial and technical meaning of trust, a simple definition of it can be summarized as such: if we have control over our data we trust in the system. For example we rely on ATM because we are sure it pays the exact amount of money we withdraw, so we have control over our money [6, 7]. So every system needs to create trust. This is trust in cloud environment too as all information of the service users is available for CSP [3]. The level of trust in cloud computing is regarded the basic or primary trust because the cloud computing is a recent technology and its role players do not have much valid and meaningful knowledge about each other [9]. Therefore trust has a positive impact on the understanding of the cloud computing application [30]. Maybe distinction between the social-based and technical meaning of trust will be useful in presenting durable and dynamic trust while trust in cloud computing of course in case of trust being necessary in all considerations [19, 31]. Persistent trust is the long run trust on the essential features or infra-structures. This is because of rather stable social and technological mechanisms [19]. Dynamic trust is the trust on special mods, contexts or on the summary or variable information which can be achieved through context-based social and technological mechanisms. Persistent social-based trust in hardware or software system is tool or device to create assurance on technological-based trust because persistent social-based trust guarantees application and maintenance of the hardware or software system. Also there is a connection between social-based trust and technological-based trust through vouching mechanisms because it is important to know who is vouching for something as well as what they are vouching; so the social-based trust should it be ignored of anytime [19].

5. EQUATIONS

Based on the discussions of this paper and the economic crisis in the world especially in developed countries, it seems that dunning following years those countries and the active companies in those countries employ new fiscal policies to decrease their cost and increase revenue operation. Therefore the utilization of recent and new technologies which are profitable and reasonable economically and exploitation ally will increase revenue. In this direction the cloud computing as a technology created to decrease costs and increase exploitation is paid more attention and will develop meaning fully. However to put this technology among the main options to be used in different countries policies and programs, There is an urgent need to create better security, trust and motivation among the users to use cloud-based services. As mentioned before, the most important concerns and challenges ahead of cloud computing technology are the lack of trust in the service providers and lack of suitable security for these services. Also its current security controls and protocols are used in other IT environments; on the other hand the SLA does not include all necessary security services. Another main challenge which probably threatens using cloud environment is the lack of enough and necessary attention to create a reasonable and suitable attention by the service providers which can be a big hindrance and obstacle in from of the successful and active companies in this field. This is so while most companies employ various methods and tools to gain the trust of people to use their services today. An example can be success in getting a valid certification from a reliable international institution. One of the reasons to found such an institution is that the reliance of people on them which are impartial and without any dependence on a certain government or company is high. According to this approach we think the foundation of such an institution to ward security certification degree to the cloud service providers is necessary because this kind of institution can provide an accurate and impartial monitoring and supervision over the operations of those providers and check and control the security level and the quantity of the provided services. In this case the public and companies acceptance of using cloud technology and its various provided services will be increased and the dream of complete application of this technology will come true. It is worth to explain here that institution itself will be a factor to create an atmosphere a sense of completion among the service providers and increasing trust and security because the providers must increase the level of

security of their services and gain the public trust in order to get the security rank and certificate. We also suggest that the members of this international institution should come from different cloud-application countries in order to regulate the necessary rules and criteria to measure the validity an reliable security in the service providing companies regarding the conditions and regulations of the member parties and their respected demands and considering these criteria the security level should be given to the providers. Therefore the users can choose the best and most appropriate providers to get their services in cloud environment in view of that security rank or certification.

6. CONCLUSIONS AND FUTURE WORKS

Doing this survey we concluded that there are some important and high obstacles like trust and reliance on the service providers, ahead of speeding up the application of cloud computing technology. So the active companies in the cloud-based service providing in order to succeed and attract clients to use their services should overcome these impediments. We see a respected and valid international institution is necessary to reach the reliable security and needed trust in the provided security as people always trust more in the companies which have valid and credible certification from respected and well-known institutions and applicant their services more easily and confidently. In addition some other things can be done in future to facilitate and encourage application and utilization of cloud technology including divergence and create variety, expanding and facilitating the access to the provided services and also various providers being available so that the users can choose their favorite services easily and confidently. Besides these issues the rules for transferring and exchanging data should be reviewed and totally revised and in order to ease and secure the data exchanging between some countries or continents without any problems the SLA should be completed. The other task which should be done in future is the exchange and transfer of the experience of the cloud-application countries with other countries. This can accelerates the progress and development of this technology and removes the problems and impediments facing it. As the last words, we can claim that this newly-appeared technology can be successful in future only if the providers of the services and governments make the necessary security and enough trust available to attract the consumers to use the services.

REFERENCES

[1] Yashpal Kadam, “Security Issues in Cloud Computing A Transparent View”, International Journal of Computer Science & Emerging Technologies, Vol-2 No 5 October, 2011.

[2] Mohamed Al Morsy, John Grundy and Ingo Müller, “An Analysis of The Cloud Computing Security Problem”, In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30 Nov 2010.

[3] H. Takabi, J.B.D. Joshi, G.Ahn., “Security and Privacy Challenges in Cloud Computing Environments”, IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, p.24-31, 2010.

[4] M. Monsef, N. Gidado, “Trust and privacy concern in the Cloud”, 2011 European Cup, IT Security for the Next Generation, p.1-15, 2011.

[5] M. Firdhous, O. Ghazali, and S. Hassan, Trust and Trust Management in Cloud Computing – A Survey, Inter Networks Research Group, University Utara Malaysia, Technical Report UUM/CAS/InterNetWorks/TR2011-01, 2011.

[6] Farhad Soleimanian Gharehchopogh, Sajjad Hashemi, “Security Challenges in Cloud omputing with More Emphasis on Trust and Privacy”, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, Vol. 1, ISSUE 6, pp. 49-54. 2012.

[7] D. Zissis, D. Lekkas, “Addressing cloud computing security issues”, Future Generation Computer Systems, Volume 28, Issue 3, P. 583–592, March 2012.

[8] Mahbub Ahmed, Yang Xiang, Shawkat Ali, “Above the Trust and Security in Cloud Computing: A Notion towards Innovation”, 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp.723-730, 2010.

[9] V.KRISHNA REDDY, Dr. L.S.S.REDDY, "Security Architecture of Cloud Computing", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 9, pp.7149-7155, September 2011.
[10] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Elsevier, Network and Computer Applications, Vol. 34, p.1-11, 2010.
[11] K, Sachdeva, Cloud Computing: Security Risk Analysis and Recommendations, Master Thesis, University of Texas, Austin, 2011.
[12] Philipp Zech, "Risk–Based Security Testing in Cloud Computing Environments", 011 Fourth IEEE International Conference on Software Testing, Verification and Validation, pp.411-414, 2011.
[13] Fariborz farahmand, "Risk Perception and Trust in Cloud", ISACA JOURNAL VOLUME 4, pp.1-8, 2010.
[14] Hoover, J. N.; R. Martin; "Demystifying the Cloud," InformationWeek, June 2008.
[15] Weiss, A.; "Computing in the Clouds," netWorker, vol. 11, issue 4, p.16-25, 2007.
[16] D. Jamil, H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journal of Engineering Science and Technology, Vol. 3, No. 4, p. 2672-2676, 2011.
[17] S. Qaisar, K.F. Khawaja, Cloud Computing: Network/Security Threats and Countermeasures, Interdisciplinary journal of contemporary research in business, Vol.3, No 9, p. 1323-1329, 2012.
[18] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical EditorBill Meine, Elsevier Publishing, 2011.
[19] Siani Pearson, "Privacy, Security and Trust in Cloud Computing", HP Laboratories, appeared as a book chapter by Springer, UK, 2012.
[20] Cloud Security Alliance (2009)" Security Guidance for Critical Areas of Focus in Cloud Computing"., v2.1, English language version, December. http://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf
[21] Vaquero L, Rodero-Merino L, Morán D, Locking the sky: a sur-vey on IaaS cloud security. Computing, 91:93–118, 2011.
[22] Jaeger PT, Fleischmann KR, Public libraries, values, trust, and e-government. In: Information Technology and Libraries, 26(4), 2007.
[23] Rousseau D, Sitkin S, Burt R, Camerer C, Not so Different after All: a Cross-discipline View of Trust. Academy of Management Re-view, 23(3):393-404, 1998.
[24] Wang Y, Lin K.-J, Reputation-Oriented Trustworthy Computing in E-Commerce Environments. Internet Computing, IEEE, 12(4):55–59, 2008.
[25] Singh S, Morley C, Young Australians' privacy, security and trust in internet banking. In: Proceedings of the 21st Annual Conference of the Australian Computer-Human interaction Special interest Group: Design: Open 24/7, 2009.
[26] Osterwalder D, Trust Through Evaluation and Certification. So-cial Science Computer Review. Sage Publications, Inc., 19(1):32-46, 2005.
[27] Best SJ, Kreuger BS, Ladewig J, The effect of risk perceptions on online political participatory decisions. Journal of Information Tech-nology & Politics, 4, 2005.
[28] Nissenbaum H, Can Trust be Secured Online? A theoretical perspective. Etica e Politica, 2, 1999.
[29] Giff S, The Influence of Metaphor, Smart Cards and Interface Dialogue on Trust in eCommerce, MSc project, University College London, 2000.
[30] R.J.W. Welten (Rob). Towards the cloud-The role of trust and perceived privacy risk on the adoption of cloud computing, MasterThesis, Tilburg University, Netherlands, 2009.
[31] Pearson S, Casassa Mont M, Crane S, Persistent and Dynamic Trust: Analysis and the Related Impact of Trusted Platforms. In: Trust Management, Proc. iTrust 2005, LNCS 3477, Peter Herrmann, Valérie Issarny, Simon Shiu (eds), 355-363, 2005.

Authors

Sajjad Hashemi is a M.Sc. student in Computer Engineering Department, Science and Research Branch, Islamic Azad University, West Azarbayjan, Iran.
Email: iau.hashemi@gmail.com