Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy

Farhad Soleimanian Gharehchopogh, Sajjad Hashemi

Abstract— Cloud computing is known as the newest technologies in IT field which causes some worries for consumers and its producers due to its novelty. Looking at its literature, we can see the privacy and security aspects and trust are the main concerns. It creates an important hindrance for using by users. So we decided to evaluate some factors such as security for the acceptance of cloud computing. In this paper, we highlighted envision about security emphasizing for the maintenance of privacy and trust in accepting the cloud computing. As a result, we are proposed new recommendations for improving security, decreasing risks, increasing trust and maintaining privacy which they are necessary to adopt cloud computing.

Index Terms— Cloud Computing, IaaS, SaaS, PaaS, Trust, Privacy, Security, Challengers.

1 Introduction

CLOUD computing is an important means with significant potential in reducing costs by improving and increasing functions and economic outcomes which can boost collaboration, agility, and scale [1]. This technology can bring about much opportunity for great organizations and IT corporations in developed countries, but these opportunities faced challenges such as security which is amongst main concerns in this field [2]. If security preparations are put improperly, all fields in cloud computing like managing private data in a general net will face problems [3]. In other words, using weak security steps and procedures and pay no attention to privacy for cloud computing the calculation pattern may result in a big fiasco [1]. It can be said that the security is the vital highway regarding to adopt with cloud computing. If the producers of this technology can overcome this great hitch or minimize it, the cloud computing will be the frontier of IT and its adaptation will be facilitated. So from the service provider's view, security is a necessity for internet and resource protecting and providing trust to these resources. The main concerns in cloud computing are security, trust, maintaining privacy, and how to provide trust in adopting, sharing functional programs, hardware in a sphere we don't know who handles our information [2, 4]. In literation there are few studies about privacy and trust in adopting cloud computing. Also, there are most studies about technical problems connected to cloud computing. Here, we consider security emphasizing trust and privacy in the modern cloud computing and make reference that trust and privacy is among the main obstacles of adopting it. Also we scrutinized the performed studies in this field and tried to look at the weak prints and offered some suggestions.

Farhad Soleimanian Gharehchopogh is Currently Ph.D candidate in Department of Computer Engineering at Hacettepe University and honour lecture in Computer Engineering Department, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran. Email:bonab.farhad@gmail.com, website:www.soleimanian.com.

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

The paper deals with security challenges in cloud computing environments with more emphasis on trust and privacy perspectives. It is organized as follows: in the next section, we reviewed previous related works in this domain. Section 3 includes the cloud computing definitions, features and deployment models of it. In the section 4, we describe the existed challenges in security, trust and privacy. Section 5, is proposed discussion about new approaches and resolutions in optimized security of cloud computing. Finally, section 6, is highlighted the results of this study.

2 Previous Works

Tsaiw et al. in [5] introduced a four - foiled framework (four-tier framework) to improve based on web. It was interesting but had a remark on just one facet of the process. Isolating resources for the security of data during processing is done by isolating processor caches in virtual machines and isolating those virtual caches from hypervisor caches [6]. The problems of privacy and control can't be solved unless just to trust to service-level agreements (SLAs) or by keeping the cloud itself private [7]. According to the platform computing assessment 8 out of 10 firms choose internal clouds and want to keep in-house cloud initiatives. Milne [8] suggests a simple way which is widely employed among UK corporations. This is why they employ private clouds "in-house". Of course, private cloud has limited function and more cost for firm, so provided the increased security. Other models of cloud will be better and functional for corporations. Nurmi et al. in [9] provided a preview with one of existing home-grown clouds (Eucalyptus) to show their open-source cloud computing. They conclude using their previous experiments that, "EUCALYPTUS is helping to supply the research community with a much needed, open-source software framework around which a user-base of cloud-computing researchers can be developed" . Also, Khalifehlou and Gharehchopogh [10] are presented new directions in cloud computing environments. They are described the various methods for more security in cloud environments. In reference [7], a security framework is provided dynamically different methods which one its component refers to security maintenance by archiving and accessing by meta data in order to restore when the war's

data fail or damage. Each segment of this framework is provided to the applications as one or multilayers in the format of "security as a service" to meet necessary functions [7]. The study introduces the concept of security of cloud according the real worlds security systems in which the amount of security depends on the property and organization of person. Maybe this is a good suggestion but it should be clear whether security is provided to gather with the service or not. Here the provider should pay some part of his attention to security problems. It may undermine and reduce the improvement of service-providing [11, 7]. Jamil et al. [12] study four security problems an including XML signature element wrapping, browser security, cloud malware injection attack and flooding attacks and their reactions. They believe that these security systems need deep and comprehensive analysis because of attacks may use different vulnerable points which can cause unauthorized access to data by hackers or the invaders may put a damaging service on the cloud system for special purpose and this can amount to loss for users or even the system itself [12]. Che et al. [13], studied security models and cloud computing strategies. They want to show the status of existing security in cloud computing and introduce some works to improve the level of security in this computing security also the studied the most favorite security models in cloud computing security for example multiple tenancy model, accumulation model cube model and a summary of the risks obtained from different organizations. Finally, they offered some security strategies according their structure, operation and security of response the event for solving the common security problems of cloud computing [13]. D. Zissis et al. [4] pointed to security problems in their paper and divided their aim into two parts. First they studied the security of cloud using exclusive security needs and in the second part they tried to offer a solid solution to remove the potential treats. In the paper, they offer trust as a special security feature on cloud sphere. The suggested solution of encoding based on public key related to SSO and LDAP which is wholesomeness and confidentiality of the respected data and communications (to ensure identification) [13]. A combination of PKI, SSO and LDAP can show many of treats related to coherence, confidentiality, accuracy and accessibility of data. Also, Monsef et al. [2] devoted their attempts to the concerns about private area and trust in cloud. This study is done following some concerns on privacy and trust as a main function in cooperation of cloud. These factors have important roles in decreasing complete support of corporations from business and work field of cloud. Different ideas and structures have been discussed in this paper in order to avoid the mentioned problems like three foiled structure of protecting data to meet users various needs. So, the industry's dealing with this subject will be clear. Firdhous et al. [3] discussed the matter from different angles and various definitions of sciences from "trust". Then they studied trust in cloud computing and categorized the latest developments in the area. Takati et al. [1] worked on security and privacy challenges in the cloud computing which we can mention identification check and identification management (IDM) access control, trust, coherence management, privacy and protecting data. In this paper, cloud providers and venders should share security and privacy maintenance in cloud computing share. But hinted the degree of sharing is different depend on different models which is essential in developing cloud [1].

3 CITATIONS

There are many definitions for cloud computing but no consensus on single and unique definitions. The US National Institute of Standards and Technology (NIST) defines it as follows [1]: "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." Cloud computing is a model to facilitate access based on web to a set of format table computing resources (such as nets, servers, saving spheres & functionality programs) which can be easily provided or freed without need to interference of service provider or any struggle of users. On other common & acceptable definition is of Mater et al. [2, 14] "A very exact scalable instrument, capable of technology-enabled service, which is available easily on the internet when needed." The main idea of Cloud computing is to build a virtual computing pool emphasizing wide range of computing with connected nets to let the users & consumers share hard & software resources dynamically & pay according their real use. So computing ability can be buying and sell cheaply just like electricity, water, gas and so on [13]. Now, it is time to understand the main feature, deployment models, procedures of using its services and protection in order to fully comprehend and adopt the cloud computing [1]. The five key features are [12]:

1) Service demand on self: at which the user can access some computing components such as server, Storage space, net & other computing resources from every provider easily & automatically.

2) Ubiquitous network access: which say the facilities are accessible on net and can be accessed using standard procedures. This procedure supports strong & weak clients as laptop and mobile phones.

3) Location-independent resource pooling: shows the availability of the necessary resources at one pool (location) dynamically to provide service for different clients. These resources can include spaces of storing, memory, band width of net and virtual machine.

4) Rapid elasticity: by which different abilities can be provided quickly with good flexibility and improved or released rapidly. In other words the provided and improved services are available quickly for the users.

5) Measured service: These features provide supervision control and reporting of resources and can report the amount of resource using clearly to the users and the providers of the infrastructure. So, all these features show integrity and transparency by means of clouds [1].

Various models of clouds are: public cloud, private cloud, and community cloud, hybrid cloud [1]. Public clouds are available for everyone and accessibly by different service providers in which the resources programs and web services are provided through internet and general organizations help to build their infrastructures [15]. The best-known forms of access to public cloud is through the internet, other forms of public cloud offerings can take the form at more of the application layer, or

Platform as a Service, like Google's App Engine and Windows' Azure Services platform, as well as Amazon's service specific cloud hosting Simple DB [16]. While private cloud is specific to an organization so everyone in that organization can access to data, services and other applications while others out of organizations cannot [15]. In this case the cloud infrastructures are used only for one organization [16]. So, private cloud infrastructure management and maintenance of organization information wholly have done by the organization themself [1]. Since private clouds are well, private, some of the security concerns of a public cloud may not apply. However, just because they are private does not mean that they are necessarily more secure. In a private cloud, considerations such as securing the virtualization environment itself (such as hypervisor level security, physical hardware, software, firmware and so on) must still be addressed, whereas in a public cloud, you would rely on the provider to do so [16]. Similarly the community clouds are planned for special range of clients and its infrastructure is shared by some organizations and a defined group supports special tasks such as the security needs. Of course this kind of dada sharing has caused some worries including mission, security requirements policy and compliance considerations. It has tremendous capability for entities or companies which are subject to legal restrictions, identical regulatory or compliance. The last form is the hybrid clouds which are a combination of two or more clouds (including public, private and community clouds). In fact it is an area which uses multiple internal or external cloud service providers [15]. Hybrid clouds are formed when an organization builds out a private cloud and wishes to leverage public or community clouds and also are the linking of the two or more clouds is what would be called a hybrid cloud [16].

4 THE SECURITY CHALLENGES IN CLOUD COMPUTING

4.1 Security

Security in cloud computing (or briefly "cloud security"), refers to a wide range to a wide range of technologies. It established controls to protect companies' information, applications and related infrastructures to cloud computing. In fact in IT industry the most important factor to secure the success of a system is the security of information [11]. Cloud computing in the area of IT industry can't be excluded from this fact. Here in which the users do not have control over where and why their information be saved, the role of security providing is more important and it decreased the amount of trust towards services. All security risks in internet are present in clouds too because of service providing by internet, consequently security data in clouds is a burdensome and difficult tasks [7]. Cloud systems also use routine protocols and security frameworks in internet (like security and data encryption protocols) but they are not context oriented, so they need a powerful set of security and policy protocols to transfer data satisfactorily and safely [11, 7]. Cloud computing provide various services in three forms which are [1]: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Security requirements in these models in cloud area are different levels. This is where the security responsibilities for both user and provider have different levels in different models [7]. Security requirements are discussed below. The provided service by SaaS is for application usages on the cloud's performing infrastructure with the possibility of access through web browser [11]. In this section the client manages the cloud infrastructure such as net, servers, storing spaces, operating systems, even applications to limited degree of adjustments at user level [16]. So, companies are not interested to SaaS. Consequently companies' security concerns (worry) are as the main challenge in adaptation of SaaS in clouds [11, 17]. In order to cope with the clients concerns (worry) about the security of data and application in SaaS, the security steps suitable and useful for client depend on the service provider to prohibit the possibility of data reviewing of each other [7]. In addition to guarantee the availability of applications when was required [7, 18]. Using cloud computing along with the pay-as-you-go approach helps the software service providers to invest on the better providing of services for clients thus the following security components should be considered as integral parts of the application of SaaS to improve and establishment process [7]: Data security, Network security, Data locality , Data integrity, Data segregation, Data access, Authentication and authorization, Data confidentiality, Web application security, Data breaches, Virtualization vulnerability, Availability, Backup, Identity management and Sign-on process. In PaaS services, the client can put the purchased applications under the cloud infrastructure [11]. Again the client doesn't manage the cloud infrastructure by controlling the application on net, servers, storage space [16]. But it can be able to control or manage the applications. Any security under applications level such as host and avoiding net penetration is in the domain providers and control, so the provider provides strong guarantees for inaccessibility of data in the applications in question [7].

Another quality of security to propose is the entitlements presented by the PaaS platform. Regarding to the cost advantages of PaaS, there are efficiencies to be obtained when considering PaaS as a resolution to enforce usual entitlements across all applications in an enterprise or organizations [19] .In fact, PaaS is similar to SaaS, but with PaaS, the service is the entire application environment, and PaaS contains the computing platform, the development and solution stack [16]. Google's App Engine is an example of PaaS architecture [10] .IaaS, includes processing potential, storage space, nets and other basic computing resources, even operating system and applications [16]. The client doesn't manage or control the infrastructure but has control over operating system, storage space and available applications. In this kind of service, a virtual server on cloud is available completely for client [11]. In IaaS, the improvers can have effective control over security as long as there is no security hole in virtualization management [7]. Moreover in the virtual machines theory, it is possible to show these problems but in reality there are lots of security problems [20, 21]. The other factor, having trust on the providers on whose hardware the data are stored because the virtualization of "everything" is progressing in communication and information society so full protecting and controlling of data for their owners without considering the physical place, is of much importance [11]. Many techniques have been used to reach maximum trust and security in cloud resources [22]. IaaS, faces various degrees of security problems depending on the model of cloud in hand

and it looks the public cloud are more vulnerable to risks than private clouds [7]. In cloud area, data are transformed through infinite infrastructure machines of third-party as well as there is a possibility of data failure by unwanted infrastructure [7]. This is known as a procedure for getting physical security.

4.2 Trust

Simply put, trust is keeping promise. It is based on an assurance which a promised action will be surely done and kept [2, 23]. However if we get little and unnecessary information about our demand from system, it is clear that our trust will be affected adversely, so trust is gained when our expectations are met and we get full services. The concept of created trust between two concerned parties in a transaction can be explained as follows [4, 24, and 10]. "An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required". From other angle, it can be said that trust means that if we have control over our data, we trust the system. For example, we trust ATM because we have confidence that it will give us the exact amount we want to withdraw and we have control over our money. Unlike when we use ATM to deposit money, we are not having control; over our money after we must have allowed the machine to consume the money [2]. This is also the same feeling the consumer have over their data in the cloud [2, 23]. Thus trust as a relating protocol among providers and users of cloud services, is created as a continuous process and play an important role in cooperation [13]. So, trust is little at first and increases gradually. The start of trust is considered as primary trust. This level of trust is defined as the primary trust since the cloud computing are new technologies and their players doing not have significant and comprehensive information from each other [13]. It is worth saying here that the importance of trust of different organization is different according to their data in cloud system [25]. Trust will have a positive effect on the perceived usefulness of cloud computing [2, 13]. Trust in a cloud environment depends heavily on the selected deployment model, as governance of data and applications is outsourced and delegated out of the owner's strict control [4]. Hoffman et al. [27] found in their study that 95% of the consumers did not provide personal information to websites. 63% of them indicated that they did not provide personal information because of they do not trust those who are collecting the data. So, trust seems to have an impact on the acceptance of technologies [27, 28, and 29]. Also, Geffen et al. [30] states that trust increases the probability that the customer will gain the expected benefits.

4.3 Privacy

Privacy is human's fundamental right and can be summarized into four forms [26, 31]:

1. Physical privacy: This focus on everyone the right of intangibility of his body, with exception of lawful restrictions.
2. Relational privacy: it offers confidentiality of mail telephone, and telegraph, with exception of lawful restrictions.
3. Environmental privacy: It is the entrance of a residence versus the will of the occupant is not permitted, with exception of lawful cases.
4. Informational privacy: it means that (1) everyone has the right of respect of a private life, with exception of lawful restrictions, (2) the protection of the private life regarding to the recording and providing of personal data as stated by the law, and finally (3) it offers to the prescripts concerning the perusal of recorded personal data and the application of recorded personal data, as well as correction of these data as stated by the law.

An important aspect in informational privacy is personal data, which personal data is called privacy sensitive information [26] and include (1) "any information that could be used to identify or locate an individual (e.g. name and address) or information that can be correlated with other information to identify an individual (e.g. credit card number and postal code internet protocol (IP) address) and also information that is considered to be sensitive such as collection of surveillance camera images of public places, (2) sensitive information: "information on religion or race, health, sexual orientation, union membership or other information that is considered private", (3) usage data: data on behavioral information, for example recently visited websites and product usage history, and (4) unique device identities: all other types of information that can be uniquely related to a user device, for example IP addresses and unique hardware identities [26, 32]. The security model in cloud computing services should match the national regulations and follow lots of rules [33, 32]. These regulations and rules at first aimed to protect data which can be used to identify an individual [33].

5 Recommendations

Many groups and organizations are interested in developing security solutions and necessary standards for clouds [7]. Cloud security alliance gathers the provider's solutions, non-profits and the peoples who discuss about the current and future methods and some valuable solutions to secure the incoming data. In addition the cloud standard web site is being developed to collect data on standards related to clouds by some interested researchers. The best security solution for web users is an employment framework that has strong security architecture [7]. The reasonable solutions of security problem in cloud computing have some elements [33] as follows. First the users should be notified and informed about how and where their data are sent similarly they must know how and from where they get input. Second the service providers must assure and provide a data protecting agreement on privacy during contract available for users. This kind of responsiveness produces a control mechanism to increase and boots the users trust on providers compare to primary trust. Third the service providers should accept some duties and commitment against their clients in order to create security standards and keeping privacy [33] which is possible through official contracts among them. We suggest that the current standard protocols designers and developers create new security and transformation protocols using the current technologies and techniques which naturally enhance security to a large extent. As a result, their acceptance, authenticity and validity will be regarded positively by users. Therefore, this will be a factor in creation a general and public trust in cloud computing usages. In order to protect privacy in cloud computing, we also suggest strict regulations and rules that they prepare and exclude by states along with continuous and comprehensive monitoring to reach the ideal point. Moreover, an organization for security as a medium between provider and user should be built to secure data transfer security in clouds aiming safe data transformation so that no one except the organization itself have information about the mechanisms

and handled algorithms of data transformation and the user can see the input or make it ready to transfer in cloud space by a decoder (software or even a special hardware) which the provider provides for him. In this case even the provider doesn't have direct access to data because of the security providing medium prohibits illegible and unlawful access to data using security algorithms. So, trust in cloud systems will be enhanced and the users' interest to use this technology will be increased. In addition, the providers concerns about security will be answered and they will do their best to improve services and so there is any need to provide security by them.

6 Conclusion

It requires users to get special trainings on data switching and decoding in to secret data by special software. In this study we showed the main problem is the lack of trust on cloud systems and also keeping privacy. So, strong security methods and policies should be created to justify adaptation of this technology. One main factor in encouraging the public to using cloud computing technologies and making trust is widespread propaganda. Since, making know has its various advantages. Besides introducing the advantages of this technology it should be noticed that there are also some potential security risks because of cloud computing uses the sub-structures of the internet. Hence, changing the current transferring protocols is a procedure and approach to confront these risks. Meanwhile, security and privacy can never be assured and secured 100% in these areas. As a result, each cloud providers must have information about the data transferring mechanisms and algorithms except the organization itself.

References

[1] 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, 2010, p.24-31,.

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

[3] 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.

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

[5] W. Tsai, Z. Jin, and X. Bai,"Internetware computing: issues and perspective", Proceedings of the first Asia-Pacific symposium on Internetware. Beijing, China: ACM, p.1–10., 2009.

[6] H. Raj,R. Nathuji, A. Singh, and P. England ,"Resource management for isolation enhanced cloud services.", Proceedings of the 2009 ACM workshop on cloud computing security, Chicago, Illinois, USA,2009, p.77–84.

[7] 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.

[8] J. Milne, Private cloud projects dwarf public initiatives, 2010, http://www.cbronline.com/news/private_cloud_projects_dwarf_public_initiatives_281009 [accessed: 30 April 2012].

[9] D. Nurmi,R. Wolski,C. Grzegorczyk, G. Obertelli, S. Soman, L. Yousef,"The Eucalyptus Open-Source Cloud-Computing System." 2009 9th IEEEACM International Symposium on Cluster Computing and the Grid, 2009, p.124–131.

[10] Z.A. Khalifehlou, F.S. Gharehchopogh, "Security Directions in cloud Computing Environments", 5th International Conference on Information Security and Cryptology (ISCTURKEY2012), Ankara, Turkey, 17-19 May 2012, p.327-330.

[11] K, Sachdeva, Cloud Computing: Security Risk Analysis and Recommendations, Master Thesis, University of Texas, Austin, 2011.

[12] D. Jamil, H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journal of Engineering Science and Technology, Vol. 3 No. 4, 2011, p. 2672-2676.

[13] J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, Procedia Engineering, Vol. 23, p.586-593, Elsevier, 2011.

[14] T. Mather, S. kumaraswamy, S. Latif, Cloud Security and privacy: an Enterprise perspective on Risk and Compliance, Governance An International Journal Of Policy And Administration, O'Reilly Media, Inc., p. 312, 2009.

[15] 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.

[16] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical EditorBill Meine, Elsevier Publishing, 2011.

[17] H. Lo,R. Wang, J.P. Garbani, E. Daley, F. Iqbal, and C. Green, The State of Enterprise Software, Forrester report, 2009

[18] V. Choudhary, "Software as a service: implications for investment in software development." 40th Annual Hawaii International Conference System Sciences 2007 (HICSS 2007), Vol.18, p. 209, IEEE, 2007.

[19] A. Gupta, The Java EE7 Platform: Developing for the Cloud, [Available that: http://www.slideshare.net/arungupta1/java-ee7-latest Last available 01, May 2012], p.1-79, 2012.

[20] CR. Attanasio, “Virtual machines and data security”, Proceedings of the workshop on virtual computer systems, New York, NY, USA: ACM; 1973, p. 206–209.

[21] S. Gajek, L. Liao, J. Schwenk, “Breaking and fixing the inline approach”, Proceedings of the ACM workshop on secure web services SWS ’07. New York, NY, USA: ACM, 2007, p.37–43.

[22] M. Descher, P. Masser, T. Feilhauer, A.M. Tjoa, D. Huemer, “Retaining data control to the client in infrastructure clouds.”, 2009 International Conference on Availability, reliability and security, ARES ’09, 2009, p. 9–16.

[23] Khaled M Khan and QutaibahMalluhi, "Establishing Trust in Cloud Computing", IT Professional, vol. 12, no. 5, p. 20 - 27, 2010.

[24] W. Kim, Cloud Computing: Today and Tomorrow, Journal of Object Technology, vol. 8, no.1, January-February 2009, pp. 65-72.

[25] P. Kumar, V.K. Sehgal, D.S. Chauhan, P.K. Gupta, M. Diwakar, Effective Ways of Secure, Private and Trusted Cloud Computing, Journal of Computer Science, Vol.8, p.412-421, 2011.

[26] R.J.W. Welten, Towards the cloud-The role of trust and perceived privacy risk on the adoption of cloud computing, Master Thesis, Tilburg University, Netherlands, 2009.

[27] D.L. Hoffman, T.P. Novak, and M. Peralta, Building Con Trust Online. Communications of the Association for Computing Machinery. Vol. 42, No. 4, P. 80 – 85. April 1999

[28] B. Friedman, P.H. Kahn, and D.C. Howe, Trust Online, Communications of the Association for Computing Machinery. Vol. 43, No. 12, P. 34 – 40. December 2000

[29] D.H. McKnight, V. Choudhury, and C. Kacmar, Developing and Validating Trust Measures for e-Commerce: An Integrative Typology, Information Systems Research. Vol. 13, No. 3, P.334–361. September 2002.

[30] D. Gefen, E. Karahanna, and D.W. Straub, Trust and TAM in Online Shopping: An Integrated Model, MIS Quarterly. Vol. 27, No. 1, P. 51 – 89. March 2003

[31] A. Singh, M. Hemalatha, Cloud Computing for Academic Environment, International Journal of Information and Communication Technology Research, Volume 2 No. 2, February 2012, p. 97-101.

[32] S. Pearson, A. Charlesworth, ”Accountability as a way Forward for Privacy Protection in the Cloud”, Computing, Vol.5931, Springer, p.131-144, 2009.

[33] Fei Hu, MeikangQiu, Jiayin Li, Travis Grant, Draw Tylor, Seth Mccaleb, Lee Butler, Richard Hamner, “A Review on Cloud Computing : Design Challenges in Architecture and Security”,Journal of Computing and Information Technology, Vol.19, p.25-55. 2011.

[34] K. Pardeep, K Vivek, C.S. Durg, P.K. Gupta and D. Manoj, Effective Ways of Secure, Private and Trusted Cloud Computing, International Journal of Computer Science Issues, Vol. 8, No. 2, p.412-421, 2011.