International Journal of Software Engineering & Computer Systems (IJSECS)
ISSN: 2289-8522, Volume 2, pp. 58-65, February 2016

DOI: http://dx.doi.org/10.15282/ijsecs.2.2016.5.0016

DATA SECURITY ISSUES IN CLOUD COMPUTING: REVIEW

Hussam Alddin Shihab Ahmed, Mohamad Fadli Bin Zolkipli

Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang,
26300 Gambang, Pahang, Malaysia
Email: hussamalddin12@gmail.com
Phone: +601111222089.

ABSTRACT

Cloud computing is an internet based model that empower on demand ease of access and pay for the usage of each access to shared pool of networks. It is yet another innovation that fulfills a client's necessity for computing resources like systems, stockpiling, servers, administrations and applications. Securing the Data is considered one of the principle significant challenges and concerns for cloud computing. This persistent problem is getting more affective due to the changes in improving cloud computing technology. From the perspective of the Clients, cloud computing is a security hazard especially when it comes to assurance affirmation issues and data security, remain the most basically which backs off for appropriation of Cloud Computing administrations. This paper audits and breaks down the essential issue of cloud computing and depicts the information security and protection of privacy issues in cloud.

Keywords: Cloud Security; Data privacy; Cloud Computing.

INTRODUCTION

Cloud computing is a suitable model for whenever required using the system for access to a commonly used pool of processing assets configurable whenever needed to be that can be quickly discharged and provisioned with negligible managerial efforts (Mell and Grance, 2011). Cloud computing can be characterized as "Cloud is a distributed and parallel computing system" comprising of a collective visualized which is inter-connected system which are monitored dynamically and then shown as one or multiple unified resources of computing based on the Service Level Agreements (SLA). This agreement is created amongst the Service Providers (Buyya et al., 2009). It is a computing style wherein capabilities related to IT are provided to consumer as a "Service" rather than an item utilizing from the web.

The main fundamental objective of the cloud computing is to give versatile and economical whenever required a high quality service levels. Numerous designers of cloud-based applications put up a great effort in the struggle towards assimilating the security. In distinctive cases, designers simply can't give a basic arrangement towards true security with as of now sensible imaginative Technological capacities (Marston et al., 2011). The building design or the development demonstrating of the Cloud Computing incorporates various cloud parts teaming up with each other about the different data they are hanging on as well, as needs be helping the customer to get to the obliged data on a speedier rate.

Regarding the matter of cloud it is more centered upon the front and back ends. The frontend is the customer who requires the information, while the backend is the various

information stockpiling storage devices, server which makes the cloud (Stanoevska-Slabeva et al., 2010).

The complete paper is grouped as follows: Starting with Section 2 depicts the related work identified with cloud computing, Section 3 examines the idea of cloud, Section 4 gives in point of interest explanation of Security in Cloud Industry.

Section 5 deals with Cloud Computing security issues. Section 6 shows the recently implemented security solutions for privacy protection and data security. This paper closes the different exchange and issues of information security in Cloud Computing. For the search regarding the Literature which integrates searching websites in the internet, collecting published and articles of conferences.

RELATED WORK

Nowadays, Cloud computing security has turned into a fascinating exploration region and it has pulled in tremendous interest of investment in commercial enterprises. Cloud Security Alliance examined and addressed to a wide area of security through guidances to security for significant regions of centre in cloud computing (Cloud Controls Matrix, 2011). In additional, Kresimir et al., (2010) examined abnormal state of issues related to security in the model of cloud computing, such as payment, information integrity, protection of delicate and personal data. Grobauer et al, (2010) talked about vulnerabilities found in the security of the cloud platform. The author gathered the conceivable vulnerabilities into, cloud attributes related, security controls related, innovation related. Subashini and Kavitha (2010) talk about the security difficulties and limitations of the cloud service delivery model, mostly concentrating on the SaaS (Software-as-a-Service) delivery model. A few studies have been done identifying with issues related to security in cloud computing. Yet this study displays an itemized comprehensive investigation of security concerns and difficulties in cloud computing concentrating on the variety of deployment and the delivery services of cloud computing.

CLOUD COMPUTING

In this area we will research the cloud computing from three angles including its essential and vital qualities, delivery models and deployment models, as demonstrated in Figure 1.

Understanding of cloud computing

Normally when users join the cloud computing they cloud see cloud as an application on its own, document, or device. Most of the components in the system of cloud such as operating systems that manages the connections of hardware are unseen. User interfaces that the cloud computing starting with can be seen by specific user. This is how when a particular user gives his demand to gain an access to management of the system. By finding the proper resources and then calling the appropriate service of monitoring systems.

Cloud computing is mostly used for storing of data. When data been stored on multiple service providers. The users get to see a virtual server. This is appears when storing a data with specific name in a certain place. This is cannot be happen in the reality. It’s just need to be locate the cloud virtual space.

Cloud computing is a model for empowering helpful, and sharing pool of configured resources. And is consist of various service model (Arnold, 2009) as seen bellow

- **Infrastructure as a service (Iaas):** Lease handling, stockpiling, system cutoff and other vital figuring assets are in all actuality, empowers purchasers to deal with the operating systems, applications, stockpiling, and system network connectivity.

- **Software as a service (Saas):** the capability of application access from different users. Software given as a service to the customers as indicated by their prerequisite, empowers buyers to utilize the administrations that are facilitated on the server of cloud.

- **Platform as a service (Paas):** Customers are given stages access, which empowers them to place their particular modified programings and different cloud computing applications.

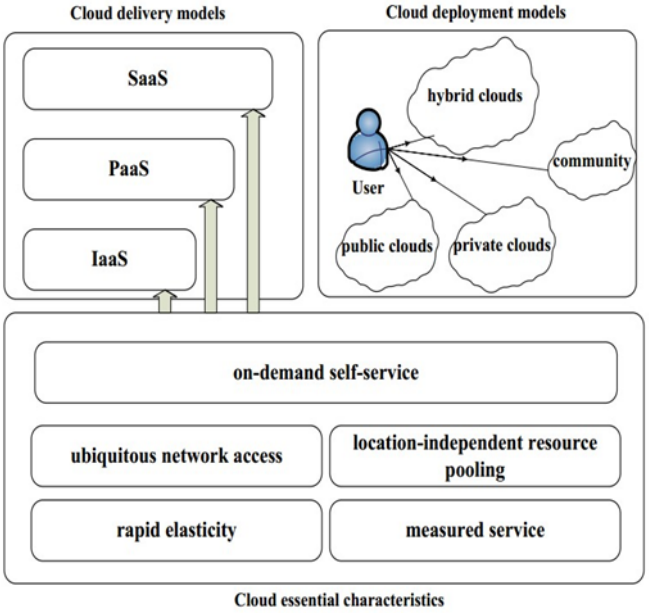

Figure 1. Cloud architecture

Cloud Computing Deployment Models

Security issues starts with the cloud delivery models. Cloud computing consist of four deployment models types (Global Netoptex Incorporated, 2009).

1. Public cloud: the Public cloud portrays conventional cloud computing, whereby resources are dynamically monitored on a self-service basis over the internet which is finely grained. This is done through implementing a third party service provider offering and sharing the bills and the resources via a registering utility basis. This cloud service focuses on a pay per usage model similar to the metering system for power and electricity, making it a very flexible and adaptable, thus servicing high spikes

in demand for optimizing the cloud service (Wang, 2011). However, the Public Cloud have a lower security when compare to other cloud models. This is due to putting extra load of guaranteeing all information and application access on this public cloud which are not threatened by various malicious attacks.

2. Private cloud: the private enterprises are used and controlled the resources in the private cloud. It's mostly organized in the data center of enterprises and managed by service provider or internal personnel. The main model advantage is the security, QoS and compliance are under the enterprises control (Dilton et al., 2010).

3. Hybrid cloud: it's a mixture of multiple cloud infrastructure (community, public, or private) that keep on a distinctive entities, but are connected through proprietary or standardized technology, that enables application proprietary and data (Mell and Grance, 2011).

4. Community cloud: It is an infrastructure of cloud that pooled by many administrations and supports communities that has mutual concerns (e.g., policy, compliance consideration, missions, and security requirements).That might be managed by a third party or organization, and may be available on or off premises.

Cloud security Industry

In order to block security obstacles' from happening at most extreme degree, the constitution of cloud security industry ought to be clarified. The three parts of cloud security industry are demonstrated as follows, they may be.

Cloud Vendors: various cloud service provider such as Microsoft (Wang et al., 2009), IBM (Zeng, 2008) and Amazon (Roy et al., 2010), provided solutions for deploying the cloud computing security in order to enhance the security of such service platform in terms of service continuity, user data security and service competency. A number of these solutions mainly relied on ID audit, ID authentication and encryption of data.

Operators: there are two main approaches concerned with securing the cloud computing seen from the perspective of administrators. One of them is achieving a central control on the platform via joining the current system of security with a cloud computing technology. The other point of view is developing security services in the cloud computing platform and provide them for their clients as can be seen from some network operators who already utilized such aspect.

Security Vendors: established vendors of IT security solutions in the market of cloud computing, provide their own products and solutions for the cloud computing platforms. Two cloud perspectives can be seen, one is from the server while the other is from the client perspective. The first perspective is basically attempting to neutralize threats found on the server before reaching the client, this can be achieved through creating an enormous lists system. The second perspective mainly functions on conventional and traditional approaches.

For the above mentioned roles found in the cloud security industry, the operators are able to push the cloud security thus providing customers with security services, these operators collaborate with security vendors in order to provide applications or

security services to customers by implementing the advantages from the network operators in collaboration with Data encryption solutions, audit and ID authentication solutions provided by cloud vendors, hence offering end to end solutions of security in the cloud computing paradigm.

CLOUD COMPUTING SECURITY ISSUES

Recently, one of the fastest growing technologies in IT industry is the cloud computing due to its rapid development.Minor businesses are now grasping the benefit provided from utilizing the cloud where they able to get swift access to commercial applications to enhance their resources and infrastructure exponentially with minimum costs. However certain hazards came with the growth of this technology especially the concern with how safe this technology is with sensitive information. The issues can be categorized and seen as bellow:

1. Data access control: Due to lack of secured access to secret or private data, illegal access can be done with such lack of security. With respect to the security concerns related to the cloud based system, the major issue is the Sensitive Information in a cloud computing environment. For a long time if the Information exists in the cloud, there will be a risk of unapproved or unauthorized access (Bower et al., 2009).

2. Privacy: aside from the normal computing models, the cloud computing uses a computing technology that is virtual which means that the user information are placed in different virtual areas instead of being stationary in one single physical space, which in turn, the protection of private data will encounter various legal systems. However, users may disclose and spread hidden data upon accessing the services of cloud computing. In this case, attackers are able to analyze such data when they are leaked (Muntés-Mulero and Nin, 2009).

3. Reliability: the similar issues can be found in cloud server as well as the personal residential servers. As seen in the server of cloud, they also encounter slowdowns and downtimes. The distinction is customers gain higher dependency on the provider of cloud service in cloud computing model. A huge contrast can be found in the cloud service provider's model, on one occasion where you pick a specific CSP, you might be sealed inside, hence bringing a possible security hazard to businesses.

4. Legal issues: by the year 2009, major service suppliers, amazon for example, are providing web services to significant online markets through creating confined rail and road networks, allowing the users to pick zones of availability (Kantarcioglu, 2011). This is regardless to the attempts to bring this subject to a lawful situation. On the other hand, there are still many concerns that are stuck with how safe and confidential the submitted information to these websites starting from a single individual reaching to higher levels of legislation.

5. Open standard: open standard are consider to be a pillar to growth and development of cloud computing. Many of the cloud service providers uncover API (application program interface).That are normally documented well enough, nonetheless they are specific to their employment which makes them operational for a single unique application. A few service vendors have already employed APIs (Kissel, 2006) from

others, in addition to various numbers of open standards that are currently being developed such as the interface used in open cloud computing platform of OGF. The OCC (open cloud consortium) (Gajanayake et al., 2011) is undergoing the development of agreements on standards to be used in early cloud computing practices

RECENTLY IMPLEMENTED SECURITY SOLUTIONS FOR PRIVACY PROTECTION AND DATA SECURITY

In June, 2009, IBM created a fully homomorphic scheme of encryption, Homomorphic encryption has an important impact on cloud computing. Taking the cloud service providers analytical service, the company transform the data in encryption for instance with the utilization of Homomorphic encryption, complex scientific operations are performed without trading off the encryption. With the help of this approach the data can be processed without the use of decryption. Roy and Ramadan joined a DIFC (Decentralized Information flow control) with differential mechanism for privacy protection turning them into information generation, then calculated stages and established a system for protecting the privacy called Air Vat. This framework helps in preventing of privacy leakage without the approval of Map-Reduce figuring methodology. The key management is the major problem for data encryption solutions. Enough experience is needed to manage the keys which the user does not have. Such type of issues in solved by KMIP (Key Management Interoperability Protocol) and OASIS (Organization for the Advancement of structured Information Standards). Regarding Information integrity verification, the check has to be done due to exchange of data, time cost and fees of data transfer, the user does not have expertise in uploading after verification. About the integrity checking of information, in view of information correspondence, exchange expenses and time cost, the clients are unable to first download information in order to confirm its accuracy and then later transfer that same information. Also as the information is dynamic and not static in cloud storage, conventional information integrity solutions arrangements are no longer applicable.

The public data integrity verification is supported by NEC Lab's provable Data Integrity (PDI). As per Cong Wang (Wang et al., 2009) the data which is stored dynamically in the cloud, he then proposed a mathematical way to verify its integrity. The tool for Client based Privacy Management was then developed by Mow bray, where he stated and proposed such tool which is a user focused trust model that helps the users to take control over the storage and utilizations of the most critical and sensitive information in the cloud. The issues that existed in technologies of Privacy Protection (such as Kanonymous, information pre-processing methods and Graphical Anonymization) risen when they are applied to large data and then an analysis is done to the current solution.

FUTURE WORK

Cloud computing in its current state is not fully developed and still a lot of exploration has to be performed. After completing our current work we are still asserting that security is considered to be the most vital threat to the clients and the vendors of cloud computing alike. Many experts such as Researchers, Vendors and IT Security Professionals are still experimenting and conducting studies in this particular field of technology along with a wide range of models and devices have been proposed yet nothing productive is found. While performing exploration on issues of security found

in cloud computing, we came to the realization that there are no accessible benchmarks on security to establish secure cloud computing. In our future works, we will further explore this aspect of security and its guidelines to ensure a much better cloud computing experiences in terms of security.

CONCLUSION

In this paper, the center of focus is on security issues in cloud computing. It is absolute necessary to consider security and protection when planning and utilizing cloud computing services. We talked about security difficulties, for example, information stockpiling security, information transmission security, and application security, security on cloud integrity and security identified with third-part assets. To distinguish high hazard risk on the cloud security, a likelihood of danger is also additionally derived. We conclude stating that to improve the revolutionary of cloud computing in the Internet, it is vital to reinforce the security capacities or capabilities.

REFERENCES

Arnold, S. (2009). Cloud computing and the issue of privacy. KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

Bowers, K.D., Juels, A., Oprea, A. (2009). Proofs of retrievability: Theory and implementation. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 43-54.

Buyya, R., Yeo, C.S., Venugopal, S. Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, 25:5 99616, 2009

Cloud Controls Matrix, Version 1.2, Cloud Security Alliance, August 26, 2011, URL:https://cloudsecurityalliance.org/wpcontent/uploads/2011/08/CSA_CCM_v1.2.xls

Dillon, T., Wu, C. and Chang E. (2010). Cloud Computing: Issues and Challenges, 2010 24th IEEE International Conference on Advanced Information Networking and Applications, 1550-445X/10.

Gajanayake, R., Iannella, R. and Sahama, T. (2011). Sharing with Care an Information Accountability Perspective," Internet Computing, IEEE, 15, 31-38.

Global Netoptex Incorporated. (2009). Demystifying the cloud. Important opportunities, crucial choices. pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

Grobauer, B. Walloschek T. and Stöcker, E. (2010). Understanding Cloud Computing Vulnerabilities. IEEE Security and Privacy, vol. 99, 2010.

Kantarcioglu, M., Bensoussan, A. and Ru, S. (2011). (Celine) Hoe Impact of Security Risks on Cloud Computing Adoption Forty-Ninth Annual Allerton Conference.

Kissel, R., Scholl, M., Skolochenko S., Li, X. (2006). Guidelines for Media Sanitization. NIST Special Publication 800-88, September-2006, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

Kresimir P. and Zeljko H. (2010). Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 344-349.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011). Cloud computing the business perspective. Decision Support Systems, 51(1), 176-189.

Mell, P., Grance, T. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145.

Muntés-Mulero V., Nin, J. (2009). Privacy and anonymization for very large datasets. In: Chen P, ed. Proc of the ACM 18th Int'l Conf. On Information and Knowledge Management, CIKM 2009. New York: Association for Computing Machinery, 2117-2118.

Roy I., Ramadan, H.E., Setty, S.T.V., Kilzer, A., Shmatikov, V., Witchel. (2010). Airavat: Security and privacy for MapRednce. USENIX Association, 297-312.

Stanoevska-Slabeva, K., Wozniak, T. (2010). Grid and Cloud Computing-A Business Perspective on Technology and Applications, Springer-Verlag, Berlin, Heidelberg.

Subashini, S. and Kavitha V. (2010). A survey on security issues in service delivery models of cloud computing. J Network Comput Appldoi:10.1016/j.jnca.2010.07.006. Jul., 2010.

Wang, C., Wang, Q., Ren, K. and Lou W. (2009). Ensuring Data Storage Security in Cloud Computing. Proceedings of the 17th International Workshop on Quality of Service, 1-9.

Wang, Z. (2011). Security and privacy issues within the Cloud Computing. International Conference on Computational and Information Sciences, 2011.

Zeng K. (2008). Publicly verifiable remote data integrity. In: Chen LQ, Ryan MD, Wang GL, eds. LNCS 5308. Birmingham: Springer-Verlag, 419.434.