Volume 4, No. 1, January 2013
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

EMPOWERING CLOUD SECURITY THROUGH SLA

Deveeshree Nayak[*1], Er. Muheet Ahmed Butt[2], Er. Majid Zaman[3] and Dana AL Themazi[4]
[*1]Research Scholar KIIT University Bhubaneswar, India
deveeshree@gmail.com
[2]Scientist,PG Department of Computer Science, Unvierstiy of Kashmir, J&K India
ermuheet@gmail.com
[3]Scientist,Directorate of IT &SS, University of Kashmir, J&K, India
zamanmajid@rediffmail.com
[4]MITCS Student at Ahlia University, Bahrain Internet Exchange, Bahrain
d.altehmazi@gmail.com

Abstract: Cloud computing is a cumulative collection of technologies. It shares on-demand computing resources that are positioned and disposed efficiently. In spite of several benefits, numerous challenges are there such as Data security, Performance, Data Locking, Access control, Bandwidth costs, Internet Dependency, Data confidentiality, Auditability, Application and Availability. SLA (Service Level Agreement) plays a vital role in cloud computing. Each service associates with a specific SLA. This is collaboration between service providers and consumer. Therefore, SLA has to define the level of security and their intricacy established on the services to make the consumer realize about the implementation of security policies. The proposed research paper tries to evaluate the challenges in enforcing security for cloud computing services and describe the necessity of a regularization of SLA.

Keywords: Cloud Computing,Service Level Agreement (SLA), Current SLA, Regulations of SLA.

INTRODUCTION

Cloud Computing is a consumer oriented technology which delivers virtualized computing resources (CPU, Memory, storage, operating system and software Applications) to the consumer via Internet (public cloud) and intranet (private cloud). According U.S. NIST (National Institute of Standards and Technology) which describes Cloud computing as a model which is 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 [16].

This is a fundamental class of systems that delivers services to the remote consumers[2]. The services accessed through cloud systems can be primarily classified into three categories such as Infrastructure as a Service (IaaS), Platform as a Service(PaaS) and Software as a Service(SaaS)[1,5,and 6]. Consumers can utilize these features like on demand service, broad based network access, pooled resources and good quality of service. IaaS is a standardized infrastructure specifically optimized for the customer's applications [6, 7]. PaaS developers are concerned only with web based development [7].In spite of outdid business and technical advantages of cloud computing, there are several concern and limitations. E.g. To fulfill SLA criteria in cloud is a measure problem between the service provider and service consumer.

Service Level Agreement (SLA) is a negotiated legal agreement between two parties, i.e. customer and service provider. Operational-level agreements (OLA) however may be used by internal groups to support SLAs.Clouds have different architecture established on services pertaining to data, software, and hardware. The data in the cloud stored in a consolidated location. The data as well as processing is done somewhere on server. So, the clients should have trust in service provider's availability as well as data security. Some prototypes of cloud computing are presented to maintain the consistency between cloud providers and consumers involved in the collaboration process [18-20]. Some mechanisms focus on the revenue and Quality of Services (QoS), and some are introduced to maximize the cloud consumers or providers' revenue [21, 22].

In this paper, section II describes Literature Survey, section III explain about cloud security challenges and precautions section IV discusses about the service level agreement and present SLA's in cloud computing, and section V deliberates how to standardize SLA's followed by the final conclusion.

LITERATURE SURVEY

The dread in cloud deals with the various security threats to these cloud environments. There are different type of clouds such as Private Cloud, Public Cloud and Hybrid Cloud environments. The levels of security varies depends upon the types [8] of these environments used. Various security issues such as violation of Data Integrity, Phishing and Botnet (running remotely on a collection of machines) pose serious threats to the organizations data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has presented new security challenges [17].

The explosion of Cloud technology has lot of security challenges for the consumer and service provider's. Security issues like securing, testing and utilizing of data. It proved that the client does not have any control over the data. La'Quata Sumter et al. [9] states: The increase growth of cloud computing has carried an alarm about the "Cloud

computing Security". Cloud services are flexible but configuration is extremely complicated using web interface but wrong configuration may lead to venerable security threats [10].

Data integrity is a measure problem in cloud services due to advance uses [11]. There are several risks in public cloud like end user trust, Insider access, visibility, risk management, Client and server side protection, access control and identity management explained in [12]. Other cloud securities are Data forensics and post investigation in cloud computing [13], Security risk and security assurance of the cloud users [9],SSH tunnel, verifiable integrity and end-to end services isolation through VPN [14],Secure Query processing and Data Sharing System Analysis and Forensics, Query correctness assurance [15] .

CLOUD SECURITY CHALLENGES AND PRECAUTIONS

Traditional Security involves intrusions attacks that will be made possible by moving into the cloud. Different parameters are VM-level of Attack and susceptibilities in the VM technology in multi-tenant architectures. Here several consumers use a multi-tenant model, "with different physical and virtual resources dynamically assigned and reassigned according to consumer demand" [16].

Cloud Provider vulnerabilities appear in SaaS level, such as an SQL-injection and cross site scripting vulnerability. Recently it has been identified in Sales force.com. Expanded network Attack here the consumer must guard the infrastructure used to interact with the cloud, Authentication and Authorization indicates Login-in of unauthorized user is vulnerable to cloud provider which will create catastrophic damage to the cloud services. Phishing here phishers steals the password of the valid and users and enjoy the services provided in the cloud.

Data Availability is the most common problems with the cloud provider.Here providers are unable to fulfill consumer demand at right time. Network failure makes the cloud user paralyzed.Third Party Data Control about the data is a lack of control and transparency. Here ultimate sufferer is cloud consumer.Third party control does not provide any guarantee for retention of data for a specific time period.

Auditability means thereis no sufficient transparency in the operations of the cloud provider. Currently, this transparency is provided by documentation and manual audit.However there is no specific guideline to perform onside audit when there is a distributed and dynamic multi-tenant computing environment spread all over the globe. In Data Lock in data itself be locked in a proprietary format, and there are also issues in training and process. There is another problem in cloud where user having no control over the frequent changing cloud based service, "with different physical and virtual resources dynamically assigned and reassigned according to consumer demand" [16].

CLOUD SLA

Due to the dynamic nature in cloud, continuous monitoring on Quality of Service (QoS) attributes is necessary to enforce SLAs [1].The service level agreement is the only authorized agreement between the service provider and client. Although cloud consumers do not have access over the fundamental figuring resources, they do need to ensure the excellence, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery.

This SLA serves as a foundation between the consumers and the providers to begin transactions. The QoS attributes act significant part of an SLA (such as response time and throughput). However significant changes in the agreement must to be closely supervised [3]. Evaluating the quality of cloud providers' approaches in security point of view is difficult, because many cloud providers will not expose their infrastructure and applications to their customers. Due to complex nature of consumer demands, a simple "measure and trigger" process may not work for SLA enforcement [4]. Attention in designing SLA improves the trust and therefore can increase throughput from the agreement. The study in this paper provides guidelines to research community in designing high yield SLAs.

CURRENT SLA

This document is applicable to all services delivered directly to the customer from the service provider. Third party is not involved here.

SLA Credit Demand:

To properly claim credit due a consumer must open a sales ticket by sending an email to provider. Then he has to provide all the information like contact information .Then it can be managed with future bill.

Credit problem:

Consumer can claim his credit amount repeatedly by violating rule .These cases is not acceptable according to present policy.

Network:

In public and private cloud service provider give full assurance about secured VPN connection, unlimited bandwidth between servers, advanced intrusion detection system, unlimited upload /download from servers, access to contracted services and traffic analysis.

Hardware Renovations:

The cloud service provider promises hardware renovations within stipulated time after failure. Hardware renovations must be scheduled and confirmed in advance through the online ticketing system. Failure to install the hardware within stipulated time will result in a waiver of any one time installation fees.

REGULARIZATION OF SLA

SLA has to deliberate about the SLA security risk, prevention methods and recovery solution. Users' feedback should record and modification should be done according to it.

Restricted user access:

Processing of sensitive data outside network creates vital level of risk. So service provider should supply specific information to authorized users and access control should be given to the authorized Administrator.

Monitoring agreement:

Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this inspection are signing that customers can only use them for the most minor functions.

Data location:

In cloud, the consumer does not have any knowledge regarding the storage of data. So it is threat to privacy of user data. Provider should mention in the agreement where the data is stored? What will happen to the data once services terminates? Weather it has been destroyed or not.

Data security:

Data is shared in public environment. Here encryption plays a dynamic role.So cloud provider give the confirmation that encryption is designed and evaluated by experienced experts.

Rescue:

Even if user does not have knowledge where your data is, a cloud Provider should tell us what will happen to the data in case of a disaster. Is there any backup to our data? In which way we can retrieve?

Investigative provision:

Strong legal action need to be taken if provider or consumer violates agreement rule.

CONCLUSIONS

Cloud computing security threats will remain a vibrant threat in the global world as long as information is available and transmitted across the internet. Data security must be assured So that users can have confidence in their activity on the internet. This paper describes about the cloud computing security issues; role of SLA in cloud computing and need of regularization of current SLA. A service provider may decide to delegate the tasks to other cloud providers, transparent to the consumer to avoid significant SLA violation and to improve level security in the SLA.

REFERENCES

[1] Anthony T. Velte, et.al, “Cloud Computing a Practical Approach,” McGraw Hill Companies, ISBN: 978-0-07-162695-8, 2010.

[2] Armbrust, M., Fox, A., Gri_th, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee,G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M.: Above the clouds: A berkeley view of cloud computing. Tech. Rep UCB/EECS-2009-28, UC-Berkeley, Feb 2009.

[3] Keller, A., Ludwig, H.: The wsla framework: Specifying and monitoring service level agreements for web services. J. Netw. Syst. Manage. 11(1) (2003) 57-81

[4] Ludwig, H., Keller, A., Dan, A., King, R., Franck, and R.: Web service level agreement (WSLA) language specification. IBM Corporation (2003)

[5] Al Tehmazi ,D ,EL KADHI ,N ; Paper in Global QoS Framework for Cloud Security: A Paradigm Shift toward a New Trust Concept; WORLDCAM 2012, CSREA Press , ISBN: 1-60132-230-5, 2012.

[6] John W. Rittinghouse and James F. Ransome, (2009), “Cloud Computing: Implementation, Management, and Security”, New York, Auerbach Publications.

[7] Linthicum. David S., September 29, 2009, “Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide”, Addison-Wesley, USA-Boston, ISBN-13: 979-0-13600922-1, 2009.

[8] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.

[9] R. La’Quata Sumter “Cloud computing Security Risk Classification”, ACMSE 2010, Oxford, USA

[10] SorenBleikertz et al, “Security Audits of Multi-tier Virtual Infrastructure in Public infrastructure clouds”, CCSW 2010, Chicago, USA.

[11] F. Lombardi and R. Di pietro, “Transparent security for cloud,” SAC ’10 March 22-26 2010, Sierre, Switzerland.

[12] Wayne A. Jansen, “Cloud Hooks: Security and Privacy Issues in Cloud Computing”, 44th Hawaii international conference on system sciences 2011.

[13] Rongxing et al,”Secure Provenance: The essential Bread and Butter of data forensics in cloud computing”, ASIACCS’10, Beijing, China

[14] Mladen A. Vouch, “Cloud Computing issues, Research and implementation”, Journal of Computing and Info. Tech., 2008, 4, 235-246

[15] Wenchaoet al, “Towards a Data-centric View of Cloud Security”, CloudDB 2010, Toronto Canada

[16] P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15," 21. Aug 2009.

[17] Y. Chen, V. Paxson, and R. Katz, "What’s New about Cloud Computing Security?" 2010

[18] Mohammed Alhamad, Tharam Dillon, Elizabeth Chang,“SLA-Based Trust Model for Cloud Computing” 13th Intnl. Conf. on Network-Based Information Systems, 2010:pp.321-324.

[19] P. Patel, A. Ranabahu and A. Sheth, Service Level Agreement in Cloud Computing[C]. Conference on Object Oriented Programming Systems Languages and Applications, Orlando, Florida, 2009, USA.

[20] Mohammed Alhamad, Tharam Dillon, Elizabeth Chang, “Conceptual SLA Framework for Cloud Computing,”4th IEEE Intnl. Conf. on Digital Ecosystems and Technologies, 2010: pp.606-610

[21] Mario Macas, J. OriolFito, JordiGuitart. “Rule-based SLA Management for Revenue Maximisation in Cloud Computing Markets,” Intnl. Conf. on Network and Service Management, 2010: pp.354-357.

[22] A. Andrzejak, D. Kondo, S. Yi. "Decision Model for Cloud Computing under SLA Constraints," 18th Annual IEEE/ACM IntnlSymp. On Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 2010: pp.257-266.

