Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.8 No.2, 2019, pp.40-43

DOI: https://doi.org/10.51983/ajcst-2019.8.2.2143

Research Key Techniques of Data Security in Public Cloud

Sheik Saidhbi
Assistant Professor, Department of Information Systems, Faculty of Informatics, University of Gondar, Ethiopia
E-Mail: sfajju.syed@gmail.com
(Received 1 March 2019; Revised 17 March 2019; Accepted 19 April 2019; Available online 27 April 2019)

***Abstract* - Internetworking security has become one of the biggest uprising points of concern now days. People are gettingattached more and more to the internet in order to fulfill theirdemands. Not only customers but also the IT based companiesare also getting themselves relying on up growing technologycalled as cloud computing. Cloud is a branch of computerscience that provides the services on lease. In this paper wewill make a comparative analysis of various technical securityissues towards cloud computing, cloud deployment basedsecurity and model based security issues. A comparative analysis has been made at the end of the paper.**
Keywords: **Cloud Computing, Security Issues, Cloud Models**

I. INTRODUCTION

With the progression in the period the innovation is gettingincreasingly and more extensive. Individuals now a day's getthe administrations as per their requests thus ly they don't need to pay superfluous for the things they don't need to utilize.Cloud computing is one the developing innovation which givethe administration of programming on rent. Cloud computingpermits the client to make requests and give the administrations as need by the clients. Cloud computing is productive and adaptable however keeping up the steadiness of preparing such a variety of occupations in the cloud computing environment is an exceptionally complex issue with security of data to which is getting much consideration by the scientists [1]. Cloud computing as such is the moralstory of the web [2]. The cloud specialist organizations should sure about that they get the security flanks appropriate, for they are the ones who will assumed the liability if things turn out badly. Cloud framework offers many advantages likequick sending, pay-for-utilize, lesser costs, adaptability, flexibility, universal system get to, more noteworthy versatility, hypervisor insurance against system assaults, easerecuperation and information stockpiling arrangements, on request security controls, continuous identification of framework altering and fast re-constitution of administrations [3].

The real favorable position of cloud computing in whichwe can pay-for-use for any product i.e. on the off chance that aclient doesn't have a specific programming that he needs toutilize say MS word, the client can utilize that specific programming on the cloud framework by paying for it. Cloudframework comprises of three administration models in lightof the asset center [4] i.e. SaaS, PaaS and IaaS. Within thispaper our key goal is to deliver an evolution and qualifiedstudy of various cloud computing security issues. First we willbounce an outline of all the security issues either model based or deployment based. At the last we will conclude the paper in a tabular form.

II. TECHNICAL SECURITY ISSUES IN CLOUD COMPUTING

In this discussion, we present some security issues related to Cloud Computing. Each issue is explained briefly and tells show it makes an impact on the cloud system technology.

A. Xml Signature Attack: There are numerous conventions that utilization the XML Signature for their verification and trustworthiness. To those conventions XML Signature assault is extremely normal and called as XML Signature Element Wrapping [5]. As this sort of assault applies on the web benefits so it's clear that it is regular in the distributed computing as well. The underlying message shows a message sent by an honest to goodness customer. The body contains a demand for the document marked by the sender. The Signature is encased in the messageheader and allodes to the marked message. The messagesection utilizes an X Pointer to that contains the estimation of "body". In the event that an aggressor spies such a message, hecan play out the assault as took after. The first assemblage ofmessage is moved to a crisply embedded wrapping component (giving the assault its name) inside the message header, andanother body is made. This body contains the all operation the intruder needs to perform with the first sender's approval, here the demand for the specific record. The subsequent message will even now contain a substantial mark of an honest to goodness client. Since the first mark still exist in the messages to the trespasser can without much of a stretch get to the data on the cloud thus can alter it.

B. Browser Security: The fundamental component of Cloud computing is that it can be accessed from anyplace remotely. The customer PC utilized for verification and for I/O and that PC additionally charges to the cloud for the further operation. So clearly to access anyframework or a system the browser is a key point. With concentrating on the Same Origin Policy (SOP) [6], this report unfurls numerous weaknesses of browser security in cloud frame work. For this examination we need to consider TLS, which is utilized for host validation and encryption of information. The deficiencies in the Web browsers are that it can't straight forwardly make XML Signature or XML Encryption. As Data must be scrambled through TLS, and marks are just utilized as a part of the TLS handshake. In herethe browser goes about as detached information stockpiling. Since the

browser itself can't produce cryptographically legitimate XML tokens to verify against the Cloud, this is finished with the assistance of a trusted out sider. With the anatomies of scripting dialects (as JavaScript) into Web pages, it got to be distinctly essential to characterize get to rights for these scripts. So it's a characteristic thing, the browser withsame cause, [7] permits the operations of read/compose operations and to forbid any entrance to content from an alternate starting point.

C. Cloud Malware Injection Attack: Among the key assaults on the cloud framework the malware infusion assault is an extensive assault endeavor goes for infusing a noxious administration execution into the Cloud framework. Such sort of Cloud malware fills for a specific need. The motivation behind cloud malware is enemy that might run from listening in by means of moment information alteration to full usefulness changes or blockings. To make the enemy the malware needs to make its own particular execution module (SaaS or PaaS) or virtual machine case (IaaS), and add it to the Cloud framework.

D. Flooding Attacks: Out sourcing is a major aspect of Cloud Computing consists in basic operational tasks to a Cloud system provider. Among these basic tasks, maintenance of server hardware is the most important one. So instead of operating an own, internal data center, the paradigm of Cloud Computing enables companies (Users) to rent server hardware on demand (IaaS). This approach is economically beneficial when it comes to dynamics in server load, as for instance day-and-night cycles can be attenuated by having the data traffic of different time zones operated by the same servers. No doubt the feature of providing more computational power on demand is appreciated in the case of valid users but it poses severe troubles in the presence of an attacker. The corresponding threat that arises or may arise is flooding attacks, in which basically an attacker sending a large amount of meaningless requests to a certain service.

As each of these requests has tobe processed by the service implementation in order to determine its invalidity and due to this heavy load it causes a certain amount of workload per attack request, which creates flood of requests usually would cause a Denial of Service to the server hardware [8], [9]. In the specific case of Cloud Computing systems, the impact of such a flooding attack is expected to be amplified drastically. This is due to the different kinds of impact. Flooding of requests then further may lead to halt the running system and it makes easy to attack of denial of service. The denial of service is of two types direct and indirect [10].

III. CLOUD DEPLOYMENT BASED SECURITY

In the cloud deployment model, networking, platform, storage and software infrastructure are delivered as facilities that gauge up or down conditional to the mandate. The Cloud Computing model has three main deployment models which are:

A. Private Cloud: Private cloud is another term that a few merchants have usedto depicts offerings that copy cloud figuring on private systems. It is a set up inside an association's inward endeavor data center. In the private cloud, versatile assets and virtual applications gave by the cloud merchant are pooled together and accessible for cloud clients to share and utilize. It contrasts from general society cloud in that all the cloud assetsand applications are overseen by the association itself, like Intranet usefulness. Usage on the private cloud can be much more secure than that of general society cloud in view of it predetermined inward introduction. Just the association and assigned partners may have entry to work on a particular Private cloud. [12]

B. Public Cloud: Public cloud portrays cloud registering in the conventional standard sense, whereby assets are powerfully provisioned ona fine-grained, self-benefit premise over the Internet, through web applications/web administrations, from an off-webpage outsider supplier who offers assets and bills on a fine-grained utility figuring premise. It is ordinarily in view of acompensation for every utilization display, like a prepaid power metering framework which is sufficiently adaptable to provide food for spikes popular for cloud optimization. Public clouds are less secure than the other cloud models since it places an extra weight of guaranteeing all applications and information got to on the public cloud are not subjected to malicious assaults [13].

C. Hybrid Cloud: Hybrid cloud is a private cloud connected to at least one outercloud administrations, halfway oversaw, provisioned as asolitary unit, and surrounded by a safe system [14]. It gives virtual IT arrangements through a blend of both open and private clouds. Hybrid Cloud gives more secure control of the information and applications and permits different gatherings to get to data over the Internet. It additionally has an open design that permits interfaces with other administration frameworks. Hybrid cloud can portray arrangement consolidating a nearby gadget, for example, a Plug PC with cloud administrations. It can likewise depict designs consolidating virtual and physical, arranged resources for the most part virtualized environment that requires physical servers, switches, or other equipment, for example, a system machine going about as a firewall or spam channel.

D. The Network Security Situation on Public Cloud: With the rapid development of Internet plus, data is the core competitiveness of enterprises. Data have many kinds such as customer information, financial information andother information. At public cloud, the core data of the enterprise is generally stored in the public network storage which provided by the service provider [13]. The data whichstored in the network are more and more openness andconvenience, at the same times more and more no privacy and insecurity. During the enterprise data is transmitted and stored, it is stolen easily. It is particularly concerned about that how to encrypt core data. In order to better protect these data, more and more enterprises have

established public cloud. But there are many insecure factors in public cloudnetworks: data communications insecurity, intentional attackservers, frequent sending of service requests in the short term, which may affect the reliability of public cloud.

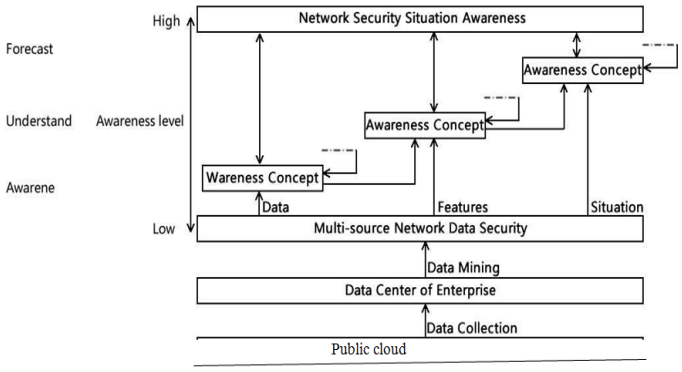

Fig. 1 Architecture graph of network security situation

IV. MODEL BASED SECURITY ISSUES

Cloud framework comprises of three conveyance models thatcharacterize the structure of the cloud framework. Threemodels in cloud framework are SaaS, PassS and IaaS. SaaS remains for software as a service in which client can utilize the information from untouchable limits of any undertaking. PaaS remains for Platform as a service that gives the stage to building up the applications on the cloud. The last one IaaS remains for infrastructure as a service which gives equipment support to cloud framework. In any case, these models additionally have some security openings that are examined as follows in the paper.

A. Issues in Software as a Service (SaaS) Model: The SaaS essentially accentuating on supplanting the oldapplication programming with the new ones as opposed tomaking the convey ability of utilization programming inwhich the security usefulness of programming application isprinciple center [11]. . The fundamental issue in SaaS is that the information is exceptionally delicate on the grounds thatit is put away on the outside the limit of big business. Forsafety efforts the customer needs to rely on the supplier in SaaS. Because of deceivability of information of each otherclients, the supplier must accomplish something so that theinformation robbery or misfortune is evaded. There islikewise another issue i.e. in the event that a specific clientneeds a similar document which is being utilized by anotherclient in the meantime yet because of safety efforts theclient can't get that record.

B. Issues in Platform as a Service (PaaS) Model: PaaS is more extensible than SaaS as it gives stage to buildup the application yet security is the fundamental issue oncemore. At the point when PaaS gives individuals to manufacture their applications on the larger amount of stage, the supplier must guarantee about detachment of informationbetween two applications.

C. Issues in Infrastructure as a service (IaaS) Model: IaaS bargains in virtualization and VMware. Any issues emerge in VM May prompts to defer in conveyance ofbundles in upper model like PaaS and SaaS. Additionally IaaS has higher security administration strategies and prompts to less security openings in it [12].

TABLE I COMPARATIVE STUDY OF TECHNICAL SECURITY ISSUES IN CLOUD COMPUTING

Security Issues	Attack Description	Effect on Cloud System	Countermeasures
Xml signature Attack	Addition of new body to novel message	Novel information altered	Usage of secure coding
Browser Security	Data is kept passively so browser is impotent to cause token of authentication	Data loss occurs	Use xml encryption in TLS
Malware Injection Attack	Malware makes its own enactment unit and swell it to cloud system	May leads to malicious service operation and incorrect code performed	Store hash values on novel service instance's file and relate it with the hash value of file

TABLE II COMPARATIVE STUDY OF MODEL BASED SECURITY ISSUES

Cloud System Models	Security Issue	Impact on Cloud System	Counter measures
SaaS	Data is available on the out outside margins	Data larceny may arise	Robust encryption technique should be used and use fine grained access
PaaS	Throughout creating applications on podium coding may blend on cloud	Incorrect code execution	Retain eye on kind of attack and avoid reflectivity of code
IaaS	Any problem antecedent in hardware may lead to late distribution of packets	Working of System may slow down	Strong security management so only hardware related threats may occur

TABLE III CLOUD COMPUTING CHALLENGES ANALYSIS

Challenges	Security Issue	Impact on Cloud System	Counter measures
Data Security	Information misfortune, phishing, botnet (running remotely on a gathering of machines) posture genuine dangers to association's information and programming	Vulnerable security threats	Strong encryption technique should be used and use fine grained access
Cost	This issue is especially noticeable if the buyer utilizes the hybrid cloud sending model where the association's information is conveyed among various open/private(in-house IT foundation) / group clouds	Limited use of Cloud	Depends upon the usage of cloud and its resources.
Charging	More Availability but less users due to higher cost charges	Limited use of cloud services (SaaS)	Depends upon the Requirement of user.
Service level agreement	Issue is the meaning of SLA determinations in a manner that has a suitable level of granularity, to be specific the tradeoffs amongst expressiveness and complicatedness, with the goal that they can cover alarge portion of the customer desires.	Trust issues	Only trusted employees should given the rights to use SLA
Cloud interoperability issue	Driving merchant locking, which precludes the capacity of clients to look over option sellers/offering at the same time so as to streamline assets at various levels inside an association?	More vitally, restrictive cloud APIs makes it extremely hard to coordinate cloud administrations with an association's own current legacy frameworks	End goal of enhancement, an association may need to outsource various negligible capacities to Cloud administrations advertised by various sellers

V. CONCLUSION

As described in the paper, though there are extreme advantagesin using a cloud-based system, there are yet many practicalproblems which have to be solved. Cloud computing is adisruptive technology with profound implications not only forInternet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related security andprivacy. As described in the paper, currently security has lot of loose ends which scares away a lot of potential users. Until aproper security module is not in place, potential users will not be able to leverage the advantages of this technology. In this paper, we presented a selection of issues of Cloud Computing security.

We investigated ongoing issues with application of XMLSignature and the Web Services security frameworks, discussedthe importance and capabilities of browser security in the Cloud Computing context (SaaS), data security issues in SaaS, security issues in PaaS and we suggested some countermeasures to avoidthe data loss and for making the cloud computing more secure.

REFERENCES

[1] "Security Guidance for Critical Areas of Focus in Cloud computing", presented by *Cloud Security Alliance (CSA)*, April 2009.

[2] Arijit Ukil, Debasish Jana and Ajanta De Sarkar, "A Security Framework In Cloud Computing Infrastructure", *International Journal of Network Security & Its Applications (IJNSA)*, Vol. 5, No. 5, September 2013, DOI:10.5121/ijnsa.2013.5502 11.

[3] Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges", *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS)* Vol. 1, No. 2, December 2011.

[4] Kashif Munir and Prof Dr. Sellapan Palaniappan, "Framework for Secure Cloud Computing", *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, Vol.3, No.2, April 2013.

[5] Navdeep Singh, Abhinav Hans, Ashish Sharma, and Kapil Kumar, "A Review on Security Issues in Cloud Computing," *International Journal of Innovation and Applied Studies*, Vol. 8, No. 3, pp. 1090–1093, September 2014.

[6] M. McIntosh and P. Austel, "XML signature element wrapping attacks and counter measures," *in SWS '05: Proceedings of the 2005 workshop on Secure web services. ACM Press*, pp. 20–27, 2005.

[7] S. Stamm, Z. Ramzan, and M. Jakobsson, "Drive-by pharming," *Indiana University Computer Science, Tech. Rep*. 641, 2006.

[8] Ayesha Malik, and Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review", *Journal of Emerging Trends in Computing and Information Sciences* 2009-2012 CIS Journal, All rights reserved,Vol.3, No. 3, March 2012.

[9] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, and Vasanth Balaand Peng Ning, "Managing security of virtual machine images in a cloud environment", *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 91-96, November 2009.

[10] Miranda Mow brayand Siani Pearson, "A Client Based Privacy Manager for Cloud computing", *Proceedings of the Fourth International ICST Conference on communication system software and Middleware*, June2009.

[11] Flavio Lombardi and Roberto Di Pietro, "Transparent Security for Cloud", *Proceedings of the 2010 ACM Symposium on Applied Computing*, pp. 414-415, March 2010.

[12] Weichao Wang, Zhiwei Li, Rodney Owens and Bharat Bhargava, "Secure and Efficient Access to Outsourced Data", *Proceedings of the ACM workshop on Cloud computing security*, pp. 55-65, 2009.

[13] Krešimir Popović, Željko Hocenski, "Cloud computing security issues and challenges", *MIPRO 2010*, May 24-28, 2010, Opatija, Croatia.

[14] TakeshiTakahashi, Gregory Blancy, Youki Kadobayashiy, Doudou Fally, Hiroaki Hazeyamay, and Shin'ichiro Matsuo, "Enabling Secure Multi tenancy in Cloud Computing: Challenges and Approaches".

[15] Nagarjuna, C.C kalyansrinivas, S. Sajida, and Lokesh, "Security techniques for multi tenancy applications in Cloud", C.C. KalyanSrinivas *et al., International Journal of Computer Science and Mobile Computing*, Vol. 2, No. 8, pp. 248-251, August 2013.