International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 8 No. 3 Sep. 2014, pp. 1090-1093
© 2014 Innovative Space of Scientific Research Journals
http://www.ijias.issr-journals.org/

A Review on Security Issues in Cloud Computing

Navdeep Singh, Abhinav Hans, Ashish Sharma, and Kapil Kumar

Department of Computer Science,
Guru Nanak Dev University, Regional Campus,
Jalandhar, Punjab, India

ABSTRACT: The Cloud computing offers a distributed system over a network in which a program or any application run on many connected computers at the same time. Cloud computing is a hosted service in which an end user can access the cloud based applications through the browser or any mobile application. Though the cloud computing is a very vast and useful technology but there are still some challenges to be solved. Among all of these there are security issues. The security is most important impact of any software or any hardware. So this paper focuses on the security issues arising from the usage of Cloud services and security issues in different service models of cloud computing.

KEYWORDS: Cloud computing, Security, Issues, virtualisation, cloud system models.

1 INTRODUCTION

The technology with less resource uses and higher with output always attract the users. Cloud computing entice the users for the same. The Cloud computing offers a distributed system over a network in which a program or any application run on many connected computers at the same time [1]. Cloud computing in other words is the allegory of the internet [2]. The cloud service providers must certain about that they get the security flanks right, for they are the ones who will took the responsibility if things go wrong. Cloud system offers many benefits like fast deployment, pay-for-use, lesser costs, scalability, elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services [3]. The major advantage of cloud computing in which we can pay-for-use for any software i.e. if a user doesn’t have a particular software that he wants to use say MS word, the user can use that particular software on the cloud system by paying for it. Cloud system consists of three service models based on the resource focus [4] i.e. SaaS, PaaS and IaaS. Software as a Service (SaaS) grants end users to use cloud applications. The Google application is good example of it. With Platform as a Service (PaaS), developer can develop applications using the programming languages and tools supplied by the cloud provider. And the last service model Infrastructure as a Service (IaaS) allows user to quickly regulate the physical resources for the applications and run any software ranging from operating systems to application software. Amazon and Amazon S3 are the best known examples. While the cloud offers spectacular advantages, but there are several security and trust issues yet to be resolved. Whether we design hardware or a software the security matters a lot. The designing of our any system is not worth if it is not secure. In the cloud system software there are also many security issues related to data and its service models.

2 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 how it gives impact on the cloud system technology.

2.1 XML SIGNATURE ATTACK

There are many protocols that use the XML Signature for their authentication and integrity process. To those protocols XML Signature attack is very common and called as XML Signature Element Wrapping [5]. As this type of attack applies on the web services so it s obvious that it is common in the cloud computing too. The initial message presents a message sent by a legitimate client. The body contains a request for the file signed by the sender. The Signature is enclosed in the message header and refers to the signed message. The message fragment use an X Pointer to that contain the value of “body”. If an attacker eavesdrops such a message, he can perform the attack as followed. The original body of message is moved to a freshly inserted wrapping element (giving the attack its name) inside the message header, and a new body is created. This body contains the all operation the invader wants to perform with the original sender’s authorization, here the request for the particular file. But the resulting message will still contains a valid signature of a legitimate user, thus he service executes the modified request. Since the original signature still exist in the message so the invader can easily access the information on the cloud and so can modify it.

2.2 BROWSER SECURITY

The main feature of Cloud, computation is that it can be access from anywhere remotely. The client computer used for authentication and for I/O and that computer further commands to the cloud for the further operation. So it is obvious that for accessing any system or a network the browser is a key point. With the focusing on the Same Origin Policy (SOP) [6], this document unfolds many shortcomings of browser security in cloud system. For this discussion we have to additionally take into account TLS, which is used for host authentication and encryption of data. The shortcomings in the Web browsers are that it cannot directly make XML Signature or XML Encryption. As Data can only be encrypted through TLS, and signatures are only used in the TLS handshake. In here the browser acts as passive data storage. Since the browser itself is unable to generate cryptographically valid XML tokens to authenticate against the Cloud, this is done with the help of a trusted third party. With the anatomises of scripting languages (as JavaScript) into Web pages, it became crucial to define access rights for these scripts. So it’s a natural thing, the browser with same origin, [7] allows the operations of read/write operations and to disallow any access to content from a different origin.

2.3 CLOUD MALWARE INJECTION ATTACK

Among the vital attacks on the cloud system the malware injection attack is a considerable attack attempt aims at injecting a malicious service implementation into the Cloud system. Such type of Cloud malware serves for a particular purpose. The purpose of cloud malware is adversary that may be ranging from eavesdropping via minute data modification to full functionality changes or blockings. To create the adversary the malware needs to create its own implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system.

2.4 FLOODING ATTACKS

Outsourcing 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 centre, 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; 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 to be 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].

3 MODEL BASED CLOUD SECURITY ISSUES

Cloud system consists of three delivery models that define the structure of the cloud system. Three models in cloud system are SaaS, PassS and IaaS. SaaS stands for software as a service in which user can use the data from outsider boundaries of any enterprise. PaaS stands for Platform as a service that provides the platform for developing the applications on the cloud. The last one IaaS stands for infrastructure as a service which provides hardware support for cloud system. But these models also have some security holes that are discussed as follows in the paper.

3.1 DATA SECURITY ISSUES IN SOFTWARE AS A SERVICE (SAAS) MODEL

The SaaS mainly emphasising on replacing the old application software with the new ones instead of making the portability of application software in which the security functionality of software application is main focus [11]. . The main issue in SaaS is that the data is very sensitive because it is stored on the outside the boundary of enterprise. For security measures the client has to depend upon the provider in SaaS. Due to visibility of data of one another users, the provider must do something so that the data theft or loss is avoided. There is also another problem i.e. if a particular user needs the same file which is being used by another user at the same time but due to security measures the user cannot get that file.

3.2 SECURITY ISSUES IN PLATFORM AS A SERVICE MODEL (PAAS)

PaaS is more extensible than SaaS as it provides platform to develop the application but security is the main issue again. When PaaS provides people to build their applications on the higher level of platform, the provider must assured about inaccessibility of data between two applications.

3.3 SECURITY ISSUES IN INFRASTRUCTURE AS A SERVICE MODEL (IAAS)

Iaas deals in virtualisation and VMware. Any issues arise in VM May leads to delay in delivery of packets in upper model like PaaS and SaaS. Moreover Iaas has higher security management techniques and leads to less security holes in it [12].

Table 1 Comparative Study of Technical Security Issues in Cloud Computing

Security issues	Attack Definition	Impact on Cloud System	Countermeasures
XML Signature Attack	Insert new body to original message	Original data information changed	use secure coding
Browser Security	Data is stored passively so browser is unable to generate tokens of authentication	Leads to data loss	Use xml encryption in TLS
Malware Injection Attack	Malware creates its own implementation module and add it to cloud system	May leads to malicious service implementation and wrong code executed	Store hash values on original service instance's file and compare it with the hash value of file
Flooding	Execution of unnecessary requests sent by intruder	Full loss of availability to intended services	Allow only authenticated service to execute and use scheduling

Table 2: Comparative Study of Model Based Security Issues

Cloud System Models	Security Issue	Impact on Cloud System	Countermeasures
SaaS	Data is present on the external boundaries	Data theft may occur	Strong encryption technique should be used and use fine grained access
PaaS	During building applications on platform coding may intermix on cloud	Wrong code execution	keep eye on type of attack and avoid visibility of code
IaaS	Any problem in hardware may lead to late delivery of packets	Working of System may slow down	Strong security management so only hardware related threats may occur

4 CONCLUSION

As described in the paper, though there are extreme advantages in using a cloud-based system, there are yet many practical problems which have to be solved. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related security and privacy. As described in the paper, currently security has lot of loose ends which scares away a lot of potential users. Until a proper 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 XML Signature and the Web Services security frameworks, discussed the 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 avoid the data loss and for making the cloud computing more secure.

REFERENCES

[1] J. Heiser and M. Nicolett, "Assessing the security risks of cloud computing," *Gartner Report, 2009. [Online*].

[2] http://en.wikipedia.org/wiki/*Cloud_computing*

[3] Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010) "Security and privacy in cloud computing: A survey. In Semantics knowledge and grid (SKG)" *2010 sixth international conference on 1–3 November 2010 (pp. 105–112). Beijing, China:IEEE."*

[4] Michael Miller, "Cloud Computing-Web Based Applications that Change the Way You Work and Collaborate Online", *Que Publishing, (August 21, 2008) ISBN-10: 0789738031.*

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

[6] Hassan Rasheed in "Data and infrastructure security auditing in cloud computing environments" *Taif University Deanship of Information Technology, Saudi Arabiaa"*

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

[8] M. Jensen, N. Gruschka, and N. Luttenberger, "The Impact of Flooding Attacks on Network-based Services," *in Proceedings of the IEEE International Conference on Availability, Reliability and Security (ARES), 2008.*

[9] M. Jensen and N. Gruschka, "Flooding Attack Issues of Web Services and Service-Oriented Architectures," *in Proceedings of the Workshop on Security for Web Services and Service-Oriented Architectures (SWSOA, held at GI Jahrestagung 2008), 2008, pp. 117–122.*

[10] M. Jensen and J. Schwenk, "The accountability problem of flooding attacks in service-oriented architectures," *in Proceedings of the IEEE International Conference on Availability, Reliability and Security (ARES), 2009.*

[11] S. Subashini V.Kavitha in "A survey on security issues in service delivery models of cloud computing" *Anna University Tirunelveli, Tirunelveli, TN 627007, India*

[12] Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja in "Cloud Computing Security Issues in Infrastructure as a Service" *Punjab Technical univ*