International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity (CIPECH14) 28 & 29 November 2014

Unfolding Various Security Brawls and Concerns of Cloud Computing

Navdeep Singh, Abhinav Hans, Ashish Sharma, Kapil Kumar
Department of CSE
Guru Nanak Dev University Regional Campus
Jalandhar, INDIA
navvdeep.singh@gmail.com, abhinavhans@gmail.com,
iamashish90@gmail.com, er.kapilkumar@yahoo.com

Abstract- The **cloud computing is a discreet system which provides a lade system for the users in which a user can surf the online software facility. The cloud system is considered as the hosted service in which a particular user can access the cloud system remotely by using mobile applications or by using the browsers. Though the cloud computing provides so many utilities but there are also some holes in the service. Amongst all the security issues of the service come on the top. The security is the most important thing whenever you design any hardware or software. If the system is not secure then it will not be worth to use it. So this paper is emphasising on some security issues and their solutions to make the cloud system better.**

Keywords- Cloud Computing, Security Issues, Virtualisation, Network Security,

I. INTRODUCTION

The technology demanding less resources and with supreme output always attracts the user. So the Cloud Computing is the one which provides the same and entices the users. The cloud computing entice the users for the same. The cloud system provides a distributed system over a network on which more than one computer or mobile phones connected on the same time [1]. Cloud computing can also be considered as the allegory of internet [2]. Cloud service providers must certain about that they get the security flanks right, they are the one which take the responsibility if the things went wrong in the cloud system. Cloud computing provides many benefits like fast deployment, software rental service, lesser cost, less hardware cost, scalability, elasticity ,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 most highlighted feature of the cloud system is the rental service i.e. if the user does not have the particular software then the particular user can use that software on the cloud and can pay for it. Obviously if the user wants to buy his own software then the hardware and software cost will be counted. So it will be better to use the cloud system instead.

The cloud system consists of three types of delivery models based on the resource focus [4] i.e. SaaS, PaaS and IaaS. Saas stands for software as a service that grants end users to use cloud applications. In the SaaS the data resides on the outer boundaries of the enterprise. The Google application store is the best example of the SaaS. The next delivery model PaaS stands for Platform as a Service in which 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. But whenever a developer designs any sort of hardware or software the first thing that took into consideration is that how secure the software or hardware is. Security is the main part of the any system. Though the cloud offers the spectacular advantages but there are also some security issues yet to be solved. Many security issues resides in the cloud system that may be access based, network based or delivery based. So in this paper we are going to discuss about the different types of security risks, there impact on cloud and some preventive measures.

II. NETWORK BASED SECURITY ISSUES IN CLOUD COMPUTING

In this paper, we present a discussion on the security issues related to Cloud Computing. Each issue is explained briefly and tells how it gives impact on the cloud system technology.

A. *Port Scanning:* As the port 80(http) that provides the web services to the user always remain open. Such type of the open ports acts as key for the intruders. Data can be theft by scanning these types of ports. So to avoid this type of the attacks [5] the open ports should be encrypted.

B. *Incomplete Data Deletion:* The cloud system also acts as big data storage element for the users. Whenever a user works on cloud system the data used or stored by the user is stored more than one

place i.e. data replicates on different place for the backup purpose therefore when a user wants to delete the data from the cloud system [6], the data cannot be deleted completely because many copies of the data reside on the different server of the cloud server. So the intruder may use the previously stored data for further change that may lead to wrong implementation of data.

C. *Secure socket layer (SSL):* Another issue in the cloud system is the SSL issue in which occurs when the SSL is not properly configured between two communicating parties. This issue may also be considered as the middle man security issues because if the SSL is not configured between two communicating parties, then the third party may hack the data [7].

D. *Network Sniffing:* The network sniffer attack is more crucial and common attack in the cloud system network. In this attack [8] the unencrypted data is hacked from the network. The unencrypted password theft is most common in this attack.

III. ACCESS BASED SECURITY ISSUES IN CLOUD COMPUTING

A. *XML Signature Attack:* In cloud computing many protocols use XML signature as authentication and integrity process. In these types of the protocols XML wrapping [9] of message is used. Though it is a good method for security but there are some holes in it. In XML wrapping message techniques the intruder may inject its malicious data that changes the original message body and that lead to change of original data information.

B. *Browser Security:* The cloud computing posses the feature of accessing the cloud system from anywhere. But it is also obvious that for accessing the cloud system browser is a key point. The web browser from same or different origin policy [10] may create a problem because of different scripting languages used in the different web browsers. And also some shortcomings in the browsers that the XML signature wrapping and encryption cannot be done directly because the data can be encrypted only in Transport Layer Security and browser also acts as passive data storage. As the browser itself is unable to create XML wrapping or encryption so it is done with the help of third party.

C. *Cloud Malware Injection Attack:* The malware injection attack is the one of considerable attacks in the cloud system that aims at injecting a malicious service in the cloud system and then that malicious service [11] is implemented. This type of attack serves for particular purpose in the Cloud system. In this attack a minute data modification done from eavesdropping that later leads to change of data or blocking of data.

D. *Opulence Attacks:* The most considerable feature of the cloud system is that it provides the rental services i.e. if a user does not have particular software then the same user can work on that particular software by online using cloud services. Though it is a big feature of cloud but there is also a threat to the service. The corresponding threat that arise or that may arise is known as flooding attack, in which a intruder eavesdrops the information and send the meaningless requests in large amount to a certain service. As each of request has to be processed and implemented in order to check whether it is valid or not. And this causes the heavy load and blockage of the data on the cloud system, which creates Denial of Service to the server hardware [12].

TABLE 1: NETWORK BASED SECURITY ISSUES AND THERE SOLUTION

Security Issue	Attack Definition	Impact on Cloud	Solution
Port Scanning	Opened ports scanned for data stealing	Theft of data	Use encryption on open ports
Incomplete Data Deletion	Data is not deleted completely on cloud server because of replication of data on different locations of cloud	Left over copies of Data can be used as malicious data and flooding	Use virtualized private network
SSL	Third party may steal the data if SSL is not properly configured	Data theft	Configure the SSL completely before data communication
Network Sniffing	Un-encrypted data may be hacked	Password hacking	Use grained encryption

TABLE 2: ACCESS BASED SECURITY ISSUES AND ITS SOLUTION

Security issues	Attack Definition	Impact on Cloud System	Solution Imposed
XML Signature Attack	Insert a new message body to the original message	Change in the form of original data	use secure coding
Browser Security	Browser is unable to generate tokens of authentication	May leads to Password and data hacking	The XML encryption can be used in Transport Layer Security in Browsers
Malware Injection Attack	Malicious data is inserted into the cloud system	Malware inserted in the data may block the data and may leads to wrong code execution	Store hash values on original service instance's file and compare it with the hash value of file
Flooding	Unnecessary requests sent by the unauthorized user	Loss of availability of intended services	Allow only authenticated service to execute and use scheduling

IV. CONCLUSION

As described in the paper though there are extreme advantages of using a cloud system but there are some problems to be resolved yet. Cloud computing is a disruptive technology with profound implications not only the internet service but also for the IT sector. Still several issues exist particularly related to security and privacy. As discussed in the paper currently security has lot of loose ends which scares away a lot of users. Until the proper module is not settled, potential users will not be able to leverage the advantages of this technology. In this paper we presented some network and access based security issues and some solutions are imposed that can make the cloud system better and 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) in "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] Cloud Security Alliance (2010). Top threats to cloud computing, version 1.0. http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf .

[6] Jamil, D., & Zaki, H. (2011a) "Cloud computing security" International Journal of Engineering Science and Technology (IJEST) , Vol.3 No.4, 3478-3483

[7] Jensen, M. (2009, September). "On Technical Security Issues in Cloud Computing" IEEE International Conference in Cloud Conouting , 109-116.

[8] Jamil, D., & Zaki, H. (2011a) in "cloud computing security" International Journal of Engineering Science and Technology (IJEST) , Vol.3 No.4, 3478-3483

[9] 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.

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

[11] Pavan Muraidhara "Security issues in cloud computing and its countermeasures" International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013 ISSN2229-5518

[12] 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 Architecture (SWSOA. Held at GI Jahrestagung 2008), 2008, pp.117-122.