International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 5 (2014), pp. 533-536
© International Research Publications House
http://www. irphouse.com /ijict.htm

Well-known Gartner's Seven Security Issues Which Cloud Clients Should Advert

Vinay Singh

M.Tech (CSE) Final Year, Galgotias University, Greater Noida, India.

Abstract

This paper presents an applied research study on cloud computing process based on gartner’s security issues .The main objective of this research study is to get knowledge about cloud computing security and the important role which will they pay for the selection of resources. Cloud computing is a model for enabling ubiquitous, 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. Cloud computing provides basically three kinds of service: Software as a Service (SaaS) , Platform as a Service and Network as a service.

Keywords: Cloud computing, software as a service, platform as service, security issues.

1. Introduction

According to the gartner’s hope cycle of emerging technologies cloud computing is generally becoming very useful and at the peak it is getting several advantages that are to be useful for the high flexibility and provide lot of resources. In this paper we will generally focus on the gartner’s seven security issues which any cloud will generally provide .Cloud computing security is generally becoming a very useful topic for providing security to any organization.

Innately, Internet is a communication infrastructure for cloud providers that use well-known TCP/IP protocol which users' IP addresses to identify them in the Internet. Similarly to physical computer in the Internet that have IP address, a virtual machine in the Internet has an IP address as well. Any malicious user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting any malicious virtual machine at that location to launch an attack . Because all of users who use same virtual machine as infrastructure, if a hacker steals a virtual machine or take control over it, he will be able to access to all users' data within it here for, The hacker can copy them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with analysis the data may be find valuable data afterward.

2. Gartner’s Seven Security Issues for Cloud Computing

Gartner’s seven security issues for cloud computing are mentioned as follows-

1) ***Privileged user access***: Sensitive data processed outside the enterprise brings with it an inherent level of risk because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs.
2) ***Regulatory compliance:*** 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
3) ***Data location*****:** When clients use the cloud, they probably won't know exactly where their data are hosted. Distributed data storage is a usual manner of cloud providers that can cause lack of control
4) ***Data segregation:*** Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure Encryption and decryption is a classic way to cover security issues but heretofore it couldn't ensure to provide perfect solution for it.
5) ***5) Recovery:*** If a cloud provider broke or some problems cause failure in cloud sever what will happen to any data? Can cloud provider restore data completely? Moreover clients prefer don't get permission to third-party companies to control their data. This issue can cause an impasse in security.
6) ***Investigative support*****:** Cloud services are specially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set .
7) ***Long-term viability****:* Ideally, cloud computing provider will never go broke or get acquired by a larger company with maybe new policies. But clients must be sure their data will remain available.

3. Review of Security Issues for Cloud Computing

Review of any security issue for any cloud computing is generally taken to be important not only to elaborate the threats and attacks that are generally effecting our whole system but also to define the current state and the most important current security issue that are to be used for the further implementation and the providing higher flexibility and also reliability to any existing system.

1) ***Forming of any question-*** Under this point we will generally focus on the concept towards the security and the key issues that are most relevant and useful. Generally cloud computing provides various services as software as a service, network as a service , infrastructure as a service and many more.
2) ***Selection of sources-*** The selection criteria through which we evaluated study sources was based on the research experience of the work, and in order to select these sources we have considered certain constraints: studies included in the selected sources must be written in such a way so that these sources must be web-available. The following list of sources has been considered: Science Direct, ACM digital library, IEEE digital library, and DBLP . Later, the experts will refine the results and will include important works that had not been recovered in these sources and will update these work taking into account other constraints such as impact factor, received cites, important journals, renowned authors, . all the sources had been defined, it was necessary to describe the process and the criteria for study selection and evaluation. The inclusion and exclusion criteria of this study were based on the research question. We therefore established that the studies must contain issues and topics which consider security on Cloud Computing, and that these studies must describe threats, vulnerabilities, countermeasures, and risks.
3) ***Execution of any review-*** under this phase we will generally elaborate and define the execution of all the available resources such as hardware, software and the network resources that are generally useful for the execution and calculating and analyzing the further result that are generally desired for it.

4. Conclusion

Cloud computing generally presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offer dare immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users.

In this paper the basic conclusion which comes is that gartner basically provide some security issue which are very useful for the cloud computing. There are various terms as grid computing and cluster computing also but there is a difference between grid computing ,cloud and cluster computing and the difference is that grid computing is generally defined as the collection of various resources as hardware resources, software resources etc. and cluster computing is generally interlinked with the clusters to be associated with it.

References

[1] Farhan Bashir Shaikh, Sajjad Haider " Security Threats in Cloud Computing"-6TH international conference on Internet technology and secured transactions,11-14 december 2011,Abu dhabi

[2] Xiang Tana, **Bo** Aib "The issues of cloud computing security in High speed railway"- 2011 International Conference on Electronic & Mechanical Engineering and Information Technology.

[3] Benedikt Martens, Marc Walterbusch and Frank Teuteberg " Costing of Cloud Computing Services: A Total Cost of Ownership Approach "-2012 45th Hawaii International Conference on System Sciences.