International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 3 (2013), pp. 163-166

http://www. irphouse.com /ijict.htm

Cloud Computing: Security and Privacy Issues

Hemendra Jha[*] and HimaniSingal[#]

** Dronacharya Group Of Institutions, Greater Noida.*
[#] Dronacharya Group of Institutions, Greater Noida.

Abstract

Cloud computing is the most growing technology these days. It has a flexible architecture with the concept of pay-as-you-go. It has proper cost and time management that servers the clients satisfactorily. Being a promising technology, cloud still poses privacy and security as the major challenges. This paper deep dives to discuss the various security issues faced in cloud computing. For an assured cloud we need secure cloud data manager, secure cloud storage manager, secure virtual machine monitor and secure virtual network monitor.Various areas where the security is found at maximum risk are: governance, compliance, trust and malicious insider. Different affected assets are found to be as: company reputation, customer trust, personal sensitive data and service delivery.

Keywords: cloud, cloud computing, privacy, security issue, vulnerabilities in cloud.

1. Introduction:

In this growing era of technology, where different trends fade on almost daily basis, a new concept has evolved that promises more longevity. This concept is known as cloud computing. It has changed the way to use the computer and the internet. Cloud computing has changed the way of running applications and storing data. Cloud computing should not be misinterpreted with network computing. In network computing, all the applications and data are hosted over single company's server and can be accessed over company's network only. Whereas, when we talk about cloud computing, we actually refer to the computer and servers present globally.

2. Architecture:

Through the eyes of developer, cloud computing is visualized as:

Infrastructure as a Service (IaaS): Basic purpose of an operating system is act as an interface between the CPU and its numerous other devices. Here the basic infrastructure of the computers and servers are provided for the development and execution of various applications. It is an on demand facility that ensures that the customer is freed from the tedious task of buying, housing and managing the components of the platform. The client has the control over the application environment settings. The security at this level is also split between the cloud provider and the client.

Platform as a Service (Paas): It is a level above the Iaas. In this the developer can obtain a scalable platform to run their applications. The advantage it offers is that the developer need not to worry about the installation, maintenance and security of the servers. Through this, thedeveloper achieve a better level of scalability, reliability and availability of their applications.

Software as a Service (Saas): It is a great revolution in the field of traditional software. The use of this service helps the developers to reduce the total cost of hardware and software development, its maintenance and operations. At this level, the security is a matter of concern for the cloud provider.

3. Major Security and Privacy Challenges:

However cloud computing is a recently evolved technology, there are several critical loopholes from the security point of view that are being discovered by developers as well as researchers while analyzing and implementing with the current cloud providers. Let us discuss various areas where security is supposed to be at stake:

Governance: Governance refers not only to the control and surveillance of the policies and standards for application development, but also the designing, implementing, testing and monitoring of deployed services. A major advantage of cloud computing is that it helps in the transformation of capital investment to the operational expenses. But if such actions are not governed by the organization or the security and privacy policies are ignored, then organization is put at risk. So while dealing with cloud services it is necessary to pay attention to the roles and responsibilities with respect to risk management. Along with this, it is necessary to acquire auditing mechanism and tools to determine the data security and verify policy enforcements. The acquired risk management system should be flexible enough to deal with changing risk aspects.

Compliance: It involves the conformity with the existing standard, regulation or law. There exists various levels of security and privacy that varies at local, state or national levels, making compliance a complicated issue in cloud computing.

- Data Location: The location where the data is stored is one of the most common compliance issue. When the data is stored within an organization, the people know where the data is stored and how to protect it. But in cloud

computing, where the information about the data location is not shared with the client, it becomes very difficult to determine whether sufficient countermeasures are taken to protect the data or not. In case of trans-border data location, the concern arises for whether the administrative, technical as well as physical safeguards are taken care of or not.

- Electronic discovery: Electronic discovery deals in the identification, processing and analysis of the electronic document in the discovery state. Documents include electronic mail, attachments, date of creation and modification of files and other data stored on a computer. If the cloud providers are not able to preserve these data in the original form, it will affect them legally.

Trust: In cloud computing, the client surrenders complete security aspects to the cloud provider only on the basis of trust.

- Insider Access : Insider access deals in the threats posed to the data not only by the current and ex-employees of the organization, but also the contractors and other third parties that has access to the company's network. Since, under cloud computing paradigm, the data is stored outside the company beyond its firewall and other risk management system, the information is put to risk by both malicious insider as well as the other clients using the same service.
- Composite Services: Cloud has various level of services such as Information as a Service, Platform as a Service and Software as a Service. It may be possible that a cloud service provider offers only one of the above mentioned services and depends on other cloud provider for other services. In this case, the security of the data is not only a matter of concern for the client's cloud provider but also the involved third party. For example, a cloud provider offers Software as a Service. It has to depend on other cloud provider for Infrastructure as a Service and Platform as a Service. Now the security of the data is to be taken care by both of the cloud providers.

4. Countermeasures:

Along with the flaws in cloud from security point of view, there are remedies available to tackle such flaws.

- **Identity and access Management**: The cloud providers should ensure that the information is centrally located and access is given on the basis of the role of the individual and his/her privilege. The cloud provider should not only maintain a log of all the users accessing the data but also keep track of all the unauthorized access attempts.
- **Fragmentation-redundancy-scattering technique**: The cloud providers should be able to tolerate intrusions and provide data security. This techniques involves of first of all breaking the data into insignificant parts such that each sub-part contains no significant data. Now these subparts are scattered in a redundant manner across different datacenters.

- **Homomorphic Encryption**: the major operations performed by the cloud is to store, process and transfer data. Encryption can be applied to the data while it is being transferred in or out of the datacenters. Now the cloud providers need to decrypt the cipher text and then process it. Currently only addition and multiplication is provided as homomorphic operation in a fully homomorphic encryption. Although this operation requires huge processing power that may affect the user response time and power consumption.

5. Conclusion:

Cloud computing is the most flourishing technology of this era. It has many promising advantages. It has enabled its users to cut short their investments and gain more from it. It has helped its clients to grow their business by investing only in what is actually required by them and lowering the time consumption in setting up the business. As every good thing has a darker side, cloud computing also has a major drawback in the form of its security and privacy concern. If these issues are resolved, then it is for sure that more and more customers shall opt for cloud computing for their task to be done. Cloud computing shall prove to be a boon not only for business men but also for the developers and normal internet users.

References:

[1] Hashizume et al. (2013), "Journal of Internet Services and Applications", http://www.jisajournal.com/content/4/1/5

[2] Janakiram, MSV (2012), "Demystifying the Cloud", www.GetCloudReady.com

[3] Jansen, W., Grance, T. (2011), "Guidelines on Security and Privacy in Public Cloud Computing", NIST, Draft Special Publication 800-144

[4] Tripathi, A., Mishra, A., (2011) "Cloud Computing Security Considerations, Signal Processing, Communications and Computing (ICSPCC)",IEEE International Conference.

[5] "UNDERSTANDING the Cloud Computing Stack SaaS, Paas, IaaS, © Diversity Limited", (2011) Non-commercial reuse with attribution permitted.

[6] Smith, L., "A health care community cloud takes shape" http://searchcio.techtarget.com/news/2240026119/a-health-care- community-cloud-takes-shape