Inspira- Journal of Modern Management & Entrepreneurship (JMME)
ISSN : 2231–167X, General Impact Factor : 2.5442, Volume 08, No. 02, April, 2018, pp. 111-114

SECURITY ISSUES AND CHALLENGES IN CLOUD COMPUTING: A CONCEPTUAL STUDY

Dr. Mahima Gupta *

ABSTRACT

Cloud Computing is an architecture which provides different computing services like storage, servers, services, applications etc. without physically acquiring them through internet. Today's most prior IT agenda is to have digitalization, operational efficiency in all business processes with reduction of complexity and difficulties at different stages. So organizations are going to transform and modernize their current IT structure to meet the requirements of competitive market. This presents challenges towards digitalization, operational efficiency and delivering a hybrid IT world of cloud computing alongside on-premises IT. So many areas like education, banking, business, healthcare etc. are moving towards the cloud architecture due to the efficiency provided by some providers like Google, Amazon, Microsoft etc. Sometimes the services on cloud architecture could be free or pay as per use pattern. Cloud Computing is completely an internet based service; therefore, the data is stored on Internet Cloud the user will have limited or no control over the data, which may create several security issues. Since the data control is at data centre which could create some challenges like leakage of data, insecure interface, resource sharing, data availability and inside attacks etc. This research paper answers, what is cloud computing, what are the different models of cloud computing and the main issues that are currently present within the cloud computing architecture. This research paper also analyzes the issues and challenges regarding security that are dealing by cloud computing users and providers and offers best practices to users as well as service providers hoping to supply best cloud services to improve their upshot in this competitive market.

KEYWORDS: *Cloud Computing, Cloud Based Architecture, Security Issues, Challenges*.

Introduction

The evolution of the Internet attached with the development of extraordinarily scalable IT infrastructure is updating the storage and distribution of information and communication technologies. These technologies include development tools, software and applications, network services, etc., which organizations, in the past, would have licensed or purchased, and installed, maintained and managed all by themselves at ridiculous costs. These technologies are now being grouped and repackaged into a well-defined outsourcing service model and presented on "pay as you use" basis, this is simply defined Cloud Computing. It is not a new concept nor any new technology nor any new computing archetype nor a new experience. Cloud computing includes various technological practices that were present long before the phrase became popular. Therefore, many of us have already been using cloud computing in some way or the other. For example, free personal email, we can access it at completely no cost from a third party server that might be hosted wherever in the world without us having any knowledge of where those servers are located. In other words, Cloud Computing is a computing model, with a large collection of systems that are connected in private or public networks, to provide extremely scalable infrastructure for application, data and file storage. With the initiation of this technology, the cost of computation, cost of hosting applications, storage and delivery of system content is reduced significantly. A public cloud network presents cloud computing services to almost anyone who can access to the internet, generally at no or very low cost. On another hand, a private cloud network is usually a private data center that

* Assistant Professor, Department of ABST, S. D. Govt. College, Beawar, Rajasthan, India.

presents cloud computing services to a limited number of registered or recognized users at a certain or shared cost. Cloud Computing is established through the Cloud Computing Stack. The Cloud Computing Stack arranges the hardware/software of a data center into various service layers. Finally, Cloud computing is a practical approach to make over a data center from a capital- concentrated set up to a fluctuating priced environment. Based on this understanding of the term 'cloud computing', there are three major elements or delivery models for cloud computing:

Infrastructure as a Service (IaaS)

Under the IaaS model, instead of purchasing large and costly infrastructure such as data center, virtual servers, network infrastructure, equipment, etc, users, generally large organizations, source the same as a service from third party service providers. The payment mechanism under this model is 'pay as you use'. The hardware cloud infrastructure allows users to expand as well as contract their require-ments based on their business needs. Example: Amazon Web Services, EC2, Gogrid.

Software as a Service (SaaS)

A software cloud is specialized software that runs on the hardware cloud. Under this model the service provider hosts several software applications for users to use the software as and when required thereby eliminating the need to install and run the software application on the user's computer and also simplify maintenance and support expenses. This service is in the form of web services and is made available to users over a network which is normally through the web/Internet. Because the service provider hosts both the application and the data, the user is free to use the service from anywhere. Example: GoogleDocs, Salesforce.

Platform as a Service (PaaS)

With PaaS, software developers can avail the platform services to develop various applications without installing and maintaining any tools on their computer. PaaS tools are hosted on service provider's IaaS. Once developed, these applications can be then be tested and deployed without much trouble and effort. Example: Facebook, Google Apps. With the help of cloud computing models, the action moves to the interface between service suppliers and multiple groups of service consumers. This architecture of cloud computing aligns so many benefits to users such as reduced cost, flexibility, increase storage, scalability, automation, resource sharing, focused approach etc. But after these pro parts of the coin, there are some cons behind this. Security issues and lots of challenges hinder the growth of this empowered technique.

Security Issues and Challenges

The three cloud services described above attract some highly considerable rates of threats. This incorporates revision of data with no appropriate backup, leading to breaches of data or unauthorized and illegal access to sensitive data. In case of appropriate backup of data being taken, it is pregnable if it is not encrypted properly. Due to the associated disadvantage of virtualization and unsecured access to resources over the cloud, both are leading to unauthorized handling of service, platform or even an infrastructure of the provider or other users. Some of the risks, challenges or issues have discussed below which may be faced in cloud computing environment.

Data Protection

Security of data is a critical element that permits scrutiny. Enterprises are cautious to buy an assurance of business data security from vendors. They have fear of losing data in this cut-throat competition and the data privacy of consumers. In many occurrences, the real storage location is not revealed, adding onto the security apprehension of enterprises. In the existing cloud models, firewalls across data centers (owned by enterprises) save this hypersensitive information. In the cloud model, the providers are accountable for sustaining the security of data and enterprises would have to keep faith on them.

Hijacking of Accounts

Attackers now have the skill to use your login information to distantly access critical data stored on the cloud. Some other methods of hijacking of accounts, involve scripting bugs and reuse of passwords, which permit attackers to easily steal credentials without detection. In the month of April 2010, Amazon handled a cross-site scripting bug that aims for even the credentials of customers.

Interception of Data

Certain countries have laws relating to interception of data. Further, at some stage in the pendency of a law suit or during a government probe, an organization may be required to allow the investigating agency to access organization data. As data resides across the clouds, it is difficult for

investigating agencies to have easy access to data. On the security front, encryption levels may differ from country to country. For example Indian law allows only 40 bit data for interception but on another side, some countries allow upto the limit of 256.

Loss of Control

Organizations can store their data on a private or a public cloud depending on the availability or economic viability of storing such data. However, the risks in relation to ownership or control while storing data on a public cloud are much higher as a public cloud operates on a non-exclusive basis. When data and applications are transferred onto the cloud, some organizations fear that such transfer may equivalent to loss of ownership or control of their data or application. It must be noted that such data and applications are the organization's property and an organization via its contractual arrangements must ensure that complete ownership and control over the same is retained.

Unknown Location of Data Storage

Generally, a customer could decide on the control and location of the data, including the location where the backup could be stored. Existing cloud computing solutions require data and applications to be stored in the cloud whose location is usually unknown and most likely organizations end up dealing with multiple clouds. This fragmentation may adversely affect the organization as the data transfer/ privacy laws of one jurisdiction may be more onerous than the other jurisdiction. This freedom could also result in the non-compliance of worldwide laws pertaining to storage and transfer of data. Also, it needs to be evaluated as to who can be held responsible and accountable in cases of data disaster where an organization's data is completely lost/destroyed.

Portability of Cloud

Many organizations may not be willing to move their private and proprietary data over the public cloud as this paradigm shift may not yet be culturally acceptable to the organizations. Cloud computing is not practicable for users having low/weak or poor internet connectivity. Still on a fast Internet connection, sometimes, web based applications can be slower than accessing a comparable software program on our desktop PC/laptop/notepad.

Incomplete Data Deletion

Incomplete data deletion is treated as hazardous one in cloud computing. When data is deleted, it does not remove the replicated data placed on a dedicated backup server. The operating system of that server will not delete data unless it is specifically commanded by network service provider. Precise data deletion is mainly not possible because copies of data are saved in duplication but also not available for usage.

Regular Backup of Data

The cloud vendor must ensure that regular backup of data is implemented that even ensure security with all measures. But this backup of data is usually found in unencrypted form leading to mistreatment of the data by unauthorized parties. In this way, backups of data also lead to variety of security menaces. As more the server virtualization adds, a very complicated problem with backup and storage is generated. Data de-duplication is listed as one of the answer to reduce backup and offline storage volumes. But it can be carried out with the mishandling of data backup.

Normalization

Many organizations may have their own procedures, standard templates, policies and guidelines which they may want to follow even when dealing in a cloud computing environment. Further, these organizations may also want the vendors to follow these procedures, standard templates, policies etc. which they normally use. Certain vendors may be unwilling to accommodate and this may result in a conflicting situation for both the parties and thereby may create a deadlock.

Technological Issue

IaaS vendors transport their services in a measurable way by contributing infrastructure. But this arrangement does not recommend strong isolation properties for a multi-tenant architecture. Hence in order to address this gap, a virtualization hypervisor intercede the access between guest operating systems and the physical compute resources.

Hijacking of Service

This is considered as one of the top most challenge in cloud computing. Hijacking of Service is associated with gaining an illegitimate control on specific authorized services by various unauthorized users. It accounts for a variety of techniques like phishing, manipulation of software and fraud.

Data Residuals

In cloud computing, for the best utilization of resources, data frequently is moved to cloud infrastructure. Consequently, the enterprise would be devoid of the location where data is put on the cloud. This is generally happen with public cloud. With this data movement, the residuals of data is left behind which may be accessed by unauthorized users. This again may create the problem of data security threats like leakage of data, data remnants and also inconsistent data.

Multi-user Environment

Multi-user Environment is one of the very vital attribute of cloud computing, which permits multiple users to run their distinct applications concurrently on the same physical infrastructure hiding user data from each other. But the shared multi-user character of public cloud combines security risks for example unauthorized access of data by other renter using the same hardware. A multi-user situation may also give a picture of some resource disputation issues when any user utilizes some lopsided amount of resources. This might be either because of sincere periodic requirements or any hack attack.

Conclusion

Cloud Computing can be perceived as a new phenomenon which is set to transform the way we use the internet, there is much to be cautious about. There are many new technologies developing at a faster rate, each with technological innovations and with the possibility of making human lives easier. But, we must be very careful to understand the security risks and challenges posed in utilizing these technologies has many advantages, but it also has different security concerns that could be raised. When data is being stored in big data centers all around the world, the data could eventually become a target for attacks or it could be altered by the employees of cloud service provider. Cloud computing has made end users both thrilled and nervous. They are excited by various opportunities provided by the cloud and are worried as well on the questions related to the security it offers. As users shift their data on cloud they would be worried with the security faults innate to the cloud environment. Thus security challenges with cloud computing has came into the view as one of the very sensible topics. This study has analyzed almost every security threat found across both the cloud models and the network and has also revealed solutions to some of them.

References

- Bashir B. & Khalique A. (2016). A Review on Security Versus Ethics. International Journal of Computer Applications. 151(11). 244-249.
- Bazaz T. & Khalique A. (2017). A Review on Single Sign On Enabling Technologies and Protocols. International Journal of Computer Applications. 149-157.
- Fayaz H. & Khalique A. (2016). A Review on Sociological Impacts of Social Networking. International Journal of Engineering, Applied Sciences and Technology. 6-12.
- Haghighat, M., Zonouz, S., & Abdel-Mottaleb, M. (2015). CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. Expert Systems with Applications. 42(21). 7905–7916.
- Jamil, D., Zaki, H. (2013). Security issues in cloud computing and counter measures. International Journal of Engineering Science and Technology (IJEST). 3(4). 2672-2676.
- Jensen M., Schwenk J., Gruschka N. & Iacono L. (2009). On Technical Security Issues in Cloud Computing. IEEE International Journal of Cloud Computing. 109-116.
- Kandukuri, B.R. , Paturi, V.R., Rakshit, A. (2009). Cloud security issues. IEEE International Journal on Services Computing. 517–520.
- Mell P. & Grance T. (2011). The NIST Definition of Cloud Computing. Computer Security Division IT Laboratory, National Institute of Standards and Technology.
- Srinavasin M. K., Sarukesi K., Rodrigues P., Manoj M. S. & Revathy P. (2010). State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment. Proceedings of the International Conference on Advances in Computing, Communications and Informatics.

♦❐♦