Volume 8, No. 2, March 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

A Survey on Cloud Computing Security Issues and its Possible Solutions

Gazala Matloob
Department of CSE, SEST
JamiaHamdard, New Delhi, India
matloobgazala@gmail.com

Abstract: The rapid increase in the popularity of cloud computing is due to its feature of sharing resources, data storage management, flexibility and scalability. Many business organizations work on cloud and some of them have their own cloud. On one hand we acquired number of benefits from cloud computing but on the other it also increases the concern of security because of the large number of valuable data is stored over the cloud and it could be accessed by anyone (unauthorized user). In this paper I tried to discuss the detailed study of the security issues of cloud computing along with it's possible security solutions.

Keywords: Cloud Computing, Cloud Services, Cloud Deployment models, Cloud Security.

I. INTRODUCTION

"Cloud Computing" is defined as the internet based computing that allows us to share resources, store and process data over the network. Due to the ability to share and store large amount of data over the network it is become critical to secure the data over the cloud. The data can be of any type ranging from business confidential information to bank details etc. information are all store on the cloud. The major security challenge with clouds is that the owner of the data may not have control of the location of data because if one wants to exploit the benefits of using cloud computing, he must also utilize the resource allocation and scheduling provided by the clouds [1]. Cloud has become main source for the hackers to attack the information system and causes the leakage of information due to the internal or the external attackers. In recent past many hacking attempts happened on private and public classified web based storage system some of these examples are as follows:

- As per McAfee, August 2012 report over few years over 72 company's data bases are hacked across 14 nations globally
- Germany losses 50 billion Euros annually due to electronic attacks on its databases
- In 2012 due to cyber-attack on Amazon Web Services customers were not able to access Netflix for around 12 hours.
- Globally one new malware is developed every 2 seconds.
- European government bodies report 4-5 hacking attempts on their system each day.

Cloud handling large amount of different mobile devices and though having massive amount of data stored on the cloud. From here the concept of Big data arises which is very popular now a days. Increase in the data on web day by day even at every second needed to be handled and should be secure from unauthorized access. Many IT companies like Amazon, MacAfee, and IBM etc. are working on the cloud data security. Some of the works are briefly discussed below:

- IBM Dynamic Cloud Security spansIaaS, SaaS and PaaS. It is designed to work together with organizations' existing security processes to create an integrated system that includes regular IT infrastructure as well as private, public and hybrid cloud setups.
- McAfee's approach is to enable organizations to develop their own security protocols, which are then applied to the cloud environment. This is achieved by securing the data that is moving between the organization and the cloud, as well as ensuring that data is securely stored in the cloud. [5]
- VMware is one of the oldest companies providing the cloud services to the organizations It provides simplified security policies that can be implemented and monitored for IT compliance without compromising the level of control and visibility. [1]

So before going into the detail discussion of cloud security issues along with it's possible solutions we will throw some light on the "services provided by the cloud" and the "types of cloud".

II. CLOUD SERVICES

Cloud computing enables the ubiquitous, convenient, on demand access to the resources environment with minimum management or service provider interaction. The cloud is composed of three service models[2][3].

Infrastructure as a Service (IaaS): It is a type of service model which provide the infrastructure to the user. It provides hardware, software, servers and storages etc. Iaas also host user applications and handle task including maintenance, backup and resiliency planning. It offers highly scalable resources that can be adjusted on demand. One of the best features of Iaas is that you have to pay according to the usage typically by hours, weeks or months. This pay-as-you-go model eliminates the expenses on the hardware and software at the user premises. IaaS providers include Amazon Web Services (AWS), Windows Azure, Google Compute Engine, Rackspace Open Cloud, and IBM Smart Cloud Enterprise[2][3].

Platform as a Service (PaaS): In this type of cloud service model provides a platform to the customer where he can run, develop and manage the applications without the complexity of building their own infrastructure. The Paas service provides the resources to the customer for the deployment of software applications according to the requirement of customer. It is useful for the project when multiple developers are working on the same platform.Amazon EC2, Windows Azure and Google Compute Engine etc., are some of example which provide the computing platform .[2]

Software as a Service (SaaS): As the name suggests it provide the software to the customer and also known as "on- demand software". One can access the software via web browser. Microsoft office, Adobe reader are some of the example of accessing the software over the cloud. Even one of famous software used in the business for the sales i.e. sales force and one of the popular Goggle app are also the SaaS examples[2][3].

III. Cloud Deployment Model

A cloud deployment model represents a specific type of cloud environment, primarily distinguished by ownership, size, and access. There are mainly following three types of the model private, public and hybrid among which the **private model** is the one for a single organization, whether managed internally or by the third party or externally.it is private to a particular business organization and can be accessed within a particular area. The benefit of this model is that high security and privacy, improved reliability and more control etc**.** In **Public model** the service is open for public use. It is for public network and access by unauthorized person so security is the main concern here. Public service providers are Amazon Web Service, Goggle and Microsoft etc. The **Hybrid model** is the combination of both public and private. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. Hybrid cloud adoption depends on a number of factors such as data security and compliance requirements, level of control needed over data, and the applications an organization uses [2].

IV.Cloud Security Challenges

Cloud model based on distributed system i.e. information is distributed over the network and the access by many unambiguous persons so to secure the information from being lost or damage is the major challenge today. The leakage or the loss of data i.e. organization internal confidential information being disclosed to the one external to the organization causes serious damage to the business organization. Below given is the figure which shows the different factors and their level of impact on security challenges[4].

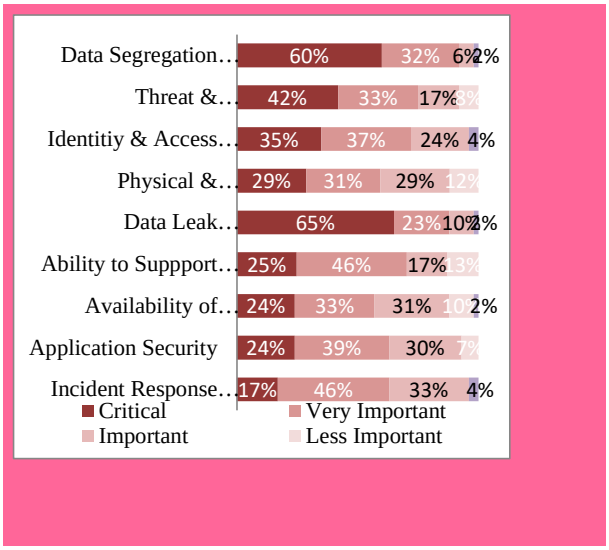

Figure: Data Security Challenges in Cloud Computing [4]

Some of the security challenges are discussed below:

- **Authentication:** There are number of unambiguous person who can access the information and it is not known who is authorized to information. Authentication of unauthorized person. Henceforth the certified user and assistance cloud must have interchangeability administration entity.
- **Integrity:** there should be security levels so that the information should only be modified by the authorized person. Hackers can eavesdrop the confidential information and can manipulate it. Man in the middle attack is a type of attack where the attacker sites between the two devices communicating and manipulate the data.
- **Access Control:** Access control refers to the .defining the level of access to the confidential information of an organization. In an organization, the employees will be given access

to the section of data based on their company security policies. The same data cannot be accessed by the other employee working in the same organization.

- **Confidentiality:** Data confidentiality is one of the important requirements. To maintain confidentiality of data and understanding its classification, users should be aware of which data is stored in cloud and its accessibility.
- **Availability:** Availability here it concerns with the data available to the person to whom it is concern[4][6]. So these are some of important challenges of security which has to be meet so that should not be leaked to the external or their will be minimum damage to the information

V.SECURITY SOLUTIONS

Encryption means coding the information into some coded form and then changing it to the original form. By encrypting the stored data avoid unknown person to know the original content of it. This is one of the best and most popular solutions. By applying the encryption algorithm like RSA, AES etc. we can secure the information at some level.

Password /Identity Management is the another method of securing confidential information. By log in id method one can access the information only if the password is known.

Biometric method is considered to be better than the traditional password method. Hackers can easily crack the password but it is difficult for the biometric recognition. Fingerprint identification, face and iris etc. are some of the popular biometric method of identification. [4]

VI. CONCLUSION

Cloud computing has given us enormous advantage of storing and accessing data with any physical storage at the work site. it also helps organization in cutting cost of storage infrastructure and it is believe to be future of data storage and management. So the security of data in cloud is of critical importance to us which can be achieved by filtering out the least frequently used data and applying encryption or password to the frequently used one. Another way can be of applying the biometric mechanism of authentication which considered being more secured than the traditional authentication approaches.

REFERENCES

1. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisinghan, “Security Issues for cloud computing”, University of Texas.
2. Manpreet Kaur, Hardeep Singh “A Review of Cloud Computing Security Issues”.
3. http://hubpages.com/technology/Cloud-Computing-Overview
4. The white book of cloud Security
5. White paper in cloud security by T systems
6. Farheen Siddiqui "State Of Art Ontological Infrastructure For Cloud Computing” International Journal of Computer & Organization Trends (IJCOT) – Volume 36 Number1 – October 2016 ISSN: 2249-2593 Pg22-26

SEMINAR PAPER
National Seminar on Cloud Computing and its Applications (March 9-10, 2017)
Organized by
Dept of Comp. Sci. & Eng, SEST, Jamia Hamdard, New Delhi (India)