International Journal of Advances in Engineering Research http://www.ijaer.com

(IJAER) 2014, Vol. No. 8, Issue No. VI, December **ISSN: 2231-5152**

CLOUD COMPUTING SECURITY CONCERNS

ASMA GULAM MOHAMED

Saveetha School of Engineering

ABSTRACT

Cloud computing is set of resources including data storage, programs and hardware offered through the Internet. Cloud computing services are delivered from data centres located in different physical places unknown to the users of these services. The actual physical location is unknown to us. Cloud computing services are developing at a very fast rate as organisations now require less computer resources for the same tasks they would have needed before. Even though cloud computing usage is increasing, there is still a lot of doubt for users relating to the security of data stored in the cloud. Cloud computing is a very financially viable option when thought of for large organisations but when we start to analyse existing statistics, it is obvious that cloud computing has one very big flaw - its lack of security. In order to give a better idea of the present situation in terms of security, in this article we review the main security concerns in cloud computing.

Keywords: Cloud computing, security, virtual, data, data privacy

INTRODUCTION

Cloud computing basically consists of a number of inter-connected computing nodes, and other hardware and/or software services that are dynamically shared between a number of users. Cloud computing services can be used from the internet, or through private networks. The main goal of cloud computing is to offer users seemingly unlimited computing and storage facilities, while reducing cost and complexity for the users.

Based on the type of service provided, cloud services can be classified into three broad categories-Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS).

Infrastructure as a Service ,as its name suggests, deals with providing infrastructure like computing facility, storage or any other hardware resource.

A common example of IaaS is Amazon, which is one of the cloud providers.

Platform as a service ,as its name suggests, provides platforms like operating system and other system software that the user can use to build customised applications.

Microsoft Azure is an example of PaaS.

Software as a Service ,as its name suggests provides software for usage by users. It deals with provision and usage of applications or service through cloud.

Google Apps is an example of SaaS. It allows collaboration on applications like event management via the internet.

However ,as with almost any computing service, there are many problems caused by the implementation of cloud computing. One of the main issues associated with cloud computing is the lack of security for data stored on the cloud. In this paper, we review the existing security concerns with respect to cloud computing.

CLOUD SERVICE DEPLOYMENT MODELS:

Irrespective of the service provided, there are four main deployment models for cloud services.

They are public cloud, private cloud, community cloud and hybrid cloud.

Public cloud: As the name public suggests, this cloud infrastructure is available to the general public or a large group of users and is owned by an organization selling cloud services.

Private Cloud: As the name private suggests, this cloud infrastructure is for a single organization only. It can be controlled by the organization itself or an external group of people. It can exist on
premises or off premises, depending on the requirement of the organisation.

Community Cloud: As the name community suggests, this cloud infrastructure is shared by a number of organizations and is used by a particular community that has common concerns policy.
It can also be managed by the organizations itself or an external organisation. Similar to private cloud, it may also be present on-premises or off-premises.

Hybrid Cloud: As the name suggests , this cloud infrastructure is a by-product of two or more cloud deployment models (private, community, or public) that remain separate entities but are bound together by standardized technology that allows data exchange.

FEATURES OF CLOUD COMPUTING

Cloud computing started in 2008 and is seen a rapid growth since then. It has various features that make it attractive to a wide range of users. Some of the features are:

1. Elasticity :

The cloud resources can be scaled up or scaled down the resources assigned to services based on the user's requirement. So, for cloud service providers , this means that once resources used by a particular user have been reduced, another user will be able to use these resources.

2. Device and Location Independent:

As cloud services are accessed through the internet, they can be used from any location and any internet supporting device. This is beneficial because now users are not location bound and do not need to use only a particular system for their applications.

3. Lower cost:

As compared to conventional systems available in the market, cloud computing services provide a more financially viable option because of a great reduction in cost for the usage of these services. For start-ups and companies looking to reduce expenditure, cost required for infrastructure is reduced by moving to the cloud because computing power, storage and other resources that they require are used from cloud so the cost to purchase them is much lower.

4.Multi-tenancy:

Multi-tenancy is a feature of cloud computing that allows efficient utilisation of resources while reducing cost for cloud service providers. As the name suggests, it allows for multiple users to simultaneously use particular resources like a data server.

SECURITY IN THE CLOUD

Since cloud services use networks for their deployment, they are vulnerable to network type attacks.

Two major attack types are Distributed denial of Service (DDOS) and Man in the middle attack.

DDOS:

If a hacker is able to hijack a server ,then the hacker could stop the cloud services from working and demand a ransom to put the services back online. One way to stop these attacks is to limit the number of users connected to a server.

Man in the Middle attack:

If the secure sockets layer (SSL) is incorrectly configured then the client authentication will not occur as it is supposed to which will lead to man in the middle attacks.

Cloud security issues can be classified as service provider security issues and end user security issues.

1 Service provider security issues

Privacy

Privacy is a major concern for organisations and individuals while adopting and using cloud resources. One of the main contributors to this concern is the lack of governance. Data privacy laws vary from country to country. Cloud users may be situated in one country while the cloud resources they are using may be in another country. In such a case, the privacy laws applicable will be those of the country the cloud resources (hardware etc) are situated in.

Lack of transparency

Cloud service providers usually do not disclose information about where and how the data is stored. The users of cloud services are generally unaware of the details about the storage of their information which leads to concerns about the security of their information. In conventional storage methods, this is never a problem since the data is stored in systems that the user owns and has full control over.

User identity

In organisations, in conventional storage systems where the cloud is not used, only authorised users can access certain data which is considered to be important. However, when an organisation uses the cloud, this is more difficult to implement.

2 End user security issues

Browser security

In cloud computing services, remote servers are where the actual processing of data is done while the clients systems are used only for input and output operations, as well as for granting permission for the usage of the cloud by the authentication process. So, it is not useful to develop platform dependent software. Rather than that platform independent software should be developed like a standard web browser. Lack of security due to unsecure browser is thus an end user security issue.

Authentication

In cloud computing services, a user can use these services only after the authentication process to verify whether or not the user is a verified user. So, authentication is especially important because in such cases, the information on the cloud will be accessible to everyone in case authentication is not performed properly. This exposes paying users to data theft.

Usernames and passwords do not guarantee enough protection so, Trusted Platform Module (TPM) is used increasingly nowadays.

Lock-in

Lock-in basically means lack of portability. It is the inability of a user to migrate from one cloud service provider to another cloud service provider in case the need arises.

Bottleneck

Data transfer Bottleneck occurs when the internet available is not of suitable speed to support the amount of data being retrieved from the cloud , stored into the cloud or processed from the cloud. This also causes a disruption in the cloud services available to the user.

CONCLUSION

Cloud computing has seen a high growth rate since its creation in 2008 and will continue to grow over the years. In order to ensure that cloud computing sees widespread usage, the security concerns associated with data storage and usage of the cloud need to be addressed urgently. Issues like information security, lack of governance and transparency, data protection all require extensive research. User security is of utmost importance in order to make cloud computing an attractive and viable option for users as compared to conventional systems available. This paper has reviewed only some of the security challenges associated with cloud computing.

REFERENCES

[1]Rizwana shaikh,M.Sasikumar "Security issues in cloud computing: A survey", International journal of computer applications, april 2012

[2]Akhil Behl,Kanika Behl "An analysis of cloud computing security issues",IEEE,2012

[3] Jensen, M. Schwenk, J. Gruschka, N. Iacono, “On technical security issues in Cloud” IEEE International Conference on Cloud Computing, 2009, Germany