International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

General Article

Security Concerns and Privacy Issues in Cloud Computing

Pulkit Chaudhary[A*]

[A]Software Engineer, Snap Step Services & Solutions Pvt Ltd, Bangalore

Accepted 05 Nov 2014, Available online 01 Dec 2014, **Vol.4, No.6 (Dec 2014)**

Abstract

Today cloud computing is the most trending and advanced technology with high future implementation in the information and technology industries. Nowadays many cloud storages or online storages are provided by a number of companies to their customers as well as to the employees. In current scenario computing infrastructure is rapidly moving towards the cloud based architecture in which the users are enabled to move their data and application software to the network and access the services on-demand. It is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet (Keiko Hashizume et al, 2013). It is an evolutionary advancement which covers elements from grid computing, utility computing and autonomic computing, into inventive deployment architecture. Cloud computing enthralls the focus of the IT industries, Government Organization and Healthcare Sector. This transition to Cloud computing has fueled concerns on a critical security issue for the success of information systems, communication and information security. A number of risks have been associated with the security of cloud computing. One major issue is the security of data stored on the provider's cloud and privacy at the time of data transmission. This paper is focused on the basic essential details and major security issues of the cloud computing.

Keywords: *Cloud Security, Encryption, cloud services, Cloud computing, Cloud security issues.*

1. Introduction

Cloud computing is basically a computing via internet in which large groups of remote servers are interconnected or networked to allow the centralized data storage, and online access to computer services or resources. A study by Gartner considered cloud computing as the first among the top ten most important technologies and with a better prospect in successive years by companies and organizations. It is a model for convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts (*Vijay.G.R et al, 2013*).

The architecture of the cloud computing involves multiple cloud components interacting with each other about the various data they are holding on too, thus helping the user to get to the required data on a faster rate(*Anitha Y et al, 2013*).

Presently it can be viewed as one of the biggest advancement in technology that took place in recent times and a new way of delivering computing services and resources. Cloud computing can be defined as the practice of networked remote servers hosted on the internet to store, process, and manage data rather than a local server. It helps to access and share files and applications over the internet on demand.

Fig 1- shows the main characteristics and benefits of cloud computing.

- Performance
- On demand self service
- Low cost
- Device independent
- Virtualization
- Maintenances
- Agility
- Application programming interface
- Location independence
- Scalability
- Multi tenancy

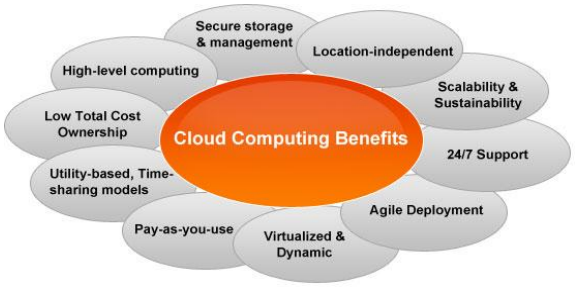

Fig. 1 Characteristics and features of cloud computing

2. Types of Clouds

There are three types of clouds namely public, private and hybrid as shown in figure 2.

2.1 Public cloud

It is also known as external cloud, in this cloud, services and infrastructure are provided off site over the internet

*Corresponding author: **Pulkit Chaudhary**

and it also has the greatest level of efficiency in terms of shared resources compared to other clouds.

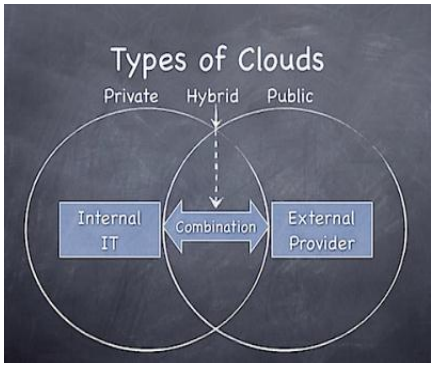

Fig. 2 Types of clouds and their roles

2.2 Private cloud

We can use it only for the single and private use (private network), and consist of private applications and services for private network only. In this cloud, services and infrastructure are maintained on a private network. Private cloud offers the greatest security and control.

2.3 Hybrid cloud

It is an integrated cloud service developed by mixing the features of both the private and public clouds to perform distinctive functions within the same organization. It provide more secure control of the data and applications and allows various parties to access information over the Internet (*Vijay.G.R et al, 2013*).

3. Types of Cloud services

The cloud service providers provide three different services based on different capabilities such as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service) (*Anitha Y et al, 2013*) as shown in fig-3

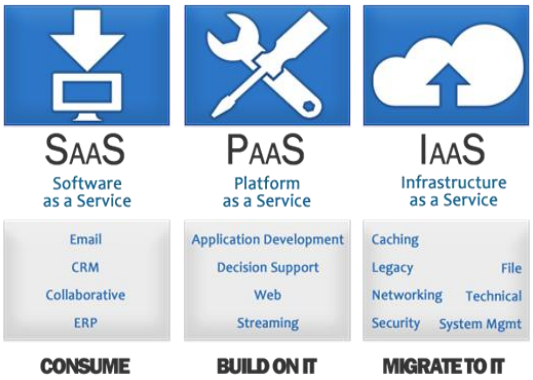

Fig. 3 Types of cloud services

3.1 PaaS (Platform as a service)

Platform as a service provides a cloud-based environment with everything required to support the complete life cycle of building and delivering web-based (cloud) applications without the cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting. Examples of PaaS providers include Amazon DB/S3 (*S.Sakr et al, 2011*), Microsoft Azure, and Google App Engine.

3.2 IaaS (Infrastructure as a service)

Infrastructure as a service provides companies with computing resources including servers, networking, storage, and data center space on a pay-per-use basis. Examples of IaaS providers include Amazon EC2, Go Grid, and Flexi Scale (*Agarwal.A et al, 2013*).

3.3 SaaS (Software as a service)

Cloud-based applications or software as a service (SaaS) run on distant computers (in the cloud). It is owned and operated by others. It connects to users computers via the Internet usually, a web browser. Examples of SaaS providers include google applications, Salesforce.com, YouTube, and Facebook.

4. Security Issues in Cloud computing

Time, cost, innovation are great benefits of cloud computing but still there are significant security concerns of cloud computing that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. Major security issues in cloud computing (*Agarwal.A et al, 2013*) are:

4.1 Privileged user access

Any data processing done outside the enterprise boundaries bring along a high level of security risk, because the outsourced services bypass the "physical, logical and personnel controls". So in order to be secure and confident you must get as much information as you can about the people and authority who manages your data.

4.2 Regulatory compliance

It's the full responsibility of the customer to maintain and focus on the security and privacy of their data, even when a service provider held it. Service providers are subjected to external audits and security certifications which makes them the model of fidelity. So the cloud computing providers who refuse to undergo such audits and security certifications can be a major security risk and privacy concern.

4.3 Data location

When a customer or user operates, functions and store data on the cloud, one cannot tell where the data is actually being hosted that means that the user does not even know or have any idea about the location and details of the cloud that is hosting the data. Ask providers if they will commit to storing and processing data in specific jurisdictions, and

whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

4.4 Data segregation

In the cloud storage the data is in a shared environment alongside data from other customers. At this point Encryption plays a major role but it is not a full cure to this problem because sometimes encryption accidents can make the data unusable .The cloud provider should provide evidence that encryption schemes and algorithms were designed and tested by experienced specialists for the proper safety of the stored data.

4.5 Recovery

In case, data on a cloud is corrupted or a situation occurs known as disaster then in this situation how can the data be restored or replicated and how much time will it consume to restore the data fully . Make sure to check that data restoration facility is provided by the cloud provider and is without complexity.

4.6 Investigative support

Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because location of data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible.

4.7 Long-term viability

Suppose a cloud service provider lost its authority and is acquired by another company then the main question arises is that – "will the data remain available after such activity or event".

Conclusion and future work

This paper explains basic essential details and different security issues of cloud computing. It is used in both smaller and larger scale organizations having some tremendous advantages for sure but it has many security issues and threats. This paper shows lack of security is the only worth mentioning disadvantage of cloud computing. The bond required between service providers and users is essential to improve cloud security and confidentiality. In future I will discuss the methodology to implement the bond between service providers and users.

References

Keiko Hashizume, David G Rosado, Eduardo Fernandez-Medina and Eduardo B Fernandez (2013), An analysis of security issues for cloud computing, *Journal of Internet Services and Applications (JISA) a springer open journal*, vol 4, pp. 1-13.

Vijay.G.R, Dr. A.Rama, Mohan Reddy (2013), Security Issue Analysis in Cloud Computing Environment, *International Journal of Engineering Research and Applications (IJERA)*, Vol. 3, Issue 1, pp. 854-857.

Anitha Y (2013), Security Issues in Cloud Computing - A Review, *International Journal of Thesis Projects and Dissertations (IJTPD)*, Vol. 1, Issue 1, pp. 1-6.

S. Sakr, A. Liu, D. M. Batista, and M. Alomari (2011), A Survey of Large Scale Data Management Approaches in Cloud Environments, *IEEE Communications Surveys & Tutorials*, vol. 13, no. 3, pp. 311-336.

Agarwal, A. and Agarwal, A. (2011), The Security Risks Associated with Cloud Computing, *International Journal of Computer Applications in Engineering Sciences*, vol 1 (Special Issue on CNS), pp. 257-259.