ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Survey on Cloud Computing and Security Issues

Rajeswari[1], Vinitha R[2], Greeshma N[3]

Sr. Asst. Professor, Dept. of ISE, New Horizon College of Engineering, Bangalore, Karnataka, India[1]

B.E Students, Dept. of ISE, New Horizon College of Engineering, Bangalore, Karnataka, India[2,3]

ABSTRACT:Cloud Computing can be defined as virtual pooled servers that provide infrastructure, application, platform based application and other facilities. It is becoming most popular and smart technology day-by-day. At the same time security of data stored in cloud is a major challenge which has to be solved immediately for cloud storage technology. Data security is defined as integrity, confidentiality, privacy and reliability of data maintained by an organization. Security concerns association with Cloud Computing is broadly classified into two categories: Security issues faced by Cloud providers and Security issues faced by their customers. This paper deals with the services provided by cloud, risk associated with it and security measures in Cloud Computing.

KEYWORDS:Cloud Computing, Deployment Models, Service Models, Security Risks, Security Measures.

I. INTRODUCTION

Cloud Computing is one of the major development in computer history [3]. Cloud Computing can be defined as the process of storing, maintaining and processing data over a network of remote servers that are hosted over the Internet. The Cloud Computing model consists of five characteristics, there delivery models, and four deployment models [11]. It defined five essential characteristics of Cloud Computing as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [10]. Cloud Computing provides the resources as per the needs of the customers. The major of this Computing technology is that the clients uses only what they need and pay according to their usage [6]. There are a number of traditional storage devices such as hard disk, but nowadays we use the various service that are available and provided by the Internet. Such recent type of storage device is Cloud. However, the Cloud Service Providers are facing a serious problem with security of the data stored on the Cloud which has to be solved quickly. By using Cloud Computing technology, we can easily and quickly access, store and manipulate our data on the Cloud.

In this paper we are discussing various type of Models for Cloud deployment, types of Cloud service models offered to the end users. The Cloud which are accessible to masses for public use is called public Clouds. The Cloud which are owned by a single company and are restricted to be used by its own set of people are called private cloud [1]. The combination of these two types is called Hybrid Cloud. The main security issue on Cloud Computing is focused in the next topic i.e. software as a service (SaaS), platform as a service (PaaS) and Internet as a service (IaaS). This paper also discusses the security risks associated with Cloud Computing and the security measures that is to be taken to overcome the risk in Cloud Computing.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

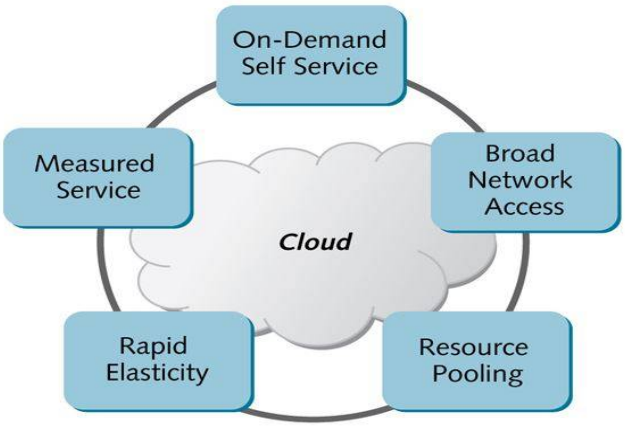

Fig.1: Cloud

II. TYPES OF MODELS FOR CLOUD DEPLOYMENT:

There are four forms of cloud in Cloud Computing:
Public cloud, Private cloud, Hybrid cloud and Community cloud.

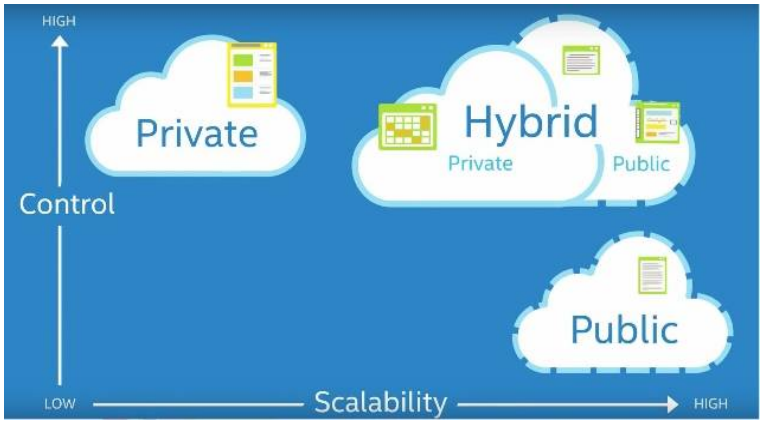

Fig.2: Cloud Deployment

A. PUBLIC CLOUDS

When the cloud services are provided over a network that is accessible for public use, it is called public cloud. Public cloud service providers use the internet to provide resources such as storage and application on a public cloud. Here the Cloud infrastructure is operated by any third party service providers or any outside organization.
Some examples of public clouds are: -
Sun cloud, Amazon web services, Oracle, Google app engine and Microsoft etc.,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

B. PRIVATE CLOUDS

In Private Cloud the Cloud infrastructure is operated exclusively for a single organization. It is more secured because of its internal usage as only specified users and own organization can access the services provided by the Cloud infrastructure. Private clouds can be expensive with typically modest economies of scale [1].

C. HYBRID CLOUDS

A Hybrid Cloud is any combination of two or more distinct cloud infrastructure. It may be a private cloud and one or more public cloud. There should be resources shared among the clouds.
Example: -*Cloud Bursting.*

D. COMMUNITY CLOUDS

A Community Cloud is specifically designed to meet the defined needs of a Community. It can be managed, operated and owned by one or more organizations in the Community, some combination of them or a third part. Third party service provider managers the shared scheme of infrastructure which is allotted by several organisations [9]. Community cloud can be considered as the cluster of private clouds [2].

III. TYPES OF CLOUD SERVICE MODELS

A. Infrastructure as a Service (IaaS)

It is used for storage, networking and various other computing resources. It gives access to web architecture such as servers, storage, software and connections. Here both dedicated and central resources are shared with contracted clients to reduce the initial cost of establishing the cloud which saves a huge amount of money from installing separate servers, processing power and networking device. The main advantage here is to add or remove any application with ease and cost effective manner [2]. Despite of cost IaaS provides only the basic security and we require a higher level of security measures for application moving into the Cloud. IaaS provides an increased amount of security control to the customer. PaaS and SaaS Clouds are a layer overlaid on IaaS.
Example: -*Amazon EC2 and Rock Space Cloud.*

B. Software as a Service (SaaS)

SaaS is the upper most layers in the Cloud stock, which encloses the software/applications for the users. In SaaS, we don't write our own application program but we use someone else's application. SaaS has the minimum customer control on security. The advantage of SaaS is that there is no need to install any software on their personal computers and neither the burden of maintenance of software. Services such as software for operating system, databases, servers, network access, power and data centre space, etc. are contracted by the CSP [9].
Example: - *Web-based Email, Gmail and Sales Force.*

C. Platform as a Service (PaaS)

PaaS is used for the application created by the customer. Here applications are located without the need for managing and buying the hardware and software. It is a delivery of a Computing platform over the Web. PaaS model offers greater extensibility and greater customer control on security than SaaS but less than that of Iaas. It provides the solution stock required by the customers to build their own applications and organize their own data.
Example: - *use of programming languages such as Python, Java which is supported by the provider and Google Apps.*

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

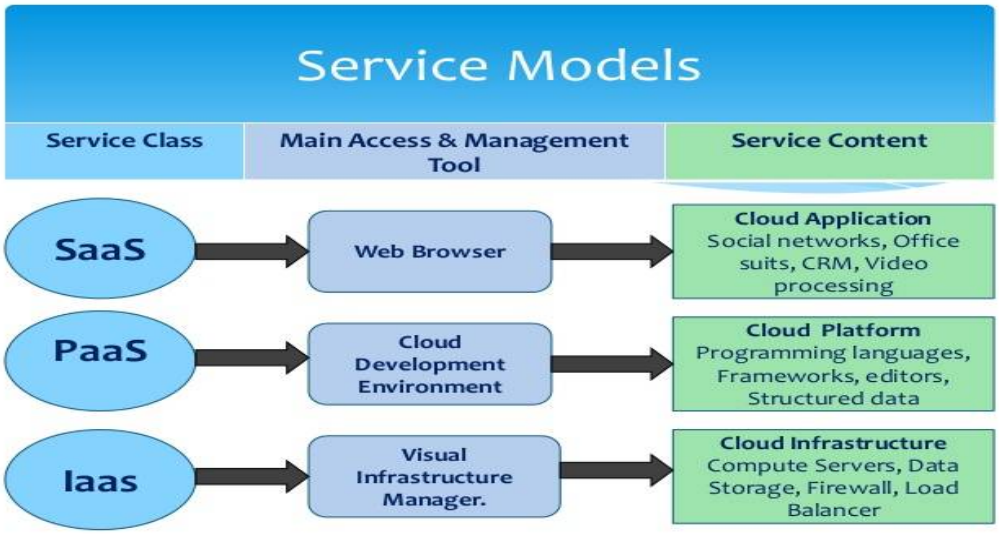

Fig.3: Cloud Service Model

IV. SECURITY RISK ASSOCIATED WITH CLOUD COMPUTING

Security risk is a composition of frequency of security threat event and magnitude of its result or effect, using their product. There are various security risks associated with Cloud Computing such as

- LOSS OF GOVERNACE
- HANDLING OF SECURITY INCIDENTS
- RESPONSIBILITY AMBIGITY
- AUTHESTICATION AND AUTHORIZATION
- ISOLATION FAILURE
- MANAGEMENT INTERFACE VULNERABILITY
- DATA PROTECTION
- APPLICATION PROTECTION
- COMPLIANCE AND LEGAL RISKS
- SERVICE UNAVAIABILITY
- MALICIOUS BEHAVIOUR OF INSIDERS
- INSECURE OF INCOMPLETE DATA
- BUSINESS FAILURE OF THE PROVIDER
- VENDOR LOCK-IN

1. Loss of Governance

User has to handover control to the Cloud provider while using Public Cloud, over a various issue that might affect security. The agreements of services given by the service provider need not provide an assurance to solve such issues. This may create a gap in security defence.

2. Responsibility ambiguity

The provider and the customer may share the responsibility of security issues. The splitting of responsibility forms a critical responsibility of unallocated responsibility of critical security issues.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

3. Authentication and Authorization

Using the Internet use can access the Cloud resources from anywhere in the world. Thus establishing the identity of a user with certainty is very important requirement. Therefore, Authentication and Authorization is a critical requirement to assure security.

4. Isolation Failure

The main feature of Public Cloud Computing is the shared resources and Multi-tenancy. The isolation of storage, memory, reputation and routing between tenants becomes an issues which has to be solved for secure Cloud operations.

5.Compilance and Legal Risks

The customer as to be completely satisfied with the service provider by the Cloud service provider before hiring the Cloud service. The Cloud provider should have appropriate certificates in place and must be verified by the customer themselves.

6. Handling of Security incidence

The customer may submit detection, reporting and successive management of security incidence to the Cloud service provider. However, these incidences affect the customer. It is important to discuss the notification rules in the Cloud service agreement.

7.Management interface Vulnerability

Usually by using Internet we can access the interfaces to manage Public Cloud resources. When combined with remote access and web browser Vulnerability they access large number of resources and they cause increased risk. Than traditional hosting provider.

8.Application Protection

The Cloud Provider is given the responsible for the infrastructure security. By incorporating more controls at the user, application and data level the organizations need to re-plan the perimeter security at the network level.

9.Data Protection

Loss or unavailability of data as well as unauthorized exposure or leakage of sensitive data is covered in data protection. Keeping a track on the data handling practices of the Cloud provider is impossible for a customer. This greatly increases in the case of multiple transfer of the data.

10.Malicious Behaviour of Insiders

When the lack of knowledge about Cloud vendor programs and processes the risk of malicious insiders will increase [11].The insiders enjoy the access and authorizations within an organization and thus create malicious actions and cause substantial damage. Such activity may occur within the customer organization or the provider organization hence increases the risk in the cloud computing environment.

11.Business Failure of the Provider

Business failures could cause unavailability of data and application necessary to the customer's business over an extended period.

12.Service Unavailability

This problem could be caused by hardware, software or communication network failures[1].

13.Vendor Lock-In

Ownership services of a particular cloud service provider makes the customer depend on the provider only. Non-appearances of portability of data and applications among cloud service providers creates a chance of unavailability of data and service in the instance of a change in providers; thus this causes a security issue. Shifting of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

provider becomes a tough task because of the absence of interoperability, if interfaces related with cloud services restricts the customer to a particular provider.

14.Insecure or Incomplete Data Deletion

The data of the user may not be totally deleted after termination of a contract with a provider. Duplicate copies of the data will be usually present, and there is chance of mixing this data with other customer's data. Thus then dedicated hardware, the benefit of multi-tenancy poses a considerable risk to the customer.

There are multiple risks concerning the privacy needs faced by Cloud Computing customers.
They are: -

a. For Cloud Users:

The Cloud user information is tracked in intrusive way without informing Cloud user or taking their approval on the data collection and analysis.

b. For Enterprise Customers:

The risk of interfering with local laws or enterprise policies, losing enterprise reputation, market share.

c. For Cloud Service Provider:

The risk of lawsuits due to failing to conform to local regulations or reputation loss.

d. For Data Stored On the Cloud:

The leakages of customer's data. [4]

V. SECURITY MEASURES IN CLOUD COMPUTING

Security is one of the biggest concern in Cloud Computing [12]. In a network, there is no complete security solution to secure data and app, or services, but satisfactory risk management can reduce the level of risks [8]. Data Security defines that the data or information security is the process of protecting the data from unauthorized users, preventing alterations and restricting the access of sensitive information [5]. There are lots of security measures associated with Cloud Computing such as the Cloud provider must make certain that their infrastructure is protected and secure, at the same time the customer must ensure that the provider has taken a proper security measures to protect their information. The last security measures are to protect the Cloud user against the provider. A correct and regular understanding and analysis of security measures is highly required to protect security in Cloud Computing. "Cloud Computing security refers to a set of policies, technologies and controls deployed to protect data, applications and the associated infrastructure of Cloud Computing" [7].

VI. CONCLUSION

Cloud Computing is the most important Computing and storage technology which is growing tremendously day-by-day. In this paper we have discussed about Cloud Computing technology, services offered, risks/threats associated with it and the security measures to overcome these risks. Along with the increasing demand of Cloud Computing services the need for security is also increasing. This to provide better and secure service to the customers we maintain the balance of these two components hand-in-hand.

REFERENCES

1. Wg Cdr Nimit Kaura, Lt Col Abhishek Lal-Survey Paper on Cloud Computing Security. International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017.
2. Prof.(Dr.) Pradeep Kumar Sharma, Prof.(Dr.) Premala Shankar Kaushik, Payal Jain, Shivangi Agarwal, Kamlesh Dixit – Issues and Challenges of Data Security in a Cloud Computing Environment. Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017.
3. Akshay A Nayak, Sridhar.N.K, Poornima G R, Dr. Shivashankar – Security Issues in Cloud Computing and its Counter Measure. International Conference On Recent Trends in Electronics Information Communication Technology, 2017.
4. Ayman M. EI – Zoghby, Marianne A. Azer – Cloud Computing Privacy Issues, Challenges and Solutions. International Conference on Computer Engineering and Systems (ICCES), 2017.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

5. S.Rajeshwari, R.Kalaiselvi-Survey of data and storage security in cloud computing. In proceedings of the IEEE International Conference on Circuits and systems (ICCS), PP.76-81,2017.
6. Prachi Garg, Dr. Sandeep Goel, Dr. Avinash Sharama – Security Technology for Cloud Computing Environment. International Conference on Computing, Communication and Automation (ICCCA), 2017
7. Anil Barnwal, Satyakam Pugla, Rajesh Jangade Various Security Threats and their Solution in Cloud Computing International Conference on Computing Communication and Automation (ICCCA), 2017.
8. Gaurav Jain, Vikas Sejwar – Improving the Security by using Various Crypto GraphicTechniques in Cloud Computing. International Conference on Intelligent Computing and Control Systems (ICICCS), 2017.
9. G.Shanmugasundaram, V.Aswini, G.Suganya – A Comprehensine review on Cloud Computing Security. International conference on Innovations in information Embedded and Communication system (ICIIECS), 2017.
10. Kanagavalli Rangasami, Vagdevi S – Comparative study of Homomorphic Eneryption methods for secured data operations in Cloud Computing. International Conference on Electrical, Electronics, Communication, Computer and optimization Techniques (ICEECCOT), 2017.
11. Ting-ting yui, Ying-guo zhu- Research on Cloud Computing and Security. International Symposium on distributed Computing and Applications to Business, Engineering and Science, 2012.
12. Mutum Zico Meetei- Cloud Computing and Security Measure. International Congress on Image and Signal processing (CISP), 2013.