International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Cloud Computing – An Overview

Rashmi Jatain
Research Scholar, CSE Department , Maharishi Dayanand University , Rohtak, Haryana, India

ABSTRACT

Cloud computing is the internet depend technology which is providing the services to user, small and large organization on demand. Cloud computing stored the user data and maintain in the data canter of cloud provider like Amazon, Oracle, Google, Microsoft etc. There are number of users used cloud to store their personal data, so that data storage security is required on the storage media. The major concern of cloud environment is security during upload the data on cloud server. Data storage at cloud server attracted incredible amount of consideration or spotlight from different communities. For outsourcing the data there is a need of third party. This research paper discuss what is cloud computing, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry.

Key words: Security Issues, Cloud Security, Cloud Architecture, Cloud Platform.

I. INTRODUCTION

Cloud computing is distributed architecture with centralize server. The Cloud computing is internet depend technology which provide computing services in the form of Infrastructure as services (Iaas), platforms as service (Paas) and Software as Service (SaaS) to the user.

The user does not require knowledge or expertise to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Cloud computing providers deliver common online business applications which are accessed from servers through web browser [1].As resources are utilize, they are measured and payment is made on the basis of the utilization of the services to the CSP (Cloud Service Provider).

The mechanism [2] model of cloud storage consists of four layers: storage layer which stores the data, basic management layer which ensures security and stability of cloud storage itself, application interface layer which provides application service platform, and access layer which provides the access platform.

The basic cloud storage environment represented as below:

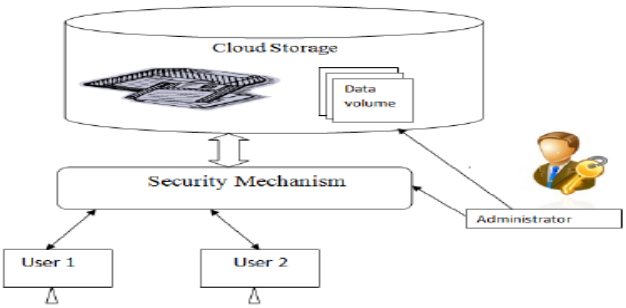

Figure 1. Cloud Storage Environment

II. MODELS OF CLOUD SERVICES

Cloud Serviced is divided into three categories i.e.
Infrastructure as a Service (IaaS).
Software as a Service (SaaS), and
Platform as a Service (PaaS).

a) Infrastructure as a Service (IaaS)-:

In this refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.[3]

b) Software as a Service (SaaS)-:

In this model in which an application is hosted as a service to customers who access it via the Internet. When the software is hosted off-site, the customer doesn't have to maintain it or support it. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support [4].

c) Platform as a Service (PaaS)-:

Is another application delivery model. PaaS supplies all the resources required to build applications and services completely from the Internet, without having to download or install software. In this model, user does not manage the infrastructure like network, servers, operating systems and storage but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

III. CLOUD DEPLOYMENT MODEL

Public Cloud: Public cloud means no access restrictions can be applied and no authorization and authentication techniques can be used ,which are which are accessible on internet from a minor party, which detached assets and charges its clients on the basis of utility. describes the conventional meaning of cloud computing that is accessible, effective ways and means, Cloud organization is possessed and accomplish by a supplier who suggest its retune to public domain. E.g. Google, Amazon, Microsoft offers cloud services via Internet. There are different benefits of public cloud model.

- ✓ Cost Effective
- ✓ High Scalability
- ✓ Reliability
- ✓ Flexibility
- ✓ Location Independence

Private Cloud:

Private cloud can be owned or leased and managed by the organization or a third party and exist at on premises or offpremises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted.

One of the best examples of a private cloud is Eucalyptus Systems [4]. There are different benefits of private cloud model.

- ✓ High Security and Privacy
- ✓ More Control
- ✓ Improved Reliability

Hybrid Cloud

A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services [6].A hybrid cloud comprises assets from both private and public providers will definitely become the demanded choice for enterprise For example, for general computing enterprise could selects to make usage of external services, and its own data Centre's comprises it own data Centre's. Hybrid cloud model has number of advantages (benefits).

There are different benefits of private cloud model.

- ✓ Scalability
- ✓ Security
- ✓ Flexibility
- ✓ Coast efficiencies

I.

IV. CLOUD KEY SECURITY CHALLENGES

There are some clouds key Security challenges are [7]:

Authentication:

Throughout the internet data stored by cloud user is available to all unauthorized people. Henceforth the certified user and assistance cloud must have interchangeability administration entity.

Access Control:

To check and promote only legalized users, cloud must have right access control policies. Such services must be adjustable, well planned, and their allocation is overseeing conveniently. The approach governor provision must be integrated on the basis of Service Level Agreement (SLA).

Policy Integration:

There are many cloud providers such as Amazon, Google which are accessed by end users. Minimum number of conflicts between their policies because they user their own policies and approaches.

Service Management:

In this different cloud providers such as Amazon, Google, comprise together to build a new composed services to meet their customers need. At this stage there should be procure divider to get the easiest localized services.

Trust Management:

The trust management approach must be developed as cloud environment is service provider and it should include trust negotiation factor between both parties such as user and provider. For example, to release their services provider must have little bit trust on user and users have same trust on provider.

SECURITY ISSUES

Cloud computing can provide different services like as a Platform as a service (PaaS), Software as a service (SaaS), Infrastructure as a service (IaaS) so that, security of corporate data in the cloud is difficult, Each service has their own security issues.

Data Security: Data Security refers as a confidentiality, integrity and availability. These are the major issues for cloud vendors. Confidentiality is defined as a privacy of the user data in the cloud system. Confidentiality are designed to prevent the sensitive information from unauthorized or wrong people. In this stores the encryption key data from enterprise C, stored at encrypted format in enterprise D. that data must be secure from the employees of enterprise D. Integrity is defined as the correctness of data, there is no common policies exist for approved data exchanges. Data are not lost or modified by unauthorized users. Availability is defined as data is available on time, any place as user requires. As its web native As its web-native nature, cloud

computing system enables its users to access the system (e.g., applications, services) from anywhere. This is true for all the cloud computing systems (e.g., DaaS, SaaS, PaaS, IaaS, and etc.).

Regulatory Complaince: Customers are eventually accountable when the security and completeness of their own data is taken by a service provider. Traditional service providers more prone to outsource surveys and security certification. Cloud computing providers reject to endure the scrutiny as signaling so these customers can only make usage of paltry operations [11].

Data Locations: When users use, they probably won't know exactly where their data will hosted and which location it will stored in. In fact, they might not even know what country it will be stored in. Service providers need to be asked whether they will accomplish to storing and alter data in particular [13].

Trust Issue: Trust is also a major issue in cloud computing. Trust can be in between human to machine, machine to human, human to human, machine to human. Trust is revolving around assurance and confidence. In cloud computing, user stores their data on cloud storage because of trust on cloud. For example people use Gmail server, Yahoo server because they trust on provider.

Data Recovery: It is defined as the process of restoring data that has been lost, corrupted or accident.

V. APPLICATIONS

There are a few applications of cloud computing [9] as follows:

1) Cloud computing provides dependable and secure data storage canter.
2) Cloud computing can realize data sharing between different equipments.
3) The cloud provides nearly infinite possibility for users to use the internet.
4) Cloud computing does not need high quality equipment for the user and it is easy to use.

VI. CONCLUSION

Cloud computing is the new technology widely adopted by the organization in all over the world. Once organization take decision to move the data over the cloud, organization lose the control over the data. Thus, the amount of protection needed to secure data. Security of the Cloud relies on trusted computing and cryptography. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In this paper, we have discussed the first models of cloud computing ,security, availability and integrity issue. Establishing trust is the way to overcome these security issues as it establishes entities relationship quickly and safely. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture. There is no doubt that cloud computing has bright future.

VII. REFERENCES

[1]. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE IntConference on High Performance Computing and Communications, pp825-830, Dalian, China, Sep2008,ISBN: 978-0-7695-3352-0

[2]. Kant, Dr Chander, and Yogesh Sharma"Enhanced Security Architecture for Cloud Data Security." International Journal of Advanced Research in Computer Science and Software Engineering 3.5 (2013): 571-575

[3]. Rabi Prasad Padhy, Manas Ranjan Patra Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges," IRACST - International Journal of Computer

Science and Information Technology & Security (IJCSITS), Vol1, No2, December 2011.

[4]. RL Grossman, "The Case for Cloud Computing," IT Professional, vol11(2), pp23-27, 2009, ISSN: 1520-9202

[5]. BRKandukuri, RPaturi V, ARakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp517-520, 2009

[6]. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon,"On technical Security Issues in Cloud Computing,"Procof IEEE International Conference on Clou Computing (CLOUD-II, 2009), pp109-116, India, 2009

[7]. Rabi Prasad Padhy, Manas Ranjan Patra Suresh Chandra Satapathy, "A REVIEW OF CLOUD COMPUTING SECURITY ISSUES," IRACST - International Journal of Advances in Engineering & Technology, June, 2015(IJAET), Vol8, Issue 3, pp397-403,ISSN- 22311963.

[8]. Santosh Kumar and RHGoudar "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey," International Journal of Future Computer and Communication, Vol1, No4, December 2012.

[9]. SZhang, SFZhang, XBChen, and XZHuo, "Cloud Computing Research and Development Trend," In Proceedings of the 2010 Second International Conference on Future Networks (ICFN '10)IEEE Computer Society, Washington, DC, USA, pp93-97DOI=10.1109/ICFN.201058

[10]. GHughes, DAl-Jumeily & AHussain," Supporting Cloud Computing Management through an Object Mapping Declarative Language", 2010 Developments in Esystems engineering