International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 743-746 www.ijaem.net ISSN: 2395-5252

Cloud Computing and Cloud Security

Rashmi
Adarsh College, Bhiwani

Date of Submission: 21-06-2020 Date of Acceptance: 07-07-2020

ABSTRACT
Cloud computing is a recent trend in IT that moves computing and data away from desktop and portable PCs into large data centers.With the advancement of technology users want to use the internet services over the light weight portable devices rather than some deskrop PC. Because users won't have powerful machines, who will supply the computing power? The answer to this question lies with cloud computing. The future of computing is in the cloud. This paper presents the basics of cloud Computing. This paper also discuss the various models cloud has to offered.
Cloud security is an important concern because it contains many technologies including databases, operating system, networking,virtulization, transaction management, resource scheduling and memory management. Therefore, security of all these resources applicable to cloud computing. This paper discusses the security of data in cloud computing.
KEYWORDS: Data Security, Cloud Computing, Data Protection, Privacy, Risks and threats

I. INTRODUCTION
Cloud computing is a new technology based on distributed processing, parallel computing and grid computing, and is one of the hottest topics in the field of information technology."A network solution for providing inexpensive, reliable, easy and simple access to IT resources" [1]. Cloud computing is the use of remote servers on the internet to store, manage and process data rather than a local server or your personal computer. Cloud computing comes with several features like on demand self-service, Broad network access, Resource pooling, Rapid elasticity etc. By adopting a cloud service into your enterprise, what could it possibly do to widen the scope of your operations? There are huge benefits of cloud computing which includes the scaling up and down of computing resources according to your needs. You pay less amount as it reduces the cost of hardware upgrades and maintenance. By signing up for a cloud service, you are essentially making your data more secure using their industry-grade security protocols.

II. CLOUD MODELS
Each of the cloud models has their own set of benefits that could serve the needs of various businesses

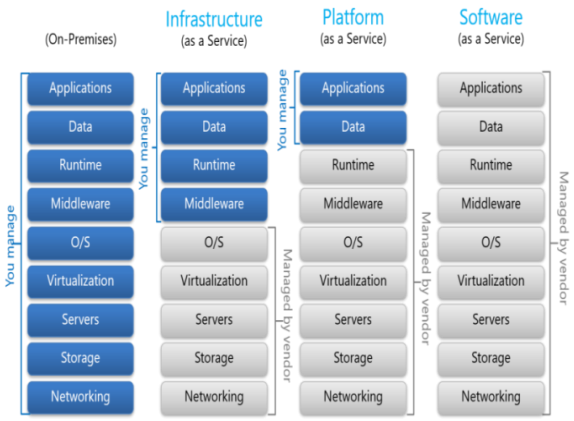
2.1 Service Models
Service models means the kind of services the cloud offers. Cloud models come in three types: SaaS(Software as a Service),IaaS(Infrastructure as a Service) and PaaS(Platform as a Service)

SaaS(Software as a Service):
Using SaaS or Software as a Service we can easily access the cloud based web applications. The third party vendor take care of all the computing resources, you only need to access the web application using a web browser.
cloud provider leases applications or softwares which are owned by them to its client. Some known example of SaaS includes Google G Suite, Microsoft Office 365.

IaaS(Infrastructure as a Service):
IaaS provides virtualized computing resources over the internet. No worries about the underlying physical machine. Abstract the user from the physical machine. You have the access to the operating system of the server. IaaS providers supply computing infrastructure such as virtual server space, bandwidth, network connections, IP addresses, and load balancers. With this service model, your enterprise is responsible for managing applications, data, operating systems, middleware, and runtime.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 743-746 www.ijaem.net ISSN: 2395-5252

PaaS(Platform as a Service):
The cloud provider gives the ability to the customer to deploy customer created application using programming languages, tools etc that are provided by the cloud provider.



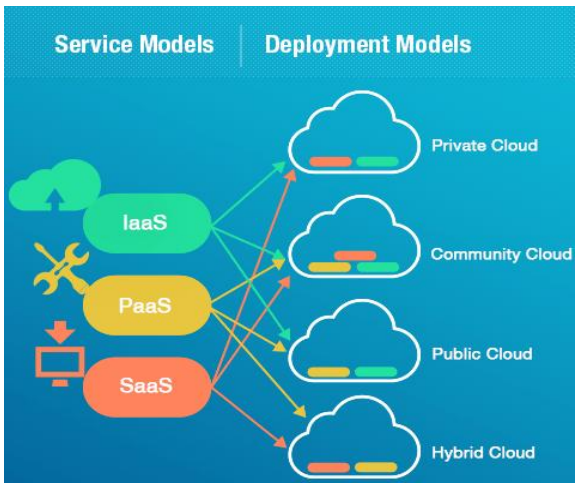
2.2 Deployment Models
Deployment models means in what way you can upload your application on cloud. There are four types of deployment models.

Private Cloud:
Private Cloud also termed as 'Internal Cloud; Private cloud is used for the individual organization that need to store sensitive information.It is costly as compared to public cloud but provide high security and privacy of data. The cloud platform is implemented in a cloud-based secure environment that is guarded by advanced firewalls under the surveillance of the IT department that belongs to a particular organization. Private clouds are deployed under the firewall of the organization's intranet which provide better network performance. Because all the resources available in a private cloud is for the use of single organization, so resources may not be utilized in an optimum way. So utilization of all the resources in a private cloud is a challenge.

Public Cloud
Public cloud service are the distributed service. It can be shared by more than one organization.Public cloud are owned and operated by third-party service providers. Public cloud decreases expenses. Another advantage of public cloud infrastructures is that they quickly and easily provide on-demand scalability.
Some of the examples of those companies which provide public cloud facilities are IBM, Google, Amazon, Microsoft, etc. Customers have no control over the location of the infrastructure.

Community Cloud:
It is a mutually shared model between organizations that belong to a particular community such as banks, government organizations, or commercial enterprises. Community members generally share similar issues of privacy, performance, and security. This type of deployment model of cloud computing is managed and hosted internally or by a third-party vendor.

Hybrid Cloud:
Hybrid Cloud is another cloud computing type, which is integrated, i.e., it can be a combination of two or more cloud servers, i.e., private, public or community combined as one architecture, but remain individual entities. Further, as part of this deployment of cloud computing model, the internal, or external providers can provide resources.
A hybrid cloud is ideal for scalability, flexibility, and security. A perfect example of this scenario would be that of an organization who uses the private cloud to secure their data and interacts with its customers using the public cloud.



III. CLOUD SECURITY

Cloud security is an important concern because it contains many technologies including databases, operating system, networking,virtulization, transaction management, resource scheduling and memory management. Therefore, security of all these resources applicable to cloud computing. For example ,networks that connects two clouds must be secured. Mapping between the virtual machines to the physical machine has to be done with high concern of security. Data security includes

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 743-746 www.ijaem.net ISSN: 2395-5252

encryption of data and appropriate policies are enforced for data sharing. Algorithms that allocate resources and managing the memory must be secured.

Meta-data spoofing Attack:

In cloud system, client's request is executed based on authentication and authorization, It is highly possible that meta data exchange between the web server and web browser. An attacker can take the advantage during this exchange of metadata. Then cloud service suffers from eavesdropping and deadlocks.

Virtualization:

Virtulalization is a basic element of cloud computing which is used to delivering the core values of cloud computing.virtualization is the process of running a virtual instance of a computer system that do not actually exist in physical. By using this technique we create a functional copy of operating system in another operating system. Hypervisor is used to run a guest operating system in a host operating system as a virtual machine. Hypervisor is a special function that can be the main target if it is vulnerable.

If a hypervisor is not up to the mark, then the whole system can be compromised and the data can be harm. Therefore, Virtualization incur some potential risks to data in the cloud.

Another type of risk associated with the virtualization is allocation and de-allocation of resources. Virtual Machine operation data is written in memory and before the another allocation if the memory is not free, then there is a high chances for data exposure to the next VM which is not desirable [3]. The Solution to above problems is that hypervisor function must not be vulnerable. Resources should be carefully allocated, used and data must be properly authenticated before de-allocating the resources.

Data Breaches:

Usually cloud data is stored in centralized storage facilities, which is open to public and can be a big cause for data leakage. Storage resources are complicated systems that are combination of hardware and software implementations and can cause exposure of data if a slight breach occurs in the public cloud[4].

Multitenancy:

Multitenancy means multiple users share the same computing resources in a cloud. Despite the fact that they share resources, cloud customers aren't aware of each other, and their data is kept totally separate.

Multitenancy is an important component of cloud computing; Cloud computing become less practical without sharing of resources or multitenancy. Since multiuser shares the same computing resources like CPU, Memory etc. Then there is a more possibility of threats not only for single user but for multiple users. In such case there is always a high risk of accidentally leaking private data to other users. Multitenancy exploits can be exceptionally risky because one fault in the system can allow another user or hacker to access all other data [5]. These types of issues can be taken care of by wisely authenticating the users before they can have access to the data. Several authentication techniques are in use to avoid multitenancy issues in cloud computing [6].

IV. DATA SECURITY IN CLOUD

In cloud computing the requirements of data security depends on which service models(SaaS,PaaS,IaaS) we are using. Usually in networking we can secure our data using encryption but in cloud computing we need more than that because we are not only just transmit or sharing data but data is permanently resides on the other server. Thus in Cloud computing we divide the security in two states of data. Data at Rest which means data is stored in the cloud and Data in Transit which means data is sharing or transmitting in and out of the cloud . Confidentiality, and integrity of data is based on the characterstics of data protection mechanisms,procedures, and processes.

Data At Rest:

Organization does not have physical control over the data if they are not maintaining a private cloud. So, this issue is solved by having a private cloud but that is not possible in all cases as it costs more.

Data in Transit:

Data security in cloud computing involves more than data encryption. Requirements for data security depends upon on the three service models SaaS, PaaS, and IaaS. Two states of data normally have threat to its security in clouds; Data at Rest which means the data stored in the cloud and Data in Transit which means data that is moving in and out of the cloud. Confidentiality, and Integrity of data is based upon the nature of data protection mechanisms, procedures, and processes. The most significant matter is the exposure of data in above mentioned two states.

V. CONCLUSIONS

The concept of cloud computing comes from distributed computing, parallel computing and grid computing. How Everything goes from desktop PC's to lightweighted portable devices to internet to cloud. Cloud computing provides companies with new options for managing infrastructures and new business models. However Cloud computing is revolutionizing how information technology resources and services are used and managed, but this comes with great security challenges. It will be difficult to provide end-to-end security because of the complexity of the cloud. There are lots of issues concerning with cloud computing like data security, security over network, application resources and many more. The goal of achieving security in cloud is to store and manage data that is not controlled by the owner of the data.

REFERENCES

[1]. Dikaiakos, M.D., Katsaros, D., Mehra, P., et al.: Cloud Computing: Distributed Internet
[2]. Computing for IT and Scientific Research 13, 10–13 (2009)
[3]. F. Sabahi, "Virtualization-level security in cloud computing," 2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, pp. 250–254, 2011.
[4]. Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.
[5]. A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, "Security risks and their management in cloud computing," 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., pp. 121–128, 2012.
[6]. T. Mather, S. Kumaraswamy, and S. Latif, "Cloud Security and Privacy," p. 299, 2009.

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 02 Issue: 01 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com