**A Review of Cloud Computing Security Issues**

Manpreetkaur

Chandigarh group of college, Landran

Cutemani.shergill@gmail.com

***Abstract:As Cloud Computing becomes prevalent, sensitive information are being increasingly centralized into the cloud.. Number of users used cloud to store their data.Data storage security is defined as the security of data on the storage media. As security is one of the major concerns in cloud environment for preventing data deployment during upload.Recently outsourcing of data storage at cloud servers has attracted incredible amount of consideration or spotlightfrom different communities. However, outsourcing the data to a third party. Cloud server causes the security and privacy issues to become critical concern. This has raised the important security issue of how to prevent and control unauthorized access to data stored in the cloud. This paper discuss the concept of what a cloud and its security issues. This paper pays much attention on the security issues of cloud computing.***

1. **INTRODUCTION**

The term “Cloud Computing” generally describes the fact that computing services of any form in Information Technology like infrastructure, platforms, or applications could be arranged and used through the internet. Infrastructure upon which cloud is built upon is a large scaled distributed infrastructure in which shared pool of resources are generally virtualized, and services which are offered are distributed to clients in terms of virtual machines, deployment environment, or software. Hence it can be easily concluded that according to the requirements and current workloads, the services of cloud could be scaled dynamically. As many resources are used, they are measured and then the payment is made on the basis of consumption of those resources .

According to the definition of[4], cloud computing is “it is a significant distributed computing model that is directed by financial prudence of balance, in which stake of isolate, fundamental, loading, podium in which a facilities are supplied as per the request of exterior foreign clients through the internet”. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud storage[6] specifies the storage on cloud with almost inexpensive storage and backup option for small enterprise. The actual storage location may be on single storage environment or replicated to multiple server storage based on importance of data. Typical cloud storage system architecture includes a master control server and various clients. The mechanism [6] 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:

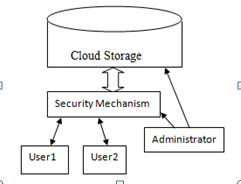


Figure 1: Cloud Storage Environment

1. **Cloud Services Models**

**Cloud Infrastructure as a service (IaaS):** A provider provides a virtual infrastructure where computing resources including processing units, storage, and network could be provisioned in order to setup a deployment environment for their software system. A customer has flexibility to manage and control a software stack to be deployed ranging from an operating system, middleware, and applications. There are different issues in IaaS such as:

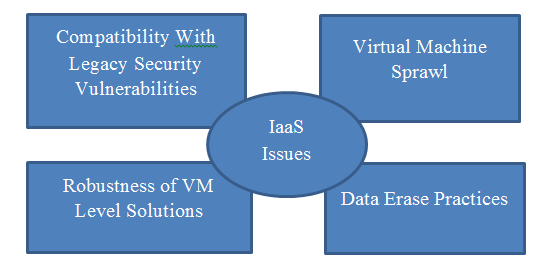


Figure 2: IaaS Issues

**Cloud Platform as a service(PaaS):** PaaS provides customers with the capability to develop and deploy applications based on tools and programming languages supported by the providers. This hosted \*platform is configurable in a limited manner based on a provided set of APIs. Examples of this classof services include Google App Engine, Windows Azure Platform and rack space. There are different issues in PaaS such as:

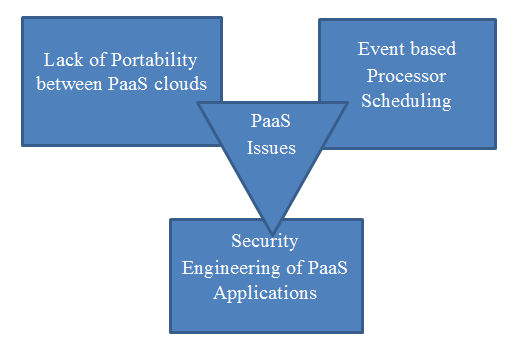


Figure 3: PaaS Issues

**Cloud Software as a service(SaaS):**SaaS provides the capability to use the applications which run on cloud infrastructure. These applications are accessible through standard interfaces such as web browser or an e-mail client. SaaS offers the experience of getting to work on applications and data from anywhere at any time by using various forms of devices.

**Cloud Network as a service(NaaS):**NaaS provides the capability to use the network services and inter-cloud network connectivity services. These services involve the optimization of resource allocations by considering network and computing resources. NaaS services include flexible and extended VPN, and bandwidth.

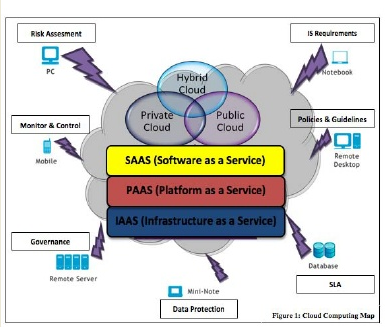


Figure 4: Cloud Computing map [2]

1. **Cloud Deployment Models**

**Public Cloud:** Public cloud describes the conventional meaning of cloud computing that is accessible, effective ways and means, which are accessible on internet from a minor party, which detached assets and charges its clients on the basis of utility.The cloud infrastructure is owned and managed by a provider who offers its services to public. E.g. Google, Amazon, Microsoft offers cloud services via Internet. There are different benefits of public cloud model. The following figure shows some of those benefits:

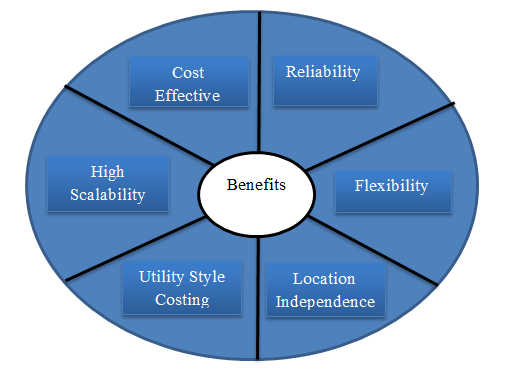


Figure 5: Benefits of Public Cloud

**Private Cloud:** Private cloud is a term used to donate a proprietary computing architecture provisioned services on corporate networks. Big enterprises usually used this type of cloud computing to permit their private network and information centre administrators to effectively become in-house ‘service providers’ catering to customers within the corporation. The cloud infrastructure is built for a specific organization, but might be managed by a third party under a service level agreement. Only single organization preferred to operate via corporate cloud. There are advantages(benefits) of internal cloud model.. The diagram given below depicts a few of these advantages(benefits):

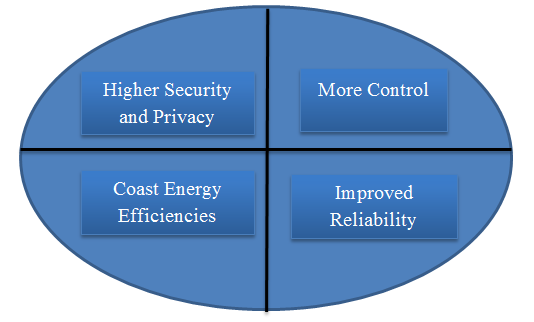


Figure 6: Benefits of Private Cloud

**Hybrid Cloud:** A hybrid cloud comprises assets from both corporate and public providers will definitely become the demanded choice for enterprises. The hybrid cloud is a combination of both corporate cloud and public cloud.. For example, for general computing enterprise could selects to make usage of external services, and its own data centres comprises it own data centres. Hybrid cloud model has number of advantages(benefits).The diagram given below reveals some of those advantages(benefits):

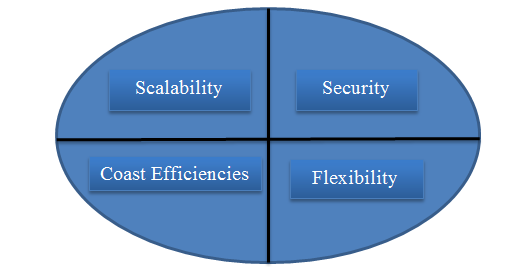


Figure 7: Benefits of Hybrid Cloud

1. **Cloud Computing Characteristics**

**On Demand self-service:** A cloud might individually attain computing possibilities, as per the use of different servers, network storing, as on request, without communicating with cloud provider.

**Broad Network Access:** Services are delivered across the Internet within a standard mechanism and access to the services is possible through assorted customer tools.

**Resource pooling:** A multitudinous model is employed to serve different types of clients by making pools of different computing resources, as per the request of customers these have different resources which can be assigned and reassigned dynamically.

**Rapid Elasticity:** Capabilities might be elastically provisioned or rapidly released. From customers view, the provided possibilities comes out to be limitless and must have the capability to purchase in any quantity at any time.

**Measured Services:**The provision procured by clients are measurable. The use of asset will be directed, estimated,and accused for contributor and asset.

1. **Cloud Security challenges**

There are some key security [2] challenges are:

**Authentication:** Throughout the internet the 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.

1. **Security Feature in Cloud Computing**

There are several main challenges for building a secureband trustworthy cloud system:

**Outsourcing:** Outsourcing brings down both capital expenditure and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services. In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive data is out of the owners control.

**Massive data and intense computation:** Cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored, it is impractical to hash the entire data set. To this end, new strategies and protocols are expected.

1. **Security Issues**

The security of corporate data in the cloud is difficult, as they provide different services like software as a service (SaaS), Platform as a service (PaaS), Network as a service (NaaS), Infrastructure as a service (IaaS). Each service has their own security issues [1]

**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 data. 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. Availability is defined as data is available on time.

**Regulatory Complaince:** Customers are eventually accountable when the security and completeness of their owm data is taken by a service provider.Traditonal serviceproviders 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 [5].

**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 arbitration, and on the basis of their customers will they make a fair accomplishment to follow local privacy requirement [3].

**Privileged user access:** Outside the resource data that is processed contains anindigeneous risk, as deploy services, avoid the mortal, consistant and human resource manage IT shops works on the house programss.

**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 revolve around assurance and confidence. In cloud computing, user strore 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.

1. **Conclusion**

Cloud computing is latest technology that is being widely used all over the world..Number of cloud platforms are available now in educational as well as in enterprises circle.ss This paper discusses the concept of Cloud computing to achieve a complete definition of what a Cloud is and its security issues. These issues mentioned above will be the research hotspot of cloud computing. There is no doubt that cloud computing has a bright future.

1. **Refrences**

1)B.R kandukuri, R.Paturi V, and A.Rakshit, “cloud security issues”,2009 IEEE International Conference on Services Computing, sep. 21-25, 2009, Bangalore, India, pp. 517-520.

2)Chandrahasan, R. Kalaichelvi, S. ShanmugaPriya, and L. Arockiam. "Research Challenges and Security Issues in Cloud Computing." *International Journal of Computational Intelligence and Information Security* 3.3 (2012): 42-48.

3)Feng-Tse Lin, Teng-San Shih, “Cloud Computing: The Emerging Computing Technology,” ICIC Express Letters Part B: Applications (ISSN: 2185-2766), v1, September 2010, pp. 33-38.

4)Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud Computing and Grid Computing 360-Degree Compared CoRR. *abs/0901.0131*.

5)G. Hughes, D. Al-Jumeily& A. Hussain,” Supporting Cloud Computing Management through an Object Mapping Declarative Language”, 2010 Developments in E-systems engineering.

6)Kant, DrChander, 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.

7)Yunqi Ye, Liangliang Xiao, I-Ling Yen, FarokhBastani, “Secure, Dependable, and High Performance Cloud Storage”, 2010 29th IEEE International Symposium on Reliable