Security Issues in Hybrid Cloud Computing

Kalpit Soni[1], Parulben D. Sindha[2]

[1]Ph.D. Research Scholar, Charotar University of Science and Technology (CHARUSAT), Changa, Gujarat, India
[2]Ph.D. Research Scholar, Charotar University of Science and Technology (CHARUSAT), Changa, Gujarat, India

Abstract: ***Cloud computing is solution in which resources such as hardware, software, network and storage requirement are provided to the user as per the demand. Basically Cloud computing is the combination of private cloud and public cloud. This paper focuses on the overview of security issues which may arise while adopting the hybrid clouds. It also focuses on the risks involved with the uses of hybrid clouds.***

Keywords: Cloud computing, Hybrid Cloud, Private Cloud, Public Cloud

1. Introduction

Cloud computing is a relatively new business model in the computing world. In an October 2009 presentation titled "Effectively and Securely Using the Cloud Computing Paradigm,"[1] by Peter Mell and Tim Grance of the National Institute of Standards and Technology (NIST) Information Technology Laboratory, Cloud computing is defined as follows: "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [2]

The idea of Cloud computing is based on a very fundamental principal of *'reusability of IT capabilities'* [3] Cloud computing describes applications that are extended to be accessible through the Internet. These Cloud applications use large data centers and powerful servers that host Web Application and Web Services [4] (IEEE 2008) anyone with a suitable Internet connection and a standard browser can access a Cloud application. For example mail server. Cloud computing is described by NIST with the help of five characteristics, three service models and four deployment models [5].

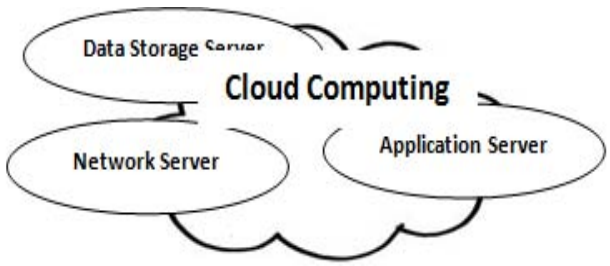

Figure 1: Cloud Computing

2. Five Characteristics

- On demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

1) On-demand self service provides automatic computing capability management to systems, without requiring human interaction.
2) Broad network access allows heterogeneous clients. Such as mobile phones, laptops to connect to Cloud systems over the network
3) Resources pooling in Cloud systems is available as pooling resources for multiple consumer which is able to dynamically assign and reassign according to consumer demand.
4) Rapid elasticity offers rapidly and elastically provision of capabilities. We can grow and shrink our capacity very quickly in minutes or hours.
5) Measure service provides monitoring, controlling & reporting of resources usage.

3. Three Cloud Service Models

- Infrastructure as a service (SaaS)
- Platform as a service (PaaS)
- Software as a Service (IaaS)

Infrastructure as a Service: Service provider bears all the cost of servers, networking equipment, storage and back-ups. We just have to pay to take the computing service. And the users build their own application software's. Amazon EC2 is an example of this type of services [6]

Platform as a Service: Service provider only provider platform for user. It helps user saving investment on hardware and software. The customer has the freedom to build his own application, which run on the provider's infrastructure, to meet manageability and scalability requirement of the application. PaaS provider offers a predefined combination of OS and application servers. Google Gc engine and force.com are an example of this type of services [7].

Software as a Service: In this model, a complete application is offered to the customer, as a service on demand. A single instance of the services runs on the Cloud & multiple end users are serviced. On the customer's side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted and maintained. Today SaaS is offered by companies such as Google, salesforce, Microsoft, Zoho,etc [8].

Figure 2: Example of resources provided by Cloud computing

4. Four Cloud Deployment Models

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud

Clouds can be categorized in different types depending on who owns and them.

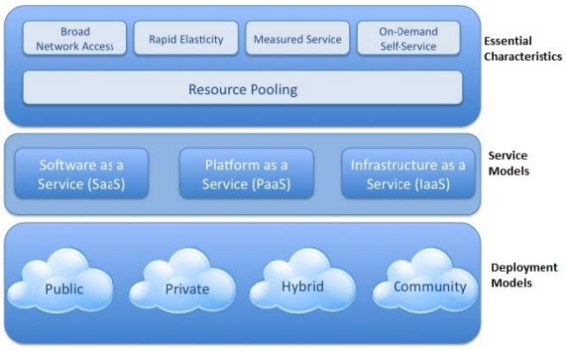

Figure 3: NIST visual model of Cloud computing definition

Private Cloud: This is a Cloud which can be used and operated by a single organization. Eucalyptus, Ubuntu Enterprise Cloud (UEC - powered by Eucalyptus) , Amazon VPC (Virtual Private Cloud), VMware Cloud Infrastructure Suite, Microsoft ECI data center are example of Private cloud.

Public Cloud: This is a Cloud which can be owned by large corporation. Google App Engine, Microsoft Windows Azure, IBM smart Cloud, Amazon EC2 are example of Public cloud.

Community Cloud: This is a Cloud which can be shared by multiple organizations for some specific requirements. Google apps for government, Microsoft apps for government community Cloud are example of Community cloud.

Hybrid Cloud: This is a Cloud which owns the features of more than one Clouds types from the above three. Windows Azure, VMware vCloud are examples of Hybrid cloud.

5. Benefits of Hybrid Cloud

Hybrid clouds offer the cost and scale benefits of public clouds while also offering the security and control of private clouds. The following are some of the possible benefits for those who offer cloud computing-based services and applications:

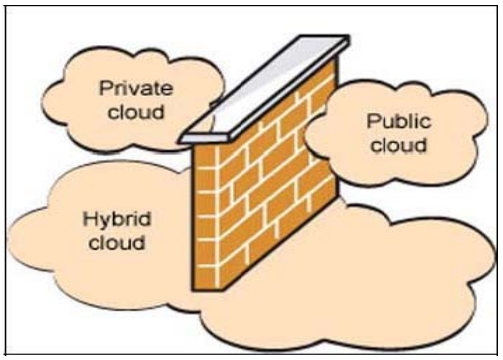

Figure 4: Hybrid Cloud Computing

Cost Savings: It is the major benefit of using Cloud computing. Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. It improves resource allocation for temporary projects at a reduced cost because the use of public clouds removes the need for investments to carry out these projects. In hybrid cloud, public clouds can be used for development and testing while private clouds can be used for sensitive data.

Business Agility: A Hybrid cloud offers both the advantages available in a private cloud deployment along with the ability to rapidly scale using public clouds. It supplies support for cloud bursting, using the public clouds for an unexpected need for additional IT resources. It also provides drastic improvements in the overall organizational agility, because of the ability to add public clouds for unexpected addition computer resources requirements and also support the pure private cloud for fulfilling the requirement of the secured information, data and process.

Maintenance: Cloud service providers do the system maintenance, and access is through APIs that do not require application installation onto PCs, thus further reducing maintenance requirements.

6. Security Issue

There are a number of security issues associated with cloud computing but Hybrid cloud allows the organization to place their partly on the cloud and the rest of applications on their premises according to the requirements. Data and information of any organization require the high level security because any leaked or tampered in highly confidential information, intentionally or accidentally result in a big loss in finance and reputation of the organization. As the organization adopt hybrid clouds, the highly confidential data kept in to the premise's data center. For that organization has to bear the cost to develop the data center. Security issues fall into two broad categories.

- Security issues faced by cloud providers.
- Security issues faced by their customers.

As organizations use hybrid clouds for their business needs, they must understand the new security requirements of a hybrid cloud environment. While hybrid clouds offer the

security advantages of private clouds, there are some unique securities challenges that should be keep in mind while adopting the hybrid cloud.

In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. The following are some issues which can be faced while adopting the hybrid cloud.

Location of the Data: Some time applications may use resources from multiple servers in clouds. The servers are based at multiple locations and the services provided by the cloud may use different infrastructures across the organization. This situation creates compilations in providing the security to the data which are stored in cloud.

Confidentiality and integrity: Confidentiality refers to who stores the encryption keys – data from company A, stores in any encrypted format at company B must be kept secure from employees of B; thus, the client company should own the encryption keys. Integrity refers to the face that no common policies exist for approved data exchanges; the industry has various protocols used to push different software images or jobs.

Authentication: It is a process that traditionally says the privileges to the user to access particular information or access a service. There is no authority of the client to apply proper security measures to the data stored on the clouds. There is not control of the client on the management of the cloud. The providers do not like to interfere in their own methodology. It is an easy way to solve the identity needs of private clouds, but in hybrid cloud now private cloud is extend with public cloud. So it is difficult task to control the identity and access management.

Scalability: As the hybrid cloud extends the organization outside the organization's boundary, we should be very careful because doing so it opens up the larger surface area for the attack on public as well as on the private cloud also.

Data Segregation: It is a risk in the hybrid cloud computing. Public clouds are used by many users. As a result data can be kept in a shared mode in the public cloud. Due to this reason there is a chance of the user's private data to be seen by other users. If the data and the information are not protected from other users then it is a major risk to the user to keep his/her private information in the cloud.

Network Security: In hybrid cloud deployment models instead of traditional clearly defined network boundaries the borders between tenant networks can be dynamic and potentially blurred in a large scale virtual/Cloud environment. In a public cloud deployment model, sensitive data is obtained from the enterprises, processed by the SaaS application and stored at the SaaS vendor end. All data flow over the network needs to be secured in order to prevent leakage of sensitive information.

Security Policies: There are risks associated with the security policies adopted by the hybrid cloud such as how the encryption keys are managed in public cloud.

Backup and Recovery: In hybrid cloud computing some data are stored in some remote location. Because of some incident like fire, earthquake, flood or any natural calamities there may be chance of data loss. So there must be a provision to recover the data which may be loss due to the above reasons.

7. Conclusion

Growing need of the down the resource and to cut down the cost expenditure the cloud benefits are endless. But in order to achieve the best while spending less, have some security problems which are unresolved. This paper describes the various aspects of the cloud and its security. Through this paper has covered almost the security issues in the hybrid cloud environment. Although the cloud is the cheapest and the easiest way to use the resources, still it needs a security architecture which describes all the service models as well as the cloud architecture in future.

References

[1] Csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v25.ppt
[2] (http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc)
[3] Information Technology for Management: By BEHL
[4] Annual International Conference on Cloud Computing and Virtualization (CCV 2010)
[5] (http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc)
[6] www.ijera.com/papers/vol2_issue1/V21117125.pdf
[7] www.ibm.com/in/PaaS
[8] En.wikipedia.org/wiki/software_as_a_service