An Overview and Security of Cloud Computing Technology

R.Sabin Begum , Dr.R.Sugumar

R. Sabin Begum- Research scholar in Bharathiyar university, Coimbatore.

Dr.R.Sugumar- Associate Professor,VELTECH Multitech SRS Engg. College,Chennai.

***Abstract*—With the rapid development of Internet, Cloud Computing has a vast area of the application such as security services, enhance efficiency of system by utilizing resources in cost effective manner. Cloud computing is simply a service that is sold and delivered on demand over the Internet. This paper have - Firstly, models of cloud computing discussed: Service Model and Deployment model . Secondly, Risk to cloud computing are discussed. Finally, the paper will be concluded on the benefits of cloud computing.**

Index term: Cloud Computing, Deployment model, Risk, Services, Security.

I.INTRODUCTION

Cloud computing is a model for enabling 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[1].

Cloud computing can be considered a new computing paradigm with implication for greater flexibility and availability at lower cost. The cloud removes the need for you to be in the same physical location as the hardware that stores your data. Your cloud provider can both own and how the hardware and software necessary to run your home or business application.

The benefit is that you can access that same document from wherever you are with any device that can access the Internet. This is the freedom that the cloud can provide for you or your organization. In the modern distributed era different services offered in the Internet as a traditional hosting system. But in the traditional hosting system storage and usage are fixed. But the current trend in business requires dynamism in compute. This leads to the development of cloud models.

II DEPLOYMENT MODEL

Deploying cloud computing can differ depending on requirement and the following four deployment models have been identified. A cloud deployment model defines where the physical servers are deployed and who manages them. Types of clouds are (Fig1.1)

A. Private Cloud

B. Public Cloud

C. Hybrid Cloud

D. Community Cloud

A. Private Cloud

A private cloud is established for a specific group or organization and limits access to just that group. The operation may be in house or with a third party on the premises[4].

A private cloud is subject to the organization's physical, electronic and procedure security measures and thus offers a higher degree of security over sensitive code and data.

A private cloud is the obvious choice when

- Your business is your data and your applications. Therefore, control and security are paramount.
- Your business is part of an industry that must conform to strict security and data privacy issues.

Benefits:

Elasticity: Private cloud can scale to meet demand increase in IT system.
Control: Private cloud gives organization control over their data ensuring its security.

B. Public Cloud

A public cloud can be accessed by an subscriber with an internet connection and access to the cloud space.

A public cloud is the obvious choice when[5]

- To standardized workload for applications is used by lots of people, such as e-mail.
- Need to test and develop application code.
- To have SaaS (Software as a Service) applications from a vendor who has a well-implemented security strategy.
- Need incremental capacity (the ability to add computer capacity for peak times).

C. Hybrid Cloud

A third type can be hybrid cloud that is typical combination of public and private cloud. It enables the enterprise to running state-steady workload in the private cloud, and asking the public cloud for intensive computing resources when peak workload occurs, then return if no longer needed [5].

D. Community cloud

Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns. The cloud community forms into a degree of economic scalability and democratic equilibrium.

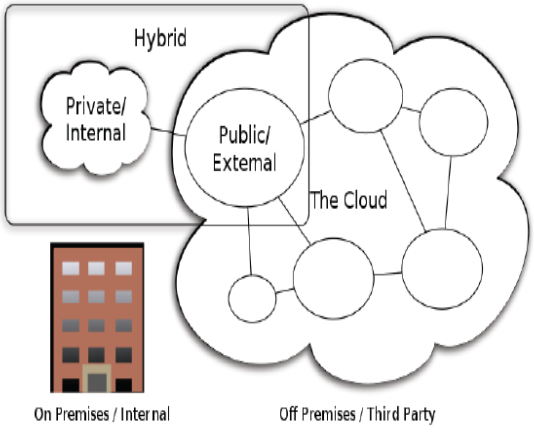

Fig 1.1

III Cloud computing Service Levels

A web Server typically has three tiers to it. Refer diagram (Fig1.2)

Software as a service (SaaS)

One of the first implementation of cloud services was Software as a Service, business application that are hosted by the provider and delivered as a service. A SaaS provider gives subscribes access to both resources and applications. This layer includes application that run off the cloud and is available to web users or enterprises on a pay-as-you-go, anytime-anywhere basis. SaaS makes it unnecessary to user to have a physical copy of software to install on your devices. SaaS also makes it easier to have the same software on all your devices at once by accessing it on the cloud. In SaaS agreement, you have the least control over the cloud. Examples are Salesforce.com, Google's Gmail and Apps, instant messaging from AOL, Yahoo and Google, and VoIP from Vonage and Skype.

Platform as a Service(PaaS)

This service layer provides a platform for creating application. PaaS solutions are essentially development platform for which the development tool itself is hosted in the cloud and accessed through a browser. A PaaS provider gives subscribers access to the components that they require to build web application without installing any tools on their computer and then deploy without any specialized system administration skills[2].

Examples are Microsoft's Azure, Sales force's Force.com, Google Maps, ADP Payroll processing, and US Postal Service offerings.

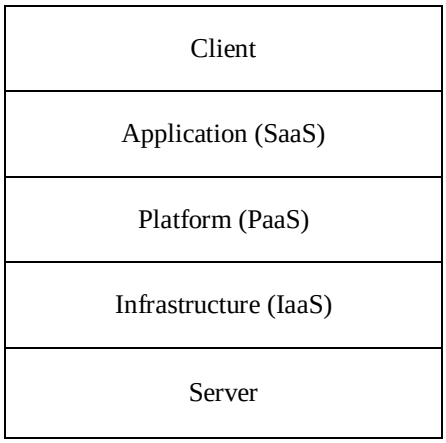

Fig 1.2

Infrastructure as a Service (IaaS)

This layer provides Servers, Network Device and storage disk are made available to organization as services on a need to basis. It any also include the delivery of operating system and virtualization technology to manage the resource . Vendors would include Amazon.com,Elastic

Compute Cloud [EC2] and Simple Storage), IBM and other traditional IT vendor[2].

IV Risks to cloud computing

A major concern with cloud computing is that the cloud provider in the cloud, that is, the software, platform and infrastructure to the user. In addition, user data also reside with the cloud provider. The risk with this type of service is that user information could be abused, stolen, unlawfully distributed, comprised or harmed. There is no guarantee that user's information could be sold to its competitor. Unfortunately, this particular risk applies to all three types of cloud delivery models, namely, SaaS, PaaS and IaaS [3].

Other risk to cloud computing also exist , and range from privacy, data protection ,ownership, location and lack of reliable audit standard to data security procedure of most pioneer cloud providers[3].

Security

Cloud computing allows providers to develop, deploy and run applications that can easily grow in capacity , work rapidly , and never fail , without any concerns on the properties and the locations of the underlying infrastructures. Cloud Computing systems are secure if users can depend on them (i.e. SaaS, PaaS, IaaS, and so on) to behave as users expect. It contains 5 goals, availability, confidentiality, data integrity, control and audit, to achieve enough security[3].

1. Availability

The goal of availability for Cloud Computing systems is to ensure its users can use them at any time, at any place. Many Cloud Computing system vendors provide Cloud infrastructures and platforms based on virtual machines. The current Cloud system vendors who are providing infrastructures and platforms based on virtual machine (e.g. Amazon, Skytab) offer the ability to block and filter traffic based on IP address and port only to secure their systems, but these facilities are not equivalent to the network security controls in most enterprises. As for redundancy, large Cloud Computing system vendors (e.g., Amazon, Google) offer geographic redundancy in their Cloud systems, hopefully enabling high availability on a single provider. In a word, Cloud Computing systems are able to provide available services in nature through hardening and redundancy strategies.

2. Confidentiality

Confidentiality means keeping users' data secret in the Cloud systems. The confidentiality in Cloud systems is a big obstacle for users to step into it. There are two basic approaches (i.e., physical isolation and cryptography) to achieve such confidentiality, which are extensively adopted by the Cloud Computing vendors[7]. The Cloud system offerings (e.g., data, services) are transmitted through public networks. There is no physical isolation could be achieved. Alternatively, Virtual Local Area Networks, and network middle boxes (e.g. firewalls, packet filters) should be deployed to achieve the virtual physical isolation [7]. Encrypted storage is another choice to enhance the confidentiality. For example, encrypting data before placing it in a Cloud may be even more secure than unencrypted data in a local data center.

3. Data Integrity

Data integrity in the Cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users). As data is the base for providing Cloud Computing services, such as Data as a Services, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task. The challenges for data integrity associated with data storage in the Cloud Computing system are as follows. Firstly, in terms of the current development of state for hard disk drivers (or solid state disks or tapes), their capacity increases are not keeping pace with the data growth [3]. Therefore, to scale up the data storage in the Cloud Computing systems, vendors need to increase the population of hard drives (or solid state disks or tapes). Secondly, disk drives (or solid state disks)are getting bigger and bigger in terms of their capacity, while not getting much faster in terms of data access.

4. Control

Control in the Cloud system means to regulate the use of the system, including the applications, its infrastructure and the data. Cloud computing system always involves distributed computation on multiple large scale data sets across a large number of computer nodes. Even more, every Internet user is able to contribute his or her individual data to the Cloud Computer systems which are located on the other side of the Internet, and make use of them. Hence, efficient and effective control over the data access in the Cloud Computing system

and regulate the behaviors of the applications (services) hosted on the Cloud Computing systems will enhance the security of systems.[9]

5. Audit

Audit means to watch what happened in the Cloud system. Audit ability could be added as an additional layer above the virtualized operation system (or virtualized application environment) hosted on the virtual machine to provide facilities watching what happened in the system. It is much more secure than that is built into the applications or into the software themselves, since it is able watch the entire access duration. For such kind of scenarios, three main attributes should be audited: Events, Logs and Monitoring. Such a new feature (i.e., audit ability added as an additional layer in the virtual operation systems) reinforces the Cloud Computing developers to focus on providing virtualized capabilities instead of specific hardware to being provided.[9]

Conclusion

Cloud computing is revolutionizing how information technology resources and services are used and managed, but the revolution always comes with new problem. Cloud computing has approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security , privacy and legal issues.
Further research under the Security issues and solution in cloud computing.

REFERENCE

[1] Mell P,Grance T(2009) Draft NIST working definition of cloud Computing http://csrc.nist.gov/groups/SNS/cloud - computing/index.html.
[2] Cyril Onwubiko "Security Issues to cloud computing"
[3] Mythry Vuyyuru,Pulipati Annapurna,"Cloud Computing Technolgy"-International journal of Soft Computing and Engineering.
[4] Introduction to cloud computing "Dialogic"
[5] Alexa Huth and james csbula "The Basics of cloud computing"
[6] "Cloud Computing" Lucid White paper.
[7] Zhou M.Zhang R. Xie W, Qian W, "Security and privacy in Cloud Computing :A Survey",2010,Sixth International Conference on semantics,Knowledge and grids.2010 IEEE,pp.105-112
[8] International Journal Of Engineering And Computer Science IISSN:2319-7242"Security issues and resource planning in cloud computing"
[9] Tharam Dillon, Chen Wu, Elizabeth Chang, 2010 24th IEEE International Conference on Advanced Information Networking and Applications ,"Cloud computing: issues and challenges".
[10] Bardin J., "Security Guidance for Critical Areas of Focus in CloudComputing,"www.cloudsecurityalliance.org/ guidance/csaguide.pdf, 2009.

