'Cloud computing' - Scenarios and the concerned issues

*Ms. Sumati, **Jatinder Pal Singh
Assistant Professor, Department of Computer Science, PCTE, Ludhiana
sumati_927@yahoo.co.in, jatinderpalsingh@live.com

Abstract

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth.

As a result, cloud computing has the potential to upend the software industry entirely, as applications are purchased, licensed and run over the network instead of a user's desktop. This shift will put data centers and their administrators at the center of the distributed network, as processing power, electricity, bandwidth and storage are all managed remotely. It affects not only business models, but the underlying architecture of how we develop, deploy, run and deliver applications.

In this paper, we are going to discuss about the concept of cloud computing, service models, what are the various ways in which it can be deployed, the scenarios in which one can use this technology and the issues that need to be taken care in such scenarios are discussed.

Key terms: Service Level Agreement (SLA), Virtual Machine (VM), Application Programming Interface (API).

1. INTRODUCTION

Cloud computing is a resource delivery and usage model; it means get resource via network. The network of providing resource is called 'Cloud'. New advances in processors, virtualization technology, distributed storage, broadband Internet access, automated management and fast, inexpensive servers have all combined to make cloud computing a compelling paradigm. This vast process power is usually got with distributed, large-scale server cluster and server virtualization software.

A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic -- a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider.

2. CLOUD COMPUTING: DEFINED

Cloud computing refers to the delivery of computing and storage capacity as a service to a heterogeneous community of end-recipients through web-based tools and applications. The name comes from the use of clouds as an abstraction for the complex infrastructure it contains.

3. SERVICE MODELS

Cloud computing providers offer their services according to three fundamental models:

Software as a Service (SaaS): The consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it's running.

Platform as a Service (PaaS): The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment but does not control the software, hardware or network infrastructure on which they are running.

Infrastructure as a Service (IaaS): The consumer uses "fundamental computing resources" such as processing power, storage, networking components or middleware. The consumer can control the operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them.

4. DEPLOYMENT MODELS

Public Cloud: Public cloud services are characterized as being available to clients from a third party service provider via the Internet. Public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions.

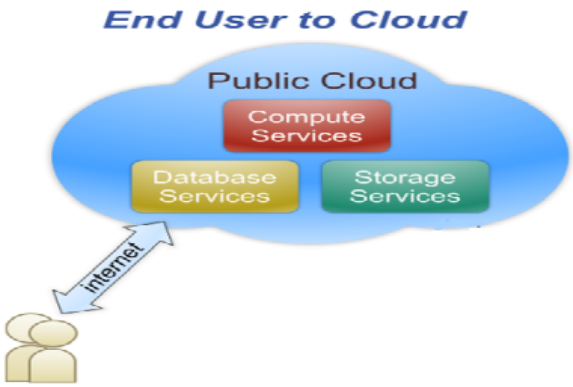
Private Cloud: A private cloud is that in which, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and designated.

Community Cloud: A community cloud is controlled and used by a group of organizations that have shared interests, such as specific security requirements or a common mission. The members of the community share access to the data and applications in the cloud.

Hybrid Cloud: A hybrid cloud is a combination of a public and private cloud that interoperates. In this model users typically outsource no business-critical information and processing to the public cloud, while keeping business-critical services and data in their control.

5. SCENARIOS WHERE CLOUD COMPUTING CAN BE USED

The Cloud usage scenarios are intended to illustrate the most typical cloud scenarios and are not meant to be an exhaustive list of realizations within a cloud environment.

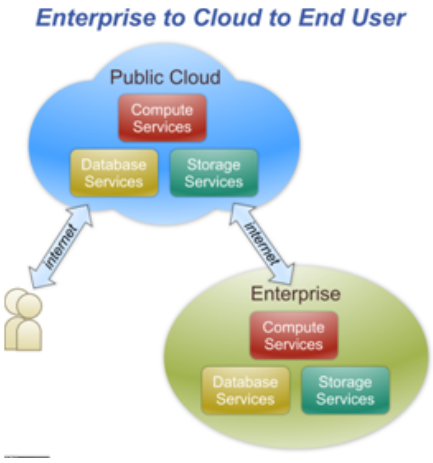


5.1 End User to Cloud: In this scenario, an end user is accessing data or applications in the cloud. Common applications of this type include email hosting and social networking sites. A user accesses the application and their data through any browser on any device. The user doesn't want to keep up with anything more than a password; their data is stored and managed in the cloud.

5.1.1 Concerned issues

• **Identity**: The cloud service must authenticate the end user.
• An **open client**: Access to the cloud service should not require a particular platform or technology.
• **SLAs**: Although service level agreements for end users will usually be simpler, cloud vendors must be clear about what guarantees of service they provide.

5.2 Enterprise to Cloud to End User: In this scenario, an enterprise is using the cloud to deliver data and services to the end user. When the end user interacts with the enterprise, the enterprise accesses the cloud to retrieve data and / or manipulate it, sending the results to the end user. The end user can be someone within the enterprise or an external customer.



5.2.1 Concerned issues

• An **open client**: Access to the cloud service should not require a particular platform or technology.

• **Federated identity**: In addition to basic identity needed by an end user, an enterprise user is likely to have an identity with the enterprise. The idea is that the enterprise user manages a single ID, with an infrastructure federating other identities that might be required by cloud services.

• **Metering and monitoring**: All cloud services must be metered and monitored for cost control, charge backs and provisioning.

• **Management and Governance**: Public cloud providers make it very easy to open an account and begin using cloud services; that ease of use creates the risk that individuals in an enterprise will use cloud services on their own initiative. Management of VMs and of cloud services such as storage, databases and message queues is needed to track what services are used. Governance is crucial to ensure that policies and government regulations are followed wherever cloud computing is used.

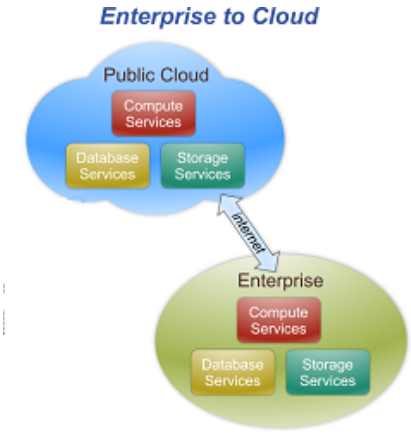
• A **Common Format for VMs**: A VM created for one cloud vendor's platform should be portable to another vendor's platform. Any solution to this requirement must account for differences in the ways cloud vendors attach storage to virtual machines.

• **Common APIs for Cloud Storage and Middleware**: Common APIs are required for access to cloud storage services, cloud databases, and other cloud middleware services such as message queues. Writing custom code that works only for a particular vendor's cloud service locks the

enterprise into that vendor's system and eliminates some of the financial benefits and flexibility that cloud computing provides.

• **SLAs and Benchmarks**: In addition to the basic SLAs required by end users, enterprises who sign contracts based on SLAs will need a standard way of benchmarking performance. There must be an unambiguous way of defining what a cloud provider will deliver, and there must be an unambiguous way of measuring what was actually delivered.

• **Lifecycle Management**: Enterprises must be able to manage the lifecycle of applications and documents. This requirement includes versioning of applications and the retention and destruction of data. There are substantial legal liabilities if certain data is no longer available. In some cases an enterprise will want to make sure data is destroyed at some point.



5.3 Enterprise to Cloud: This scenario involves an enterprise using cloud services for its internal processes. This might be the most common scenario in the early stages of cloud computing because it gives the enterprise the most control. In this scenario, the enterprise uses cloud services to supplement the resources it needs, like:

• For backups or storage of seldom-used data

• Virtual machines in the cloud to bring additional processors online to handle peak loads

• Applications in the cloud (SaaS) for certain enterprise functions

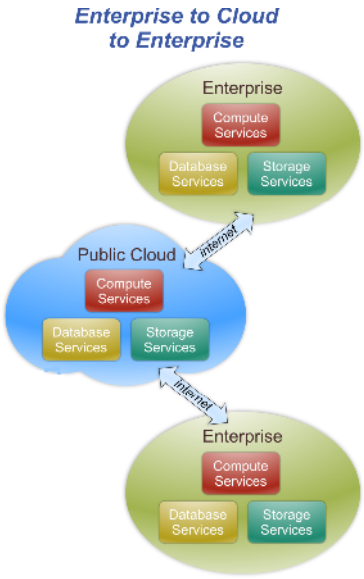
• Cloud databases as part of an application's processing. This could be extremely useful for sharing that database with partners, government agencies, etc.

5.3.1 Concerned issues

The basic requirements of the Enterprise to Cloud scenario are much the same as those for the Enterprise to Cloud to End User. Additional requirements for this are:

• **Deployment**: It should be simple to build a VM image and deploy it to the cloud as necessary. When that VM image is built, it should be possible to move that image from one cloud provider to another, compensating for the different mechanisms vendors have for attaching storage to VMs.

• **Industry-specific standards and protocols**: Many cloud computing solutions between enterprises will use existing standards. The applicable standards will vary from one application to the other and from one industry to the other.



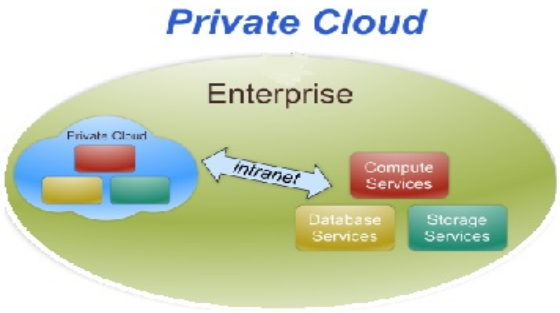
5.4 Enterprise to Cloud to Enterprise: This scenario involves two enterprises using the same cloud. The focus here is hosting resources in the cloud so that applications from the enterprises can interoperate. A supply chain is the most obvious example for this scenario.

5.4.1 Concerned issues

The basic requirements of the Enterprise to Cloud to Enterprise scenario are much the same as those for the Enterprise to Cloud scenario. Other requirements for this scenario are:

• **Transactions and concurrency**: For applications and data shared by different enterprises, transactions and concurrency are vital. If two enterprises are using the same cloud-hosted application, VM, middleware or storage, it's important that any changes made by either enterprise are done reliably.

• **Interoperability**: Because more than one enterprise is involved, interoperability between the enterprises is essential.



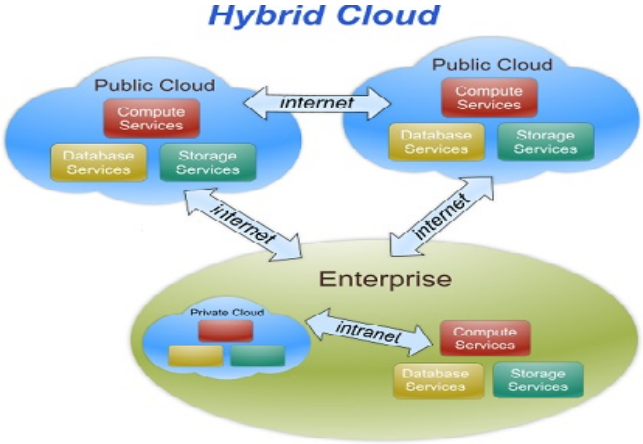
5.5 Private Cloud: The Private Cloud scenario is different from the others in that the cloud is contained within the enterprise. This is useful for larger enterprises. For example, if the payroll department has a surge in workload on the 15th and 30th of each month, they need enough computing power to handle the maximum workload, even though their everyday workload for the rest of the month is much lower.

With a private cloud, computing power is spread across the enterprise. The payroll department gets extra cycles when they need it and other departments get extra cycles when they need it. This can deliver significant savings across the enterprise.

5.5.1 Concerned issues

The basic requirements of the Private Cloud scenario are an open client, metering and monitoring, management and governance, deployment, interoperability, a common VM format, and SLAs. Keeping the cloud inside the enterprise removes many of the requirements for identity management, standards and common APIs.

5.6 Hybrid Cloud: This scenario involves multiple clouds working together, including both



public and private clouds. A hybrid cloud can be delivered by a federated cloud provider that

combines its own resources with those of other providers. The provider of the hybrid cloud must manage cloud resources based on the consumer's terms.

5.6.1 Concerned issues

All of the requirements of the previous scenarios apply here.

• **SLAs:** A machine readable, standard format for expressing an SLA. This allows the hybrid cloud provider to select resources according to the consumer's terms without human intervention.

6. CONCLUSION

When your business grows, your IT needs grow too. The scalability and speed of deployment offered by cloud computing means you can expand your IT provision instantly to meet increased requirements, and you can also scale it down again whenever you want. Waste of both time and resources is reduced, allowing you to effectively do more with less. This provides you a more efficient IT model, available on demand.

For an end user, cloud computing allows you to store, retrieve and use your data anytime and anywhere with the help of a device connected to an internet. Some of the important uses are: no need to buy resources, no need of space for these resources, and easy to move along with your resources.

7. REFERENCES:

"The NIST Definition of Cloud Computing". National Institute of Science and Technology. Retrieved 24 July 2011.

"Defining "Cloud Services" and "Cloud Computing"". IDC. 2008-09-23. Retrieved 2010-08-22.

Haff, Gordon (2009-01-27). "Just don't call them private clouds". CNET News. Retrieved 2010-08-22.

Voorsluys, William; Broberg, James; Buyya, Rajkumar (February 2011). "Introduction to Cloud Computing".

R. Buyya, J. Broberg, A.Goscinski. Cloud Computing: Principles and Paradigms. New York, USA: Wiley Press.

http://www.wikinvest.com/concept/Cloud_Computing

http://opencloudmanifesto.org/Cloud_Computing

http://arstechnica.com/business/2009/11/the-cloud-a-short-introduction/

http://www.computerweekly.com/feature/A-history-of-cloud-computing