* **What is Cloud Computing ??**

While the world is getting confused with multiple definitions and concepts around cloud computing , it become imperative to understand how is cloud computing different to traditional computing world today.

**Cloud computing** solves this problem by using multiple computers connected via a digital network, as though they were one computer providing infrastructure , platform or applications as a service .Often, the services available are considered part of cloud computing.

* **Definition of cloud computing ::**

Cloud computing offers the ability to access software or information that can be delivered on-demand, over the internet, without the need to store it locally.

Cloud computing is the realization of the long-held firm of utility computing.

The “Cloud” is a metaphor for the internet, derived from a common representation in computer network drawings showing the internet as a cloud.

**Example :**

Consider electricity and telephony services. when we come home or go to the office, we plug into the electric outlet and get electricity as much and as long as we want without knowing how it is generated or who the supplier is.

Similarly for telephony, we plug in dial and talk as long as we want without knowing what kind of networks or service providers the conversation is traversing through.

**Characteristics of cloud computing ::**

1.The illusion of infinite resources.

2.Multi-tenancy(shared resources).

3.Scale on demand(scalability).

4.Elasticity

5.Self-provisioning of resources.

6.Pay-for-play(pay as you use/go)

7.High availability and on SLA(Service level agreement).

8.Geographically distributed data centers.

**1.The illusion of infinite resources.**

-Illusion of computing and storage resources.

-User do not require capacity planning and provisioning for own individual storage and computing infrastructure.

**2.Multi-tenancy(shared resources).**

-Cloud computing is based on a business model in which resources are shared at

-Network level

-Host level

-Application level.

-Multiple user use the same resources.

**3.Scale on demand(scalability).**

-Ability to scale to tens of thousands of systems.

-Ability to massively scale bandwidth and storage space.

-Batter than length sales-and-provosion process.

-Rapidly scale the computing capabilities up or down.

**4.Elasticity**

-Rapidly increase and decrease user’s computing resources as needed.

-Release resource for other uses when they are no longer require.

-Always elastically to maintain cost efficiencies.

-If anything, the cloud is flexible and scalable to suit your immediate business needs.

-You can quickly and easily add or remove users, software features, and other resources.

**5.Self-provisioning of resources.**

-Users can self-provision for additional resources like,

-Processing Capacity

-Software

-Storage

-Network

**6.Pay-for-play(pay as you use/go)**

-Pay only for what you use.

-Do not require any upfront investment reservation or major setup fees.

-Do not incur huge capital expenditure and operating expenditure.

-Capabilities are charged using a metered.

-Fee-for-service or advertising based billing model to promote optimization of resources use.

**7.High availability and on SLA(Service level agreement).**

-Gaurantee for 24\*7 availability.

-Most cloud providers have a SLA for uptime and refund mechanism if SLA isn’t meet.

**8.Geographically distributed data centers**

-To serve customers around the globe, data centers are at multiple geographical locations.

-This require because of,

* + Legal/regulatory concerns.
  + Geopolitical considerations
  + Load balancing
  + Network latency
  + Edge caching
  + And many more….

**Essential Challenges of Cloud Computing**

* Most security problems stem from:
  + Loss of control
  + Lack of trust (mechanisms)
  + Multi-tenancy
* These problems exist mainly in 3rd party management models
  + Self-managed clouds still have security issues, but not related to above

1. **Consumer’s loss of control**
   * Data, applications, resources are located with provider
   * User identity management is handled by the cloud
   * User access control rules, security policies and enforcement are managed by the cloud provider
   * Consumer relies on provider to ensure
     + Data security and privacy
     + Resource availability
     + Monitoring and repairing of services/resources
2. **Lack of Trust in the Cloud**
   * A brief deviation from the talk
     + Trusting a third party requires taking risks
     + Defining trust and risk : Opposite sides of the same coin (J. Camp)
   * People only trust when it pays (Economist’s view)
   * Need for trust arises only in risky situations
3. **Multi-tenancy Issues in the Cloud**
   * Conflict between tenants’ opposing goals
     + Tenants share a pool of resources and have opposing goals
   * How does multi-tenancy deal with conflict of interest?
     + Can tenants get along together and ‘play nicely’ ?
     + If they can’t, can we isolate them?
   * How to provide separation between tenants?
4. **Security Issues in the Cloud**
   * In theory, minimizing any of the issues would help:
   * Loss of Control
     + Take back control
       - Data and apps may still need to be on the cloud
       - But can they be managed in some way by the consumer?
   * Lack of trust
     + Increase trust (mechanisms)
       - Technology
       - Policy, regulation
       - Contracts (incentives): topic of a future talk
   * Multi-tenancy
     + Private cloud :Takes away the reasons to use a cloud in the first place
     + VPC: its still not a separate system
     + Strong separation
5. **Minimize Lack of Trust: Policy Language**
   * + Consumers have specific security needs but don’t have a say-so in how they are handled
     + What the heck is the provider doing for me?
     + Currently consumers cannot dictate their requirements to the provider (SLAs are one-sided)
   * Standard language to convey one’s policies and expectations
     + Agreed upon and upheld by both parties
     + Standard language for representing SLAs
     + Can be used in a intra-cloud environment to realize overarching security posture
   * Create policy language with the following characteristics:
     + Machine-understandable (or at least process able),
     + Easy to combine/merge and compare
     + Examples of policy statements are, “requires isolation between VMs”, “requires geographical isolation between VMs”, “requires physical separation between other communities/tenants that are in the same industry,” etc.
     + Need a validation tool to check that the policy created in the standard language correctly reflects the policy creator’s intentions (i.e. that the policy language is semantically equivalent to the user’s intentions).
6. **Minimize Lack of Trust: Certification**
   * Certification
     + Some form of reputable, independent, comparable assessment and description of security features and assurance
     + Sarbanes-Oxley, DIACAP, DISTCAP, etc (are they sufficient for a cloud environment?)
   * Risk assessment
     + Performed by certified third parties
     + Provides consumers with additional assurance
7. **Minimize Loss of Control in the Cloud**

* Monitoring
* Utilizing different clouds
* Access control management

**Issue with clued computing**

1. Privacy
2. Compliance
3. Performance
4. Legal
5. Open source
6. Open Standard
7. Security
8. Sustainability

**Cloud Computing Advantages**

### [Storage and Scalability](http://management.cloudcomputinginsights.com/t-performance/)

No more infrastructure investments or time spent adding new servers, partitioning silos – none of that mess. With the cloud, you basically have access to unlimited storage capability and scalability.

### [Backup and Disaster Recovery](http://security.cloudcomputinginsights.com/t-backup--recovery/)

Those days of tape back-up are long gone. Most cloud providers across service types and platforms offer comprehensive backup and recovery capabilities.

### [Mobility](http://infrastructure.cloudcomputinginsights.com/t-public-cloud/)

### Your cloud , anywhere. Whether it's your development platform, suite of office tools or custom content management system – cloud mobility enables access anywhere with a Web connection (just about).

### [Cost Efficiency](http://management.cloudcomputinginsights.com/t-cost/)

Aside from storage and infrastructure costs, just think about all the other costs you can minimize with cloud services – updating and managing software or applications, hiring and training new staff and even decreased on-site energy costs.

* **[Enable IT Innovation](http://www.cloudcomputinginsights.com/development)**

Probably the most understated benefit of the cloud – it is reshaping IT into a proactively innovative bunch that focuses a lot less on manual system administration, and a lot more on improving the technology. From integration, mobility to even user personalization, giving your IT the cloud can make their jobs much easier – and more enjoyable.

## Cloud Computing Disadvantages

### [Control and Reliability](http://www.cloudcomputinginsights.com/management)

The biggest fear of cloud computing is found in its major benefit – the ability to outsource the IT burden to a specialized vendor or provider. Sure it sounds great, but with a move to the cloud you do give up the in-house control of a traditional IT department.

### [Security, Privacy and Compliance](http://www.cloudcomputinginsights.com/security)

Security can also be a concern in the cloud, particularly if you manage confidential data like customer information. Compliance in the cloud may also become an issue, which may require deploying a private cloud if you do have to secure private data.

### [Compatibility](http://www.cloudcomputinginsights.com/development)

Making sure every existing tool, software and computer is compatible with the Web based service, platform or infrastructure. While on-site IT may have a little more control in managing integration and compatibility, it is often "what you see is what you get" in the cloud.

* [**Unpredicted Costs**](http://management.cloudcomputinginsights.com/t-cost/)

Sure, the cloud can substantially reduce staff and hardware costs, but the price could end up being more than you bargained for. Migrating to the cloud is also an understated cost, and making sure the current systems that support your business while moving to the cloud could raise operating costs substantially.

* [**Contracts and Lock-Ins**](http://management.cloudcomputinginsights.com/t-slas/)

Traditional IT could be downsized, upsized, contracted-in and otherwise controlled by you. On-site hardware, software, infrastructure and platforms always carried some obligations, but now the cloud service provider, for the most part, has all the decision power.

* **Write note on a Cloud Deployment Models? (6/7 Marks)**

**Ans :**

“**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.”**

# Types of Cloud Computing :

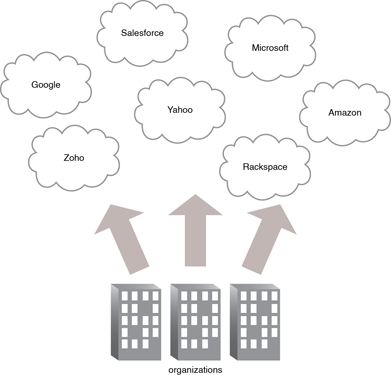
A cloud deployment model represents a specific type of cloud environment, primarily distinguished by ownership, size, and access.There are four common cloud deployment models:

* [Public Clouds](http://whatiscloud.com/cloud_deployment_models/public_clouds)
* [Community Clouds](http://whatiscloud.com/cloud_deployment_models/community_clouds)
* [Private Clouds](http://whatiscloud.com/cloud_deployment_models/private_clouds)
* [Hybrid Clouds](http://whatiscloud.com/cloud_deployment_models/hybrid_clouds)

## Public Clouds

A *public cloud* is a publicly accessible cloud environment owned by a third-party cloud provider. The IT resources on public clouds are usually provisioned via the previously described cloud delivery models and are generally offered to cloud consumers at a cost or are commercialized via other avenues (such as advertisement).

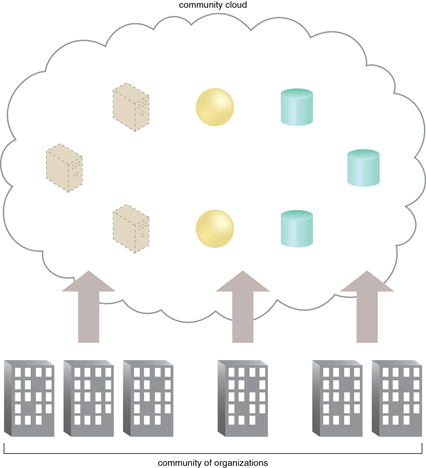
The cloud provider is responsible for the creation and on-going maintenance of the public cloud and its IT resources. Many of the scenarios and architectures explored in upcoming chapters involve public clouds and the relationship between the providers and consumers of IT resources via public clouds.



## Community Clouds

A community cloud is similar to a public cloud except that its access is limited to a specific community of cloud consumers. The community cloud may be jointly owned by the community members or by a third-party cloud provider that provisions a public cloud with limited access. The member cloud consumers of the community typically share the responsibility for defining and evolving the community cloud (Figure 1).

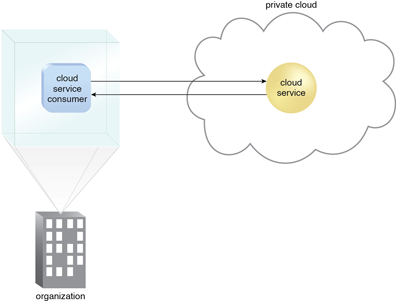
Membership in the community does not necessarily guarantee access to or control of all the cloud's IT resources. Parties outside the community are generally not granted access unless allowed by the community.



## Private Clouds

A private cloud is owned by a single organization. Private clouds enable an organization to use cloud computing technology as a means of centralizing access to IT resources by different parts, locations, or departments of the organization. When a private cloud exists as a controlled environment, the problems described in the Risks and Challenges section do not tend to apply.

The use of a private cloud can change how organizational and trust boundaries are defined and applied. The actual administration of a private cloud environment may be carried out by internal or outsourced staff.



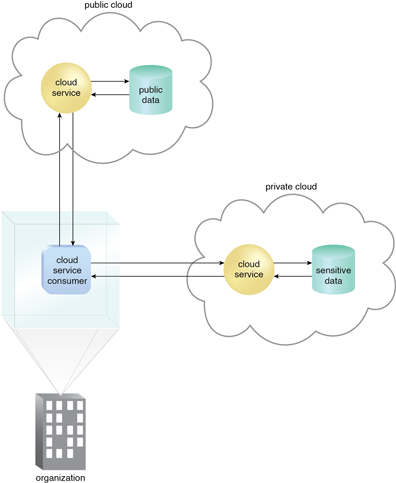
With a private cloud, the same organization is technically both the cloud consumer and cloud provider. In order to differentiate these roles:

* a separate organizational department typically assumes the responsibility for provisioning the cloud (and therefore assumes the cloud provider role)
* departments requiring access to the private cloud assume the cloud consumer role

It is important to use the terms "on-premise" and "cloud-based" correctly within the context of a private cloud. Even though the private cloud may physically reside on the organization's premises, IT resources it hosts are still considered "cloud-based" as long as they are made remotely accessible to cloud consumers. IT resources hosted outside of the private cloud by the departments acting as cloud consumers are therefore considered "on-premise" in relation to the private cloud-based IT resources.

## Hybrid Clouds

A hybrid cloud is a cloud environment comprised of two or more different cloud deployment models. For example, a cloud consumer may choose to deploy cloud services processing sensitive data to a private cloud and other, less sensitive cloud services to a public cloud. The result of this combination is a hybrid deployment model (Figure 1).



Hybrid deployment architectures can be complex and challenging to create and maintain due to the potential disparity in cloud environments and the fact that management responsibilities are typically split between the private cloud provider organization and the public cloud provider.

**Types of Cloud Computing**

* Grid Computing
* Computational Grid
* Data Grid
* Middleware Grid
* Cluster computing
* Distributed Computing
* Parallel Computing
* Utility Computing
* Cloud Computing