Unit-3
Introduction to cloud

- Introduction to Cloud Computing
- History and Evolution of Cloud Computing
- Types of clouds
  - Private clouds
  - Public clouds
  - Hybrid clouds
- Cloud Computing architecture
- Cloud computing infrastructure
- Merits of Cloud computing
- Cloud computing delivery models
  - IaaS
  - PaaS
  - SaaS
- Obstacles for cloud technology
- Cloud vulnerabilities
- Cloud challenges
- Practical applications of cloud computing.

History of Cloud Computing

When we think of cloud computing, we think of situations, products and ideas that started in the 21st century. This is not exactly the whole truth. Cloud concepts have existed for many years. Here, I will take you back to that time.

It was a gradual evolution that started in the 1950s with mainframe computing.

Multiple users were capable of accessing a central computer through dumb terminals, whose only function was to provide access to the mainframe. Because of the costs to buy and maintain mainframe computers, it was not practical for an organization to buy and maintain one for every employee. Nor did the typical user need the large (at the time) storage capacity and processing power that a mainframe provided. Providing shared access to a single resource was the solution that made economical sense for this sophisticated piece of technology

After some time, around 1970, the concept of virtual machines (VMs) was created.

Using virtualization software like VMware, it became possible to execute one or more operating systems simultaneously in an isolated environment. Complete computers (virtual) could be executed inside one physical hardware which in turn can run a completely different operating system.

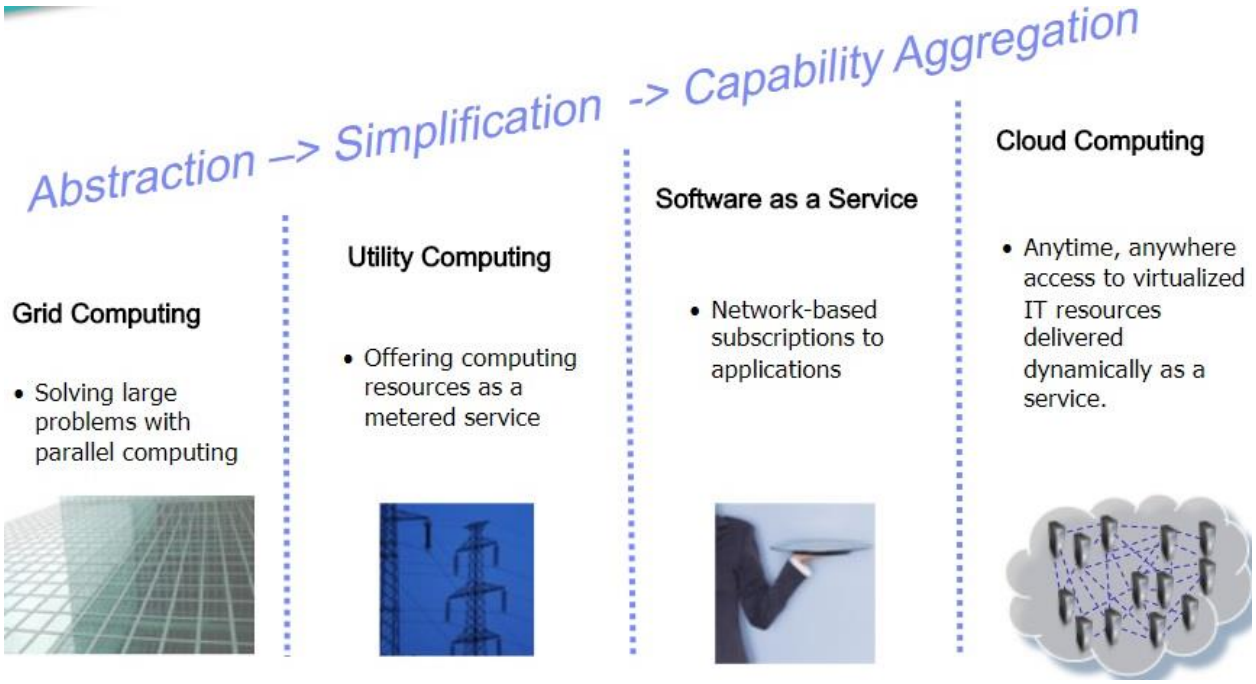
The VM operating system took the 1950s' shared access mainframe to the next level, permitting multiple distinct computing environments to reside on one physical environment. Virtualization came to drive the technology, and was an important catalyst in the communication and information evolution.

In the 1990s, telecommunications companies started offering virtualized private network connections.

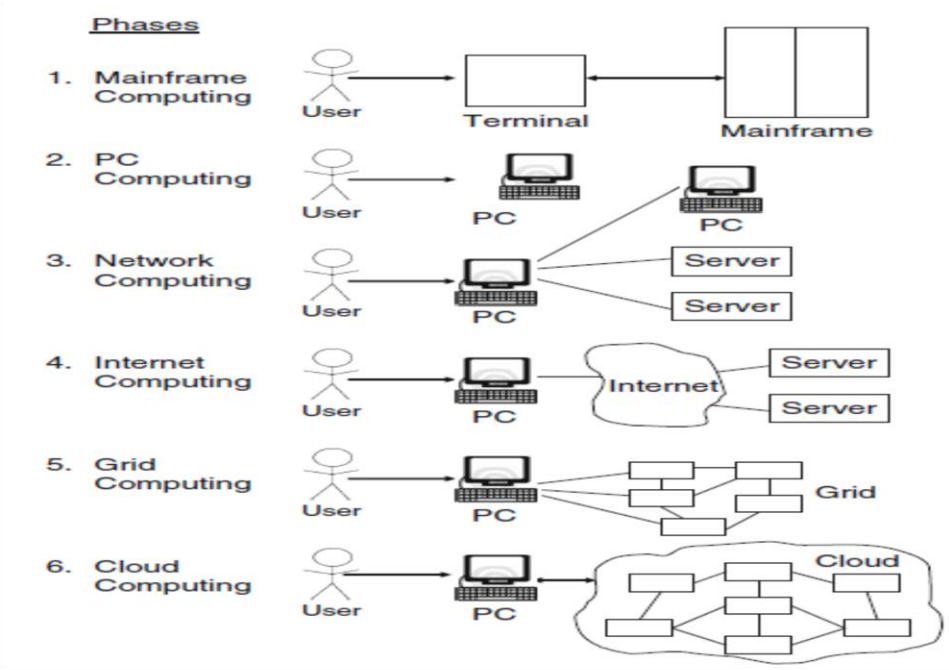
Historically, telecommunications companies only offered single dedicated point–to-point data connections. The newly offered virtualized private network connections had the same service quality as their dedicated services at a reduced cost. Instead of building out physical infrastructure to allow for more users to have their own connections, telecommunications companies were now able to provide users with shared access to the same physical infrastructure.

The following list briefly explains the evolution of cloud computing:

- Grid computing: Solving large problems with parallel computing
- Utility computing: Offering computing resources as a metered service
- SaaS: Network-based subscriptions to applications
- Cloud computing: Anytime, anywhere access to IT resources delivered dynamically as a service



Six Computing Paradigms



Source: HandBook of Cloud Computing by B. Furht and A Escalante

Evolution of Cloud Computing

- Cloud computing is a process that entails accessing of services, including, storage, applications and servers through the Internet, making use of another company's remote services for a fee. This enables a company to store and access data or programs virtually, i.e. in a cloud, rather than on local hard drives or servers.

- Cloud computing has its roots as far back in 1950s when mainframe computers came into existence. At that time, several users accessed the central computer via dummy terminals. The only task these dummy terminals could perform was to enable users access the mainframe computer. The prohibitive costs of this mainframe devices did not make them economically feasible for organizations to buy them. That was the time when the idea of provision of shared access to a single computer occurred to the companies to save costs.

- In 1970s, IBM came out with an operating system (OS) named VM. This allowed for simultaneous operation of more than one OS. Guest Operating Systems could be run on every VM, with their own memory and other infrastructure, making it possible to share these resources. This caused the concept of virtualization in computing to gain popularity.

- The 1990s witnessed telecom operators begin offering virtualized private network connections, whose quality of service was as good as those of point-to-point (dedicated) services at a lesser cost. This paved way for telecom companies' to offer many users shared access to a single physical infrastructure.

- The other catalysts were grid computing, which allowed major issues to be addressed via parallel computing; utility computing facilitated computing resources to be offered as a metered service and SaaS allowed subscriptions, which were network-based, to applications. Cloud computing, therefore, owes its emergence to all these factors.

Grid Computing

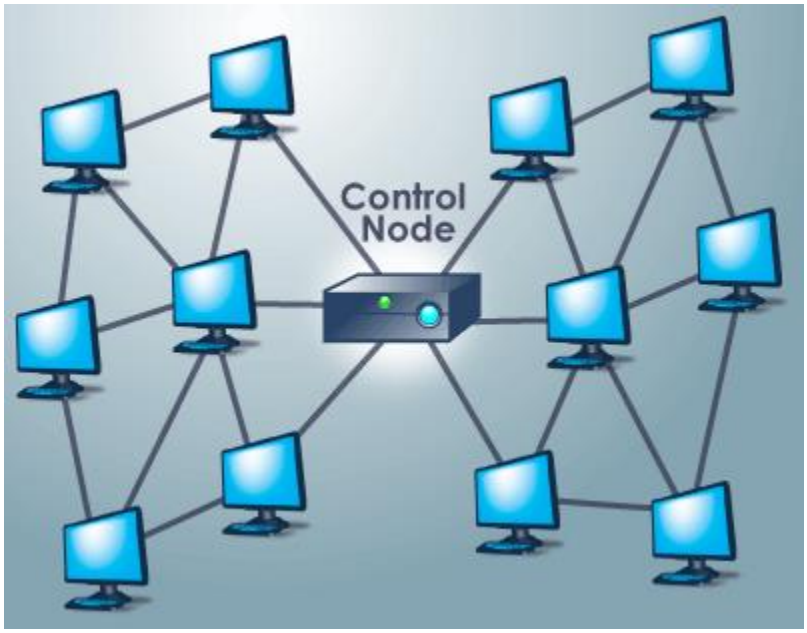
Grid computing is the collection of computer resources from multiple locations to reach a common goal. The grid can be thought of as a distributed system with non-interactive workloads that involve a large number of files. Grid computing is distinguished from conventional high-performance computing systems such as cluster computing in that grid computers have each node set to perform a different task/application.

Why Grid Computing?

- 40% Mainframes are idle

- 90% UNIX servers are idle

- 0-15% Mainframes are idle in peak hour
- 70% PC servers are idle in peak hour



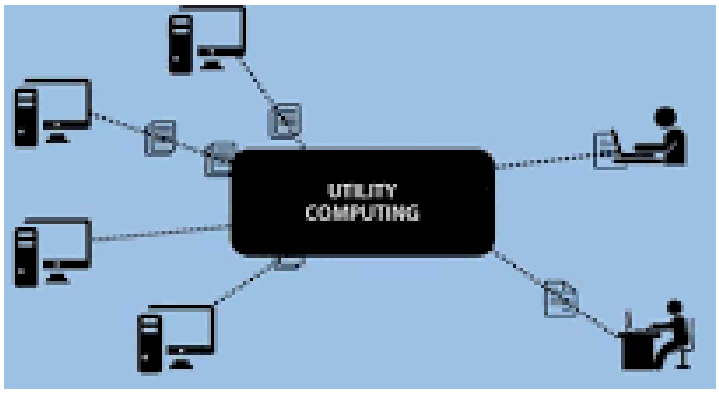
Utility Computing

Utility computing, or The Computer Utility, is a service provisioning model in which a service provider makes computing resources and infrastructure management available to the customer as needed, and charges them for specific usage rather than a flat rate.

IBM, HP and Microsoft were early leaders in the new field of utility computing, with their business units and researchers working on the architecture, payment and development challenges of the new computing model. Google, Amazon and others started to take the lead in 2008, as they established their own utility services for computing, storage and applications.

Why Utility Computing?

Utility computing helps eliminate data redundancy, as huge volumes of data are distributed across multiple servers or backend systems. The client however, can access the data anytime and from anywhere.



Software as a service

Software as a service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software". It is typically accessed by users using a thin client via a web browser.

SaaS has become a common delivery model for many business applications, including office software, messaging software, payroll processing software, DBMS software, management software, customer relationship management (CRM), Management Information Systems (MIS), enterprise resource planning (ERP), etc,

Why Software as a Service?

Software as a service is an alternative to the standard software installation in the business environment (traditional model) where a user has to build the server, install the application and configure it.

In SaaS, the user does not pay for the software itself. Instead, it works like a rental. They have the authorization to use it for a period of time and pay for the software that they are using.

Cloud Computing NIST Definition

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."

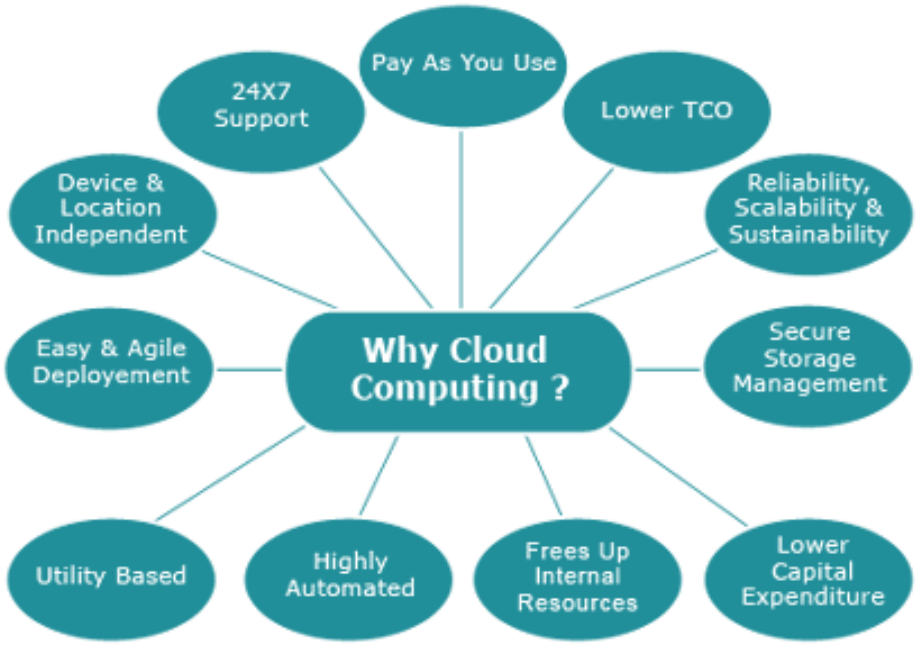
The NIST definition lists five essential characteristics of cloud computing:

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

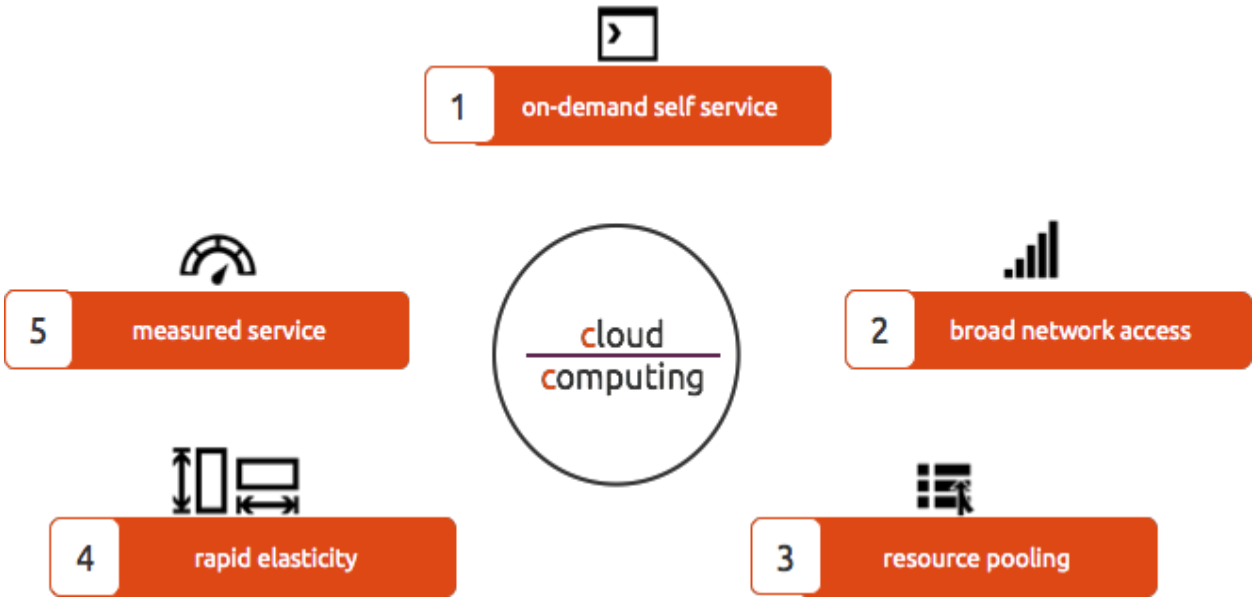
Why Cloud Computing?

Cloud computing is computing based on the internet. Where in the past, people would run applications or programs from software downloaded on a physical computer or server in their building, cloud computing allows people access to the same kinds of applications through the internet.

When you update your Facebook status, you're using cloud computing. Checking your bank balance on your phone? You're in the cloud again. Chances are you rely on cloud computing to solve the challenges faced by small businesses, whether you're firing off emails on the move or using a bunch of apps to help you manage your workload.



Five Essential Characteristics of Cloud computing



1. **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2. **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops and workstations).

3. **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacenter). Examples of resources include storage, processing, memory and network bandwidth.

4. **Rapid elasticity**: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

5. **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer.

Benefits of Cloud Computing

- **Flexibility**
- **Disaster Recovery**
- **Automatic Software Updates**
- **More Cost Efficiency**
- **Increased Collaboration**
- **Work from anywhere**
- **Security**
- **Competitiveness**
- **Environmental Friendly**

Flexibility

Cloud computing allows your employees to be more flexible – both in and out of the workplace. Employees can access files using web-enabled devices such as smartphones, laptops and notebooks. The ability to simultaneously share documents and other files over the Internet can also help support both internal and external collaboration. Many employers are now implementing “bring your own device (BYOD)” policies. In this way, cloud computing enables the use of mobile technology.

Disaster Recovery

Cloud disaster recovery (cloud DR) is a backup and restore strategy that involves storing and maintaining copies of electronic records in a cloud computing environment as a security measure. The goal of cloud DR is to provide an organisation with a way to recover data and/or implement failover in the event of a man-made or natural catastrophe.

Automatic Software Updates

Cloud suppliers do all the server maintenance required with cloud computing, including security updates. This frees up your employees, IT staff, and resources for other tasks

More Cost Efficiency

Cloud computing cuts out the high cost of hardware. You simply pay as you go and enjoy a subscription-based model. Most cloud services are paid on a subscription basis, so capital expenditure is reduced.

Increased Collaboration

When the project teams can access, edit and share documents anytime, from anywhere, they're able to do more together, and do it better. Cloud-based workflow and file sharing apps help them make updates in real time and gives them full visibility of their collaborations.

Work from anywhere

With cloud computing, if you have got an internet connection you can be at work. And with most serious cloud services offering mobile apps, you're not restricted by which device you've got to hand.

Security

According to Alert Logic's State of Cloud Security Report, on-premise server users actually suffer more security incidents than those of cloud service providers.

Competitiveness

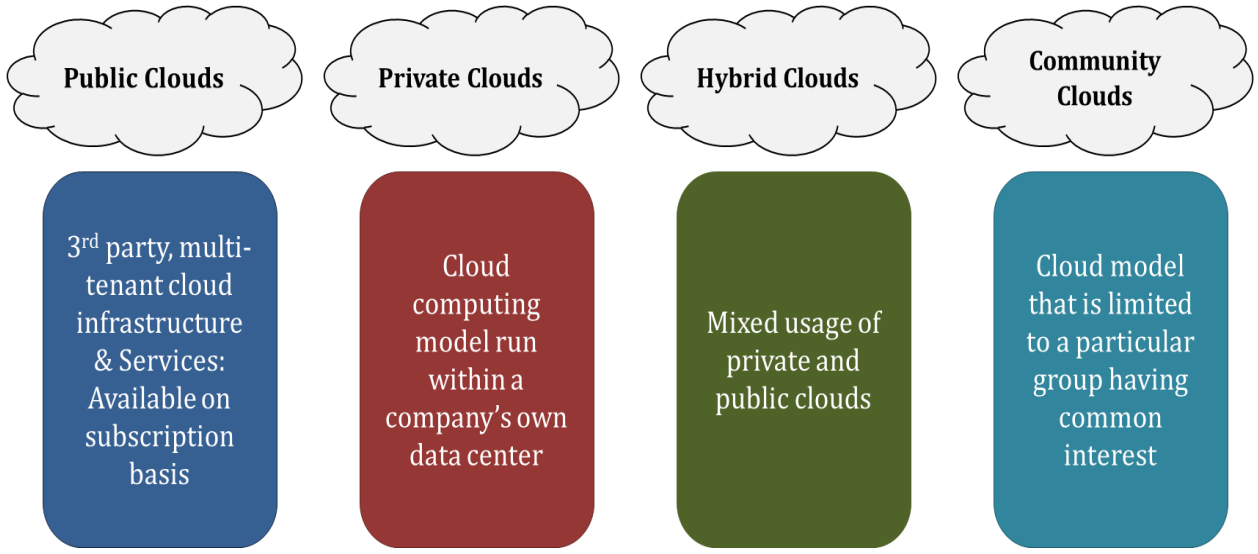
Wish there was a simple step you could take to become more competitive? Moving to the cloud gives access to enterprise-class technology, for everyone. It also allows smaller businesses to act faster than big, established competitors**.**

Environmental Friendly

The environment gets a little love too. When your cloud needs fluctuate, your server capacity scales up and down to fit. So you only use the energy you need and you don't leave oversized carbon footprints.

Cloud Deployment Models

The cloud deployment model specifies the location and management of a cloud's infrastructure. Based on the deployment, we can broadly classify cloud computing users into four categories - public cloud, private cloud, hybrid cloud and community cloud.



A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as virtual machines (VMs), applications or storage, available to the general public over the internet. Public cloud services may be free or offered on a pay-per-usage model.

Benefits of using a public cloud

- It reduces the need for organisations to invest in and maintain their own on-premise IT resources
- It enables scalability to meet workload and user demands
- There are fewer wasted resources because customers only pay for the resources they use.

Examples of public clouds include: Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.

- For users, these types of clouds will provide the best economies of scale, are inexpensive to set-up because hardware, application and bandwidth costs are covered by the provider. It's a pay-per-usage model and the only costs incurred are based on the capacity that is used.
- There are some limitations, however; the public cloud may not be the right fit for every organisation. The model can limit configuration, security, and SLA specificity, making it less-than-ideal for services using sensitive data that is subject to compliancy regulations.

Private Cloud

Private cloud is a type of cloud computing that delivers similar advantages to public cloud, including scalability and self-service, but through a proprietary architecture. Unlike public clouds, which deliver services to multiple organisations, a private cloud is dedicated to the needs and goals of a single organisation.

- Private clouds are data center architectures owned by a single company that provides flexibility, scalability, provisioning, automation and monitoring. The goal of a private cloud is not sell "as-a-service" offerings to external customers but instead to gain the benefits of cloud architecture without giving up the control of maintaining your own data center.
- Private clouds can be expensive with typically modest economies of scale. This is usually not an option for the average Small-to-Medium sized business and is most typically put to use by large enterprises. Private clouds are driven by concerns around security and compliance, and keeping assets within the firewall.

Examples of Private Clouds are VMware Vsphere/Vcenter, OpenStack, Citrix CloudStack, Eucalyptus, Microsoft System Center

Benefits of Private Cloud

- Dedicated hardware means increased security.
- The transition from physical to virtual servers leads to better flexibility.
- Fully utilize your hardware with better resource management.
- Virtual servers combined with a SAN allow for improved protection against disasters.
- Switching to private cloud computing will save you time and money.

Dedicated hardware means increased security.

- Much like a dedicated or colocated server, the security of your private cloud depends on a variety of factors. However, if you have the proper physical security, anti-virus software,

and firewall rules in place, you can rest assured your data as safe as if it were sitting right next to your desk. With a private cloud, you know where your servers are located and that the proper physical and network security is in place. You can meet and talk to those in charge of providing support for your hardware and come visit it if you like.

The transition from physical to virtual servers leads to better flexibility.

- This is one of the most alluring benefits of cloud computing. The ability to spin up and tear down a server in a matter of minutes is incredibly powerful and useful. No longer is there any wasted effort in trying to size a server beforehand when you can create a server on the fly. Need more disk space? More RAM? More CPU? No problem. With private cloud computing, you can reallocate resources in moments without worrying about finding a physical server that will have the resources your new server needs.

Fully utilize your hardware with better resource management.

- Virtualization significantly increases the value of your physical server hardware. Instead of having 5 servers that average 10% CPU utilization, you can virtualize the 5 servers on one physical server, sharing the resources. This decreases rack space, power usage, and is easier to manage. This also allows you to create copies of your servers and have them up and running very quickly, now that they have been virtualized. If you have the proper resource management tools installed on your server, you can automatically allocate the appropriate resources to a server when it needs it or turn off unused servers during low usage; an extraordinarily powerful and efficient way to manage your servers.

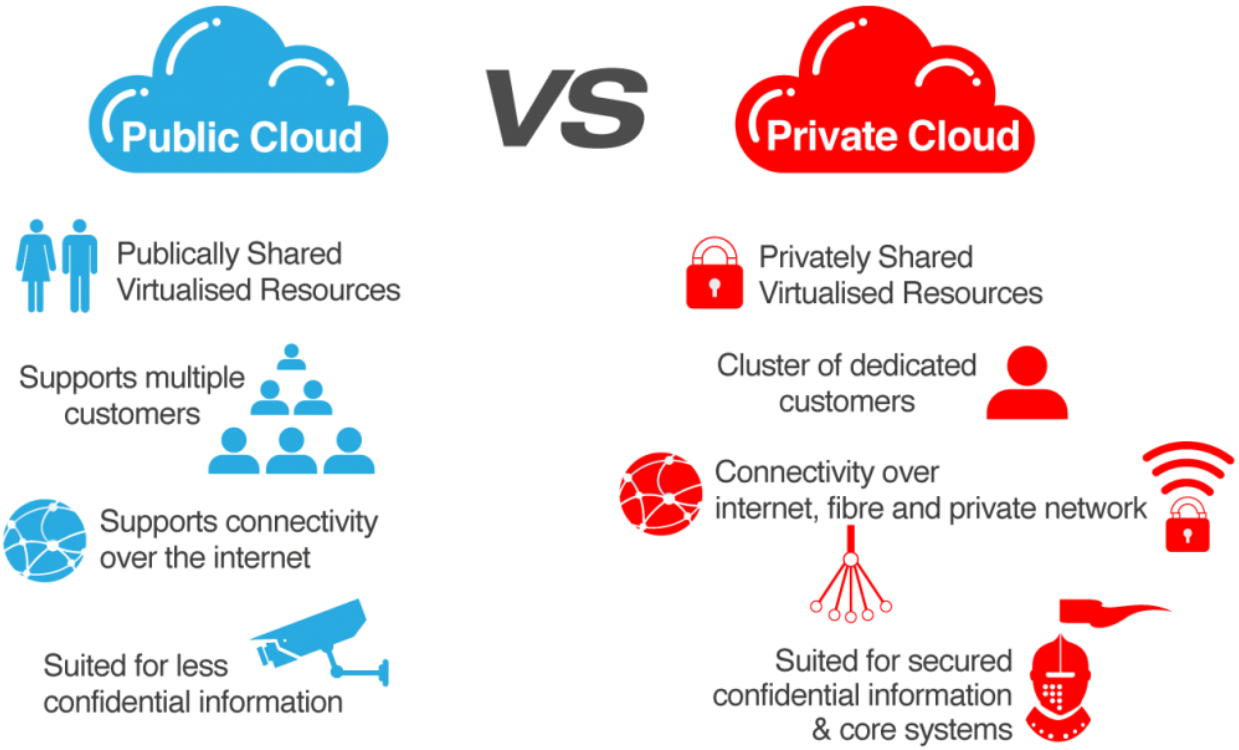
Virtual servers combined with a SAN allow for improved protection against disasters.

- When you connect a SAN to your private cloud, incredible redundancy can be achieved. Not only can you load balance between servers, automatically shifting server resources between servers on the fly, but in an N+1 environment (having at least 1 extra server than absolutely necessary), you can shut down one server without causing downtime. Imagine performing maintenance on your server like adding more RAM, replacing a hard drive, or upgrading software, without experiencing any downtime. When configured correctly you could power off one server and it would automatically shift the virtual servers over to an available server in your cloud. Taking your disaster protection up one level, you could have another SAN in another data center and perform SAN to SAN replication for a hot site DR environment capable of full recovery in less than 1 hour.

Switching to private cloud computing will save you time and money.

- The best part about a private cloud is that not only do you get all of the great benefits of virtualization and security, but it can be cheaper and less of a hassle then hosting your own servers or buying dedicated servers. If your company has more than 2 servers, it

could benefit from virtualization. If your company has more than 10 servers, it could benefit from private cloud computing with a dedicated SAN and multiple physical host servers. The public cloud revolutionized Information Technology forever; the private cloud brings the benefits to the masses.



Hybrid Cloud

Hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms. By allowing workloads to move between private and public clouds as computing needs and costs change, hybrid cloud gives businesses greater flexibility and more data deployment options.

For example, an enterprise can deploy an on-premises private cloud to host sensitive or critical workloads, but use a third-party public cloud provider, such as Google Compute Engine, to host less-critical resources, such as test and development workloads. To hold customer-facing archival and backup data, a hybrid cloud could also use Amazon Simple Storage Service (Amazon S3). A software layer, such as Eucalyptus, can facilitate private cloud connections to public clouds, such as Amazon Web Services (AWS).

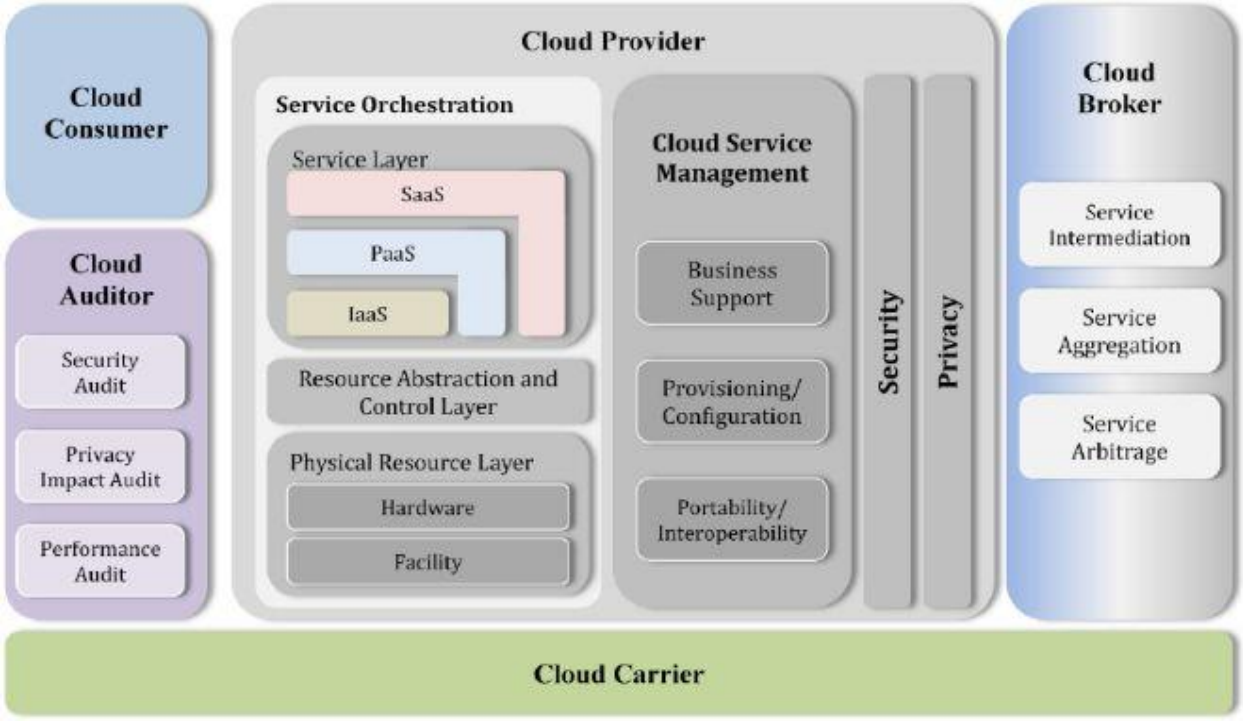
Community Cloud

A community cloud is a cloud service model that provides a cloud computing solution to a limited number of individuals or organizations that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider.

- Community clouds are a hybrid form of private clouds built and operated specifically for a targeted group. These communities have similar cloud requirements and their ultimate goal is to work together to achieve their business objectives.
- Community clouds are often designed for businesses and organizations working on joint projects, applications, or research, which requires a central cloud computing facility for building, managing and executing such projects, regardless of the solution rented.

Cloud Computing Architecture

The Overview of the Reference Architecture shown in below Figure describes five major actors with their roles & responsibilities using the newly developed Cloud Computing Taxonomy. The five major participating actors are the *Cloud Consumer, Cloud Provider, Cloud Broker, Cloud Auditor and Cloud Carrier*.



The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference.

Cloud Consumer

The cloud consumer is the principal stakeholder for the cloud computing service. A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service. The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly.

Cloud Provider

A cloud provider is a person, an organization; it is the entity responsible for making a service available to interested parties. A Cloud Provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the service

Cloud Auditor

A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through review of objective evidence. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.

Cloud Broker

As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage. A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly. A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.

Cloud Carrier

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers provide access to consumers through network, telecommunication and other access devices.

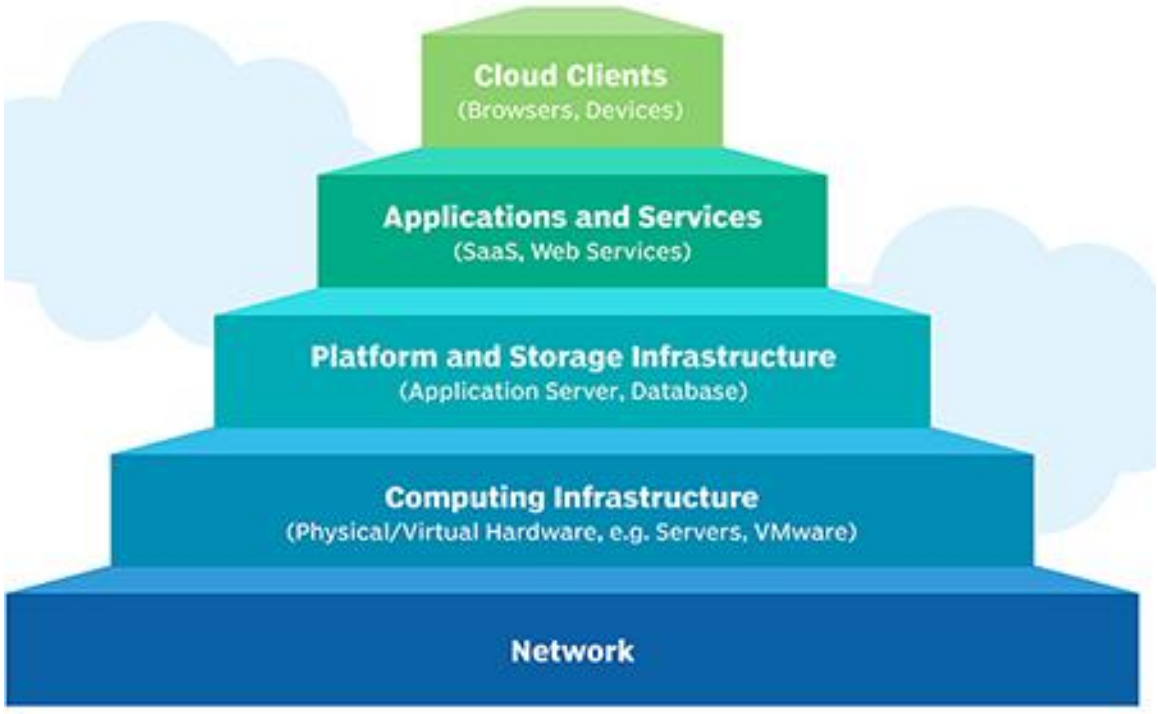
Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.

Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers.*
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Cloud Computing Infrastructure

Cloud infrastructure refers to the hardware and software components, such as servers, storage, a network and virtualization software that are needed to support the computing requirements of a cloud computing model.

Cloud infrastructure also includes an abstraction layer that virtualizes resources and logically presents them to users through application program interfaces and API-enabled command-line or graphical interfaces.



Merits of Cloud Computing

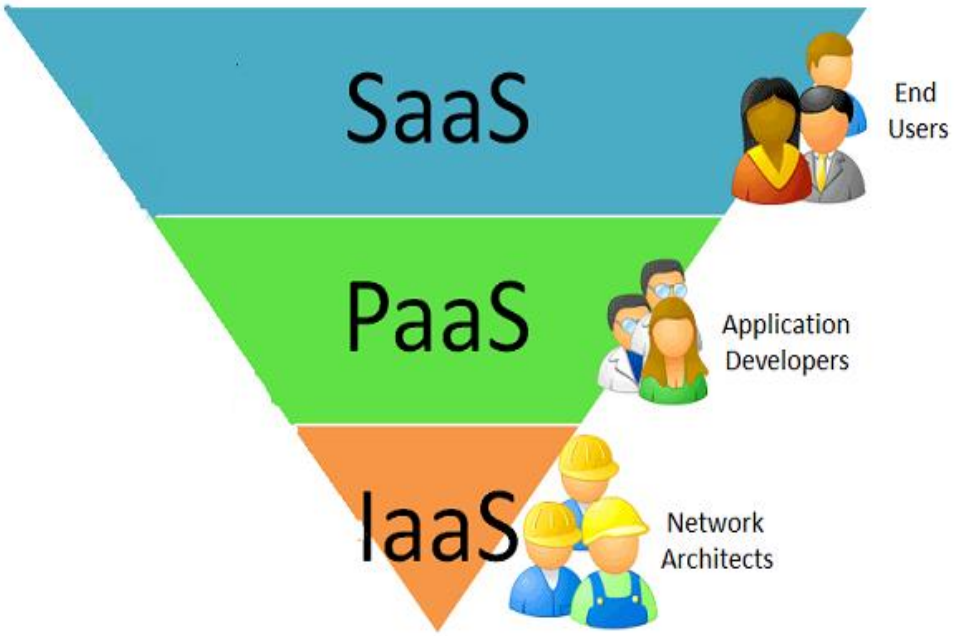
Cloud computing provides many benefits to its customers. Users can use applications on the cloud at any time and from anywhere.

Some of the major benefits of cloud computing are as follows:

- **Lower Cost**
- **Ease of Utilization**
- **Quality of Service**
- **Reliability**
- **Availability**
- **Outsourced IT management**
- **Simplified maintenance and upgrade**
- **Low barrier to entry**
- **Flexibility**
- **Return on Investment (ROI)**
- **Environmental-friendly computing**

Cloud Computing Delivery Models

Cloud delivery models are continuing to evolve as business drivers push more organizations towards a more globally distributed infrastructure. Many companies are actively moving parts of their environments into the cloud for more efficiency, agility and capabilities around growth. This is a major push which has helped data centers come to the forefront of the technological evolution and has allowed more organizations to leverage their services. Costs are coming down and the environments supporting the cloud are becoming more stable.



A *cloud delivery model* represents a specific, pre-packaged combination of IT resources offered by a cloud provider. Three common cloud delivery models have become widely established and formalized

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

Infrastructure-as-a-Service (IaaS)

Infrastructure as a Service (IaaS) is a way of delivering Cloud Computing infrastructure such as servers, storage, network and operating systems as an on-demand service. Rather than purchasing servers, software, datacenter space or network equipment, clients instead buy those resources as a fully outsourced service on demand

Characteristics of IaaS

IaaS is generally accepted to comply with the following;

- Resources are distributed as a service
- Allows for dynamic scaling
- Has a variable cost, usage based pricing model (pay per go and pay per use)
- Has multitenant architecture, includes multiple users on a single piece of hardware

- IaaS typically has enterprise grade infrastructure

Where IaaS Makes Sense

IaaS makes sense in a number of situations and these are closely related to the benefits that Cloud Computing bring. Situations that are particularly suitable for Cloud infrastructure include;

- Where demand is very volatile – any time there are significant spikes and troughs in terms of demand on the infrastructure
- For new organizations without the capital to invest in hardware
- Where the organization is growing rapidly and scaling hardware would be problematic
- Where there is pressure on the organization to limit capital expenditure and to move to operating expenditure
- For specific line of business, trial or temporary infrastructural needs

Where IaaS May Not be the Best Option

While IaaS provides massive advantages for situations where scalability and quick provisioning are beneficial, there are situations where its limitations may be problematic.

Examples of situations where we would advise caution with regards IaaS include;

- Where regulatory compliance makes the offshoring or outsourcing of data storage and processing difficult

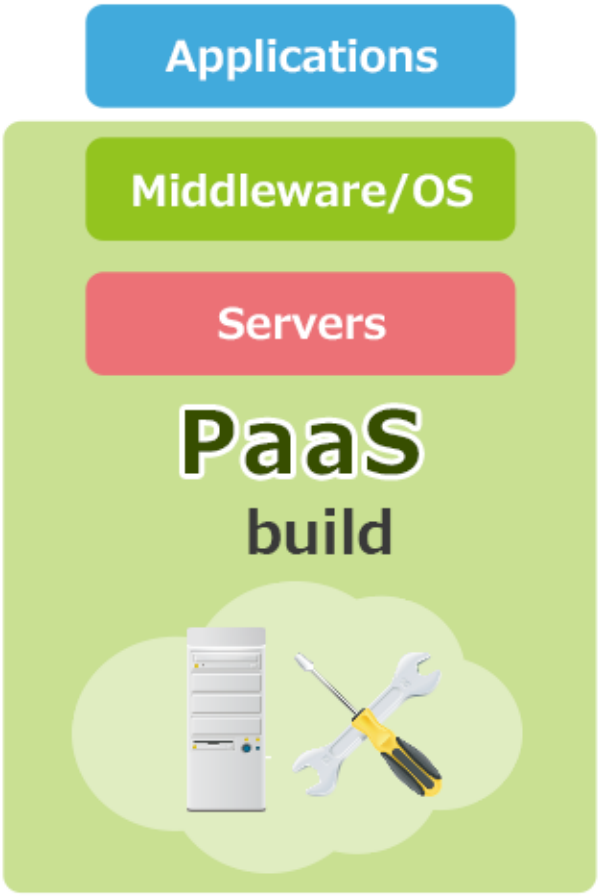
- Where the highest levels of performance are required, and on-premise or dedicated hosted infrastructure has the capacity to meet the organization’s needs

Leading IaaS vendors include:

- **Rackspace**
- **Verizon**
- **Amazon AWS**
- **Savvis**
- **GoGrid**
- **VMware vCloud**
- **Flexiscale**
- **Joyent IaaS**
- **Rightscale**
- **Eucalyptus**
- **BlueLock's IaaS**
- **Enomaly**
- **SoftLayer**
- **IBM Cloudburst**
- **Oracle Cloud Services**

Platform-as-a-Service (PaaS)

Platform as a service (PaaS) is a cloud computing model in which a third-party provider delivers hardware and software tools usually those needed for application development to users over the internet. A PaaS provider hosts the hardware and software on its own infrastructure. As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application.



Characteristics of PaaS

Key attributes of PaaS

1. **Multi-tenant architecture**

   Multi-tenant architecture is one of the key elements of PaaS model. A multi-tenant platform is one that uses common resources and a single instance of both the object code of an application as well as the underlying database to support multiple customers simultaneously. Although the technology stack in a multi-tenant deployment is shared, customers' user experience should be comparable to that of a customer using an application developed and managed by dedicated resources. The complexity of this delivery model presents a challenge to develop and deliver reliable, scalable, and secure applications where customer interactions and data are logically isolated from one another. However, multi-tenant deployment of an application leverages the economies of scale through the use of a limited set of computing resources, and lower associated deployment, upgrade, support and maintenance costs across a large number of customers. The multi-tenant architecture offers providers enhanced ability to mine aggregated data

and, in turn, respond faster to usage trends as well as to develop additional enhancements for users1 .

2. Customizable/Programmable User Interface

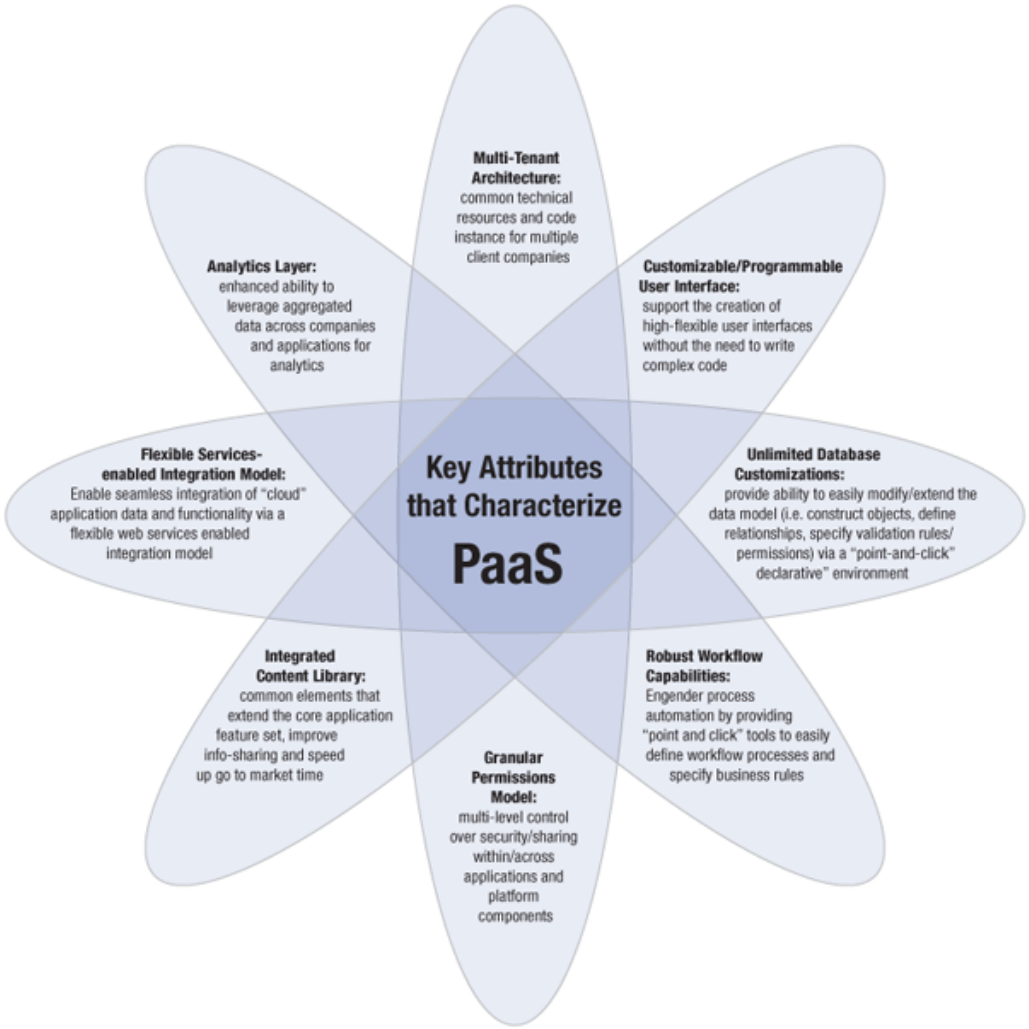
The PaaS offering should provide the ability to construct highly-flexible user interfaces via a simple "drag & drop" methodology which permits the creation and configuration of UI components on the fly. In order to jump start the construction of user interfaces/ displays, pre-defined standard UI components should be available that can be assembled in building-block fashion with minimal coding. For further customization of the UI which may be necessary to accommodate specific user requirements, there should be the option to easily leverage/invoke a tag library of other complementary, more sophisticated, re-usable UI components (i.e. grids, tree-like hierarchies, etc) through simple HTML code without the need of writing complex code. Furthermore given the growing set of internet-enabled web devices, additional flexibility to use other web technologies such as CSS, AJAX and Adobe Flex to specify the appearance of the application's interface should be available to the UI designer. The PaaS offering must afford UI designers/developers complete fine-grained control to shape the presentation of data to a specific context – for example: displaying the data in one format when viewed on a hand-held device and in another format when viewed in a desktop web browser. This "drag & drop" paradigm of constructing user interfaces, an essential capability of a robust PaaS offering provides UI designers/developers with better control over the appearance of the application's interface and permits the creation of new and sophisticated presentation layers quickly and easily without requiring much custom coding.

3. Unlimited Database Customizations

Data persistence is core to many applications and facilitating the creation, configuration and deployment of persistent objects without requiring programming expertise is a key characteristic of a powerful "cloud platform". Thus, the PaaS offering must support the construction of objects, the definition of relationships between the objects and the configuration of advanced data behavior all from within the comfort of the web browser via a "point and click' declarative paradigm. As opposed to a relational database where tables are used to store data, objects constitute the fundamental building blocks for "cloud-based" applications. Through a declarative web interface that provides complete visual control at the meta-data level, application designers/developers should be able to define objects along with the fields/attributes that determine what kind of data is stored within each object record. Specifying relationships between objects, a key requirement of any sophisticated business application, must be possible through the declarative web-based interface as well. Besides supporting the definition of 1) objects, 2) the fields that constitute the object and 3) the relationships between the objects, the ability to incorporate validation rules, permissions at the object/field level as well as the ability to specify auditing behavior must all be possible via a declarative web-based paradigm.

4. Robust Workflow engine/capabilities

Successful business process execution via process automation is the primary objective of any business application. A "cloud-platform" must offer a business-logic engine that supports the definition of workflow processes and the specification of business rules to engender process automation. A workflow process defines the different statuses a business object flows through during its life cycle. Workflow actions drive the object through different statuses within the context of a workflow process and can be triggered either through human intervention (i.e. assuming that the user has the required permission to execute/invoke the action) or an event (i.e. the creation of a specific object record). Using a combination of workflow processes, statuses, actions, events and the rules that govern actions, the application designer should be able to model almost any kind of business process using point-and-click tools within the web browser. In addition to providing a declarative fashion to model sophisticated business conditions and application behavior, the PaaS offering must offer the ability to programmatically define powerful trigger conditions using a scripting language such as JavaScript.



5. Granular control over security/sharing (permissions model)

Granular secure access to appropriate data is one of the counterstone of the PaaS model. Just within the PaaS model, secure access models might span multiple logical domains. For example, the application permission model defines access within a specific application such as basic user, user group, managers, or an administrator, to access to specific areas within the application such as standard and premium features, or areas with sensitive and non-sensitive dat. Cross-application and cross-company permission models control access and enable collaboration between the different applications accessible to a single company or legal entity. Additionally, these models manage access control of the organization that manages the platform itself. Further levels of access granularity are achieved by allowing users, or virtual entities to access specific components within PAAS based on their source. For example, it is possible to control what data is accessible depending on where the party is accessing it from2 . Some of the challenges of the granular security model include managing the complexity of the data and access segmentation, auditing the anomalies of the data access and data utilization. These models lie outside and above the standard security components such as firewalls, secure access protocols, authentication models and are not specific to the PAAS model as such.

6. Flexible "services-enabled" integration model

Platform-As-A-Service facilitates the rapid construction of applications in the cloud by providing the necessary foundational elements such as data persistence and workflow capabilities that are core/essential to the creation of any business application. However given the complex IT environments that permeate most enterprises today, the PaaS offering should leverage Service Oriented Architecture (SOA) principles to enable seamless integration of "cloud" application data and functionality residing in the "cloudplatform" with other on-premise/on-demand systems and applications. At a minimum, the PaaS offering must support a flexible integration model enabled via both SOAP and REST API calls. The respective web-services based API's should provide standard CRUD (create, read, update, delete) methods as well as search, binary file upload/download methods for working with file and image fields, methods for working with relationships, and a method for retrieving a full XML representation of an object definition and all of its components. The API's must adhere to the same permissions and access control restrictions that have been specified via the security model.

7. Analytics layer

One of exciting elements of PaaS is having access to the aggregated model. This affords a much richer opportunity for data analytics across the companies utilizing a single application, across applications, and across the companies using multiple applications. The ability to harness this opportunity provides access into utilization trends, feedback about the usage, insights into application interoperability, allows for better planning on the resource expansions, and offers additional avenues for innovation. However, it is important to keep in mind that the custodial

data itself is typically the property of the client companies, and only the aggregated trend/utilization data might have the ability to be used for analysis. Privacy is often cited as a top concern when it comes to protecting strategic business know-how and preventing the exposure of proprietary data and the identities of users within a specific PaaS application company.

8. Integrated content library

PaaS makes it possible to leverage a wide array of common content and application elements that facilitate information sharing, collaboration, training, online business, sales, lead tracking, access control, audits, integrated logging, share communication library, centralized security model, automated sign-up wizards, and a notification system among others4 . Common tagging and search functionality across all the application components and data could potentially be enabled as well5 . By itself, a single standalone application not deployed on PaaS generally lacks these powerful integrated components. A company seeking to use these services might tap into multiple separate applications and as a result lose the ability to integrate the data centrally, increase security risk by having to log in and maintain separate identities and data across multiple vendors.

Where PaaS Makes Sense

PaaS is especially useful in any situation where multiple developers will be working on a development project or where other external parties need to interact with the development process. As the case study below illustrates, it is proving invaluable for those who have an existing data source – for example sales information from a customer relationship management tool, and want to create applications which leverage that data. Finally PaaS is useful where developers wish to automate testing and deployment services.

The popularity of agile software development, a group of software development methodologies based on iterative and incremental development, will also increase the uptake of PaaS as it eases the difficulties around rapid development and iteration of software.

Some examples of PaaS include Google App Engine, Microsoft Azure Services, and the Force.com platform.

Where PaaS May Not be the Best Option

- Where the application needs to be highly portable in terms of where it is hosted
- Where proprietary languages or approaches would impact on the development process
- Where a proprietary language would hinder later moves to another provider – concerns are raised about vendor lock-in

- Where application performance requires customization of the underlying hardware and software

Software as a Service

Software as a service (SaaS) is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet.

Characteristics of SaaS

- Web access to commercial software
- Software is managed from a central location
- Software delivered in a “one to many” model
- Users not required to handle software upgrades and patches
- Application Programming Interfaces (APIs) allow for integration between different pieces of software

Where SaaS Makes Sense

- Applications where there is significant interplay between the organization and the outside world. For example, email newsletter campaign software
- Applications that have a significant need for web or mobile access. An example would be mobile sales management software
- Software that is only to be used for a short term need. An example would be collaboration software for a specific project
- Software where demand spikes significantly, for example tax or billing software used once a month

SaaS Examples: Google Apps, Salesforce, Workday, Concur, Citrix GoToMeeting, Cisco WebEx

Where SaaS May Not be the Best Option

- Applications where extremely fast processing of real time data is required
- Applications where legislation or other regulation does not permit data being hosted externally
- Applications where an existing on-premise solution fulfils all of the organization's needs

Category	Characteristics	Vendor and Products	Advantages
IaaS	Consumers are provided with virtualized hardware and storage on top of which they can build their infrastructure	Amazon Web Services (AWS), Google Compute Engine (GCE), Microsoft Azure, Rackspace, Cisco Metapod	scalability, Pay per use,no investment in physical infrastructure, location independence
PaaS	Consumers are provided with a platform for developing applications hosted in the cloud	AWS Elastic Beanstalk, Google App Engine (GAE), Windows Azure, Apache Stratos	server software, storage, tools for design and development, server-side scripting environment

SaaS	Consumers are provided with applications that are accessible anywhere and anytime	Salesforce, Google Apps, Citrix GoTo Meeting, Cisco WebEx	compatibility, automatic updates and patch management, easier administration

Obstacles for Cloud Technology

Security

Security is the first thing that leaps to mind when you start thinking about putting data online.

Before you export all of your company accounting data into the latest and greatest online accounting package, you need to take a few things into consideration:

- **Transport Layer Security:** Traditional forms of encryption for internet traffic are under attack and are no longer completely reliable
- **Software Auditing:** All software used to provide access to the service needs to be audited and maintained against vulnerabilities. This includes web server software, middleware application layer software such as PHP or .NET, all libraries used, database software, the actual code for the service, JavaScript code (because we all love Web 2.0), administrative service software, operating system etc.
- **Data Storage Security:** We need to know that our data is actually stored in a secure way, that is not accessible to other users of the service or to any Joe Soap that walks into a hosting facility, and that also has protection from hardware failures etc.
- **Personnel Security:** What level of auditing of personnel is performed by the provider? How much access do they have to actual data? What access controls, deprovisioning methods, and account management facilities are in place?
- **Decommissioning Strategy:** What happens when hardware containing sensitive data is removed from service? Can you be sure that your data is properly wiped from hard disks when they fail? What happens to your data when you decide to discontinue a service or migrate to an alternate service?

Legislation

Legal practices are increasingly using cloud computing as an alternative to 'traditional' IT provision. Cloud computing has a number of advantages, but it also carries risks which your firm should navigate carefully.

Usually very tied up with the security problems, is a problem with regard to legislation. This is such a difficult area that many companies just pretend it isn't an issue, however you need to consider not only your own country's legislation with regard to the storage of data and the export of information, but also the laws regarding the same for the country of your provider. So if you are doing business in India, and you decide to make use of a cloud-based service in the US, all of your data is immediately subject to US law. This has very big implications and adds another layer of complexity, which is usually a compliance issue with regard to data protection. If your business is storing credit-card information, or personal user data such as health information, you need to ensure that that data is stored in a way that meets your own country's legal requirements, but the requirements of your provider which might be located in a different country may not be the same. This means that you have to ensure that the legal requirements, or at least actual practices by your provider, actually match your own legal needs.

Finally, there are issues around intellectual property and data ownership. While it should seem obvious that the data is owned by the customer making use of a service, the way in which data is store and accessed usually falls to the service provider.

Integration

While cloud vendors will be quick to tell you how much money you will save using their services, exporting different facilities out onto the internet has a different associated cost that is very hard to measure, and this is the cost of integration.

Firstly, you need to consider that it is unlikely that you will be able to move every bit of your IT infrastructure into the cloud in one go. That means that existing facilities need to be integrated with online facilities so that you can keep the same, or at least very similar, business processes to those that you already have in place.

Since every business is different in terms of the software and services that they make use of, and how these pieces of infrastructure are tied together, it is unlikely that a vendor will meet your exact needs. Usually, this either requires a change to your business processes or to your current infrastructure, potentially requiring some custom development to make things work smoothly.

Perhaps the most commonly highlighted problem is that of Identity Management.

In the good old days if an employee left your company, simply revoking their account would be sufficient to prevent them from accessing facilities that they were not authorised to access. By moving different components of you IT infrastructure out into the cloud, you create something of an identity management crisis.

The problem here is that firstly, cloud vendors tend to be specific about the services they offer. That means that you might end up using a variety of different vendors for different services. This means that you have different accounts for your users hosted in a variety of different places. A user could end up with multiple passwords that need to be managed and different access rights depending on the services that they have connected to. This creates an administrative nightmare. If an employee leaves, there is no way to quickly check that access to all services has been removed.

There are movements to try to get a handle on this, such as Federation, but all of them are immature and pretty costly to implement, not to mention that you need to make sure that your cloud vendor is using the same technologies as you're interested in using. As your infrastructure becomes increasingly distributed, the cost of integrating different components that allow your business to function smoothly increases as well.

Availability

Once upon a time in IT, employees just had to make sure that LAN (Local Area Network) connectivity was operational, and then all of the users could get on with their work. By moving services out onto the cloud, they become increasingly dependent on a chain of third parties in order to access business critical data.

Inside the business, users will still need the LAN to function with the same resilience that it always had, but now they will also need to be sure that there is guaranteed uptime not only for each of the services that use on the Cloud, but for your ISP (Internet Service Provider) as well.

While certainly it is possible that having services out on the cloud actually increase availability, since an ISP failure can easily be overcome by using an alternate ISP during an outage. By using cloud services, user can suddenly access business facilities via the mobile phone, tablet or laptop computer. Realistically, however, when the internet fails within most enterprise-sized businesses, results in down-time of the business

Cloud Vulnerabilities

When deciding to migrate to the cloud, following are the cloud vulnerabilities that should be considered:

- **Session Riding**
- **Virtual Machine Escape**
- **Reliability and Availability of Service**
- **Insecure Cryptography**
- **Data Protection and Portability**

- **CSP Lock-in**
- **Internet Dependency**
- **Session Riding:** Session riding happens when an attacker steals a user's cookie to use the application in the name of the user. An attacker might also use CSRF attacks in order to trick the user into sending authenticated requests to arbitrary web sites to achieve various things.
- **Virtual Machine Escape:** In virtualized environments, the physical servers run multiple virtual machines on top of hypervisors. An attacker can exploit a hypervisor remotely by using a vulnerability present in the hypervisor itself – such vulnerabilities are quite rare, but they do exist. Additionally, a virtual machine can escape from the virtualized sandbox environment and gain access to the hypervisor and consequentially all the virtual machines running on it.
- **Reliability and Availability of Service:** We expect our cloud services and applications to always be available when we need them, which is one of the reasons for moving to the cloud. But this isn't always the case, especially in bad weather with a lot of lightning where power outages are common. The CSPs have uninterrupted power supplies, but even those can sometimes fail, so we can't rely on cloud services to be up and running 100% of the time. We have to take a little downtime into consideration, but that's the same when running our own private cloud.
- **Insecure Cryptography:** Cryptography algorithms usually require random number generators, which use unpredictable sources of information to generate actual random numbers, which is required to obtain a large entropy pool. If the random number generators are providing only a small entropy pool, the numbers can be brute forced. In client computers, the primary source of randomization is user mouse movement and key presses, but servers are mostly running without user interaction, which consequentially means lower number of randomization sources. Therefore the virtual machines must rely on the sources they have available, which could result in easily guessable numbers that don't provide much entropy in cryptographic algorithms.
- **Data Protection and Portability:** When choosing to switch the cloud service provider for a cheaper one, we have to address the problem of data movement and deletion. The old CSP has to delete all the data we stored in its data center to not leave the data lying around.
- Alternatively, the CSP that goes out of the business needs to provide the data to the customers, so they can move to an alternate CSP after which the data needs to be deleted. What if the CSP goes out of business without providing the data? In such cases, it's better

to use a widely used CSP which has been around for a while, but in any case data backup is still in order.

- **CSP Lock-in:** We have to choose a cloud provider that will allow us to easily move to another provider when needed. We don't want to choose a CSP that will force us to use his own services, because sometimes we would like to use one CSP for one thing and the other CSP for something else.

- **Internet Dependency:** By using the cloud services, we're dependent upon the Internet connection, so if the Internet temporarily fails due to a lightning strike or ISP maintenance, the clients won't be able to connect to the cloud services. Therefore, the business will slowly lose money, because the users won't be able to use the service that's required for the business operation. Not to mention the services that need to be available 24/7, like applications in a hospital, where human lives are at stake.

Cloud Challenges

Cloud computing challenges have always been there. Companies are increasingly aware of the business value that cloud computing brings and are taking steps towards transition to the cloud. A smooth transition entails a thorough understanding of the benefits as well as challenges involved. Like any new technology, the adoption of cloud computing is not free from issues. Some of the most important challenges are as follows:

- **Security and Privacy**
- **Interoperability and Portability**
- **Reliability and Availability**
- **Performance and Bandwidth cost**

Security And Privacy

- The main challenge to cloud computing is how it addresses the security and privacy concerns of businesses thinking of adopting it. The fact that the valuable enterprise data will reside outside the corporate firewall raises serious concerns. Hacking and various attacks to cloud infrastructure would affect multiple clients even if only one site is attacked. These risks can be mitigated by using security applications, encrypted file systems, data loss software, and buying security hardware to track unusual behavior across servers.

- It is difficult to assess the costs involved due to the on-demand nature of the services. Budgeting and assessment of the cost will be very difficult unless the provider has some good and comparable benchmarks to offer. The service-level agreements (SLAs) of the

provider are not adequate to guarantee the availability and scalability. Businesses will be reluctant to switch to cloud without a strong service quality guarantee.

Interoperability And Portability

- Businesses should have the leverage of migrating in and out of the cloud and switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on-premise IT.

Reliability And Availability

- Cloud providers still lack round-the-clock service; this results in frequent outages. It is important to monitor the service being provided using internal or third-party tools. It is vital to have plans to supervise usage, SLAs, performance, robustness, and business dependency of these services.

Performance And Bandwidth Cost

- Businesses can save money on hardware but they have to spend more for the bandwidth. This can be a low cost for smaller applications but can be significantly high for the data-intensive applications. Delivering intensive and complex data over the network requires sufficient bandwidth. Because of this, many businesses are waiting for a reduced cost before switching to the cloud.

13 biggest challenges when moving the business to the cloud according to Forbes Technology Council:

- **Getting it right**
- **People and processes**
- **Having a defined strategy and business objectives**
- **Getting over the psychological barriers**
- **Time, cost and security**
- **Not getting caught up in the hype**
- **Changing management**
- **Dependable technological infrastructure**
- **Accurately estimating the costs**
- **Modifying the architecture of cloud services**

- **Translating security posture to the cloud environment**
- **Determining whether to lease or own**
- **Connecting legacy systems with cloud applications**