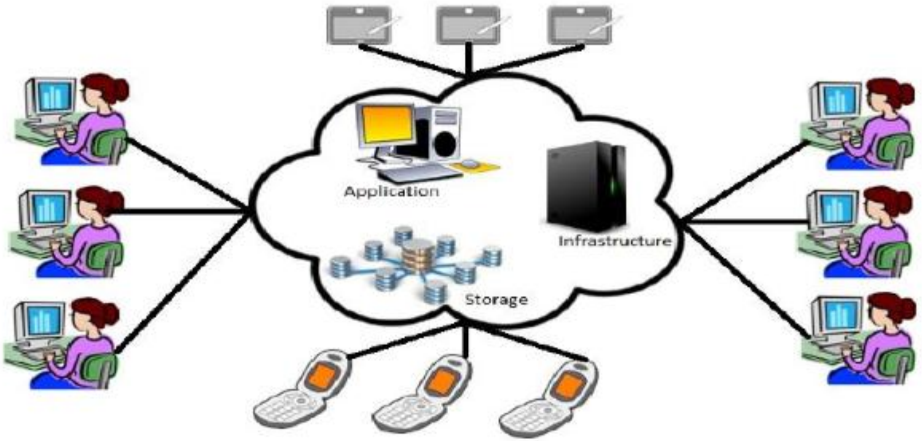
Cloud Computing
and
Identity & Access Management

Objectives

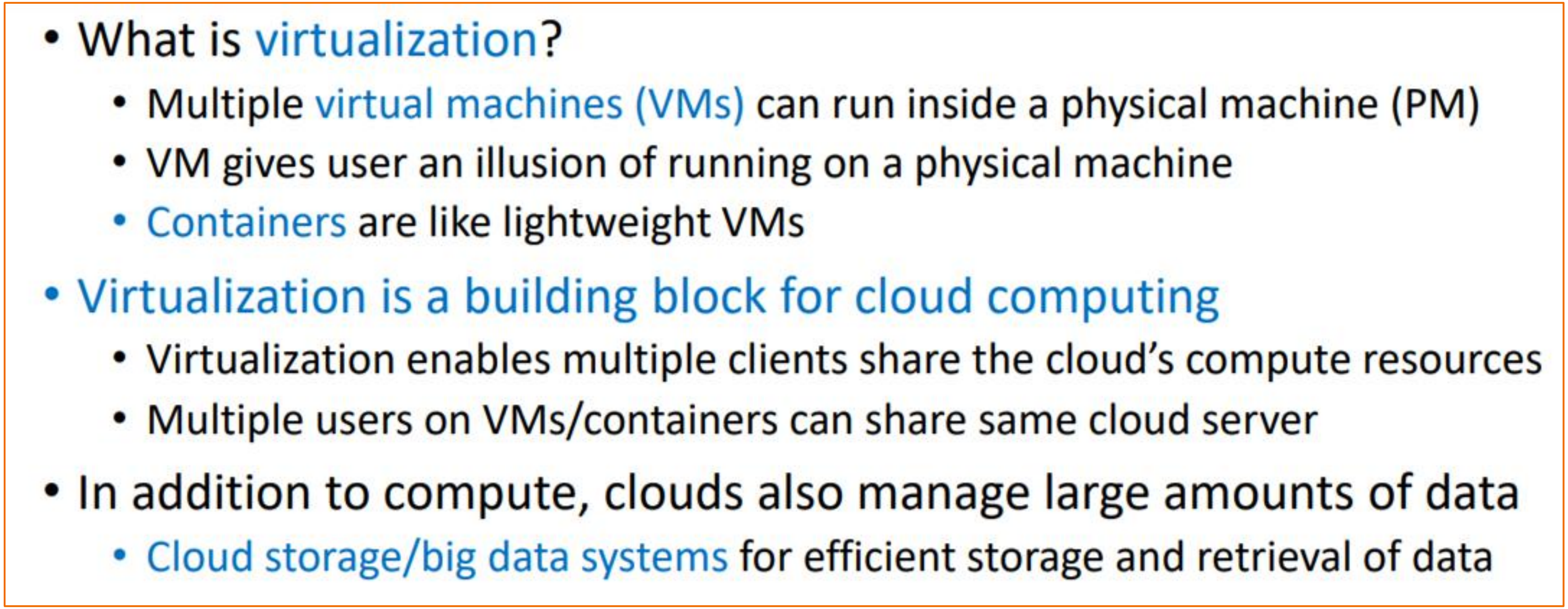
- Introduction to **Cloud**
- **Virtualization** and **Cloud Computing**
- Why Cloud Computing
- Characteristics of Cloud Computing
- Example of Cloud Applications
- Advantages of Cloud Computing
- Cloud Computing Challenges
- Cloud Computing Architecture
- Understand fundamentals around **Identity**, **Authentication**, **Authorization** & **Access Control**.

What is Cloud ?

- ➔ Cloud refers to a **Network or Internet**.
- ➔ Cloud is something, which is present at remote location.
- ➔ Cloud can provide services over network.
- ➔ Applications such as e-mail, web conferencing all run in cloud.



Virtualization and Cloud Computing



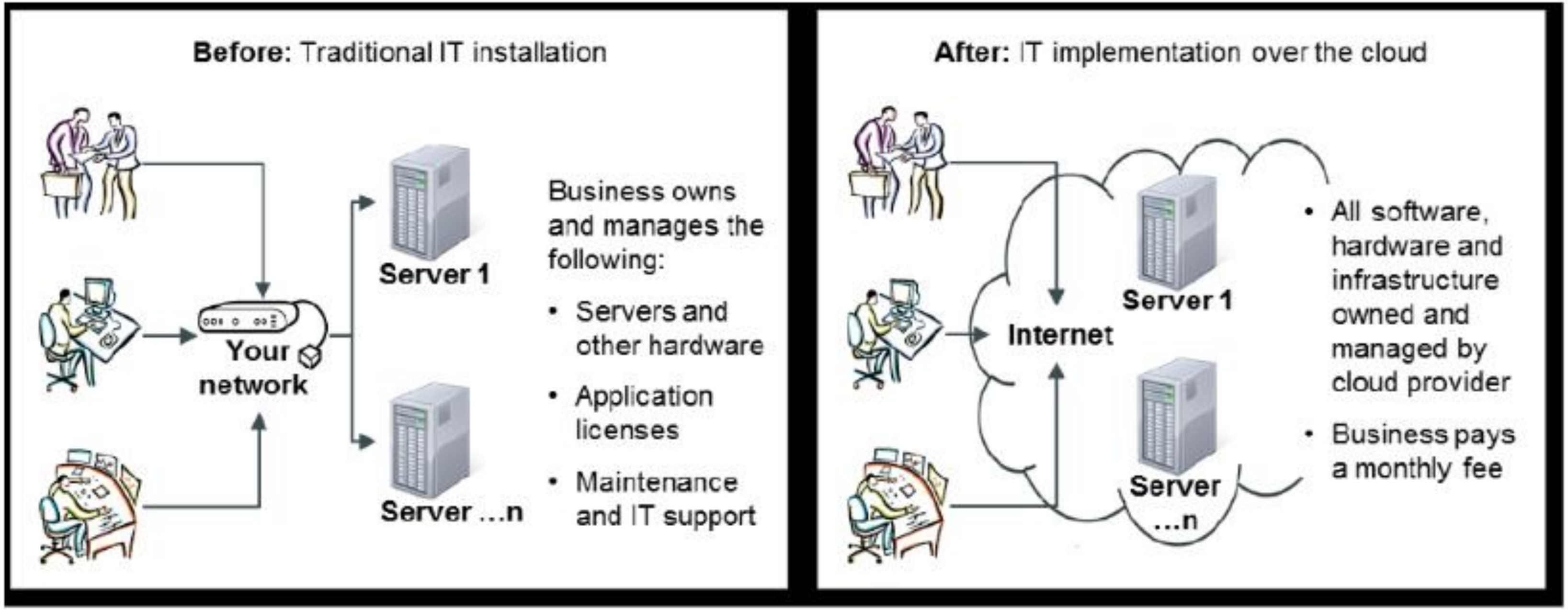
- What is virtualization?
  - Multiple virtual machines (VMs) can run inside a physical machine (PM)
  - VM gives user an illusion of running on a physical machine
  - Containers are like lightweight VMs
- Virtualization is a building block for cloud computing
  - Virtualization enables multiple clients share the cloud’s compute resources
  - Multiple users on VMs/containers can share same cloud server
- In addition to compute, clouds also manage large amounts of data
  - Cloud storage/big data systems for efficient storage and retrieval of data

What is cloud computing ?

- ➔ **Cloud Computing** refers the **delivery of computing resources over Internet.**
- ➔ Cloud Computing refers to manipulating, configuring, and accessing the applications online.
- ➔ Its offer online data storage, and application.

We need not to install a piece of software on our local PC and this is how the cloud computing overcomes platform dependency issues.
Hence, the cloud computing is making our business application mobile etc.

Cloud Computing



Before: Traditional IT installation

Business owns and manages the following:

- Servers and other hardware
- Application licenses
- Maintenance and IT support

After: IT implementation over the cloud

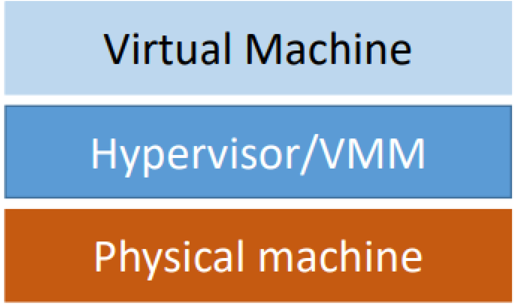
- All software, hardware and infrastructure owned and managed by cloud provider
- Business pays a monthly fee

Why Cloud Computing ?

- Public cloud providers (Amazon AWS, Microsoft Azure, Google Cloud etc) setup and maintain data centers with high-end servers
  - Powerful CPUs, lots of memory, disk storage etc., available to users
  - Organizations can also run a private cloud only for their users
- Why run applications on cloud and not on “bare metal” servers?
  - Multiplexing gains: multiple VMs can share the system resources
  - Lower overhead of maintenance: hardware/software maintained by providers
  - Flexibility: VMs can move to another machine if one fails
  - Pay as per usage: no need to invest in servers if only lightly used
- Disadvantages of running applications on cloud
  - Performance: longer delay to access servers via internet
  - Higher cost if heavily used

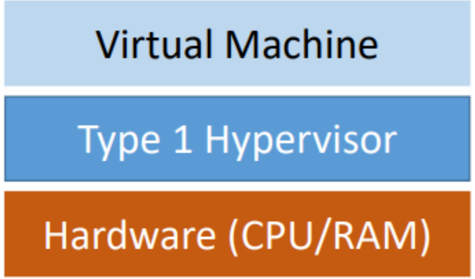
Virtualization terminology

- We will study system virtualization, or how to run one full system (OS and applications) over another OS
  - We do not cover process virtualization (e.g., Java virtual machine) which lets a single process run on a different architecture from underlying machine
- Hypervisor or virtual machine monitor (VMM): a piece of software that allows multiple VMs to run on a physical machine (PM)
  - We will study how VMMs are designed



Virtualization terminology

- Guest OS runs inside the VM, and host OS runs on the PM
- Type 1 hypervisor: runs directly on hardware, no need for host OS

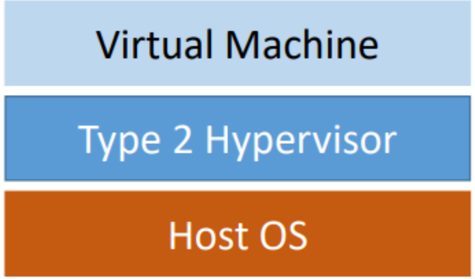


Virtual Machine

Type 1 Hypervisor

Hardware (CPU/RAM)

- Type 2 (hosted) hypervisor: runs as an application on top of host OS



Virtual Machine

Type 2 Hypervisor

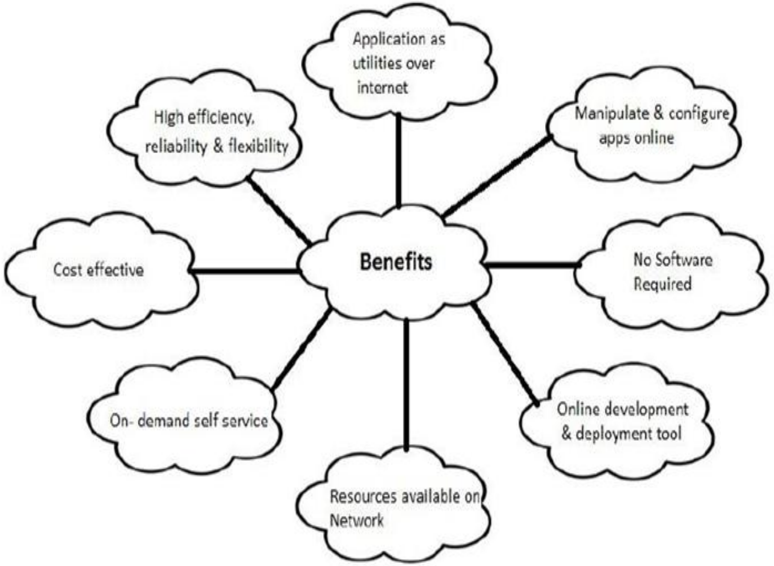
Host OS

Example of Cloud Applications

- **Clippingmagic.com :**Remove image backgrounds online. Make backgrounds transparent, white, etc. Edit, crop, rotate, fix colors,and add shadows, all you need for great photos.
- **Dropbox :**Keep your documents and files at your fingertips across all your devices using Dropbox.
- **DocuSign :**Electronic signature technology and transaction management services platform. DocuSign e-signatures are legally binding for most business and personal transactions in virtually every nation across the globe.
- **Microsoft Office 365 :**Users now may create, edit and share content from any PC, Mac, iOS, Android or Windows device in real-time.
- **Mozy :** A Cloud based data protection application.
- **Evernote :** Lets users to capture a note in any format.
- **SugarSync:** It provides backup solution. User can store and backup his files on cloud and access them from any web browser anytime anywhere.
- **Netsuite:** It is a cloud ERP and business management suite.
- **Facebook/Twitter:** Cloud based social networking application

Benefits of Cloud Applications

- One can access applications as utilities, over the Internet.
- Manipulate and configure the application online at any time.
- It does not require to install a specific piece of software to access or manipulate cloud application.
- Cloud Computing offers online development and deployment tools, programming runtime environment through **Platform as a Service model**.
- Cloud resources are available over the network in a manner that provides platform independent access to any type of clients.
- Cloud Computing offers **on-demand self-service**. The resources can be used without interaction with cloud service provider.


Application as utilities over internet
High efficiency, reliability & flexibility
Manipulate & configure apps online
Cost effective
Benefits
No Software Required
On- demand self service
Online development & deployment tool
Resources available on Network

Characteristics of Cloud Computing

➔ There are **four key characteristics of cloud computing**. They are shown in the following diagram :

★ **On Demand Self-Service**

Cloud Computing allows the users to use web services and resources on demand. One can logon to a website at any time and use them.

➔ Broad Network Access

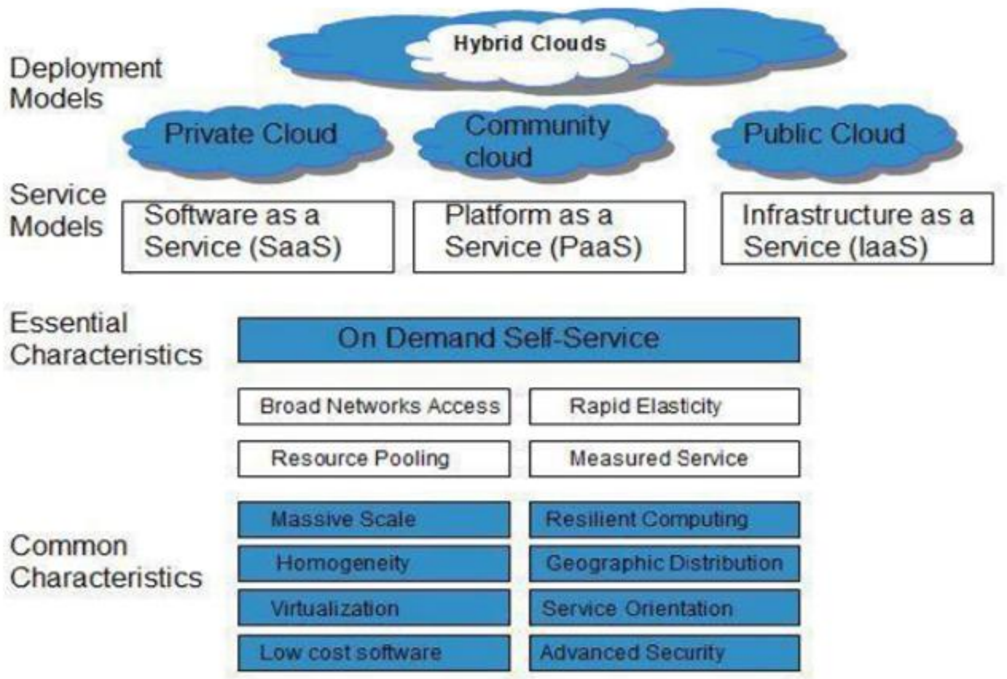
Since Cloud Computing is completely web based, it can be accessed from anywhere and at any time.

➔ Resource Pooling

One can share single physical instance of hardware, database and basic infrastructure.

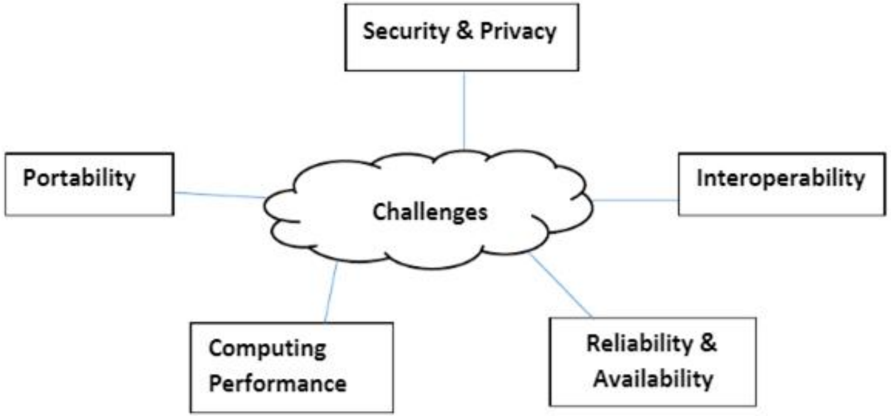
➔ Rapid Elasticity

It is very easy to scale up or down the resources at any time.



Cloud Computing Challenges

- **Security & Privacy:** Issues overcome by employing encryption, security hardware and security applications.
- **Portability:** Applications should easily be migrated from one cloud provider to another. There should not be vendor lock-in.
- **Interoperability:** It is made possible via web services.
- **Computing Performance:** To deliver data intensive applications on cloud requires high network bandwidth, which results in high cost.
- **Reliability and Availability:** It is necessary for cloud systems to be reliable and robust because most of the businesses are now becoming dependent on services provided by third-party.



Cloud Migration

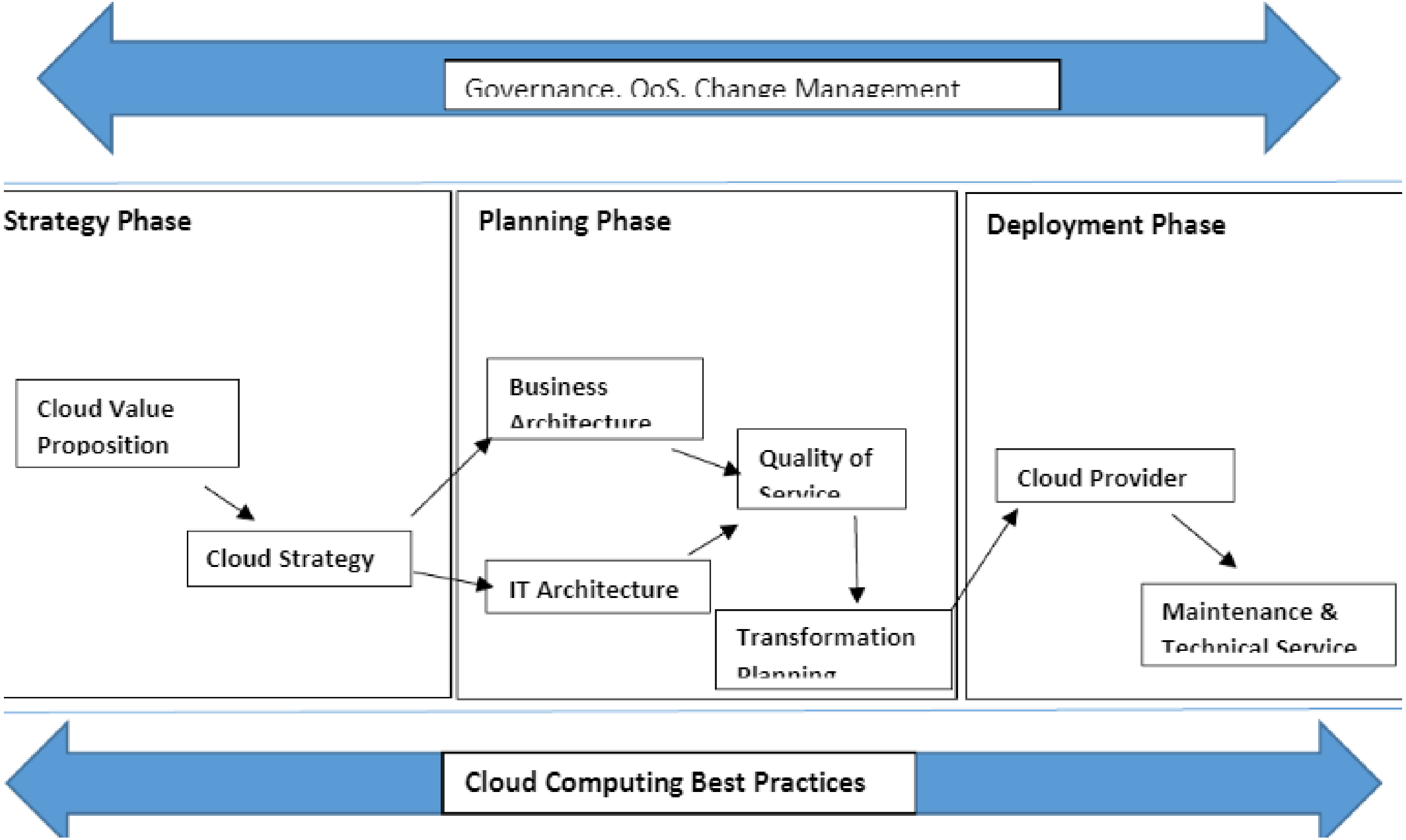
Cloud migration is the **process of moving data**, **applications or other business elements from an organization's onsite computers to the cloud**, or moving them from one cloud environment to another.

Cloud Computing – Planning

Before deploying applications to cloud, it is necessary to consider your business requirements. Following are **the issues one must have to think** about:

- Data Security and Privacy Requirement
- Type of cloud - public, private or hybrid
- Data backup requirements
- Training requirements
- Dashboard and reporting requirements
- Client access requirements

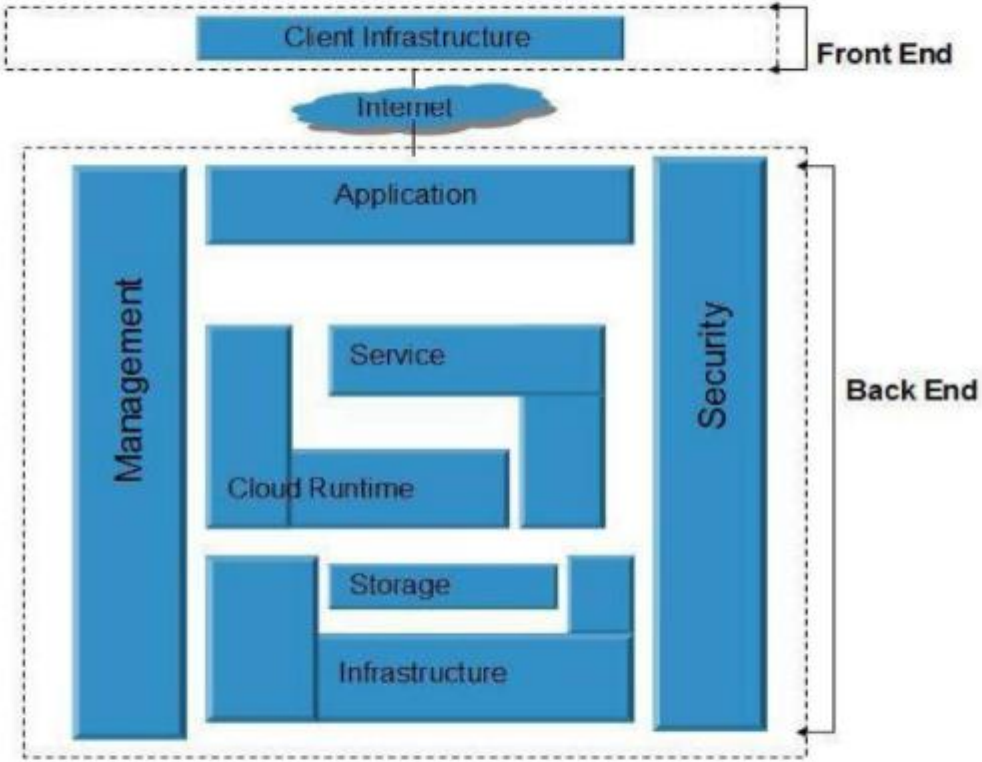
Various Planning Phases



Cloud Computing Architecture

The **front end** is the **side the computer user, or client, sees**. The front end includes the client's computer (or computer network) and the application required to access the cloud computing system.

The **back end** is **the "cloud" section of the system**. On the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services.



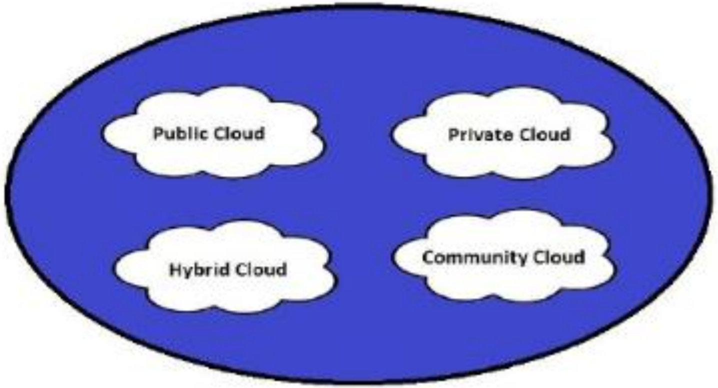
Types of Cloud

- Deployment Models
- Service Models

- **Deployment Models**

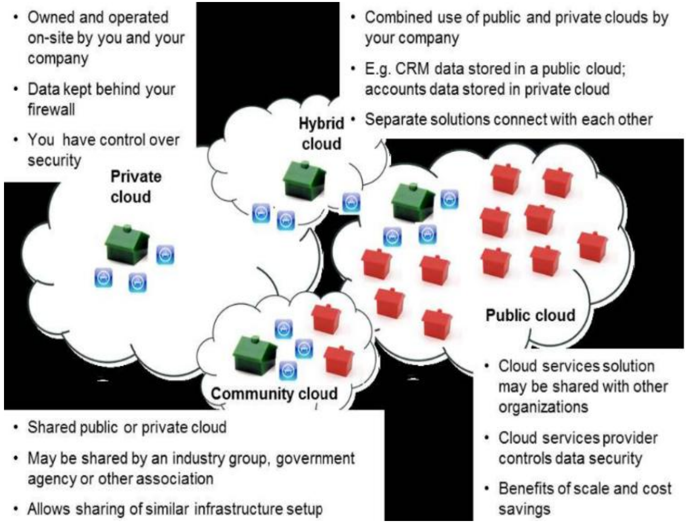
Deployment models define **the type of access to the cloud**, i.e., how the cloud is located?

Cloud can have any of the four types of access: **Public, Private, Hybrid and Community.**



Deployment Models: Types of Cloud

- **Public Cloud :** Allows systems and services to be **easily accessible to the general public**. Public cloud may be less secure because of its openness, e.g. Google, Amazon, Microsoft offers cloud services via Internet.
- **Private Cloud :** Allows systems and services to be **accessible within an organization**. It offers increased security because of its private nature.
- **Community Cloud :**Allows systems and services to be **accessible by group of organizations.**
- **Hybrid Cloud :** The Hybrid Cloud is **mixture of public and private cloud**. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.



- Owned and operated on-site by you and your company
- Data kept behind your firewall
- You have control over security

- Combined use of public and private clouds by your company
- E.g. CRM data stored in a public cloud; accounts data stored in private cloud
- Separate solutions connect with each other

- Cloud services solution may be shared with other organizations
- Cloud services provider controls data security
- Benefits of scale and cost savings

- Shared public or private cloud
- May be shared by an industry group, government agency or other association
- Allows sharing of similar infrastructure setup

Service Models

- Service Models are the reference models on which the Cloud Computing is based.

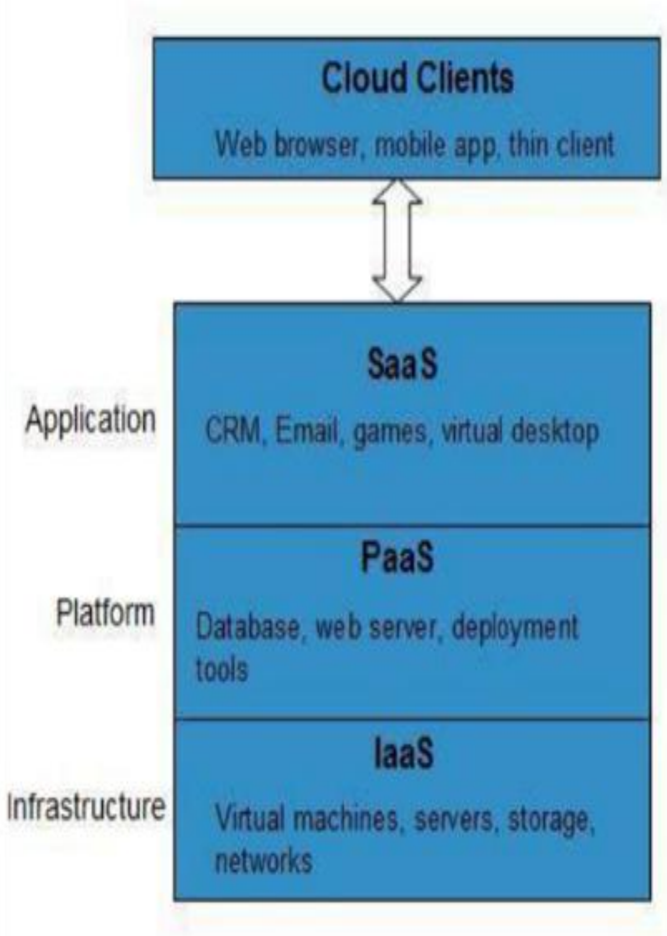
1. **Infrastructure as a Service (IaaS)**
2. **Platform as a Service (PaaS)**
3. **Software as a Service (SaaS)**

Service Models

1. **Infrastructure as a Service (IaaS)**
2. **Platform as a Service (PaaS)**
3. **Software as a Service (SaaS)**

- **Infrastructure as a Service (IaaS) :** cloud computing offering in which a **vendor provides users access to computing resources such as servers, storage and networking.** Organizations use their own platforms and applications within a service provider's infrastructure.

  - Instead of purchasing hardware outright, users pay for IaaS on demand.
  - Infrastructure is scalable depending on processing and storage needs.

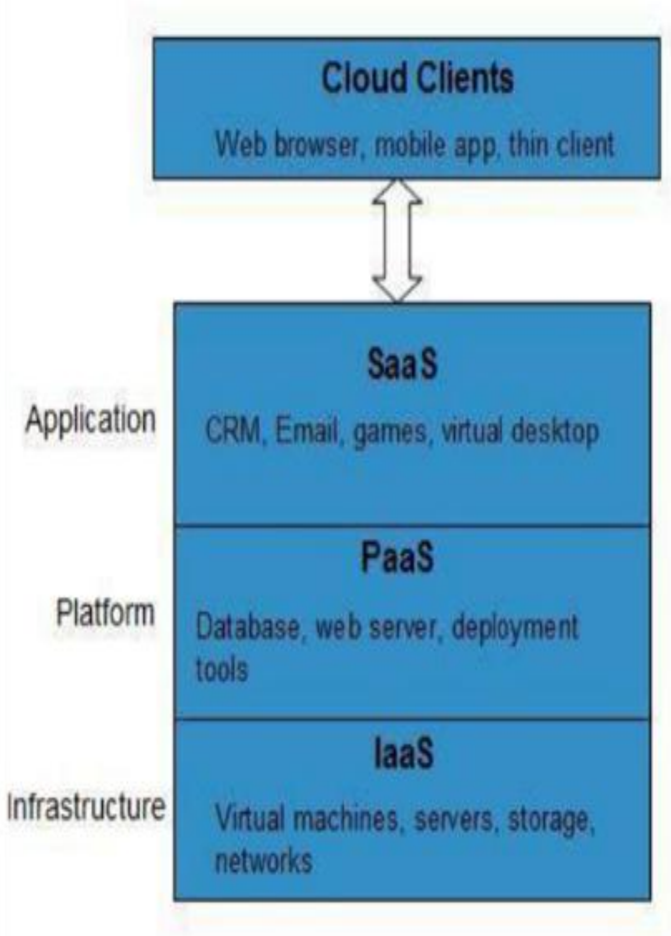

Cloud Clients
Web browser, mobile app, thin client
Application
SaaS
CRM, Email, games, virtual desktop
Platform
PaaS
Database, web server, deployment tools
Infrastructure
IaaS
Virtual machines, servers, storage, networks

Service Models

1. **Infrastructure as a Service (IaaS)**
2. **Platform as a Service (PaaS)**
3. **Software as a Service (SaaS)**

- **Platform as a Service (PaaS) :** cloud computing offering that provides users with a cloud environment in which they can develop, manage and deliver applications.

  - PaaS provides a platform with tools to test, develop and host applications in the same environment.
  - Providers manage security, operating systems, server software and backups.

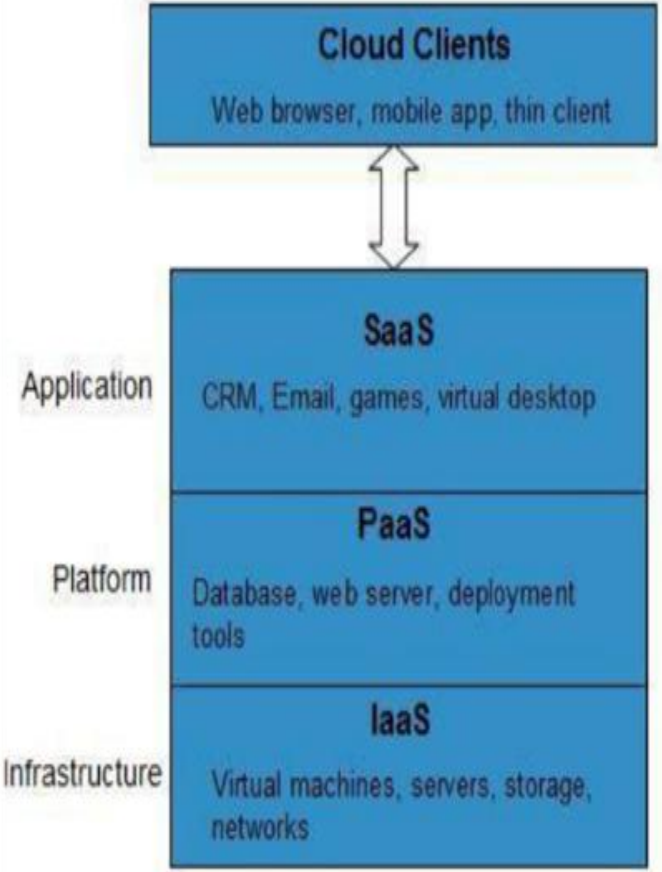

Cloud Clients
Web browser, mobile app, thin client
Application
SaaS
CRM, Email, games, virtual desktop
Platform
PaaS
Database, web server, deployment tools
Infrastructure
IaaS
Virtual machines, servers, storage, networks

Service Models

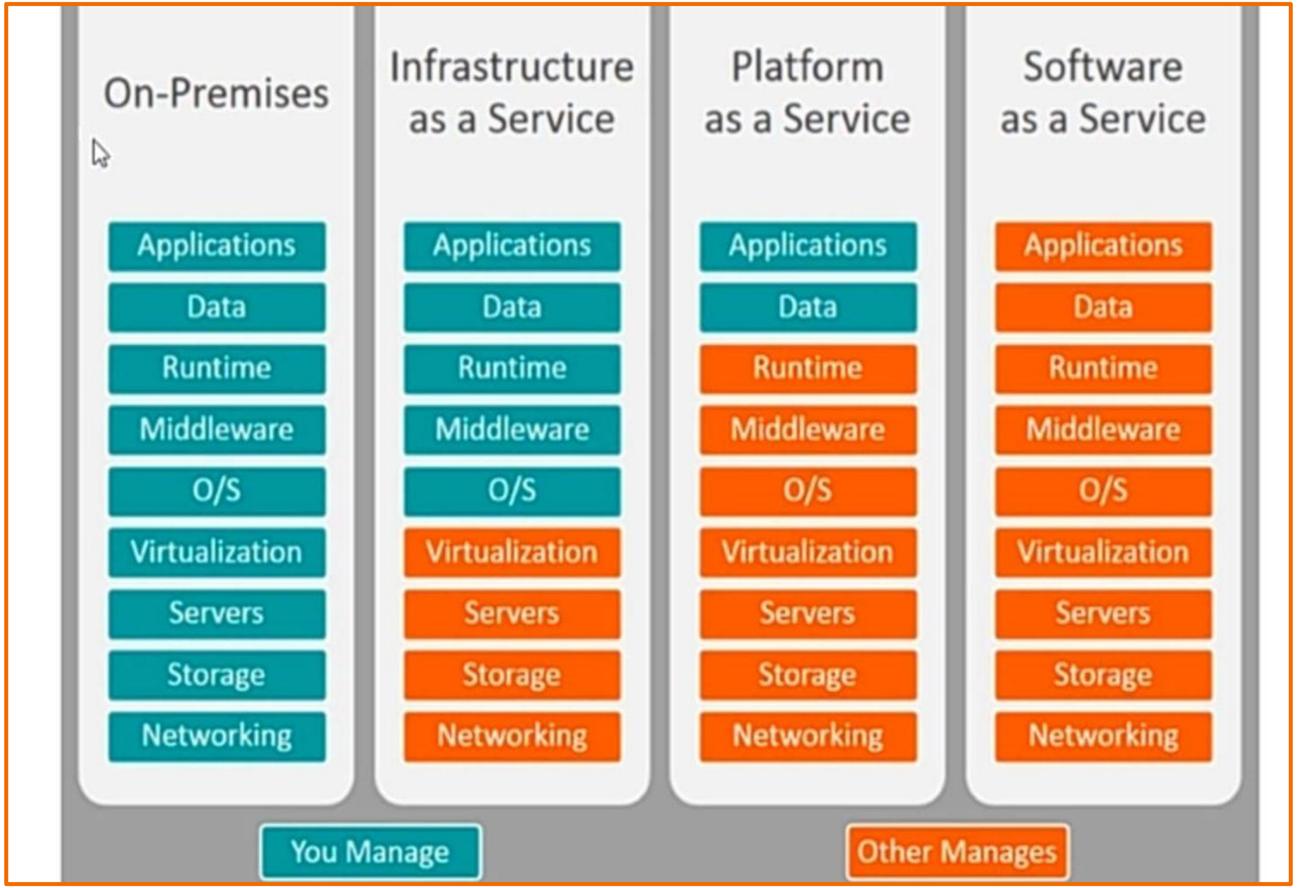
1. **Infrastructure as a Service (IaaS)**
2. **Platform as a Service (PaaS)**
3. **Software as a Service (SaaS)**

- **Software as a Service (SaaS) :** cloud computing offering that provides users with access to a **vendor's cloud-based software**. Users do not install applications on their local devices. Instead, the applications reside on a remote cloud network accessed through the web or an API.

  - Users do not have to manage, install or upgrade software;SaaS providers manage this.
  - SaaS vendors provide users with software and applications via a subscription model.


Cloud Clients
Web browser, mobile app, thin client
Application
SaaS
CRM, Email, games, virtual desktop
Platform
PaaS
Database, web server, deployment tools
Infrastructure
IaaS
Virtual machines, servers, storage, networks

Cloud Computing Service Models

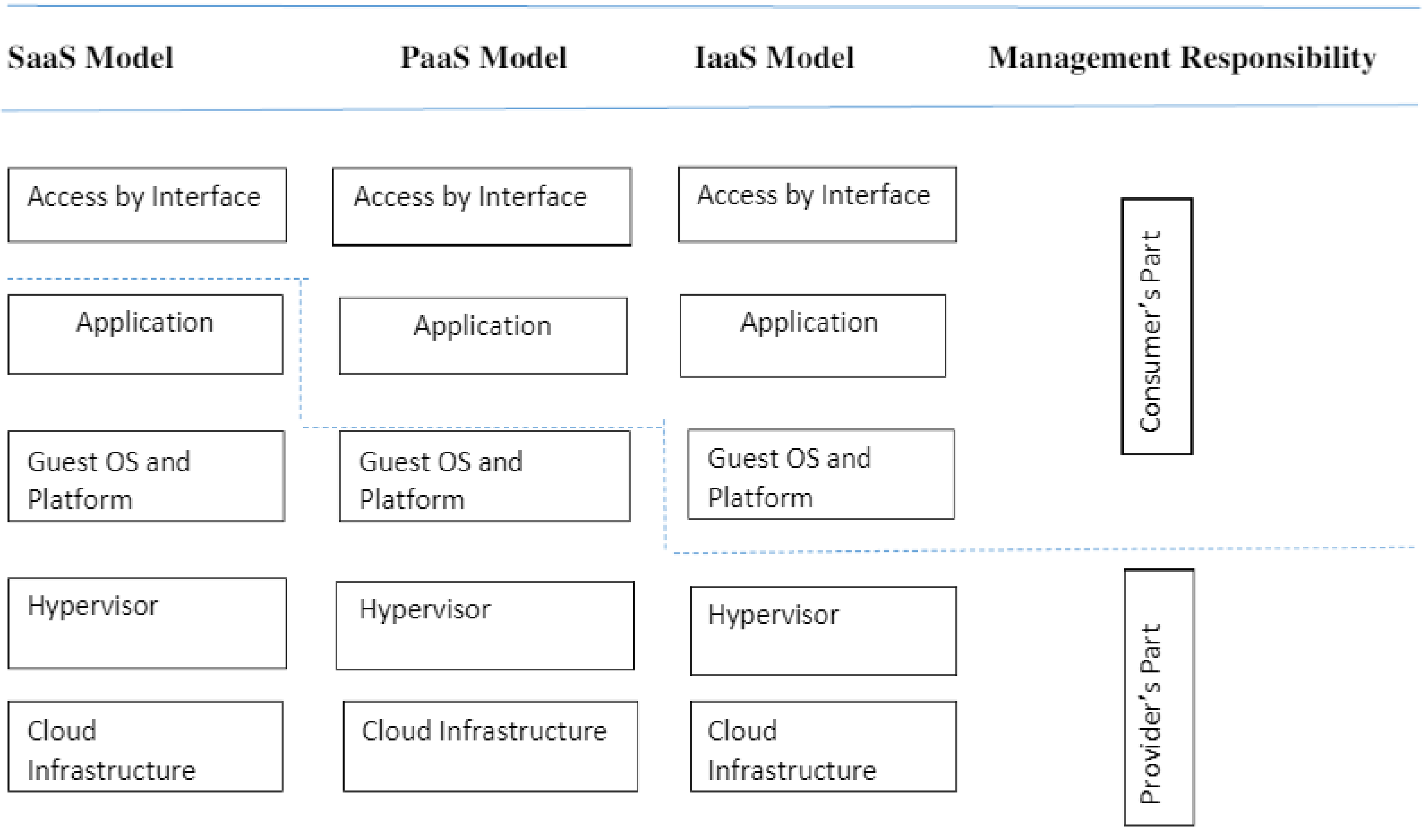


On-Premises	Infrastructure as a Service	Platform as a Service	Software as a Service
🟦 Applications	🟦 Applications	🟦 Applications	🟧 Applications
🟦 Data	🟦 Data	🟦 Data	🟧 Data
🟦 Runtime	🟦 Runtime	🟧 Runtime	🟧 Runtime
🟦 Middleware	🟦 Middleware	🟧 Middleware	🟧 Middleware
🟦 O/S	🟦 O/S	🟧 O/S	🟧 O/S
🟦 Virtualization	🟧 Virtualization	🟧 Virtualization	🟧 Virtualization
🟦 Servers	🟧 Servers	🟧 Servers	🟧 Servers
🟦 Storage	🟧 Storage	🟧 Storage	🟧 Storage
🟦 Networking	🟧 Networking	🟧 Networking	🟧 Networking

🟦 You Manage

🟧 Other Manages

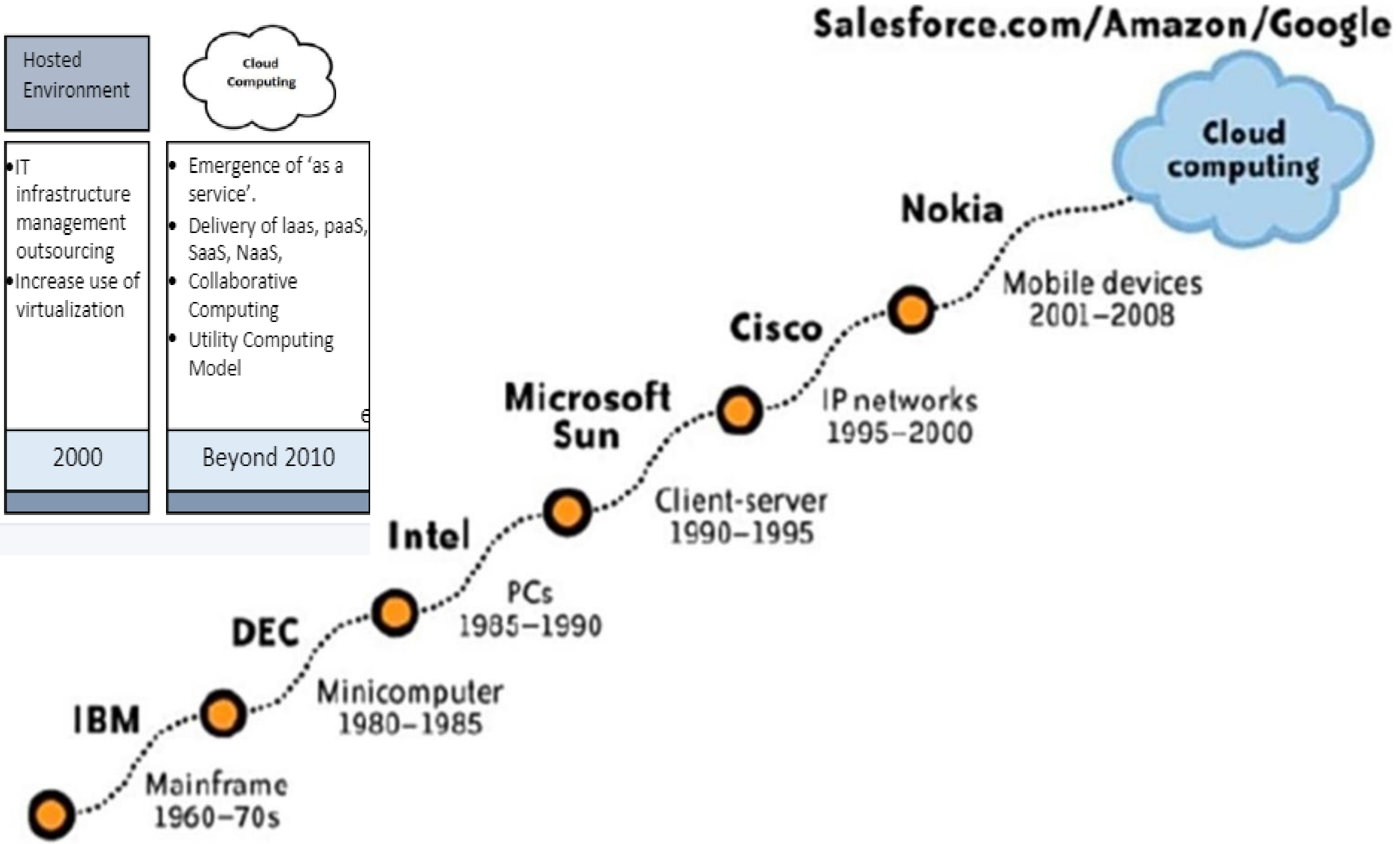
Share of Responsibilities between service provider and service consumer



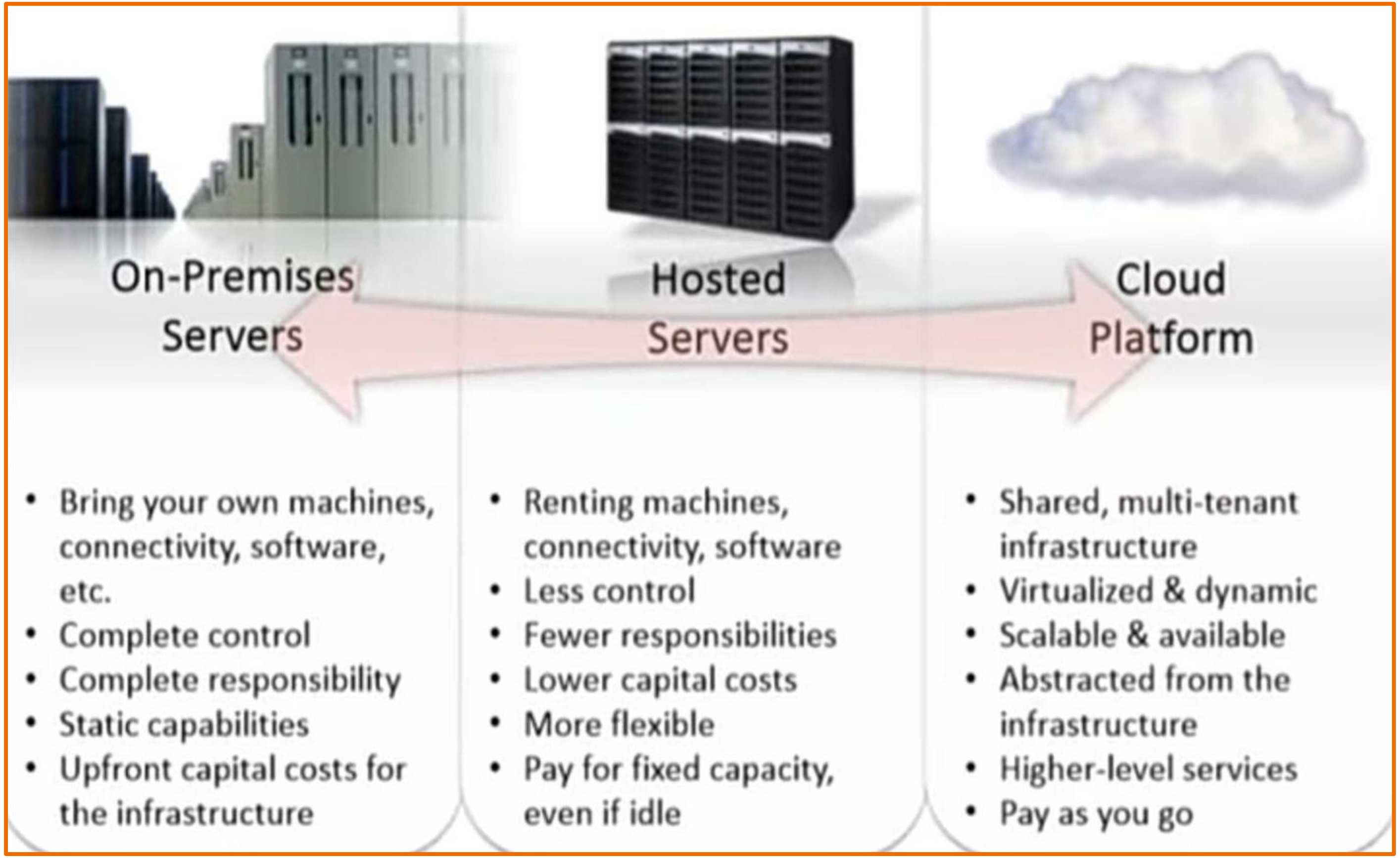
SaaS Model	PaaS Model	IaaS Model	Management Responsibility
Access by Interface	Access by Interface	Access by Interface	Consumer's Part
Application	Application	Application	
Guest OS and Platform	Guest OS and Platform	Guest OS and Platform	
Hypervisor	Hypervisor	Hypervisor	Provider's Part
Cloud Infrastructure	Cloud Infrastructure	Cloud Infrastructure	

History of Cloud Computing

Mainframes	Rise of the PC	Client/Server Architecture	Hosted Environment	Cloud Computing
• Start of Automation phase • Localized Infrastructure	• Rise in Demand of personal desktops • Decentralized computing • Birth of IT Services Industries	• Virtual Private Network offered • Demand for high bandwidth • Dot com revolution	• IT infrastructure management outsourcing • Increase use of virtualization	• Emergence of 'as a service'. • Delivery of Iaas, paaS, SaaS, NaaS, • Collaborative Computing • Utility Computing Model
1950s	1960s	1990s	2000	Beyond 2010



History of Cloud Computing



On-Premises Servers

- Bring your own machines, connectivity, software, etc.
- Complete control
- Complete responsibility
- Static capabilities
- Upfront capital costs for the infrastructure

Hosted Servers

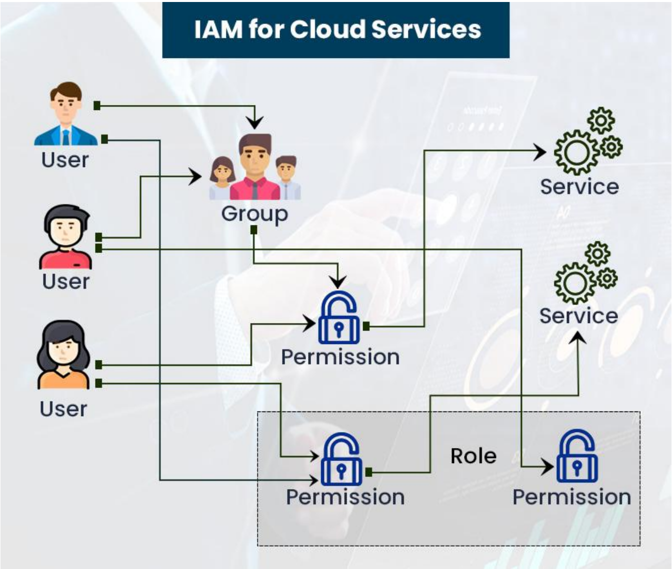
- Renting machines, connectivity, software
- Less control
- Fewer responsibilities
- Lower capital costs
- More flexible
- Pay for fixed capacity, even if idle

Cloud Platform

- Shared, multi-tenant infrastructure
- Virtualized & dynamic
- Scalable & available
- Abstracted from the infrastructure
- Higher-level services
- Pay as you go

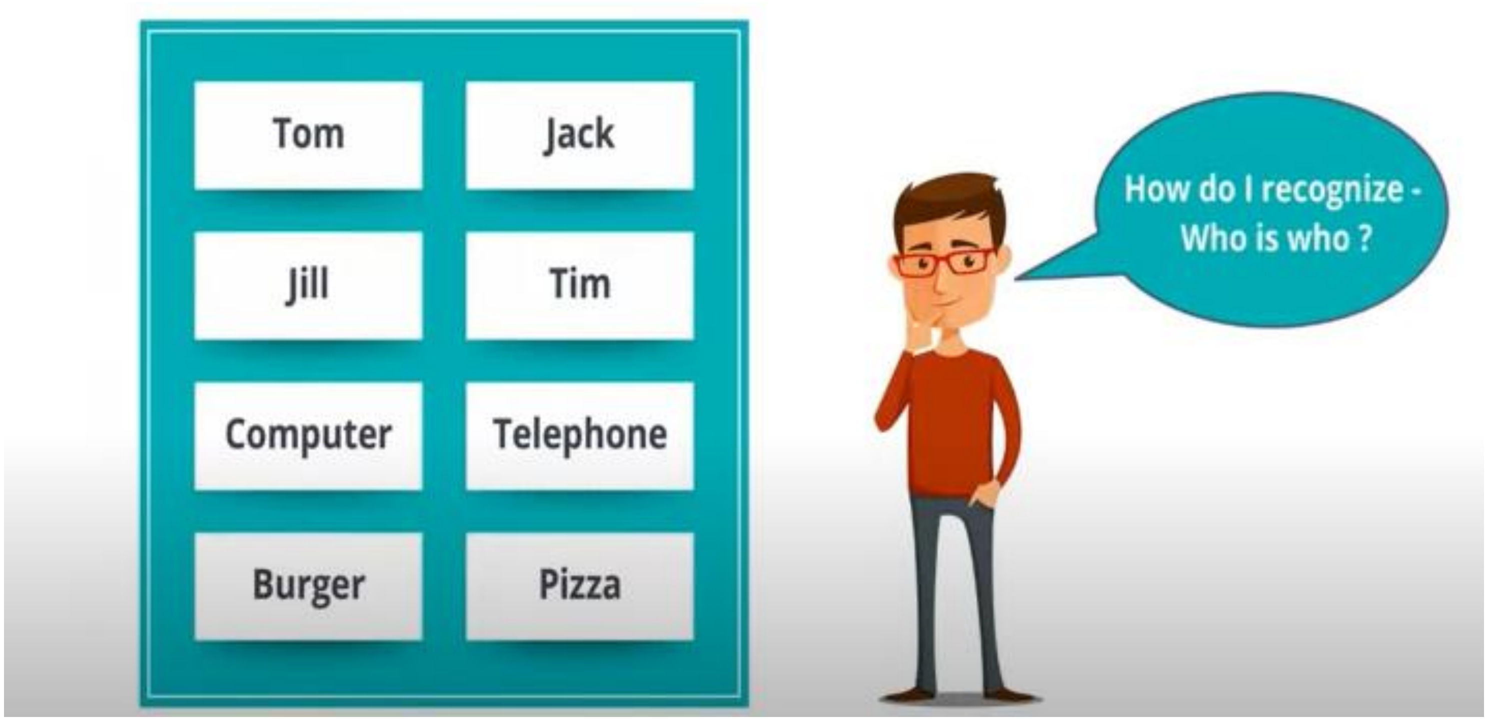
Identity and Access Management (IAM)

IAM refers to a framework or policies and technologies for ensuring that the proper people in an organization have the appropriate access to technology resources.



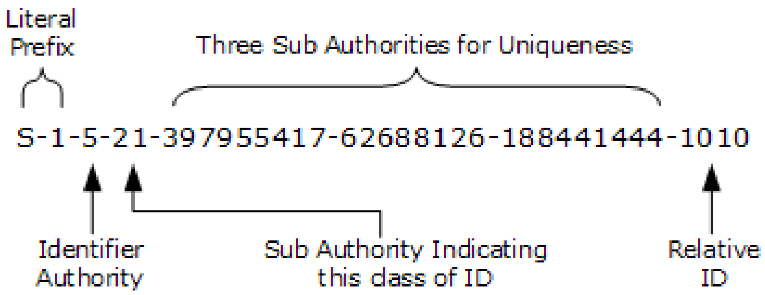
Identity (Recognition)

An IAM identity **represents a human user or programmatic workload**, and can be authenticated and then authorized to perform particular actions.

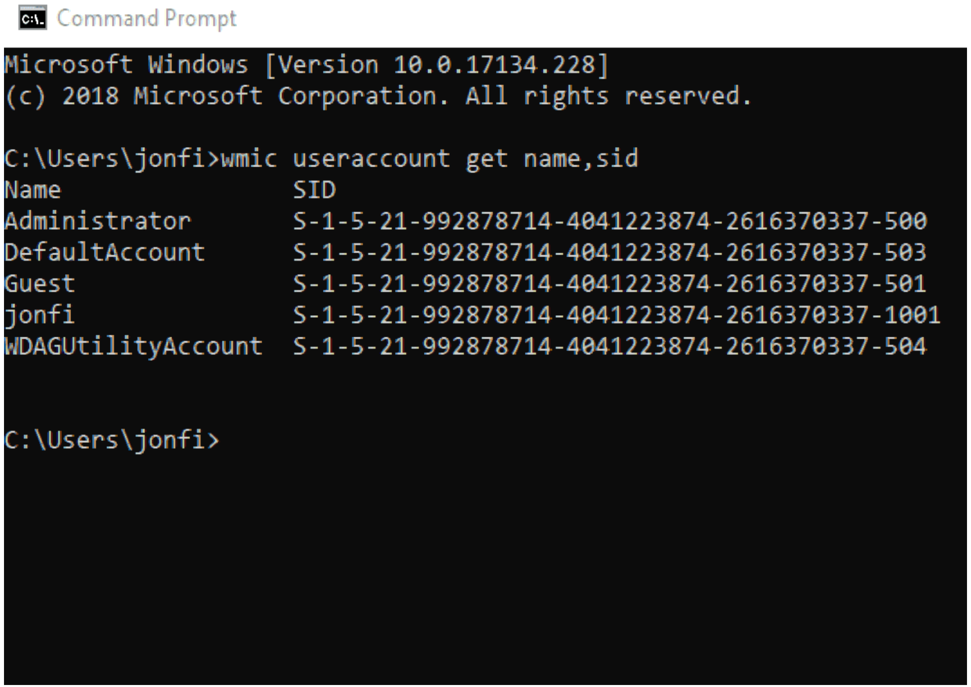


Identity (Recognition)

Identification or Recognition of individuals or their devices is possible by associating **unique & reliable user security identifiers (SID)**.



Literal Prefix
Three Sub Authorities for Uniqueness
S-1-5-21-397955417-62688126-188441444-1010
Identifier Authority
Sub Authority Indicating this dass of ID
Relative ID

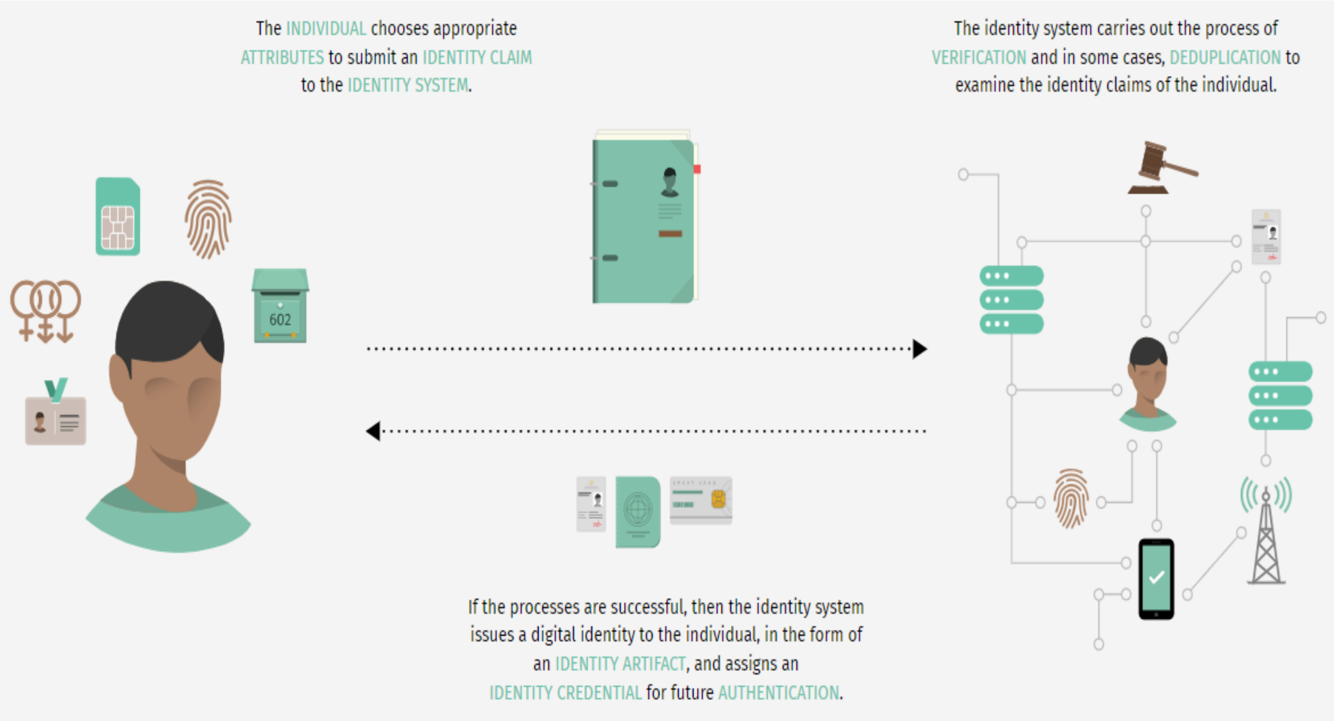


```
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\jonfi>wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-992878714-4041223874-2616370337-500
DefaultAccount      S-1-5-21-992878714-4041223874-2616370337-503
Guest               S-1-5-21-992878714-4041223874-2616370337-501
jonfi               S-1-5-21-992878714-4041223874-2616370337-1001
WDAGUtilityAccount  S-1-5-21-992878714-4041223874-2616370337-504


C:\Users\jonfi>
```

Digital Identity Artefacts

An **identity artefact** is a document or object, which can be both physical or digital, that is issued to an Individual at the end of the process of Identification, that facilitates in establishing their Identity.

- ➔ User-ID, Username, Password.
- ➔ Phone Number
- ➔ Aadhaar
- ➔ Purchasing or Medical history



The INDIVIDUAL chooses appropriate ATTRIBUTES to submit an IDENTITY CLAIM to the IDENTITY SYSTEM.

The identity system carries out the process of VERIFICATION and in some cases, DEDUPLICATION to examine the identity claims of the individual.

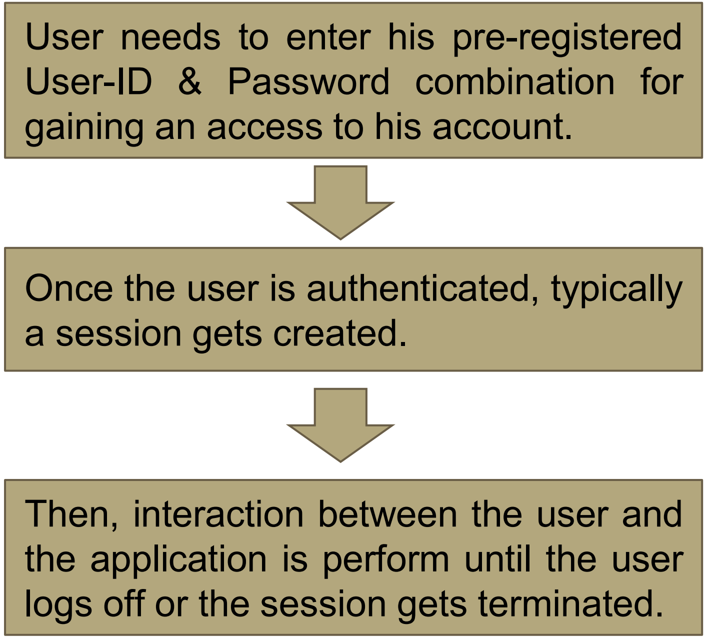
If the processes are successful, then the identity system issues a digital identity to the individual, in the form of an IDENTITY ARTIFACT, and assigns an IDENTITY CREDENTIAL for future AUTHENTICATION.

Authentication

Authentication is a process where a user proves his identity to gain access to a resource such as application, system, and so on.

During authentication the user needs to provide some pre-registered credentials in order to establish their identity.

Example : Login screen of a website.

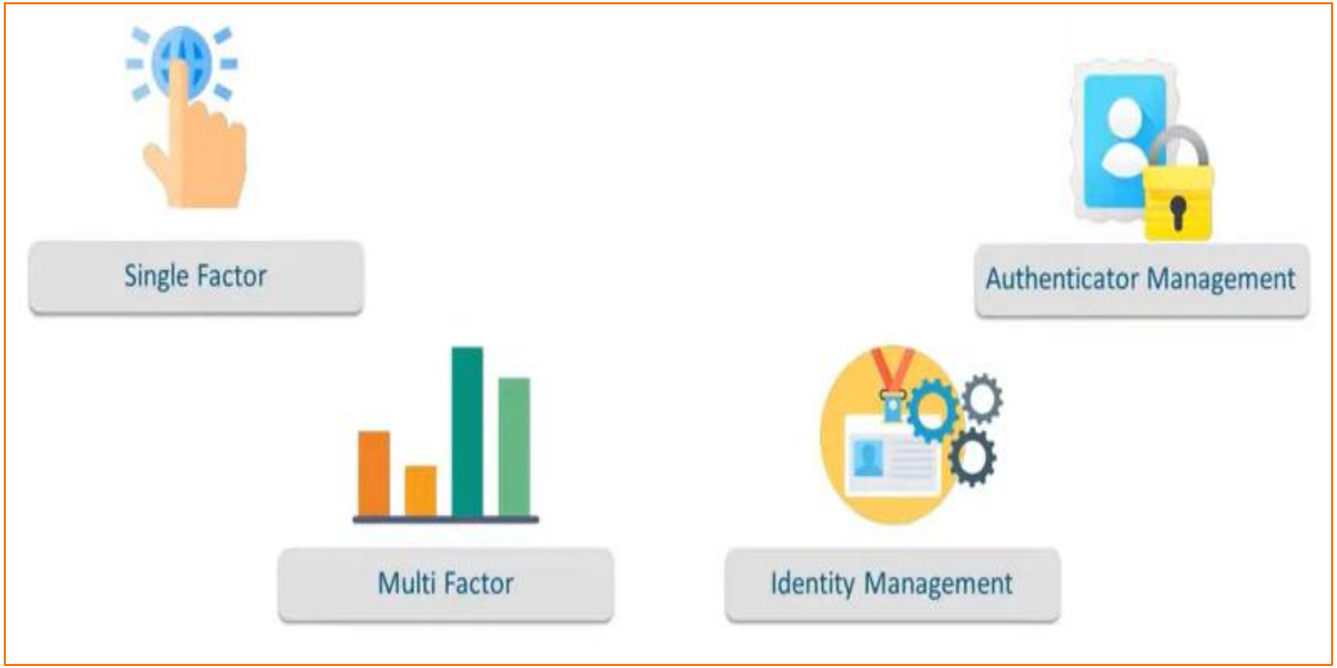


User needs to enter his pre-registered User-ID & Password combination for gaining an access to his account.

Once the user is authenticated, typically a session gets created.

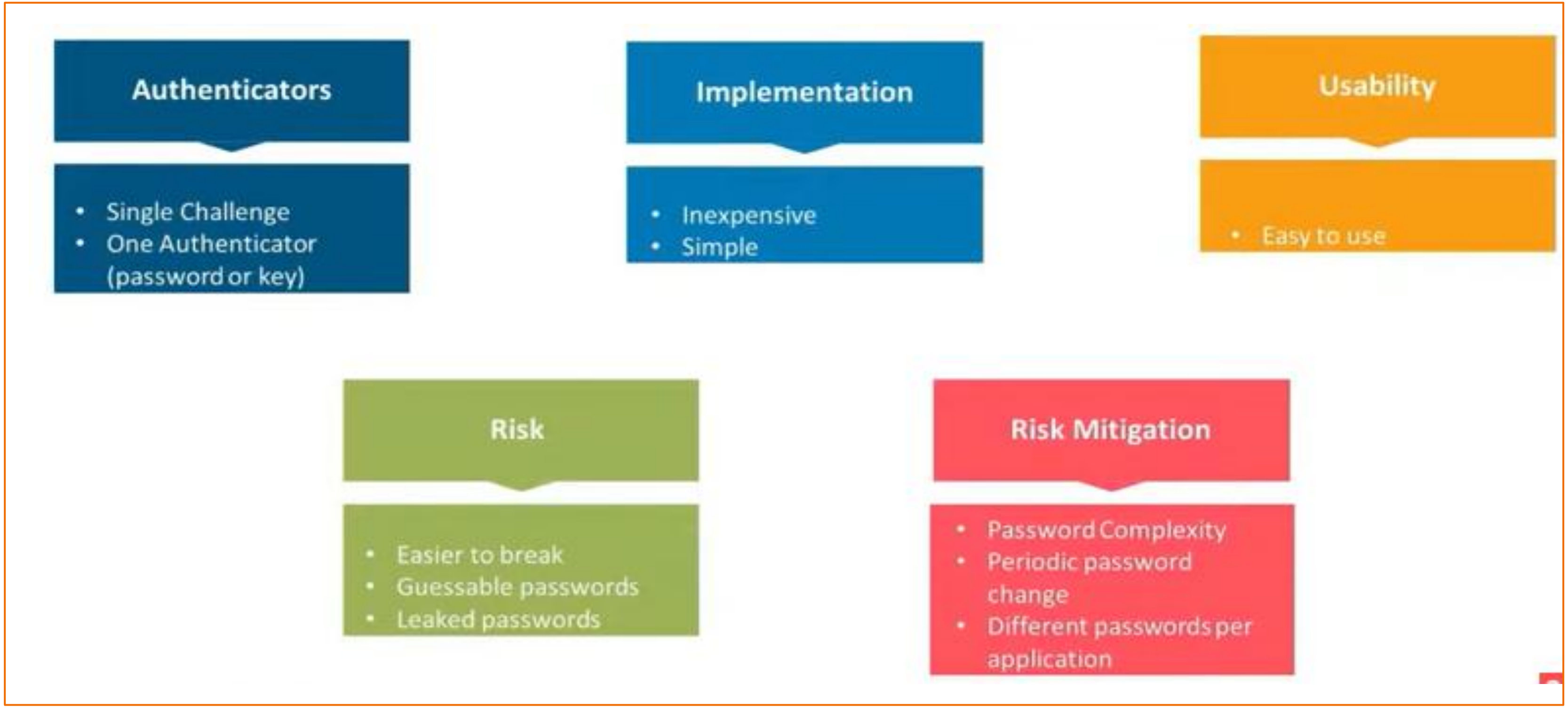
Then, interaction between the user and the application is perform until the user logs off or the session gets terminated.

Authentication Processes



Authentication Processes

➔ **Single Factor Authentication**



Authenticators

- Single Challenge
- One Authenticator (password or key)

Implementation

- Inexpensive
- Simple

Usability

- Easy to use

Risk

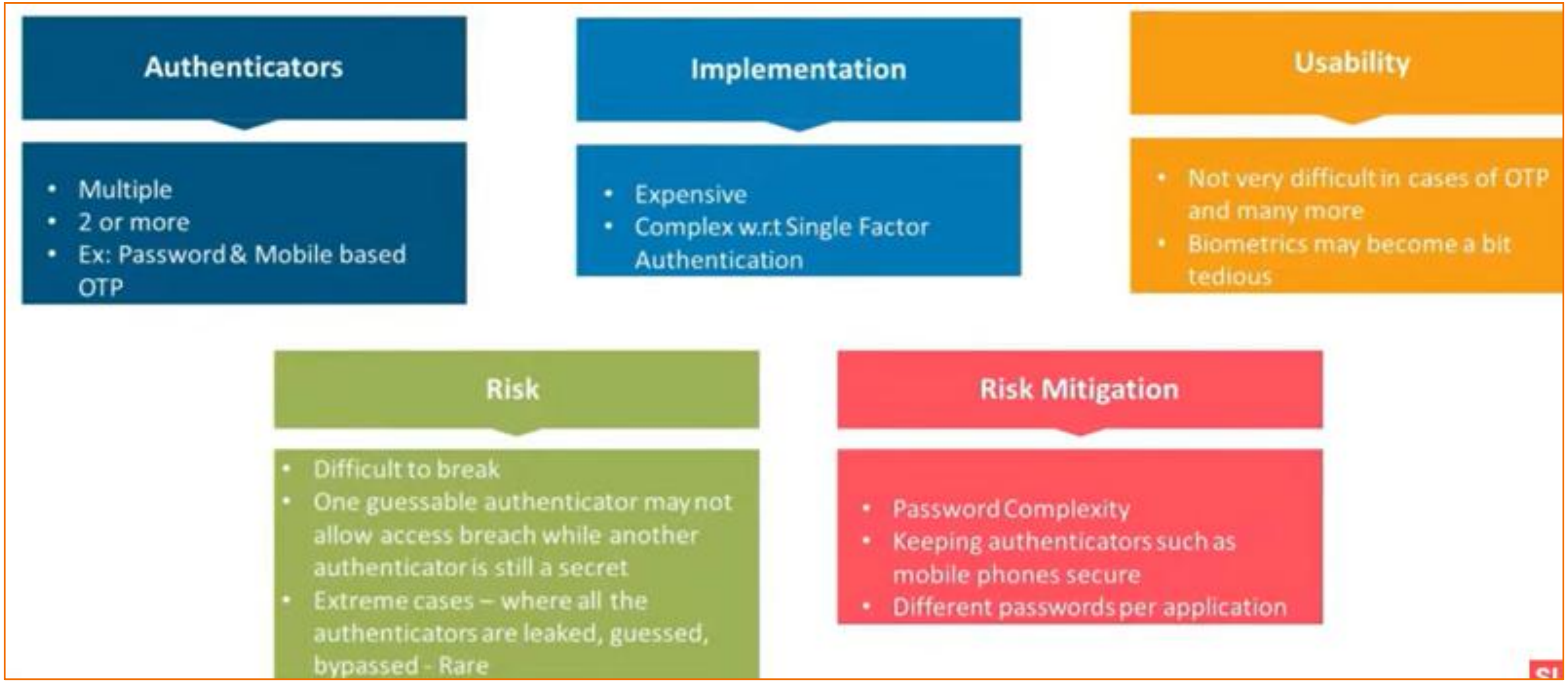
- Easier to break
- Guessable passwords
- Leaked passwords

Risk Mitigation

- Password Complexity
- Periodic password change
- Different passwords per application

Authentication Processes

→ **Multi Factor Authentication**



Authenticators

- Multiple
- 2 or more
- Ex: Password & Mobile based OTP

Implementation

- Expensive
- Complex w.r.t Single Factor Authentication

Usability

- Not very difficult in cases of OTP and many more
- Biometrics may become a bit tedious

Risk

- Difficult to break
- One guessable authenticator may not allow access breach while another authenticator is still a secret
- Extreme cases – where all the authenticators are leaked, guessed, bypassed - Rare

Risk Mitigation

- Password Complexity
- Keeping authenticators such as mobile phones secure
- Different passwords per application

Authentication Processes

➔ Authenticator Management

Step 1: Authenticators include passwords, tokens, keys,biometrics, PKI certificates, access cards and so on which helps a user, entity to prove his preverified entity and ask for access.

Step 2: Authenticator management is a key process which involves issuing, revoking, and servicing of authenticators.

Step 3: Usage of ‘Default’ valued authenticators is a risk & should be avoided as they are easily known, discoverable and guessed by attackers.

Step 4: Ensuring that authenticators are created, distributed, serviced, handled, and terminated securely is very important from security point of view.

Authorization

Authorization refers to the process responsible to determine user **permissions to access a particular resource.**

Authorization is usually performed by checking the resource access request, against a set of authorization policies typically stored in the backend.

Usually **process of Authentication verifies a user's identity and it then enables Authorization**. An authorization policy then decides what the given identity is allowed to do in the context of a particular system in concern.

Authorization Access Control

The Authorization model could also provide complex access controls based on:

- ➔ Data, information, policies including user attributes
- ➔ User roles, groups as allocated
- ➔ Access channel (IP, Geolocation)
- ➔ Time of access
- ➔ Resources requested by the user
- ➔ Business rules

Tenets of Authorization

Different attributes of authorization while authorizing a particular objects :

- ➔ SOD - Segregation of Duties
- ➔ Need to Know Basis
- ➔ Principle of Least Privilege
- ➔ Unsuccessful Logins
- ➔ Session Concurrency/ Last Login Notifications
- ➔ Notifications of System Usage

Tenets of Authorization

- **SOD (Segregation Of Duties)**

➔ SOD primarily **separates the responsibilities associated with an action of process** to decrease the opportunity for misbehaviour or policy violations.

Example : One Developer & another Tester concept.

Tenets of Authorization

- **Need To Know Basis**

➔ Minimum requirement for a particular person to carry out everyday acts to be.

➔ This principle **prevents over exposure of sensitive information** which then becomes likely to be misused.

Example 1: An employee using an allotted virtual machine may need the credentials of the local user for login however may never the credentials of the hypervisor or even the root/ admin.

Example 2: An manager in an organisation may need to know some personal information including salary information about this direct reports but may never require information about other employees in the organization.

Tenets of Authorization

- **Principles Of Least Privilege**

➔ What the actions member can performs ?

➔ Individuals or systems should only have the access necessary to perform specific activities required of their job or role.

➔ The least privilege principle ensures that what can be done with the information is **limited to the least amount of access necessary to perform those actions**.

Tenets of Authorization

- **Unsuccessful Logins**

➔ Limiting the number of unsuccessful login attempts by a user during a specific period can reduce the potential for guessing credentials.

➔ Procedures may include locking accounts after a certain number of attempts, requiring an end user to contact the help desk, or simply unlocking the account after a specific period.