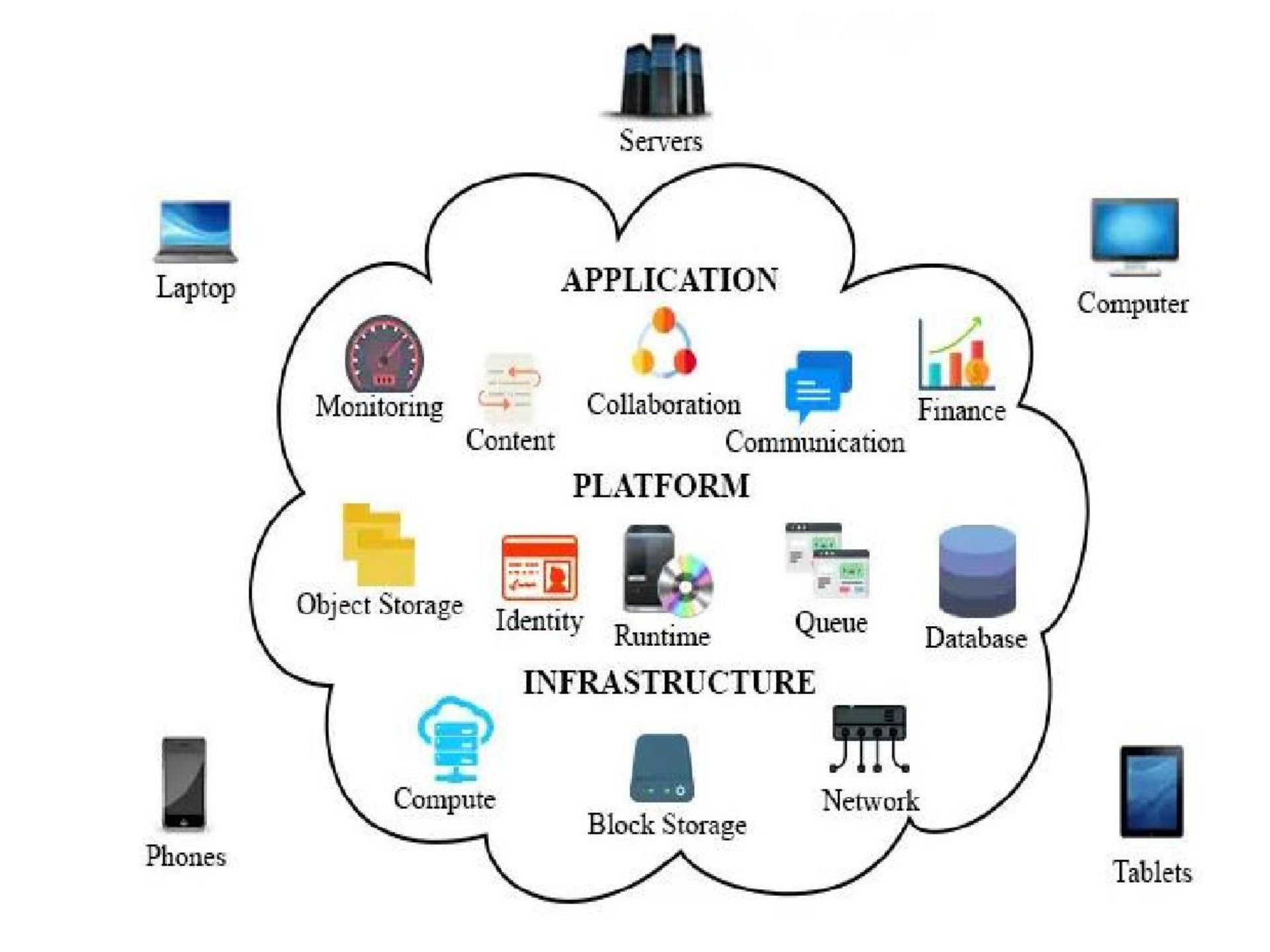
Cloud Computing

Er. Nivedita Kashyap
ABVGIET,Pragatinagar
AP CSE

Cloud Computing

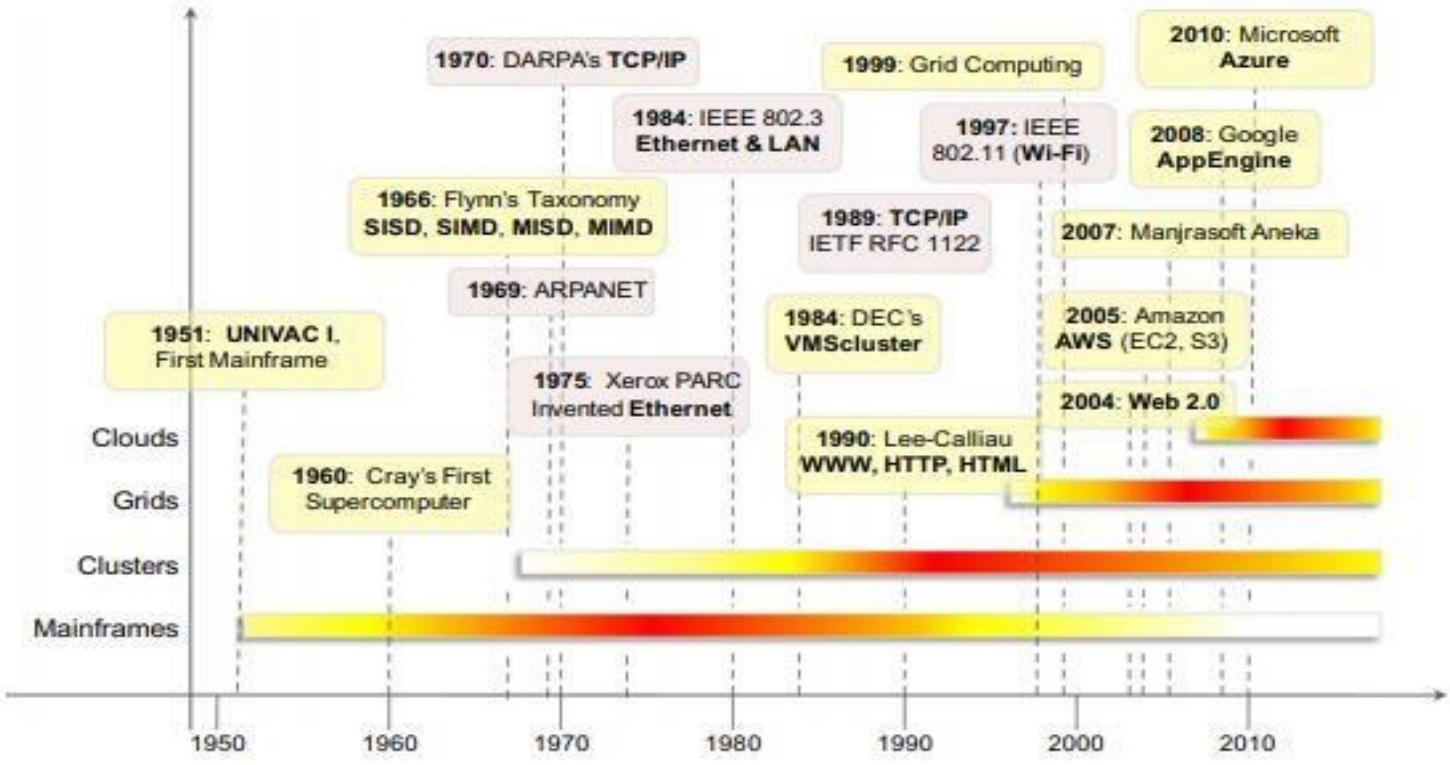
- “The cloud" refers to servers that are accessed over the Internet, and the software and databases that run on those servers. Cloud servers are located in data centers all over the world.
- By using cloud computing(uses computers to manage, process, and communicate information. It includes development of both hardware and software), users and companies don't have to manage physical servers themselves or run software applications on their own machines.


Servers
Laptop
Computer
APPLICATION
Monitoring
Content
Collaboration
Communication
Finance
PLATFORM
Object Storage
Identity
Runtime
Queue
Database
INFRASTRUCTURE
Compute
Block Storage
Network
Phones
Tablets

Historical developments

- The idea of renting computing services by leveraging large distributed computing facilities has been around for long time. It dates back to the days of the mainframes in the early 1950s. From there on, technology has evolved and been refined. This process has created a series of favorable conditions for the realization of cloud computing.

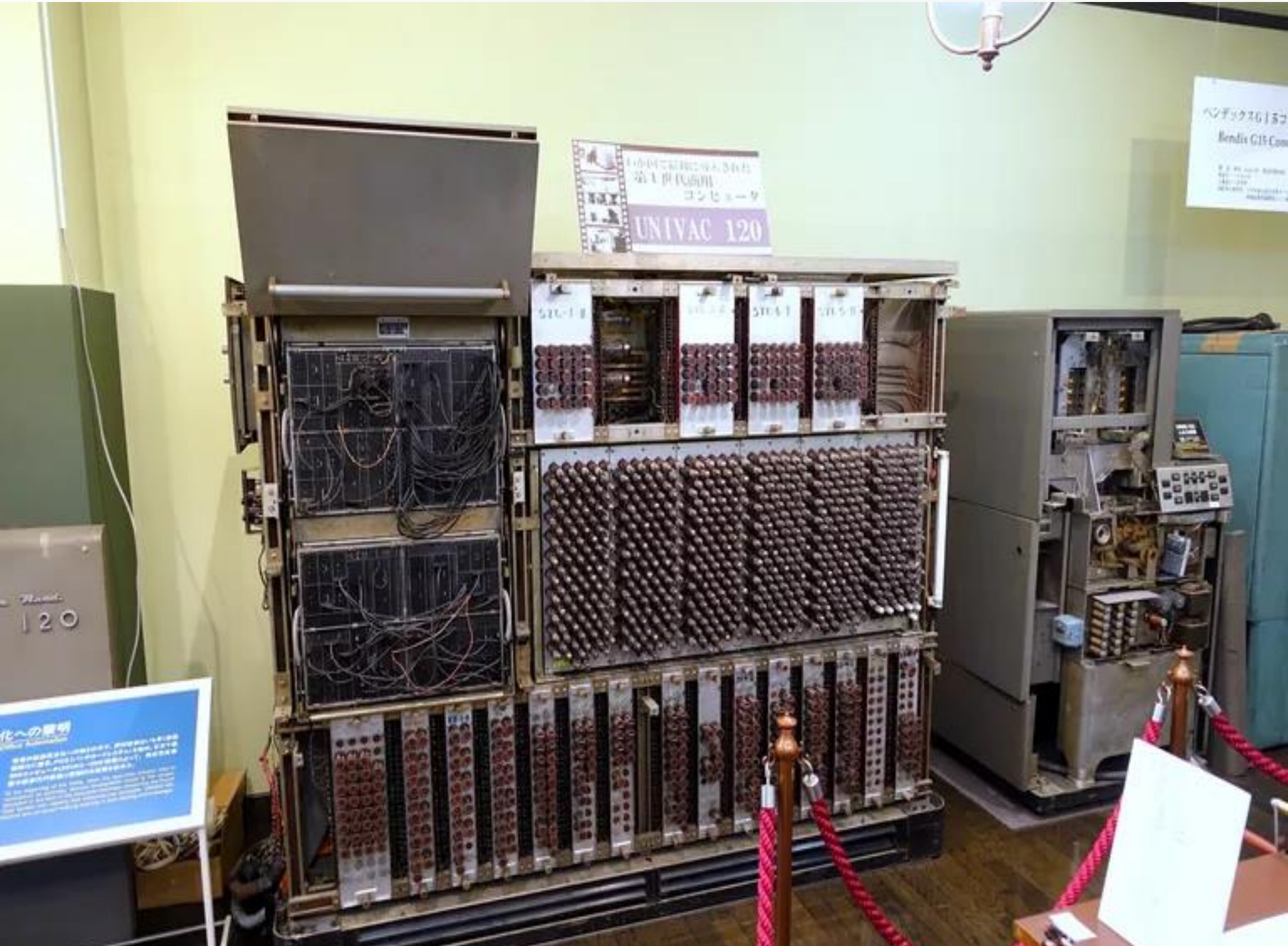
- Three major milestones have led to cloud computing: mainframe computing, cluster computing, and grid computing.



The evolution of distributed computing technologies, 1950s–2010s.

Universal Automatic Computer

UNIVAC (Universal Automatic Computer) is a line of electronic digital stored-program computers starting with the products of the Eckert–Mauchly Computer Coorporation.


UNIVAC 120

Mainframe today

Mainframes are **data servers designed to process up to 1 trillion web transactions daily with the highest levels of security and reliability**. At their core, mainframes are high-performance computers with large amounts of memory and processors that process billions of simple calculations and transactions in real time.

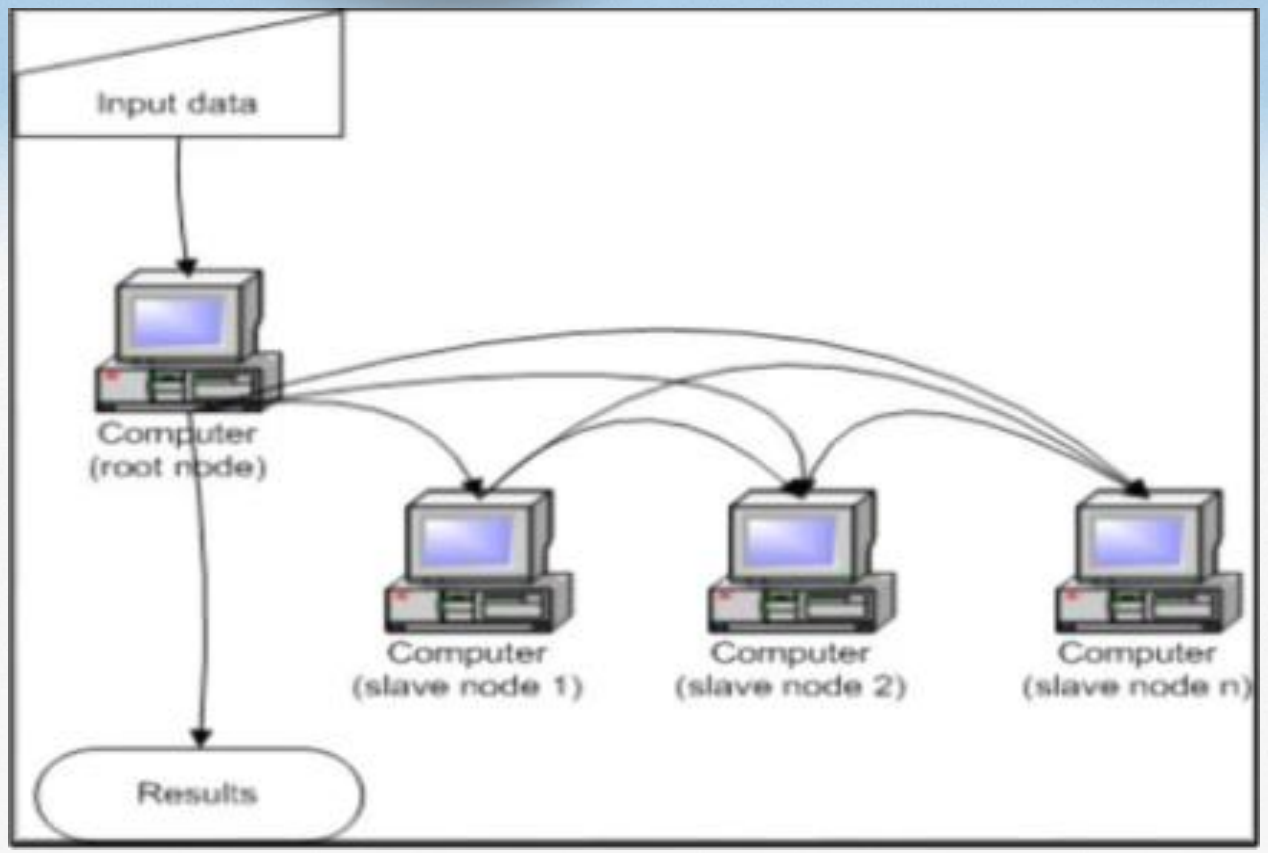
Clustering

It is the use of multiple computers, storage devices and redundant interconnection to form what appears to users as a singly highly available system.

Some of the popular implementations of cluster computing are **Google search engine, Earthquake Simulation, Petroleum Reservoir Simulation, and Weather Forecasting system**

A cluster is the type of parallel or distributed processing system, which consists of a collection of interconnected standalone computer cooperatively working together as a single integrated computing resource.

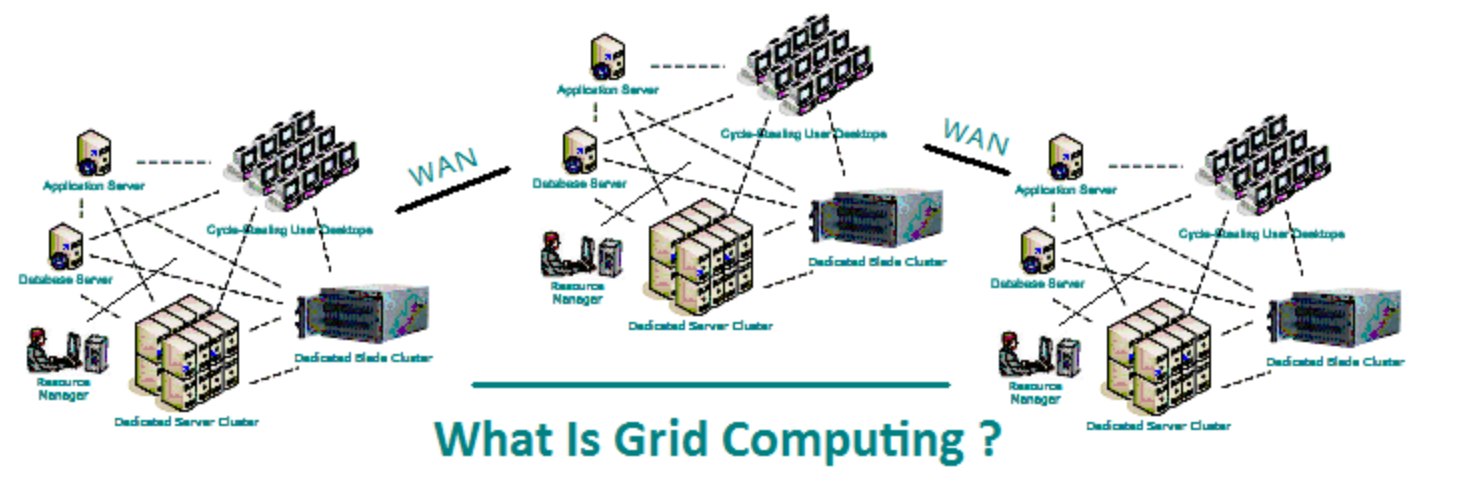
Simple cluster



Cluster Computing

Grid Computing

Grid computing is **a group of networked computers which work together as a virtual supercomputer to perform large tasks, such as analyzing huge sets of data or weather modeling**.



Cloud Computing

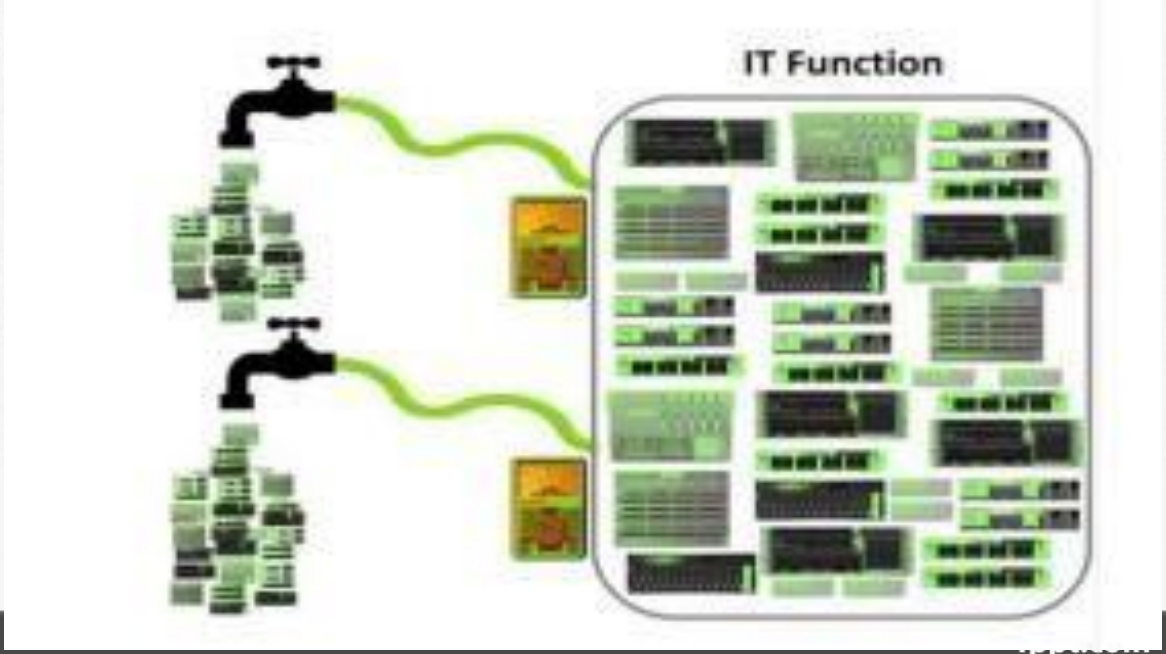
- Cloud Computing is a technology advancement that focuses on the way in which we design computing system, develop applications and leverage existing services for building software.
- It is based on the concept of dynamic provisioning, which is applied not only to services but also to compute capability, storage, networking and information Technology infrastructure in general

Cloud Computing in Nutshell

- Analogy to electricity use
- Technologies such as cluster, grid, and now cloud computing, have all aimed at allowing access to large amounts of computing power in a fully virtualized manner, by aggregating resources and offering a single system view

Contd…

- Utility computing describes a business model for on-demand delivery of computing power; consumers pay providers based on usage.



Contd……

- It denotes a model on which a computing infrastructure is viewed as a “cloud,” from which businesses and individuals access applications from anywhere in the world on demand

Contd…

- Computing itself, to be considered fully virtualized, must allow computers to be built from distributed components such as processing, storage, data, and software resources.
- Technologies such as cluster, grid, and now, cloud computing, have all aimed at allowing access to large amounts of computing power in a fully virtualized manner, by aggregating resources and offering a single system view.

Contd…

- In addition, an important aim of these technologies has been delivering computing as a utility. Utility computing describes a business model for on-demand delivery of computing power; consumers pay providers based on usage (“payas-you-go”), similar to the way in which we currently obtain services from traditional public utility services such as water, electricity, gas, and telephony.

Contd….

- Cloud computing turns IT services into utilities. Such a delivery model is made possible by the effective composition of several technologies, which have reached the appropriate maturity level.

- Web 2.0 technologies play a central role in making cloud computing an attractive opportunity for building computing systems. They have transformed the Internet into a rich application and service delivery platform, mature enough to serve complex needs.(Web 2.0 sites include **Wikipedia, Facebook, Twitter, and various blogs**, which all have transformed the way the same information is shared and delivered.)
- Service orientation allows cloud computing to deliver its capabilities with familiar abstractions
- virtualization confers on cloud computing the necessary degree of customization, control, and flexibility for building production and enterprise systems.

Contd…

- BUYYA “Cloud is a parallel and distributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements (SLA) established through negotiation between the service provider and consumers

Contd…

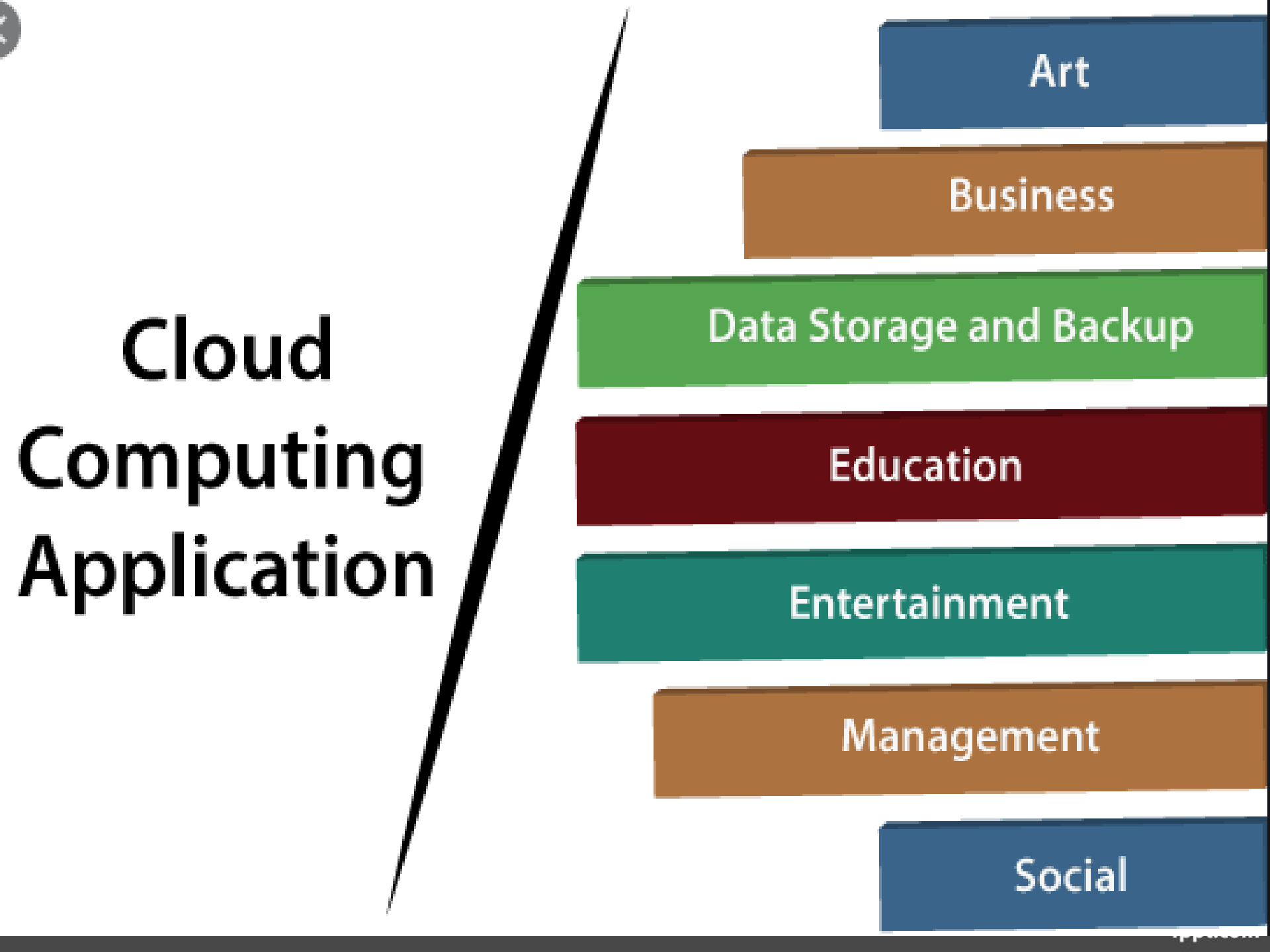
- .”NIST(National Institute of Standards and Technology)a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Contd…

- While there are countless other definitions, there seems to be common characteristics between the most notable ones listed above, which a cloud should have: ((i) pay-per-use (no ongoing commitment, utility prices);(ii) elastic capacity and the illusion of infinite resources;(iii) self-service interface(iv) resources that are abstracted or virtualised.

Cloud Computing Animation

Cloud Computing Application



Characteristics of an ideal cloud computing model:

- Scalability: You have access to unlimited computer resources as needed.
- Elasticity: You have the ability to right-size resources as required.
- Low barrier to entry: You can gain access to systems for a small investment.
- Utility: A pay-as-you-go model matches resources to need on an ongoing basis. .

Cloud Types Deployment Model: Service Model

- Deployment Model: Refers to location and management of the cloud's infrastructure
- Service Model: Consists of particular types of services that can be accessed on cloud computing platform

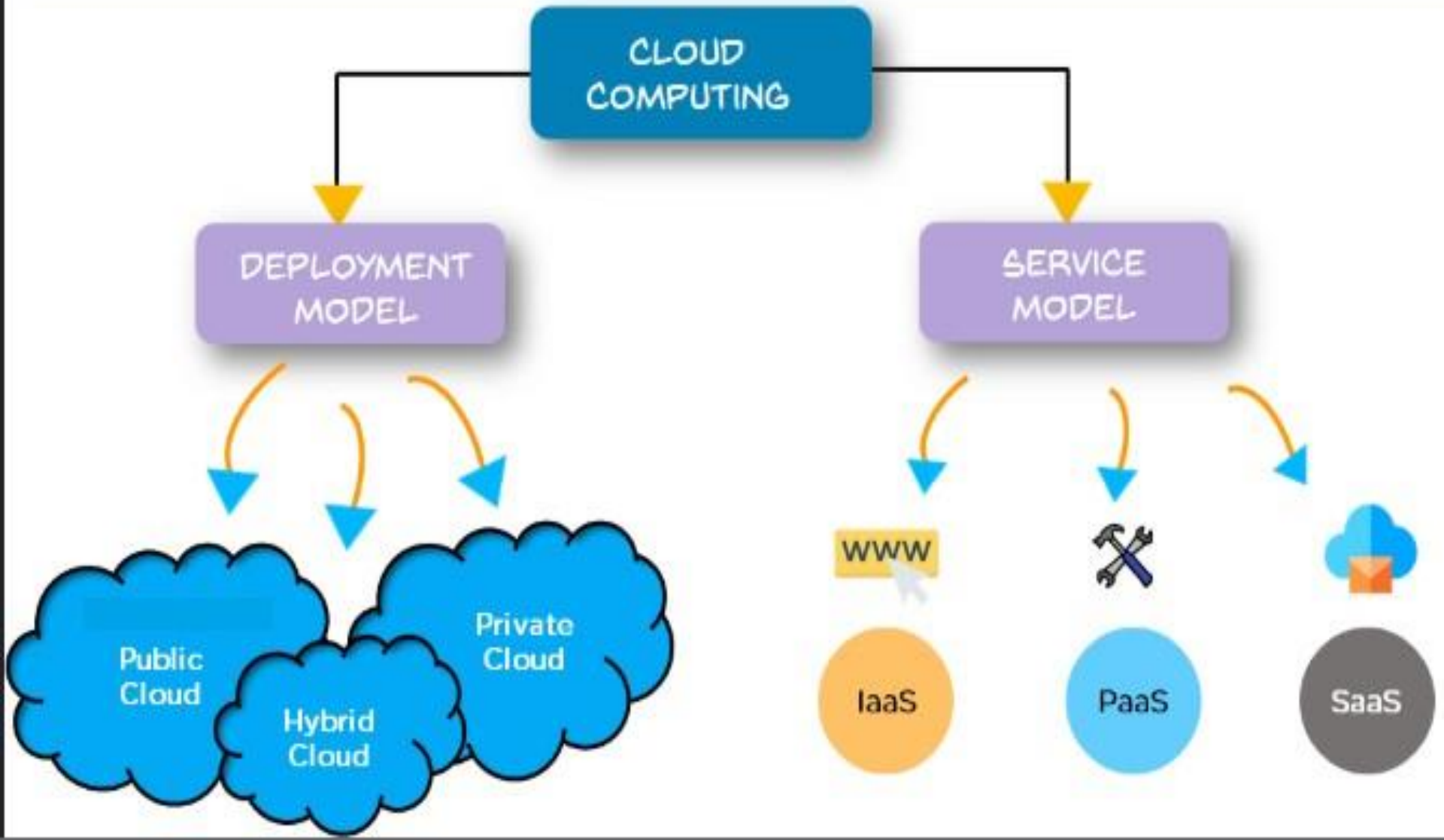
Cloud Types Deployment Model: Service Model

- Deployment Model: Refers to location and management of the cloud's infrastructure→ Deployment models describe how cloud infrastructure is physically or logically organized and where it's located

Cloud Types Deployment Model: Service Model

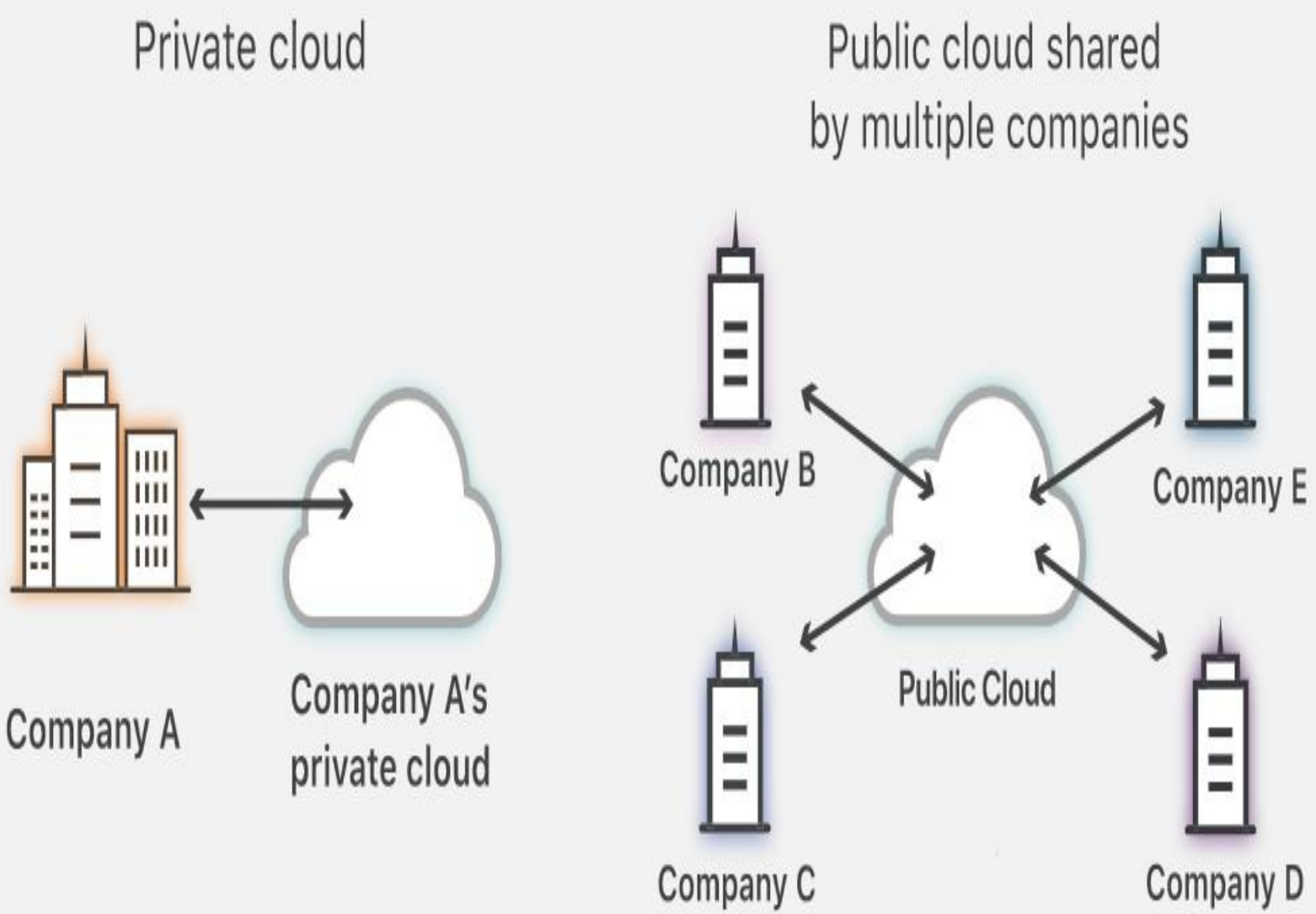
- Service Model: Consists of particular types of services that can be accessed on cloud computing platform→Service models describe how cloud services are delivered to users. The primary service models are often referred to as the "SPI" model

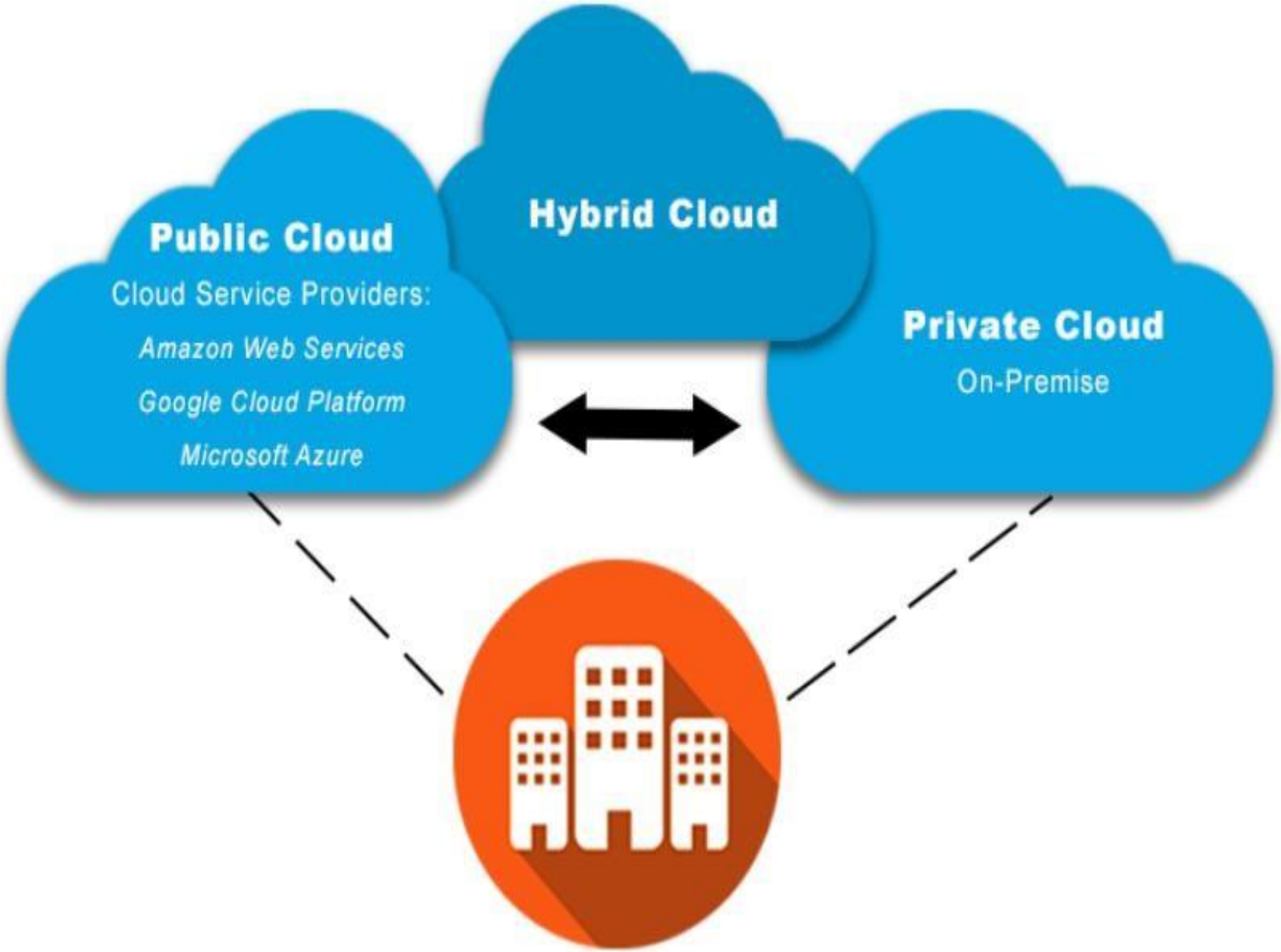
LAYERS AND TYPES OF CLOUDS



Contd….

- Public Cloud : Hosted , operated and managed by a third party system owned by organization selling cloud services.
- Private Cloud: The private cloud infrastructure is operated for the exclusive use of an organization. The cloud may be managed by that organization or a third party. Private clouds may be either on- or off-premises.


Private cloud
Company A
Company A's
private cloud
Public cloud shared
by multiple companies
Company B
Company E
Public Cloud
Company C
Company D


Public Cloud
Cloud Service Providers:
Amazon Web Services
Google Cloud Platform
Microsoft Azure
Hybrid Cloud
Private Cloud
On-Premise

- Hybrid Cloud :

A hybrid cloud combines multiple clouds (private,& public) where those clouds retain their unique identities, but are bound together as a unit.

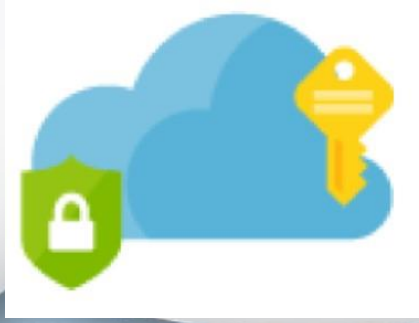
Public Cloud

- Public clouds are the most common way of deploying cloud computing.
- The cloud resources (like servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet.
- Microsoft Azure is an example of a public cloud.
- With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider.
- In a public cloud, you share the same hardware, storage, and network devices with other organizations or cloud “tenants.”
- You access services and manage your account using a web browser. Public cloud deployments are frequently used to provide web-based email, online office applications, storage, and testing and development environments.

Advantages of public clouds:

- Lower costs —no need to purchase hardware or software, and you pay only for the service you use.
- No maintenance —your service provider provides the maintenance.
- Near-unlimited scalability —on-demand resources are available to meet your business needs.
- High reliability —a vast network of servers ensures against failure.

Private Cloud



- A private cloud consists of computing resources used exclusively by one business or organization. The private cloud can be physically located at your organization’s on-site datacenter, or it can be hosted by a third-party service provider.

Contd…

- But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organization.
- In this way, a private cloud can make it easier for an organization to customize its resources to meet specific IT requirements.

Contd….

- Private clouds are often used by government agencies, financial institutions, any other mid- to large-size organizations with business-critical operations seeking enhanced control over their environment.

Advantages of a private clouds:

- More flexibility —your organization can customize its cloud environment to meet specific business needs.
- Improved security —resources are not shared with others, so higher levels of control and security are possible.
- High scalability —private clouds still afford the scalability and efficiency of a public cloud.

Hybrid Cloud

- In a hybrid cloud, data and applications can move between private and public clouds for greater flexibility and more deployment options.
- For instance, you can use the public cloud for high-volume, lower-security needs such as web-based email, and the private cloud (or other on-premises infrastructure) for sensitive, business-critical operations like financial reporting.

Advantages of hybrid clouds

- Control—your organization can maintain a private infrastructure for sensitive assets.
- Flexibility—you can take advantage of additional resources in the public cloud when you need them.
- Cost-effectiveness—with the ability to scale to the public cloud, you pay for extra computing power only when needed.
- Ease—transitioning to the cloud doesn't have to be overwhelming because you can migrate gradually—phasing in workloads over time.

Service Models

SaaS
- Software

Office Communications Online · NETSUITE · salesforce.com · ZOHO Work. Online · workday.

PaaS
- Platform

Windows Azure Platform · Live Services · Google App Engine · force.com platform as a service

IaaS
- Infrastructure

rackspacecloud · amazon web services · GOGRID · GIGASPACES

provides users with virtualized computing resources over the internet

- It is the **most flexible** type of cloud service which lets you rent the hardware and contains the basic building blocks for cloud and IT.
- **It gives complete control over the hardware** that runs your application (servers, VMs, storage, networks & operating systems).
- It's an **instant computing** infrastructure, provisioned and managed over the internet.

✓ IaaS gives you the very best level of flexibility and management control over your IT resources.

✓ It is most almost like the prevailing IT resources with which many IT departments and developers are familiar.

Examples of IaaS: **Virtual Machines** or **AWS EC2**, Storage or Networking.

- Infrastructure as a Service(IaaS)

-Deliver Infrastructure on Demand in the form of virtual Hardware, Storage and Networking. Virtual Hardware is utilized to provide compute on demand in the form of virtual machine instances

- Eg. Amazon EC2, S3, Eucalyptus, GoGrid, Rightspace Cloud,Google Compute Engine

Renting a data center form a cloud service provider

In this model,we, as a cloud customers don`t have to worry about how CSP manages their servers, storage and network

It offers a platform that includes the underlying infrastructure, development tools, and services needed to build, deploy, and manage applications.

- PaaS is a cloud service model that gives a ready-to-use development environment where developers can specialize in writing and executing high-quality code to make customized applications.
- It helps to create an application quickly without managing the underlying infrastructure. For example, when deploying a web application using PaaS, you don’t have to install an operating system, web server, or even system updates. However, you can scale and add new features to your services.
- This cloud service model makes the method of developing and deploying applications simpler and it is more expensive than IaaS but less expensive than SaaS.
- **This helps you be more efficient as you don’t get to worry about resource procurement, capacity planning, software maintenance, patching, or any of the opposite undifferentiated work involved in running your application**.

Examples of PaaS: Elastic Beanstalk or Lambda from AWS, WebApps, Functions or Azure SQL DB from Azure, Cloud SQL DB from Google Cloud, or Oracle Database Cloud Service from Oracle Cloud.

- Platform as a Service (PaaS)

-Deliver scalable and elastic runtime environments on demand that host the execution of applications.

-Backed by core middleware platform for creating abstract environment to deploy and execute application

This model is for developers and companies To create, run,test,host and deploy applications
This service model allows us to focus on applications and data

It delivers software applications and services over the internet on a subscription basis. Users access these applications through a web browser, and the software is hosted and maintained by the SaaS provider

- Software as a service (SaaS)

-Provide application and services on demand e.g office automation, Photo Editing software, Facebook., Twitter accessible through browser on demand

In this model cloud customers outsource almost everything to a cloud service provider:

1. Infrastructure
2. Data Storage
3. Networks and applications

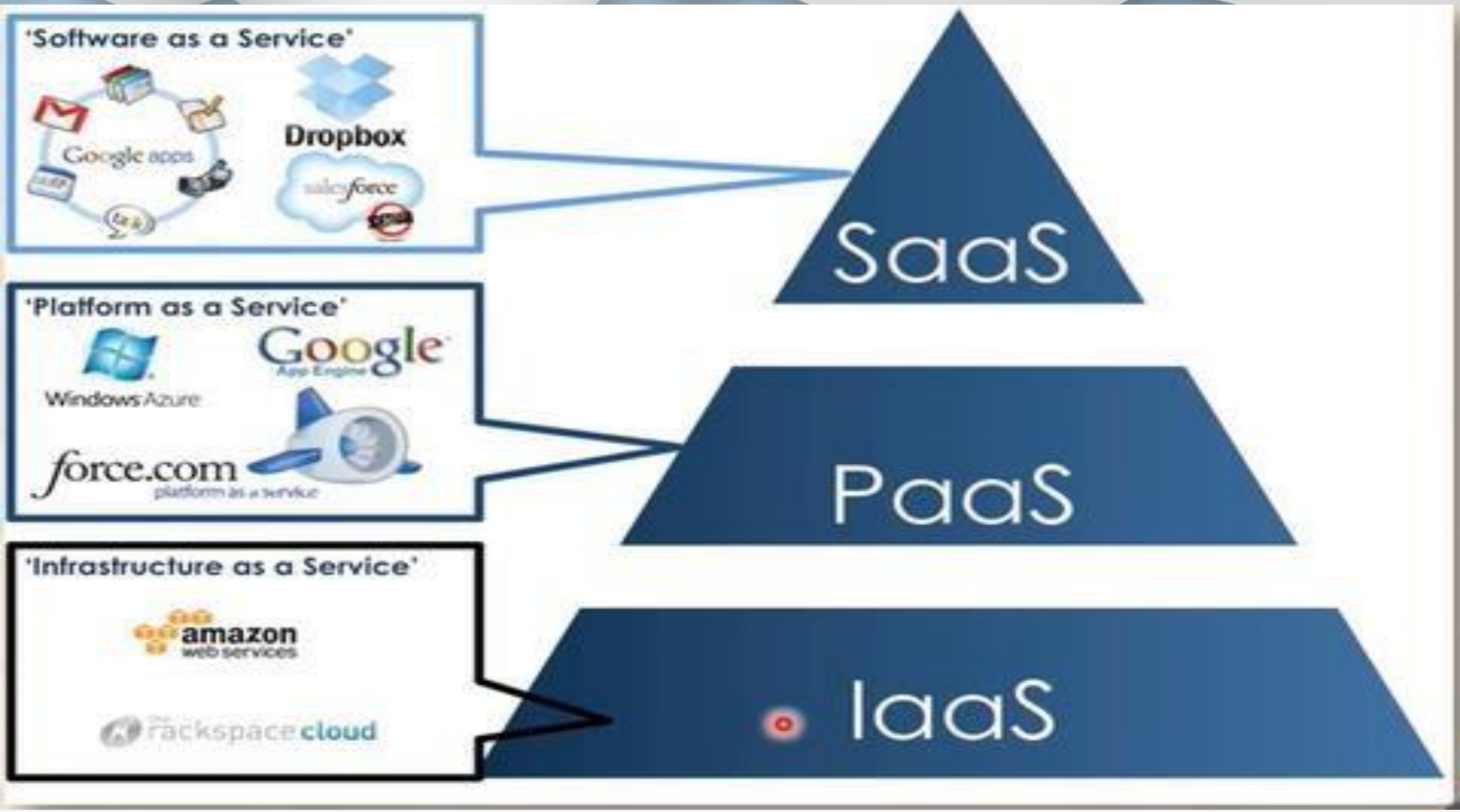
The amount of configuration ,management and trouble shooting at customers end is minimal

As a cloud customers, we do not need install any software or hardware. As long as our computer has browsers installed this. Some time we called this type of computer s thin client

SaaS would be beneficial for many smaller companies


On-site
IaaS
PaaS
SaaS
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
You manage
Service provider manages

Contd…..


'Software as a Service'
Google apps
Dropbox
salesforce
SaaS
'Platform as a Service'
Windows Azure
Google
App Engine
force.com
platform as a service
PaaS
'Infrastructure as a Service'
amazon
web services
Rackspace cloud
IaaS

Cloud Companies/Service Providers

Common Examples of SaaS, PaaS, & IaaS

Platform Type	Common Examples
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
IaaS	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

Benefits of Cloud Computing

- Lower Computational Costs
- Improved Performance
- Reduced Software Costs
- Instant Software updates
- Unlimited storage capacity
- Increased Data Reliability
- Universal Document Access
- Latest version availability
- Easier Group Collaboration/ Sharing
- Device Independence Lower computer costs;

Risk of Cloud Computing

- By whom data and application will be accessed
- Security methods for data storage and the transmission
- How data and application from various consumers reserved separately
- Where will data be stored

Limitation of Cloud Computing

- Availability service
- Data Lock In
- Data segregation
- Scaling resources
- Location of data
- Deletion of data
- Recovery and Backup

Online social networks and applications

- A **social networking service** (also **social networking site** or **social media**) is an online platform which people use to build social networks or social relationships with other people who share similar personal or career interests, activities, backgrounds or real-life connections.

One can categorize social-network services into four types:

- Socializing social network services used primarily for socializing with existing friends (e.g., Facebook)
- online social networks are decentralized and distributed computer networks where users communicate with each other through internet services.
- networking social network services used primarily for non-social interpersonal communication (e.g., LinkedIn, a career- and employment-oriented site)
- social navigation social network services used primarily for helping users to find specific information or resources (e.g., Goodreads for books)

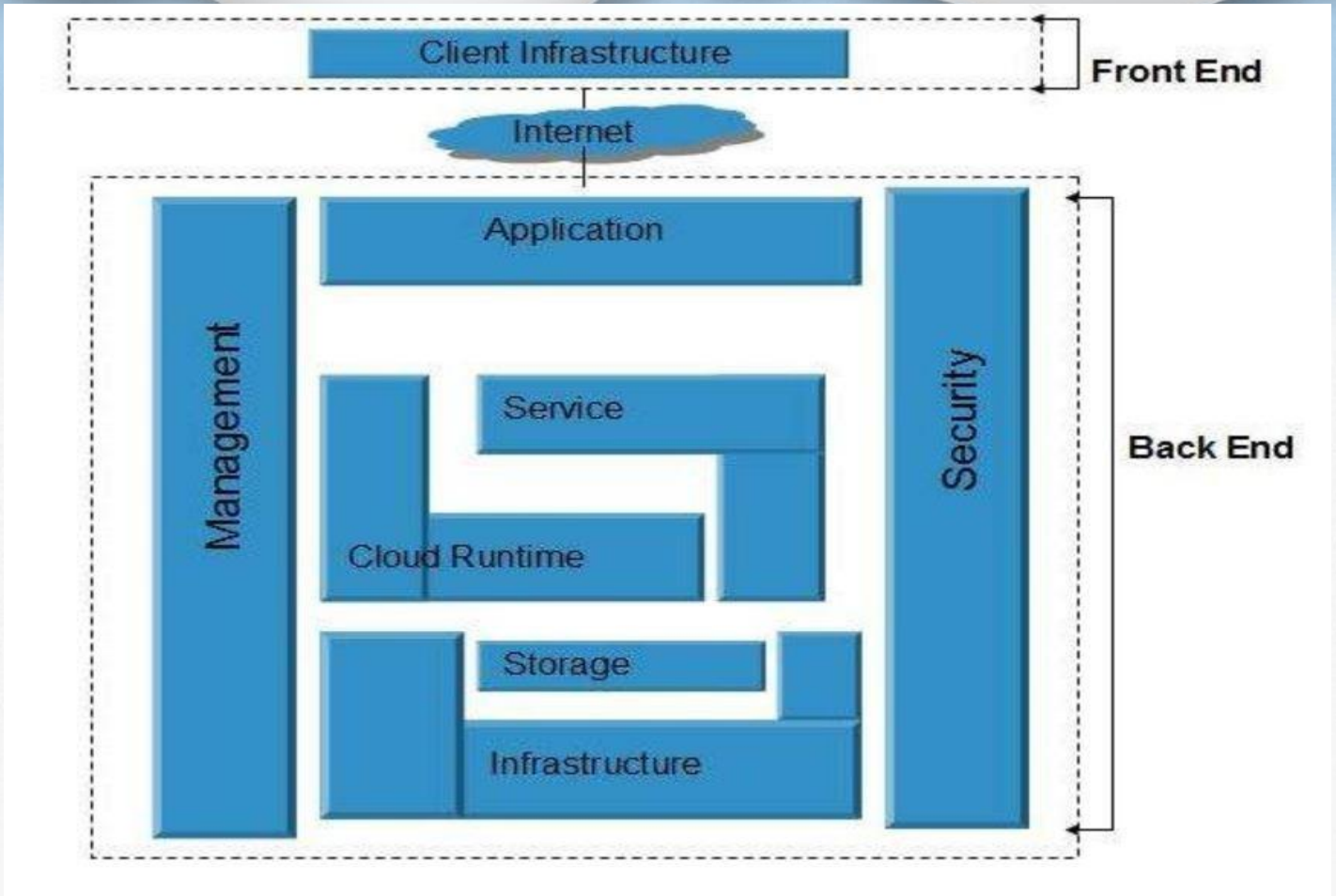
Cloud Computing

- Cloud computing is particularly valuable because it shifts capital expenditures into operating expenditures.
- It also shifts risk away from an organization and onto the cloud provider.
- Cloud computing presents new opportunities to users and developers because it is based on the paradigm of a shared multitenant utility.

Contd…..

- A cloud is an infrastructure that can be partitioned and provisioned, and resources are pooled and virtualized. If the cloud is available to the public on a pay-as-you-go basis, then the cloud is a public cloud, and the service is described as a utility

Cloud computing Architecture



- Cloud Computing architecture comprises of many cloud components, which are loosely coupled. We can broadly divide the cloud architecture into two parts:
- Front End
- Back End

Each of the ends is connected through a network, usually Internet.

Front End

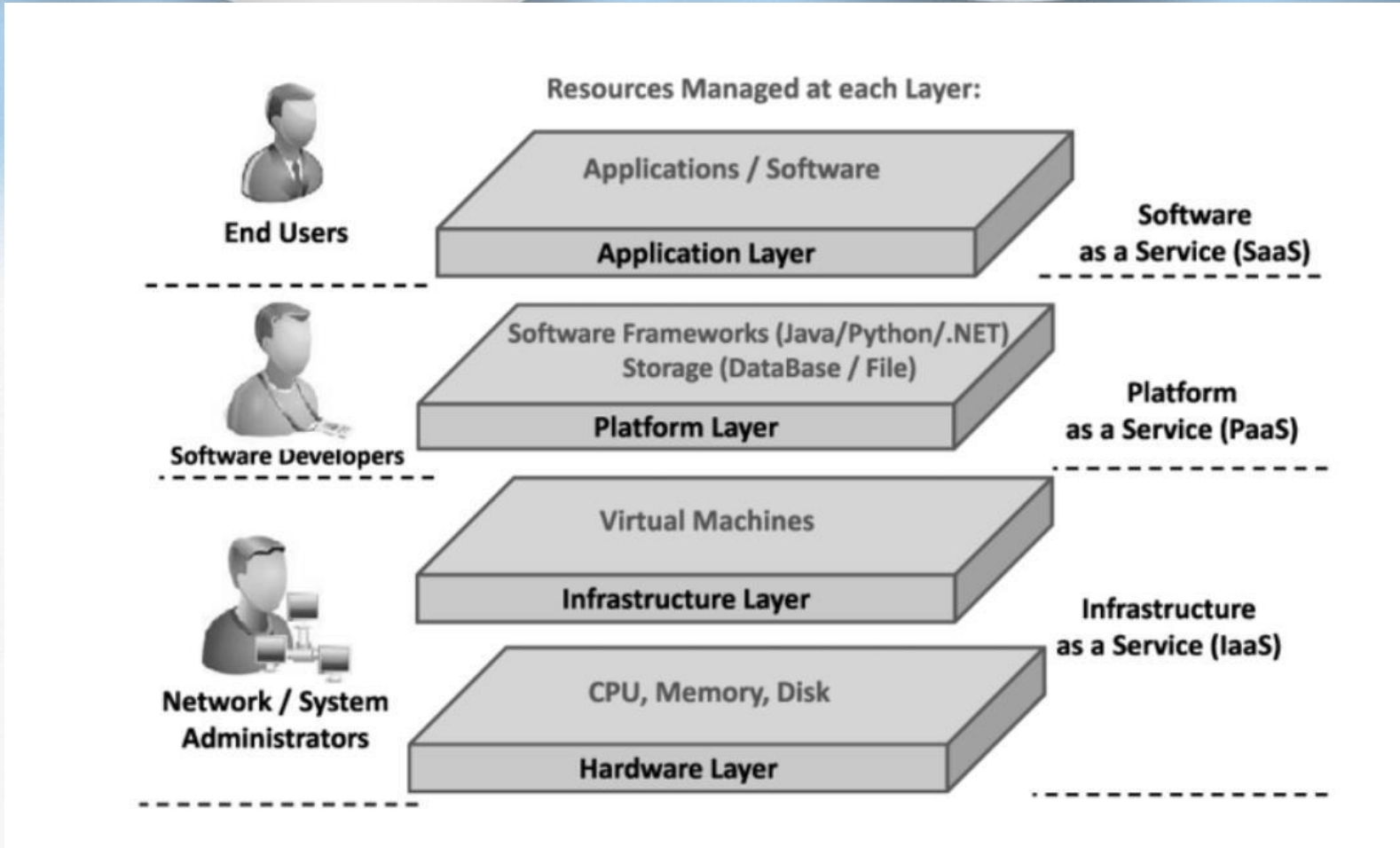
- The **front end** refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser.

Back End

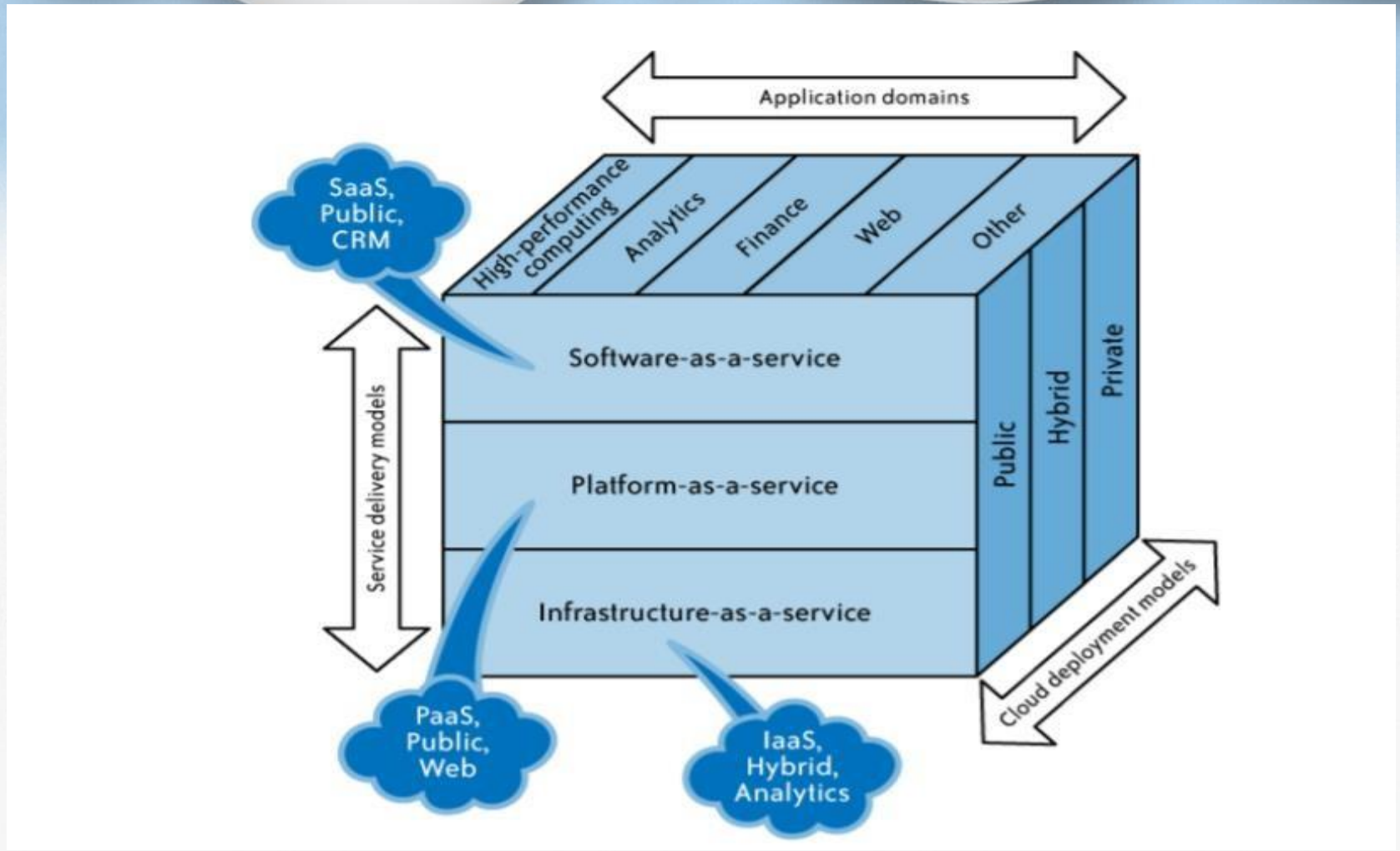
- The **back End** refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

- It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols.
- The server employs certain protocols known as middleware, which help the connected devices to communicate with each other.

Cloud Computing Layers



SPI Frame work for Cloud Computing



On demand computing virtualization at the infrastructure level

On-demand computing and virtualization at the infrastructure level combine to provide highly flexible and scalable solutions for businesses and organizations.

On-Demand Computing at the Infrastructure Level:

Cloud Infrastructure: On-demand computing at the infrastructure level typically involves using cloud services from providers like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and others.

These providers offer a wide range of infrastructure services, including virtualized servers, storage, and networking resources, which can be provisioned and managed on-demand.

On-Demand Computing at the Infrastructure Level:

Resource Allocation: With on-demand computing, organizations can provision virtualized infrastructure resources as needed.

They can scale resources up or down based on changing requirements.

For example, during periods of high demand, additional virtual servers can be created and when demand decreases, these resources can be scaled down or terminated.

Virtualization at the Infrastructure Level:

Efficient Resource Utilization: Infrastructure-level virtualization involves partitioning physical hardware into multiple virtual instances, such as VMs or containers. This maximizes the use of underlying hardware resources.

Isolation: Virtualization ensures that each virtual instance operates independently, providing isolation between different workloads. Failures or issues in one virtual instance do not affect others.

Virtualization at the Infrastructure Level:

Flexibility: Virtualization enables organizations to run multiple operating systems and applications on a single physical server, facilitating resource allocation and management.

Resource Consolidation: It allows for the consolidation of workloads on fewer physical servers, reducing hardware and energy costs.

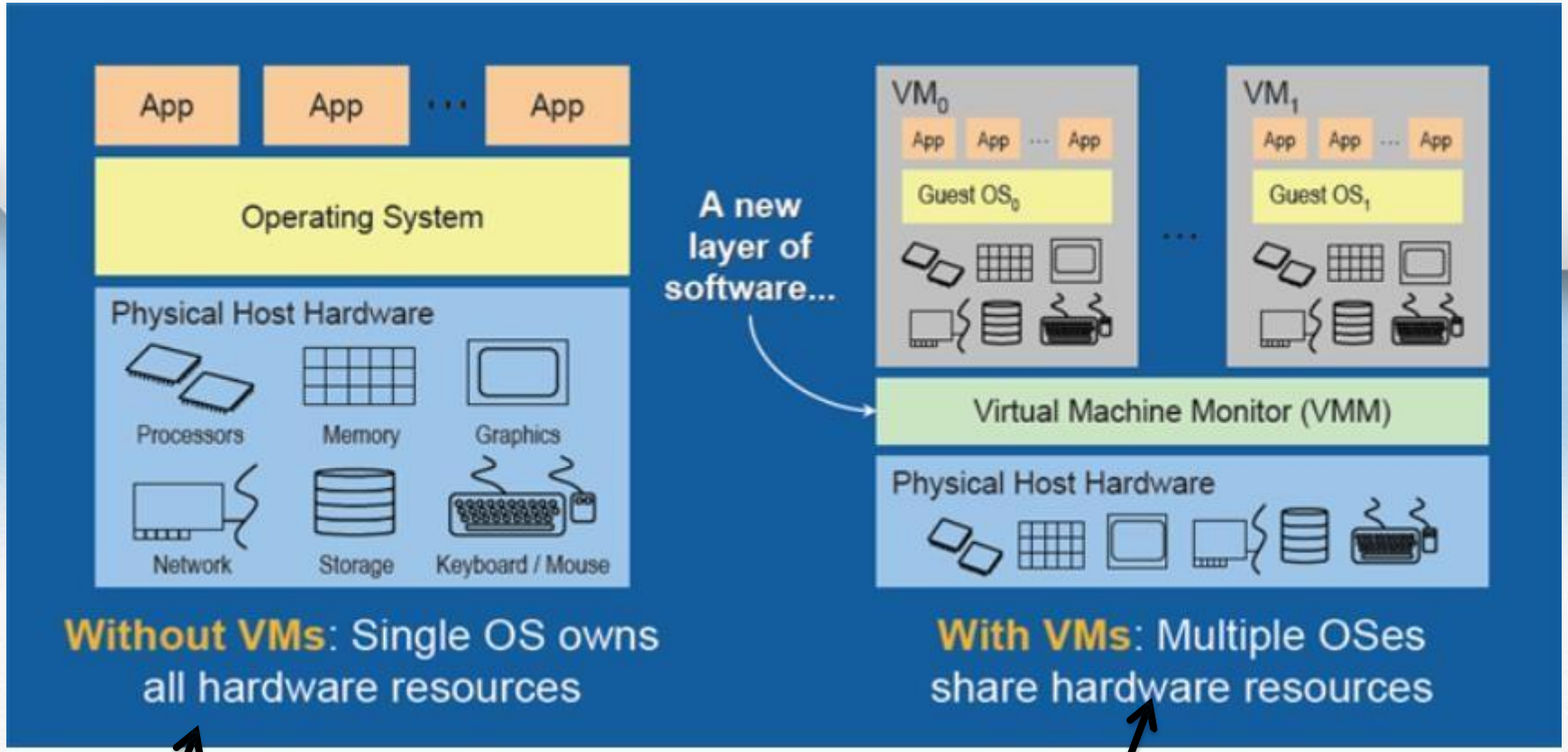
Virtualization

Virtualization is like creating virtual (not physical) copies of computers or software on a single physical machine.

It allows you to run multiple operating systems or applications on one computer, making your resources more efficient and flexible

Virtualization

- **Virtualization** is the process of running a virtual instance of a computer system in a layer abstracted from the actual hardware. Most commonly, it refers to running multiple operating systems on a computer system simultaneously.
- Virtualization enables multiple operating systems to run on the same physical platform



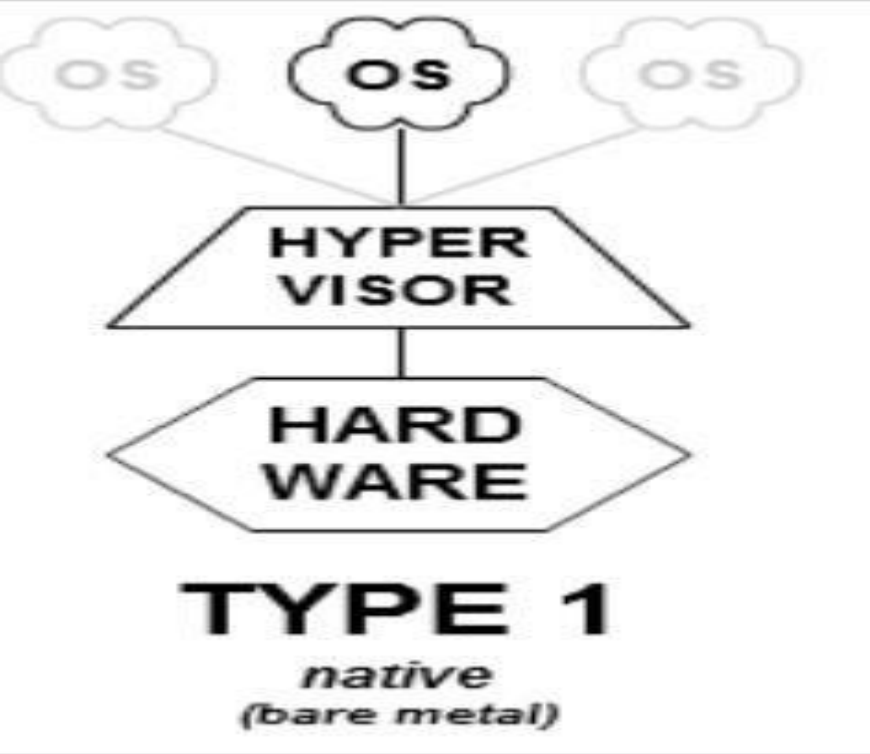
Without VMs: A single OS owns all hardware resources

With VMs: Multiple OSes, each running its own virtual machine, share hardware resources

Hypervisor

- **A hypervisor is a crucial piece of software that makes virtualization possible.** It abstracts guest machines and the operating system they run on, from the actual hardware.
- Hypervisors create a virtualization layer that separates CPU / Processors, RAM and other physical resources from the virtual machines you create.

Types of hypervisior

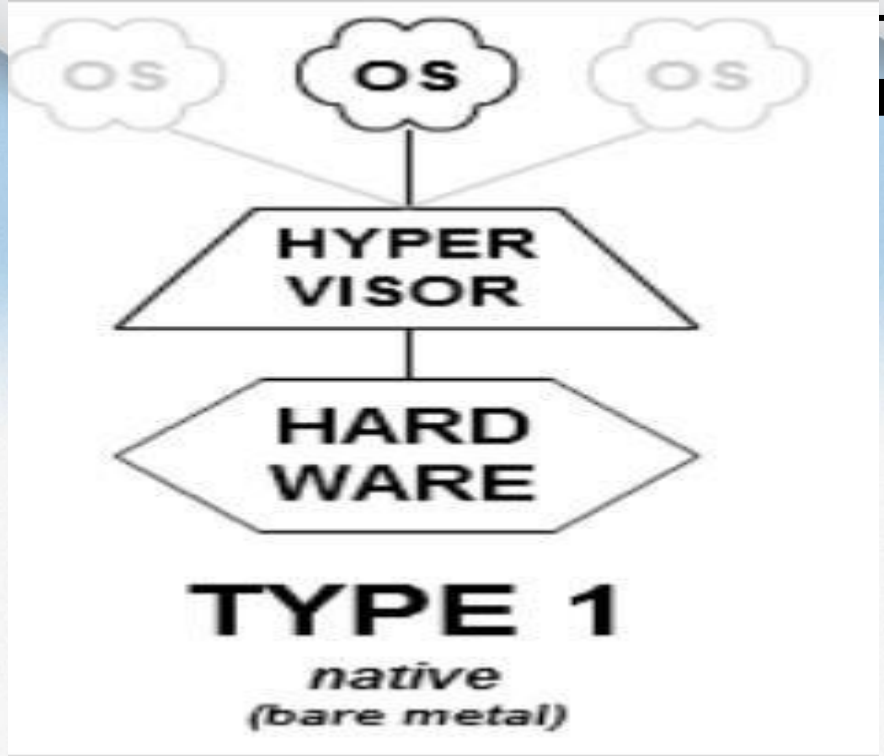


These hypervisors run directly on the host's hardware to control the hardware and to manage guest operating systems.

Type -1
HYPERVISIOR/Bare metal/native

- This type runs directly on the physical hardware.
- Examples include VMware vSphere/ESXi, Microsoft Hyper-V, and Xen.

Types of hypervisior



These hypervisors run directly on the host's hardware to control the hardware and to manage guest operating systems.

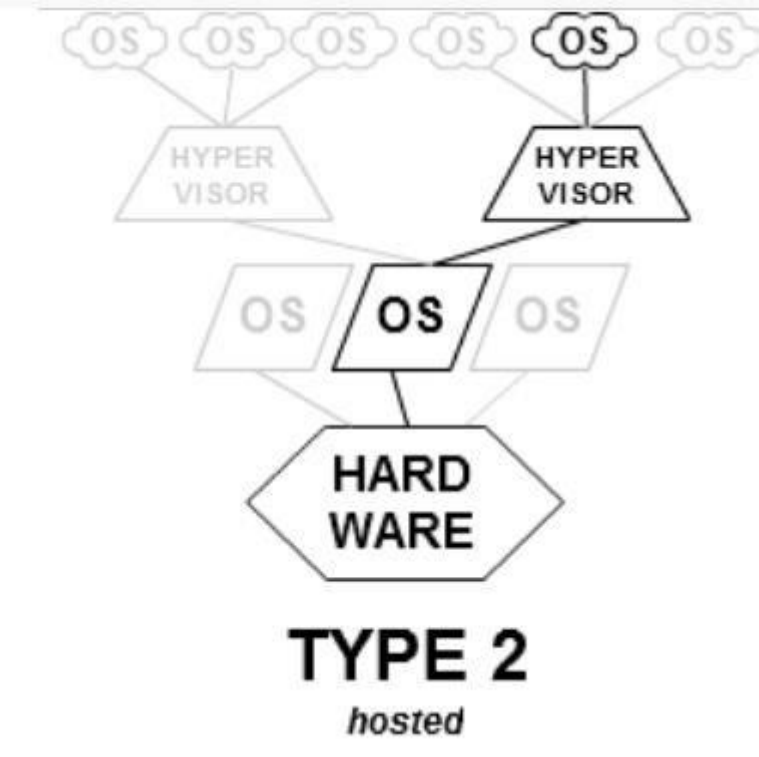
Type -1
HYPERVISIOR/Bare metal/native

- Xen is type 1 hypervisior(AWS uses Xen) providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently.
- **VMware ESXi** is an enterprise-class, **Elastic Sky X**
  Integrated
- VMware ESXi is a type-1 hyper-visors that run on server hardware's without the need of installing an additional Operating System.

KVM (Kernel-based Virtual Machine) is a virtualization technology for Linux-based systems.

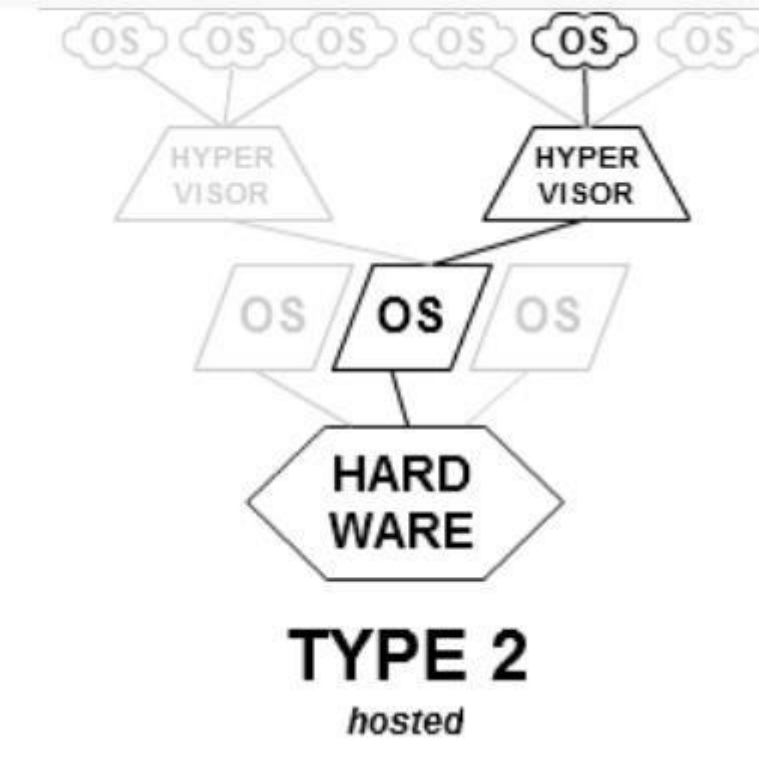
It is an open-source virtualization solution that allows you to turn Linux kernel into a hypervisor, enabling the creation and management of virtual machines (VMs).

Type 2



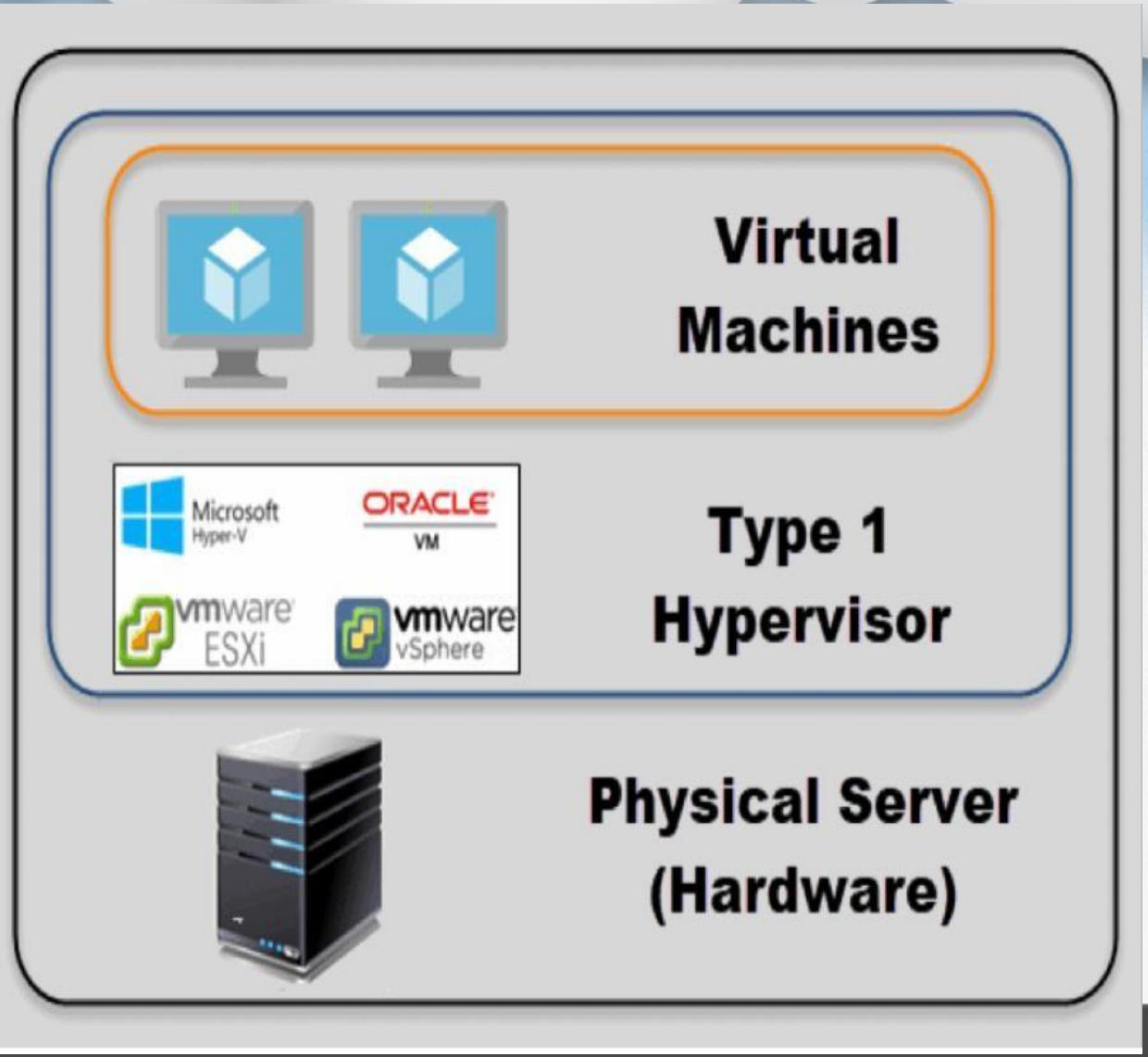
This type runs on top of an existing operating system. Examples include VMware Workstation, Oracle VirtualBox, and Parallels Desktop..

Type 2

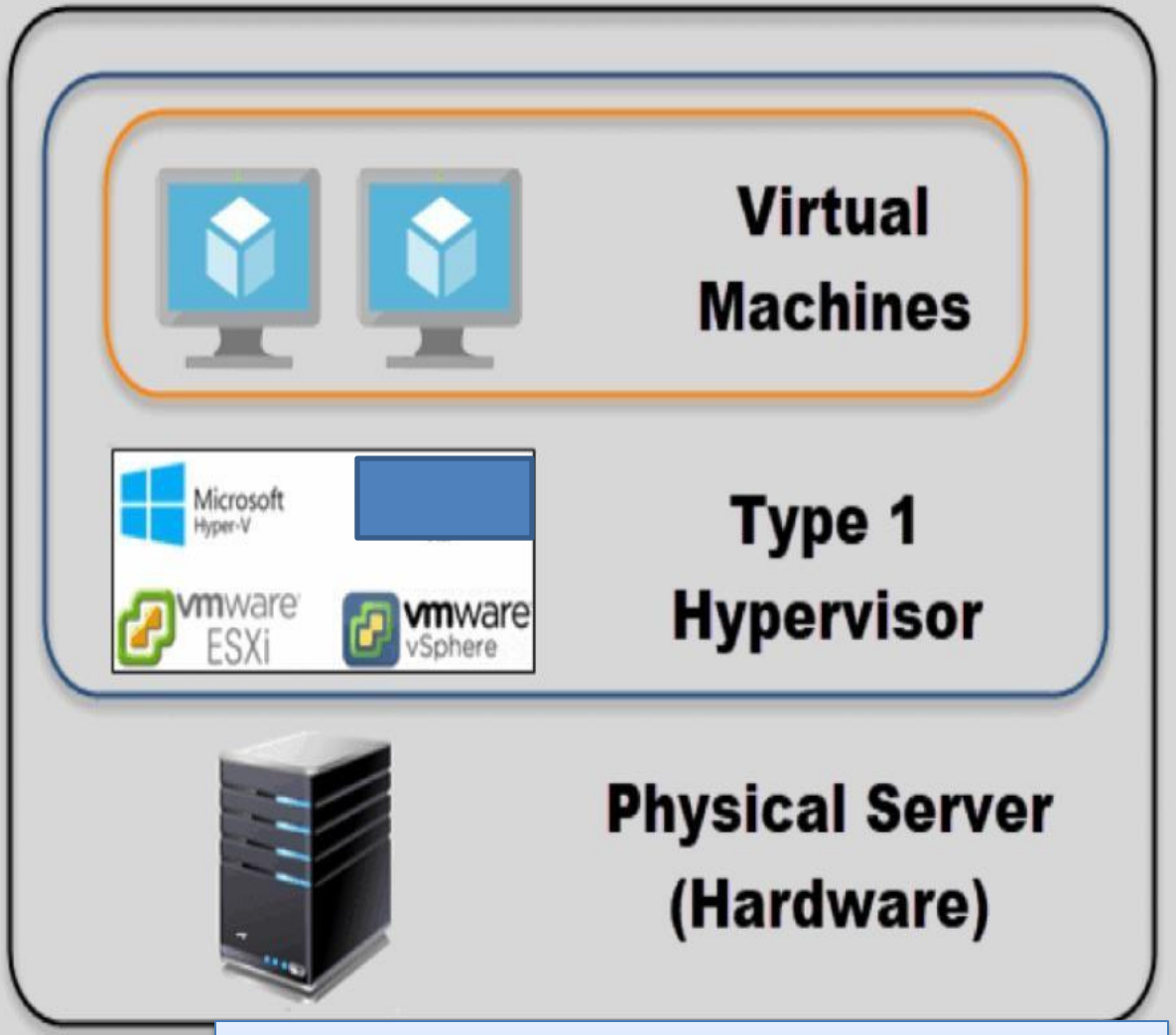


- These hypervisors run on a conventional operating system (OS) just as other computer programs do
- Type-2 hypervisors abstract guest operating systems from the host operating system
- Type -2 HYPERVISIOR/ Hosted hypervisor eg. VMware Workstation and Oracle VirtualBox and the examples of Type 2 hypervisors.

Type1 Hypervisior



A bare-metal hypervisor (Type 1) is a layer of software we install directly on top of a physical server and its underlying hardware.
There is no software or any operating system in between, hence the name *bare-metal hypervisor*



Bare-metal hypervisors can dynamically allocate available resources depending on the current needs of a particular VM.

A Type 1 hypervisor is proven in providing excellent performance and stability since it does not run inside Windows or any other operating system.

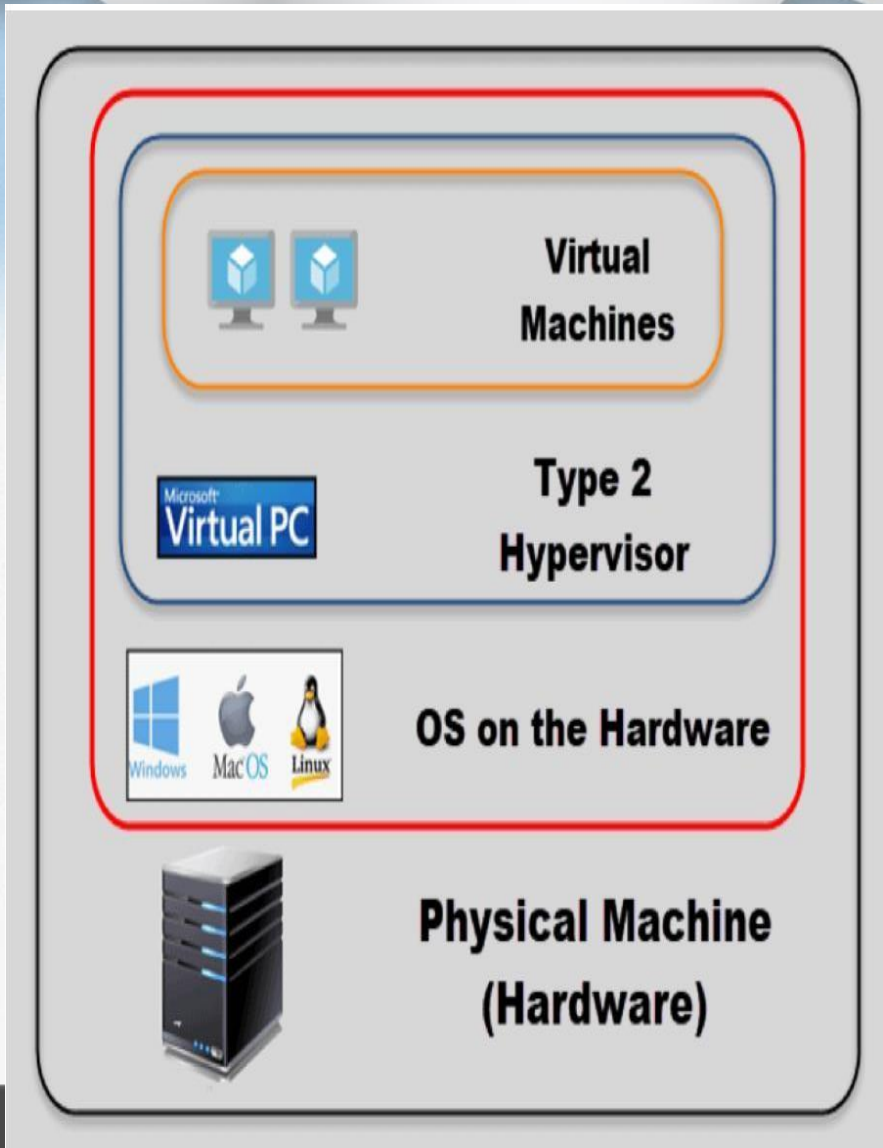
Type 1 hypervisors are an OS themselves, a very basic one on top of which you can run virtual machines.

The physical machine the hypervisor is running on serves virtualization purposes only.

You cannot use it for anything else.

Type 1 hypervisors are mainly found in enterprise environments.

Type-2 Hypervisior

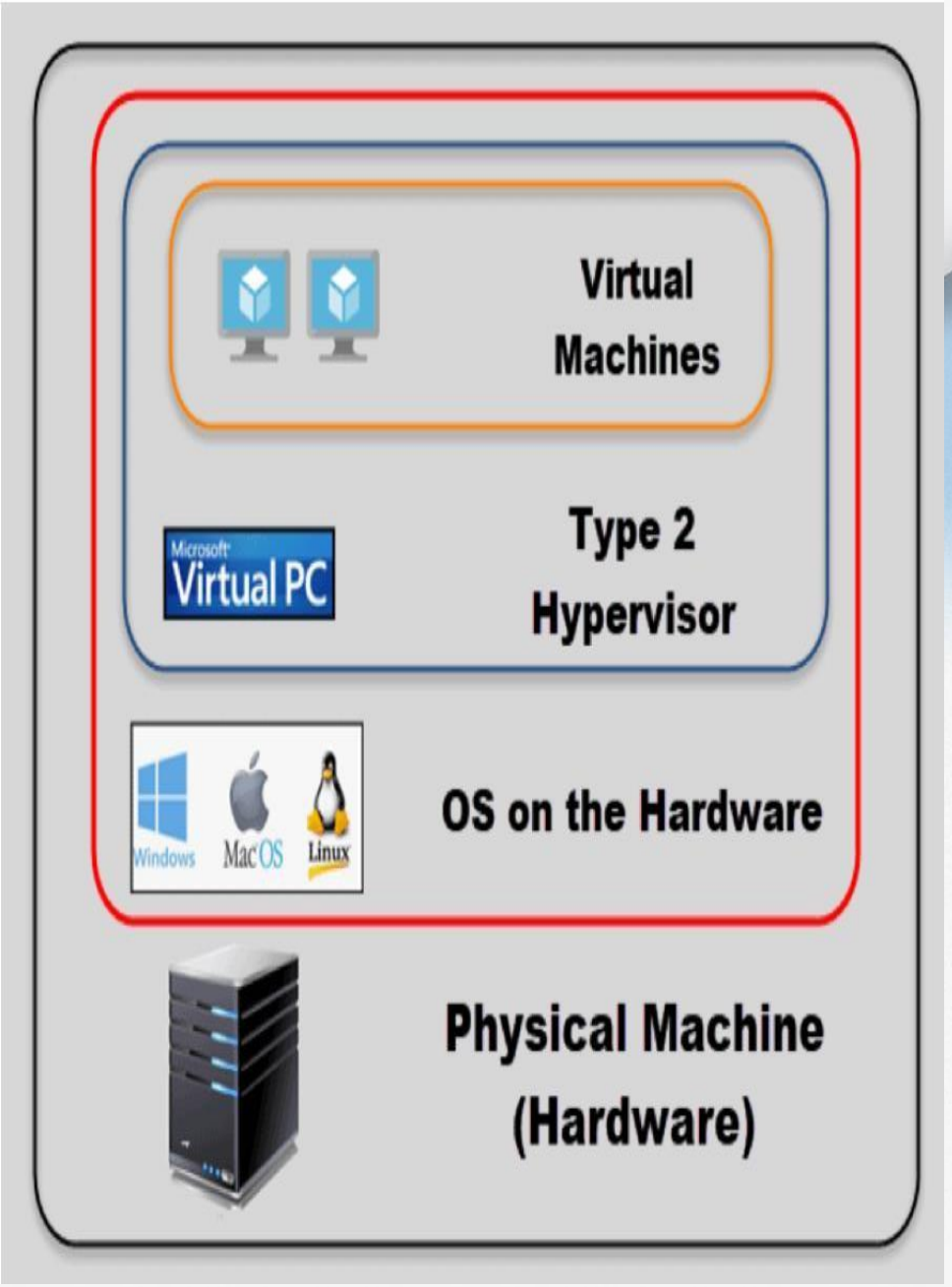


This type of hypervisor **runs inside of an operating system of a physical host machine.**

This is why we call type 2 hypervisors – ***hosted hypervisors*.**

-Hosted hypervisors have one software layer underneath. In this case we have:

- A physical machine.
- An operating system installed on the hardware (Windows, Linux, macOS).
- A type 2 hypervisor software within that operating system.
- The actual instances of guest virtual machines.



- Hosted hypervisors essentially also act as management consoles for virtual machines, you can perform any task using the built-in functionalities.

- There is no need to install separate software on another machine to create and maintain your virtual environment. You simply install and run a type 2 hypervisor as you would any other application within your OS. With it, you can create snapshots or clone your virtual machines, import or export appliances, etc.
- A type 2 hypervisor occupies whatever you allocate to a virtual machine.

Here is one example of a type 2 hypervisor interface (VirtualBox by Oracle):

Creating VMs:
After installing a hypervisor, you can create virtual machines. Each VM is like a self-contained computer with its own virtual CPU, memory, storage, and network interfaces.

Installing OSes:
Once you've created a VM, you can install an operating system on it, just like you would on a physical computer. You can install different OSes on different VMs, such as Windows, Linux distributions, macOS, and more.

Running Multiple OSes:
With your VMs set up and OSes installed, you can run them concurrently on the same physical machine. You can switch between them or even have them running simultaneously.

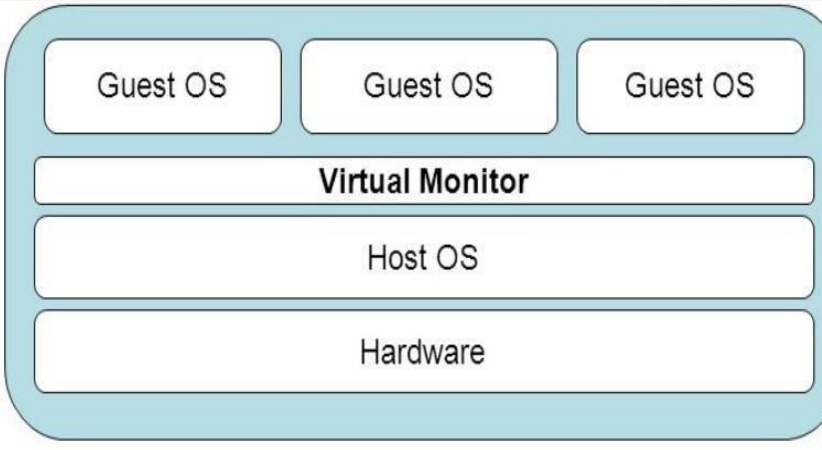
Isolation:
Each VM is isolated from the others. If one VM crashes or experiences issues, it won't affect the others. This isolation is a key benefit of virtualization.

Types of Virtualization

1. OS Virtualization
2. Server Virtualization
   a. Full Virtualization
   b. Para Virtualization
   c. OS Level Virtualization
3. Network Virtualization
4. CPU Virtualization
5. Storage Virtualization

1. OS Virtualization

- OS based virtualization is established of virtualization software prior operating system which is known as the host operating system.
- Operating System (OS) virtualization refers to the modification of a standard OS allowing multiple users to run different applications on a single computer at a time.
- **OS virtualization services** offer greater flexibility and reduced overhead



OS Virtualization is a specific form of virtualization that focuses on creating multiple virtual instances of operating systems on a single physical server or host. Each virtual instance, known as a virtual machine (VM), operates as if it has its own dedicated operating system, and multiple VMs can run concurrently on the same physical hardware.

OS virtualization is commonly used for server consolidation, resource isolation, and efficient management of workloads.
In summary, "virtualization" is a broader term encompassing various types of virtualization technologies, while "OS virtualization" specifically refers to the creation of virtual instances of operating systems. OS virtualization is a subset of the larger virtualization concept.

- In this virtualization, a user installs the virtualization software in the operating system of his system like any other program and utilize this application to operate and generate various virtual machines
- Here, the virtualization software allows direct access to any of the created virtual machine to the user. As the host OS can provide hardware devices with the mandatory support, operating system virtualization may affect compatibility issues of hardware even when the hardware driver is not allocated to the virtualization software.
- Virtualization software is able to convert hardware IT resources which require unique software for operation into virtualized IT resources. As the host OS is a complete operating system in itself, many OS based services are available as organizational management and administration tools can be utilized for the virtualization host management.

2. Server Virtualization

- Server Virtualization is the process of dividing a physical server into several virtual servers, called **virtual private servers**. Each virtual private server can run independently.

Server virtualization enables you to run multiple virtual machines (VMs) on a single physical server. VMs are isolated from each other and can run different operating systems. This technology is commonly used to maximize server hardware utilization, improve resource allocation, and simplify server management.

2. Server Virtualization

- **Server Virtualization** is the partitioning of a physical server into number of small virtual servers, each running its own operating system. These operating systems are known as guest operating systems. These are running on another operating system known as host operating system. Each guest running in this manner is unaware of any other guests running on the same host

Three Kinds of Server Virtualization:

Full virtualization is a virtualization technique where a hypervisor (virtual machine monitor) creates and manages virtual machines (VMs) that mimic the complete hardware environment of a physical computer. This means that guest operating systems (OSes) can run without any modifications, believing they are running on real hardware.

Three Kinds of Server Virtualization:

- **Full Virtualization**: Full virtualization uses a hypervisor, a type of software that directly communicates with a physical server's disk space and CPU.e.g VMware ESXi
- The hypervisor monitors the physical server's resources and keeps each virtual server independent and unaware of the other virtual servers.
- It also relays resources from the physical server to the correct virtual server as it runs applications. The biggest limitation of using full virtualization is that a hypervisor has its own processing needs. This can slow down applications and impact server performance.

Para-virtualization is a virtualization approach where the guest operating systems are modified to be aware of the virtualization layer (hypervisor) and work cooperatively with it. Unlike full virtualization, para-virtualized guest OSes are designed to use specialized APIs provided by the hypervisor.

- **Para-Virtualization**: Unlike full virtualization, para-virtualization involves the entire network working together as a cohesive unit. Since each operating system on the virtual servers is aware of one another in para-virtualization, the hypervisor does not need to use as much processing power to manage the operating systems.
- **Xen** is an open source hypervisor based on paravirtualization.

- Amazon EC2 (since August 2006) use Xen as the primary VM hypervisor for their product offerings.

OS-level virtualization

Operating System (OS)-level virtualization, also known container-based virtualization, is a virtualization technique that allows multiple isolated user spaces (containers) to share the same OS kernel of a host operating system.

Key characteristics and concepts of OS-level virtualization include:

Containerization: Containers are lightweight, portable, and isolated execution environments that package applications and their dependencies together. Each container shares the same host OS kernel but runs as an independent process with its own file system, libraries, and application code.

Efficiency: OS-level virtualization is highly efficient because it eliminates the need for multiple OS kernels. Since containers share the host OS kernel, they have minimal overhead, resulting in faster startup times and efficient resource utilization.

Key characteristics and concepts of OS-level virtualization include:

Isolation: Containers provide process-level isolation. Each container runs in its own user space, and processes within one container are isolated from processes in other containers. This isolation ensures that applications within a container do not interfere with one another.

Resource Control: OS-level virtualization solutions often include tools to control and allocate resources to containers. You can set limits on CPU, memory, and network bandwidth to ensure fair resource sharing among containers

.

Key characteristics and concepts of OS-level virtualization include:

Images and Registries: Containers are typically created from container images. Container images are lightweight, read-only snapshots of an application and its environment. Container registries (e.g., Docker Hub) store and distribute container images.

Portability: Containers are highly portable. You can create a container image on one system and run it on any other system that supports the same containerization platform. This consistency eliminates compatibility issues and ensures that applications run consistently across environments.

.

Key characteristics and concepts of OS-level virtualization include:

Security: While containers provide isolation at the process level, additional security measures, such as user namespace mapping and container runtime security scanning, are often employed to enhance container security.

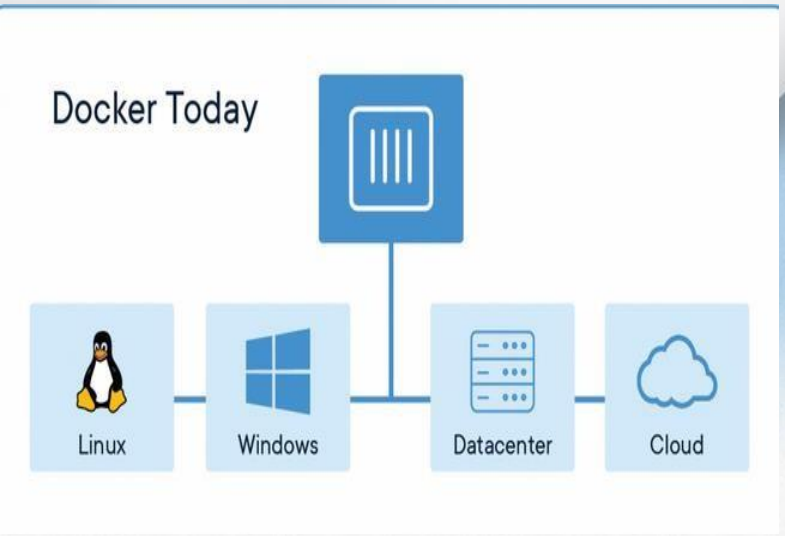
Popular containerization platforms include Docker, containerd,

- **OS-level virtualization** is an operating system paradigm in which the kernel allows the existence of multiple isolated user space instances. Such instances, called **containers** (Docker), may look like real computers from the point of view of programs running in them.
- A computer program running on an ordinary operating system can see all resources (connected devices, files and folders, network shares, CPU power, quantifiable hardware capabilities) of that computer.
- However, programs running inside of a container can only see the container's contents and devices assigned to the container.
- Examples of virtualization that uses hardware assisted are Kernel-based Virtual Machine (KVM), VirtualBox, Xen, Hyper-V, and VMware products.

Contd...

This technique virtualizes the physical server at the operating system level. Here, the host OS is a modified kernel that allows the execution of multiple isolated Containers -also known as Virtual Private Server (VPS),or virtualized server-. Each Container is an instance that shares the same kernel of the host OS. Some examples that use this technique are Linux-VServer, Solaris Zones, and OpenVZ. This implementations are widely used. The main drawback is that it does not support multiple Kernels.

Docker



Docker is a tool designed to make it easier to create, deploy, and run applications by using containers. Containers allow a developer to package up an application with all of the parts it needs, such as libraries and other dependencies, and deploy it as one package.

- Docker container technology was launched in 2013 as an open source Docker Engine.
- Docker is a set of platform as a service products that use OS-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries and configuration files; they can communicate with each other through well-defined channels.

Contd…..

- Docker is an open platform for developing, shipping, and running applications.
- Docker enables you to separate your applications from your infrastructure so you can deliver software quickly. With Docker, you can manage your infrastructure in the same ways you manage your applications. By taking advantage of Docker's methodologies for shipping, testing, and deploying code quickly, you can significantly reduce the delay between writing code and running it in production.

3. Network Virtualization

- **Network virtualization** is the process of combining **hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network.**

- Network virtualization involves platform virtualization, often combined with resource virtualization.
- The goal of network virtualization is to provide systems and users with efficient, controlled, and secure sharing of the networking resources.

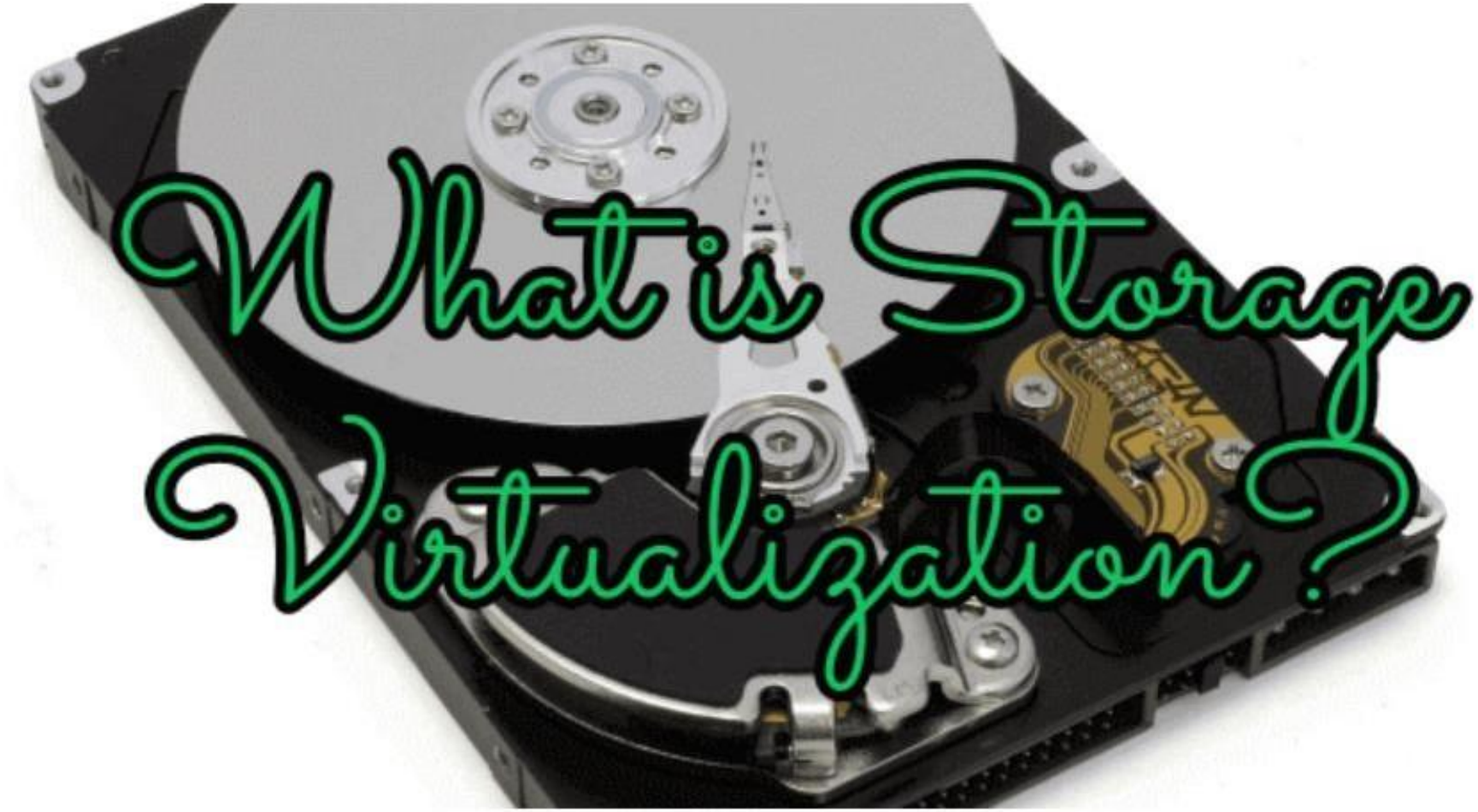
- Network virtualization is categorized as

External Virtualization→ combining many networks or parts of networks into a virtual unit

Internal virtualization→providing network-like **functionality to software containers on a single network server**

4. CPU Virtualization

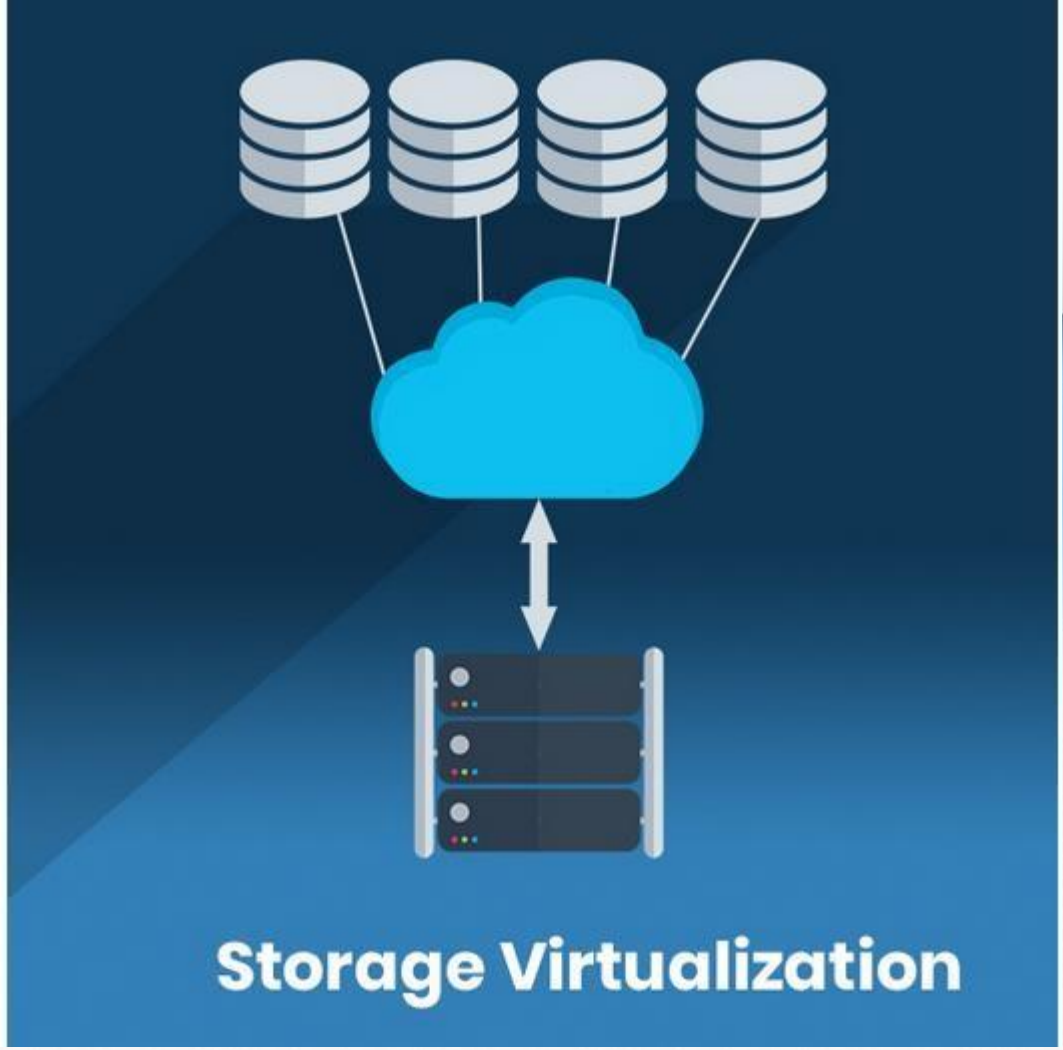
- CPU virtualization technology can abstract the physical CPU into virtual CPU. At any time the physical CPU only run one virtual CPU instruction. Every user operating system can use one or more virtual CPU, but all the CPUs are isolated with each other.



Storage virtualization is the process of representing physical storage in the logical form to any server

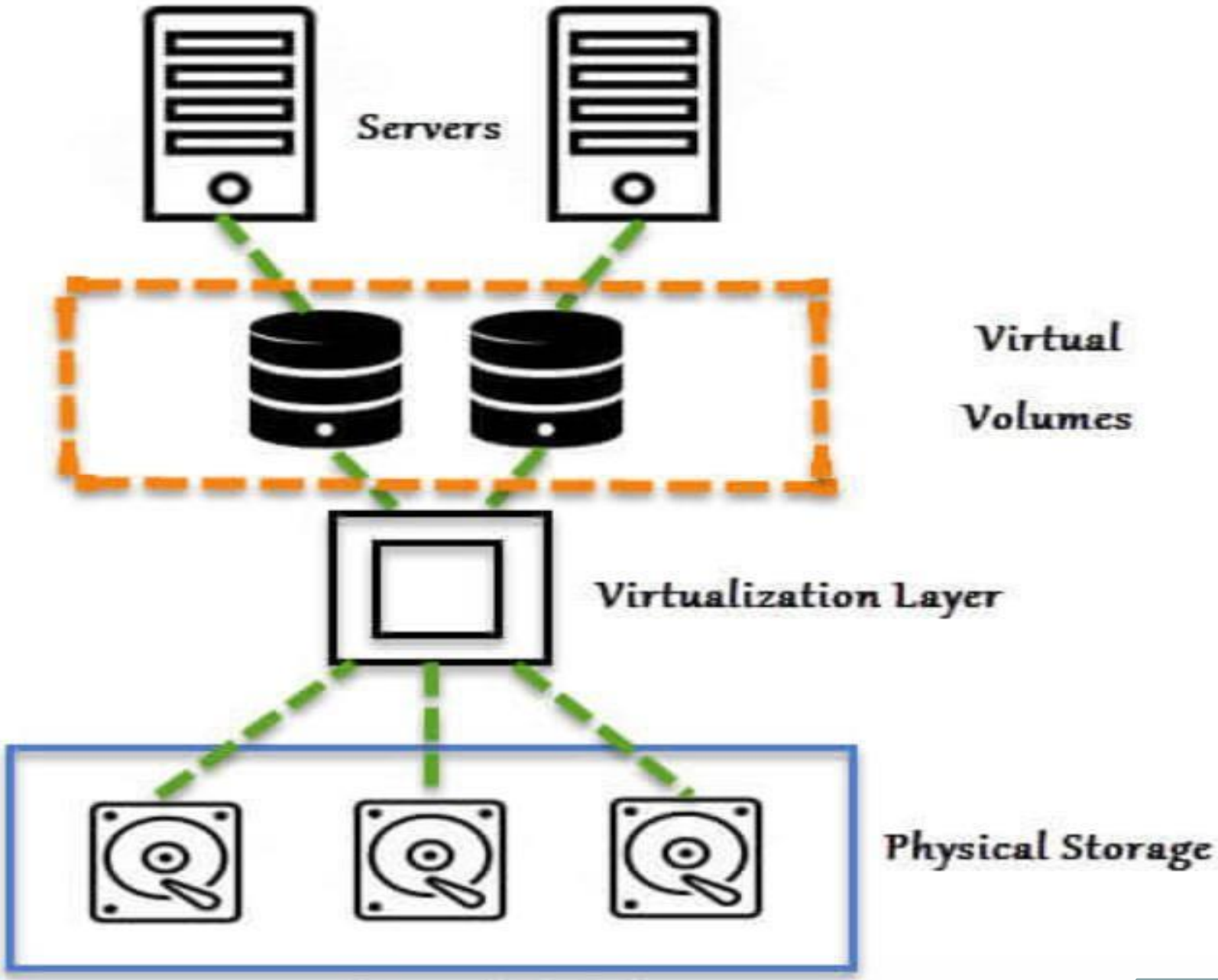
Storage Virtualization

- Storage **virtualization in Cloud Computing** is nothing but the sharing of physical storage into multiple storage devices which further appears to be a single storage device. It can be also called as a group of an available storage device which simply manages from a central console. This virtualization provides numerous benefits such as easy backup, achieving, and recovery of the data.



- Storage virtualization or cloud storage is the process of grouping the physical storage from multiple network storage devices into a single storage device.

Storage Virtualization



Storage Virtualization Advantages

- **It is highly scalable.**
- **It allows easy addition and deletion of storage without affecting any application.**
- **Easy data migration.**
- **Easy storage management.**

UNIT-2

Cloud Deployment Models:

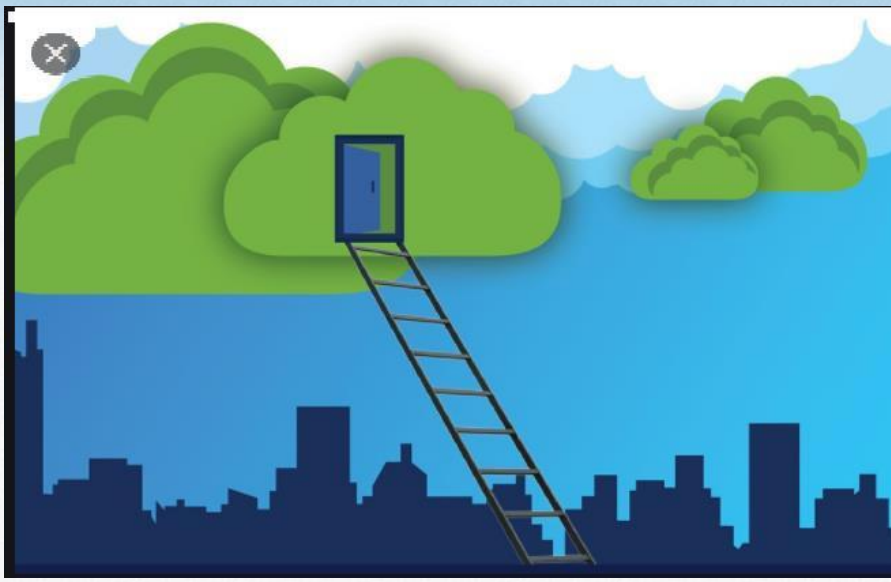
- Key drivers to adopting the cloud,
- the impact of cloud computing on users,
- governance in the cloud,
- barriers to cloud computing adoption in the enterprise.

Security Issues in Cloud Computing:

- Security in cloud computing environment,
- infrastructure security: the network level, the host level, the application level,
- data security and storage,
- aspects of data security,
- data security mitigation provider data and its security

Key Drivers to adopting the cloud

- Small Initial Investment and Low Ongoing Costs
- Economies of Scale
- Open Standards
- Sustainability



Small Initial Investment and Low Ongoing Costs

- Public cloud computing can avoid capital expenditures because no hardware, software, or network devices need to be purchased.
- Cloud usage is billed on actual use only, and is therefore treated more as an expense. In turn, usage-based billing lowers the barrier to entry because the upfront costs are minimal.

- Depending on the contract being signed, most companies can terminate the contract as preferred; therefore, in times of hardship or escalating costs, cloud computing costs can be managed very efficiently.

Economies

- Economies of Scale Most development projects have a sizing phase during which one attempts to calculate the storage, processing power, and memory requirements during development, testing, and production.
- It is often difficult to make **accurate estimates**; under- or overestimating these calculations is typical. The lead time for acquiring the equipment to support these estimates can sometimes be lengthy, thus adding to the time necessary to complete the project.
- With the flexibility that cloud computing solutions offer, companies can acquire computing and development services as needed and on demand, which means development projects are less at risk of missing deadlines and dealing with the unknown

Open Standards

- Open Standards Some capabilities in cloud computing are based on open standards for building a modular architecture that can grow rapidly and can change when required.
- Open source software is defined as computer software that is governed by a software license in the public domain, or that meets the definition of open source, which allows users to use, change, and improve the software.
- The flexibility to alter the source code is essential to allow for continued growth in the cloud solution. Open source software is the foundation of the cloud solution and is critical to its continued growth.

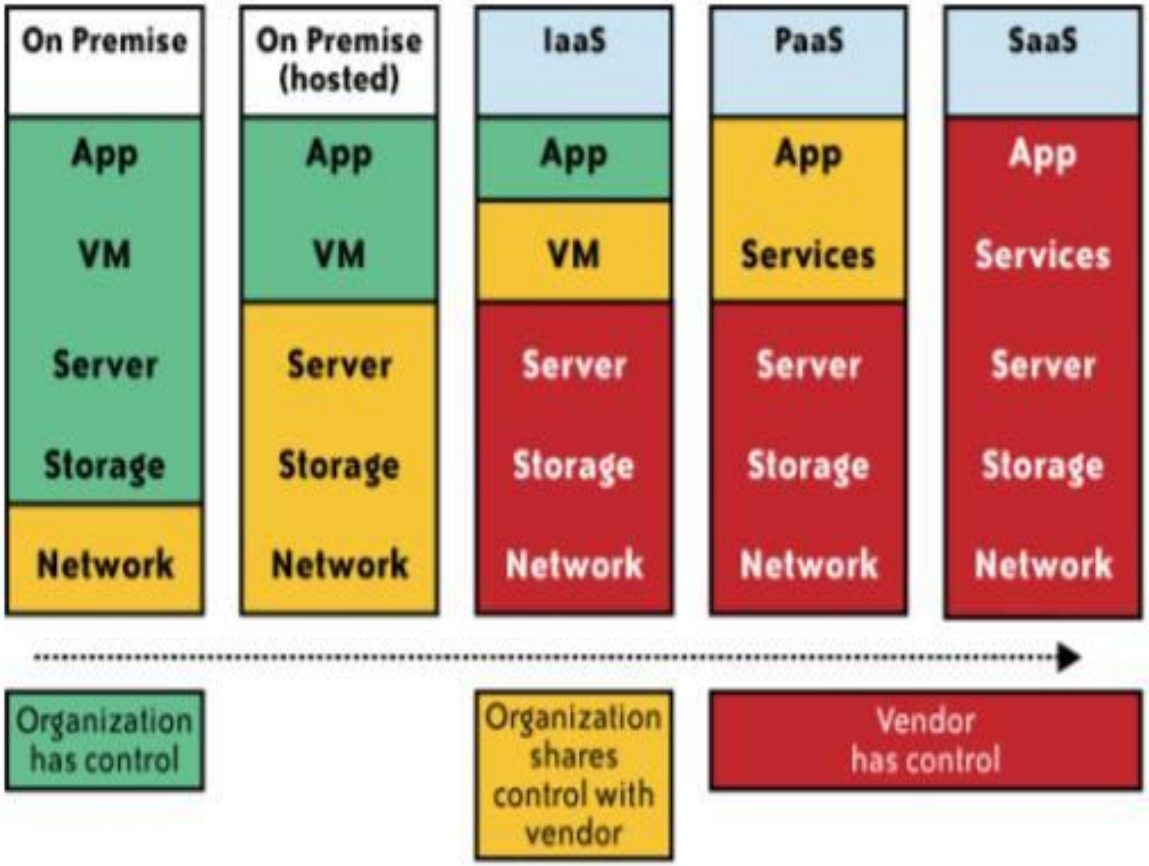
Sustainability

- Sustainability CSPs have invested considerable expense and thought into creating a resilient architecture that can provide a highly stable environment.
- Traditionally, companies have periodically struggled to maintain IT services due either to single points of failure in the network or to an inability to keep pace with business changes in both volume and the nature of transactions.
- Cloud computing allows companies to rely on the CSP to have limited points of failure, better resilience via clustering, and the ability to invest in state-of-the-art resilience solutions.

The Impact of Cloud Computing on Users

- Individual consumers
- Individual businesses
- Start-ups
- Small and medium-size businesses (SMBs)
- Enterprise businesses

Governance in the Cloud



Barriers to cloud computing adoption in the Enterprise.

- Security: How security at all levels(network,host,application and data level)
- Privacy: Organizations today face numerous different requirements attempting to protect the privacy of individual`s information and it is not clear.
- Connectivity and Open Access: The full potential depends on the availability of high speed access to all
- Reliability: Enterprise applications are now critical that they must be reliable and available to support 24/7 operation
- Interoperability:ERP
- Independence from CSPs: IT outsourcing contracts
- Economic Value
- Changes in the IT Organization

Security

- Because cloud computing represents a new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved.

- That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing.

Privacy

- The ability of cloud computing to adequately address privacy regulations has been called into question.
- Organizations today face numerous different requirements attempting to protect the privacy of individuals' information, and it is not clear (i.e., not yet established) whether the cloud computing model provides adequate protection of such information, or whether organizations will be found in violation of regulations because of this new model.

Connectivity and Open Access

- The full potential of cloud computing depends on the availability of high-speed access to all. Such connectivity, rather like electricity availability, globally opens the possibility for industry and a new range of consumer products.
- Connectivity and open access to computing power and information availability through the cloud promotes another era of industrialization and the need for more sophisticated consumer products.

Reliability

- Enterprise applications are now so critical that they must be reliable and available to support 24/7 operations.
- In the event of failure or outages, contingency plans must take effect smoothly, and for disastrous or catastrophic failure, recovery plans must begin with minimum disruption.

Interoperability

- The interoperability and portability of information between private clouds and public clouds are critical enablers for broad adoption of cloud computing by the enterprise.
- Many companies have made considerable progress toward standardizing their processes, data, and systems through implementation of ERPs.
- This process has been enabled by scalable infrastructures to create single instances, or highly integrated connections between instances, to manage the consistency of master and transaction data and produce reliable consolidated information.

Interoperability

- Even with these improved platforms, the speed at which businesses change may still outpace the ability of IT organizations to respond to these changes. SaaS applications delivered through the cloud provide a low-capital, fast-deployment option.
- Depending on the application, it is critical to integrate with traditional applications that may be resident in a separate cloud or on traditional technology.
- The standard for interoperability is either an enabler or a barrier to interoperability, and permits maintenance of the integrity and consistency of a company's information and processes.

Independence from CSPs

- Examples exist of IT outsourcing contracts that have effectively locked a customer into a service that does not meet current or evolving needs at a speed and cost that are acceptable to meet business goals.
- This could be caused by a number of factors, and is a concern if limited options exist for quickly engaging an alternative provider supplier to meet the needs without large transition or penalty costs.

Independence from CSPs

- A CSP may hold valuable data and business rules that cannot be easily migrated to a new provider. Standards to enable migration and plug and play of cloud components can help. For example, companies today depend less on the browser provider, but may depend on a proprietary data-based structure.
- Separating storage IaaS providers from processing providers can help with provider flexibility. There are downsides to going to a componentized approach, because the customer may become the integrator of these services.
- However, these may be the skills that enterprises should develop to balance the scalability of cloud computing with acceptable price performance and risk..

Economic Value

- The growth of cloud computing is predicated on the return on investment that accrues. It seems intuitive that by sharing resources to smooth out peaks, paying only for what is used, and cutting upfront capital investment in deploying IT solutions, the economic value will be there.
- There will be a need to carefully balance all costs and benefits associated with cloud computing—in both the short and long terms. Hidden costs could include support, disaster recovery, application modification, and data loss insurance

Changes in the IT Organization

- The IT organization will be affected by cloud computing, as has been the case with other technology shifts. There are two dimensions to shifts in technology. The first is acquiring the new skill sets to deploy the technology in the context of solving a business problem, and the second is how the technology changes the IT role. During the COBOL era, users rarely programmed, the expectations of the user interface varied, and the adaptability of the solution was low.

Changes in the IT Organization

- Training was delivered in separate manuals and the user used the computer to solve problems only down predefined paths.
- With the advent of fourth-generation languages, roles within IT, such as system analyst and programmer, became merged into analyst/programmer, users started to write their own reports, and new applications, including operational data stores, data entry, and query programs, could be rapidly deployed in weeks

Changes in the IT Organization

- IT’s role will change once again the speed of change will impact the adoption of cloud technologies and the ability to decompose mature solutions from hype to deliver real value from cloud technology; and the need to maintain the controls to manage IT risk in the business will increase.

Infrastructure security:The Network Level

- Ensuring Data Confidentiality and Integrity
- Ensuring the Availability of Internet-Facing Resources
- Replacing the Established Model of Network Zones and Tiers with Domains
- Network-Level Mitigation

Replacing the Established Model of Network Zones and Tiers with Domains

- The established isolation model of network zones and tiers no longer exists in the public IaaS and PaaS clouds. For years, network security has relied on zones, such as intranet versus extranet and development versus production, to segregate network traffic for improved security.

- This model was based on exclusion—only individuals and systems in specific roles have access to specific zones. Similarly, systems within a specific tier often have only specific access within or across a specific tier. For example, systems within a presentation tier are not allowed to communicate directly with systems in the database tier, but can communicate only with an authorized system within the application zone.

- The traditional model of network zones and tiers has been replaced in public cloud computing with “security groups,” “security domains,” or “virtual data centers” that have logical separation between tiers but are less precise and afford less protection than the formerly established model

Contd…

- The ***security groups*** feature in AWS(Amazon Web Services) allows your virtual machines (VMs) to access each other using a virtual firewall that has the ability to filter traffic based on IP address (a specific address or a subnet), packet types (TCP, UDP, or ICMP), and ports (or a range of ports).
- Domain names are used in various networking contexts and application-specific naming and addressing purposes, based on DNS.
- For example, Google's App Engine provides a logical grouping of applications based on domain names such as mytestapp.test.mydomain.com

  myprodapp.prod.mydomain.com.

Network-Level Mitigation

- First, note that network-level risks exist regardless of what aspects of “cloud computing” services are being used (e.g., software-as-a-service, platform-as-a-service, or infrastructure-as-a-service). The primary determination of risk level is therefore not which *aaS is being used, but rather whether your organization intends to use or is using a public, private, or hybrid cloud.
- If your organization is large enough to afford the resources of a private cloud, your risks will decrease—assuming you have a true private cloud that is internal to your network.

Contd….

- In some cases, a private cloud located at a cloud provider’s facility can help meet your security requirements but will depend on the provider capabilities and maturity.
- You can reduce your confidentiality risks by using encryption; specifically by using validated implementations of cryptography for data-in-transit. Secure digital signatures make it much more difficult, if not impossible, for someone to tamper with your data, and this ensures data integrity.

Contd…

- Availability problems at the network level are far more difficult to mitigate with cloud computing—unless your organization is using a private cloud that is internal to your network topology.
- Even if your private cloud is a private (i.e., non-shared) external network at a cloud provider’s facility, you will face increased risk at the network level. A public cloud faces even greater risk.

Infrastructure Security: Host Level

- When reviewing host security and assessing risks, you should consider the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models (public, private, and hybrid).

- Some virtualization security threats—such as VM escape (Virtual machine **escape** is an exploit in which the attacker runs code on a **VM** that allows an operating system running within it to break out and interact directly with the hypervisor. Such an exploit could give the attacker access to the host operating system and all other virtual machines (**VMs**) running on that host.), and insider threats by way of weak access control to the hypervisor—carry into the public cloud computing environment.

- The dynamic nature (elasticity) of cloud computing can bring new operational challenges from a security management perspective

SaaS and PaaS Host Security:

- CSPs do not publicly share information related to their host platforms, host operating systems, and the processes that are in place to secure the hosts, since hackers can exploit that information when they are trying to intrude into the cloud service.

- Hence, in the context of SaaS (e.g., Salesforce.com, Workday.com) or PaaS (e.g., Google App Engine, Salesforce.com's Force.com) cloud services, host security is opaque to customers and the responsibility of securing the hosts is relegated to the CSP.

- Since virtualization is a key enabling technology that improves host hardware utilization, among other benefits, it is common for CSPs to employ virtualization platforms, including Xen and VMware hypervisors, in their host computing platform architecture. You should understand how the provider is using virtualization technology and the provider's process for securing the virtualization layer.

IaaS Host Security: IaaS customers are primarily responsible for securing the hosts provisioned in the cloud. Given that almost all IaaS services available today employ virtualization at the host layer, host security in IaaS should be categorized as follows:

Virtualization Software Security:

- The software layer that sits on top of bare metal and provides customers the ability to create and destroy virtual instances.

- Virtualization at the host level can be accomplished using any of the virtualization models, including OS-level virtualization (Solaris containers, BSD jails, Linux-VServer), paravirtualization (a combination of the hardware version and versions of Xen and VMware), or hardware-based virtualization (Xen, VMware, Microsoft Hyper-V). It is important to secure this layer of software that sits between the hardware and the virtual servers. In a public IaaS service, customers do not have access to this software layer; it is managed by the CSP only.

Threats to the hypervisor: The integrity and availability of the hypervisor are of utmost importance and are key to guaranteeing the integrity and availability of a public cloud built on a virtualized environment.

"Blue Pill" attack on a hypervisor. A malware that executes as a hypervisor to gain control of computer resources.

Customer guest OS or Virtual Server Security:

- The virtual instance of an operating system that is provisioned on top of the virtualization layer and is visible to customers from the Internet; e.g., various flavors of Linux, Microsoft, and Solaris. Customers have full access to virtual servers.

- The dynamic life cycle of virtual servers can result in complexity if the process to manage the virtual servers is not automated with proper procedures.
- From an attack surface perspective, the virtual server (Windows, Solaris, or Linux) may be accessible to anyone on the Internet, so sufficient network access mitigation steps should be taken to restrict access to virtual instances. Typically, the CSP blocks all port access to virtual servers and recommends that customers use port 22 (Secure Shell or SSH) to administer virtual server instances. Some of the new host security threats in the public IaaS include:

1. Stealing keys used to access and manage hosts (e.g., SSH private keys)
2. vulnerable services listening on standard ports (e.g., FTP, NetBIOS, SSH)
3. Hijacking accounts that are not properly secured (i.e., weak or no passwords for standard accounts)
4. Attacking systems that are not properly secured by host firewalls

Infrastructure Security: The Application Level

- Application-Level Security Threats
- End User Security

Who Is Responsible for Web Application Security in the Cloud?

1. SaaS Application Security
2. PaaS Application Security
3. IaaS Application Security

Infrastructure Security: The Application Level

- Application or software security should be a critical element of your security program. Most enterprises with information security programs have yet to institute an application security program to address this realm.

- Designing and implementing applications targeted for deployment on a cloud platform will require that existing application security programs reevaluate current practices and standards. The application security spectrum ranges from standalone single-user applications to sophisticated multiuser e-commerce applications used by millions of users.

- Web applications such as content management systems (CMSs), wikis, portals, bulletin boards, and discussion forums are used by small and large organizations. A large number of organizations also develop and maintain custom-built web applications for their businesses using various web frameworks (PHP,† .NET,‡ J2EE,§ Ruby on Rails, Python, etc.). According to SANS(SysAdmin, Audit, Network, and **Security**.), until 2007 few criminals attacked vulnerable websites because other attack vectors were more likely to lead to an advantage in unauthorized economic or information access.

Infrastructure Security: The Application Level

- Cross-site scripting (XSS) (is a code injection attack executed on the client side of a web-application) and other attacks have demonstrated that criminals looking for financial gain can exploit vulnerabilities resulting from web programming errors as new ways to penetrate important organizations

- Attacker inject malicious script through the web browser.
- The malicious script is executed when the victims visits a web page or web server
- Steel cookies,session tokens and other sensitive information
- Modify the content of website

Application-Level Security Threats

- **According to SANS,(SysAdmin, Audit, Network, and Security.) web application vulnerabilities in open source as well as custom-built applications accounted for almost half the total number of vulnerabilities discovered between November 2006 and October 2007.# The existing threats exploit well-known application vulnerabilities**

- **including cross-site scripting (XSS), SQL injection, malicious file execution, and other vulnerabilities resulting from programming errors and design flaws. Armed with knowledge and tools, hackers are constantly scanning web applications (accessible from the Internet) for application vulnerabilities.**

- **They are then exploiting the vulnerabilities they discover for various illegal activities including financial fraud, intellectual property theft, converting trusted websites into malicious servers serving client-side exploits, and phishing scams.**

- **DoS(Denial of Services)and DDoS(Distributed denial of Services) attacks that can potentially disrupt cloud services for an extended time. a DDoS attack on Twitter on August 6, 2009, brought the service down for several hours .**

End User Security

- Customer of a cloud service, are responsible for end user security tasks—security procedures to protect your Internet-connected PC—and for practicing “safe surfing.” Protection measures include use of security software, such as anti-malware, antivirus, personal firewalls, security patches, on Internet-connected computer.

- To achieve end-to-end security in a cloud, it is essential for customers to maintain good browser hygiene. This means keeping the browser (e.g., Internet Explorer, Firefox, Safari) patched and updated to mitigate threats related to browser vulnerabilities. Currently, although browser security add-ons are not commercially available, users are encouraged to frequently check their browser vendor’s website for security updates, use the auto-update feature, and install patches on a timely basis to maintain end user security.

SaaS Application Security

- The SaaS model dictates that the provider manages the entire suite of applications delivered to users. Therefore, SaaS providers are largely responsible for securing the applications and components they offer to customers.
- Extra attention needs to be paid to the authentication and access control features offered by SaaS CSPs.
- Usually that is the only security control available to manage risk to information.
- Some SaaS applications, such **as Google Apps**, have built-in features that end users can invoke to assign read and write privileges to other users. However, the privilege management features may not be advanced, fine-grained access and could have weaknesses that may not conform to your organization's access control standard

CONTD….

- One example that captures this issue is the mechanism that Google Docs employs in handling images embedded in documents, as well as access privileges to older versions of a document.
- Embedded image that can be integrated directly into the email source code. Embedded image do not need to be downloaded by recipient they are shown directly in the image program.
- No protection for embedded image and an image`s continued existence on the Google`s server after its containing document has been deleted.
- Lack of authentication means the image URL could be accessed by the 3rd parties without the documents' owner.
- Google correctly noted that the image URL would have been known to only to those with the previous access to image and someone with such access could have saved the image anyway and disclosed the saved image with anuthorized.

Google Privacy Blunder Shares Your Docs Without Permission

- In a privacy error that underscores some of the biggest problems surrounding cloud-based services, Google has sent a notice to a number of users of its Document and Spreadsheets products stating that it may have inadvertently shared some of their documents with contacts who were never granted access to them.

- According to the notice, this sharing was limited to people “with whom you, or a collaborator with sharing rights, had previously shared a document” – a vague statement that sounds like it could add up to quite a few people. The notice states that only text documents and presentations are affected, not spreadsheets

PaaS Application Security

PaaS vendors broadly fall into the following two major categories:

• Software vendors (e.g., Bungee, Etelos, GigaSpaces, Eucalyptus)

•CSPs (e.g., Google App Engine, Salesforce.com's Force.com, Microsoft Azure, Intuit QuickBase)

Organizations evaluating a private cloud may utilize PaaS software to build a solution for internal consumption.

- It is recommended that organizations evaluating PaaS software perform a risk assessment and apply the software security standard similar to acquiring any enterprise software.
- PaaS cloud (public or private) offers an integrated environment to design, develop, test, deploy, and support custom applications developed in the language the platform supports. PaaS application security encompasses two software layers:

1. Security of the PaaS platform itself (i.e., runtime engine) .
2. Security of customer applications deployed on a PaaS platform.

CONTD……..

PaaS CSPs (e.g., Google, Microsoft, and Force.com) are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications. Since PaaS applications may use third-party applications, components, or web services, the third-party application provider may be responsible for securing their services. Hence, customers should understand the dependency of their application on all services and assess risks pertaining to third-party service providers. Until now, CSPs have been reluctant to share information pertaining to platform security using the argument that such security information could provide an advantage for hackers.

However, enterprise customers should demand transparency from CSPs and seek information necessary to perform risk assessment and ongoing security management.

IaaS Application Security

IaaS cloud providers (e.g., Amazon EC2 &GoGrid) treat the applications on customer virtual instances and therefore are completely agnostic to the operations and management of the customer's applications.

- The entire stack—customer applications, runtime application platform (Java, .NET, PHP, Ruby on Rails, etc.), and so on— runs on the customer's virtual servers and is deployed and managed by customers. To that end, customers have full responsibility for securing their applications deployed in the IaaS cloud. Hence, customers should not expect any application security assistance from CSPs other than basic guidance and features related to firewall policy that may affect the application's communications with other applications, users, or services within or outside the cloud

CONTD….

Web applications deployed in a public cloud must be designed for an Internet threat model, embedded with standard security countermeasures against common web vulnerabilities (e.g., the OWASP Top 10).

Open Web Application Security projects➔ Standard awareness documents for developers and web application security.

Top 10 web application security risk

- **Injection**
- **Broken Authentication**
- **Sensitive data exposure**
- **Broken Access Control**
- **Security Misconfiguration**
- **Cross site Scripting**
- **Insecure Deserialization**
- **Using Components with known vulnerabilities**
- **Insufficient logging and Monitoring.**

Data Security and Storage (Overview)

- Data-In Transit: data in motion
- Data –at-rest: inactive data that is stored physically in the digital form (DB,Warehouse,spreadsheet,mobile devices etc)
- Processing of data, including multitenancy
- Data lineage: where and when the data was specifically located within the cloud

e.g , the data might have been transferred to a cloud provider, such as Amazon Web Services (AWS), on date x1 at time y1 and stored in a bucket on Amazon's S3 in example1.s3.amazonaws.com,
then processed on date x2 at time y2 on an instance being used by an organization on Amazon's Elastic Compute Cloud (EC2) in ec2-67-202-51-223.compute-1.amazonaws.com, then restored in another bucket, example2.s3.amazonaws.com, before being brought back into the organization for storage in an internal data warehouse belonging to the marketing operations group on date x3 at time y3. Following the path of data (mapping application data flows or data path visualization) is known as data lineage.

Data Security and Storage

- Data provenance: **Integrated of data and data is accurately calculated e.g SUM((((2*3)*4)/6)-2=$2**
- Data remanence: Residual representation of digital data that remains even after attempts have been made to remove or erase the data. Various techniques have been developed to counter data remanence.
- Clearing&Sanitizing

Data-in-transit

- To insure the security of data in transit it is not only important to use a vetted encryption algorithm, but also it is important to ensure that the service protocol provides confidentiality as well as integrity (e.g., FTP over SSL [FTPS], Hypertext Transfer Protocol Secure [HTTPS], and Secure Copy Program [SCP])—particularly if the protocol is used for transferring data across the Internet. Encrypting data and using a non-secured protocol (e.g., FTP or HTTP) can provide confidentiality, but does not ensure the integrity of the data

Data-in-transit

- With regard to data-in-transit, the primary risk is in not using a vetted encryption algorithm.
- It is also important to ensure that a protocol provides confidentiality as well as integrity (e.g., FTP over SSL [FTPS], Hypertext Transfer Protocol Secure [HTTPS], and Secure Copy Program [SCP])—particularly if the protocol is used for transferring data across the Internet

DATA-AT REST

- Although using encryption to protect data-at-rest might seem obvious, the reality is not that simple. If you are using an IaaS cloud service (public or private) for simple storage (e.g., Amazon's Simple Storage Service or S3), encrypting data-at-rest is possible—and is strongly suggested. However, encrypting data-at-rest that a PaaS or SaaS cloud-based application is using (e.g., Google Apps, Salesforce.com) is not always feasible.
- Data-at- rest used by a cloud-based application is generally not encrypted, because encryption would prevent indexing or searching of that data.

DATA-AT REST

- Generally speaking, with data-at-rest, the economics of cloud computing are such that PaaS based applications and SaaS applications is to use a multitenancy architecture.
- In other words, data, when processed by a cloud-based application or stored for use by a cloud- based application, is commingled with other users' data (i.e., it is typically stored in a massive data store, such as Google's BigTable).

Data-at-Rest

- Although applications are often designed with features such as data tagging to prevent unauthorized access to commingled data, unauthorized access is still possible through exploit of an application vulnerability. Although an organization's data-in-transit might be encrypted during transfer to and from a cloud provider, and its data-at-rest might be encrypted if using simple storage (i.e., if it is not associated with a specification application), an organization's data is definitely not encrypted if it is processed in the cloud (public or private). For any application to process data, that data must be unencrypted.

Data-at-Rest

- Although using encryption to protect data-at-rest might seem obvious, the reality is not that simple. If you are using an IaaS cloud service (public or private) for simple storage (e.g., Amazon's Simple Storage Service or S3), encrypting data-at-rest is possible—and is strongly suggested. However, encrypting data-at-rest that a PaaS or SaaS cloud-based application is using (e.g., Google Apps, Salesforce.com) as a compensating control is not always feasible.

Data Lineage

- Whether the data of an organization has been put into the cloud is encrypted or not, it is useful and might be required (for audit or compliance purposes) to know exactly where and when the data was specifically located within the cloud
- **Data lineage** includes the data origin, what happens to it and where it moves over time.

Data Lineage

- For example, the data might have been transferred to a cloud provider, such as Amazon Web Services (AWS), on date x1 at time y1 and stored in a bucket on Amazon's S3 in example1.s3.amazonaws.com, then processed on date x2 at time y2 on an instance being used by an organization on Amazon's Elastic Compute Cloud (EC2) in ec2-67-202-51-223.compute1.amazonaws.com, then restored in another bucket, example2.s3.amazonaws.com, before being brought back into the organization for storage in an internal data warehouse belonging to the marketing operations group on date x3 at time y3.

Data Lineage

- Following the path of data (mapping application data flows or data path visualization) is known as data lineage, and it is important for an auditor's assurance (internal, external, and regulatory). However, providing data lineage to auditors or management is time-consuming, even when the environment is completely under an organization's control. Trying to provide accurate reporting on data lineage for a public cloud service is really not possible..

Data Provenance

- Even if data lineage can be established in a public cloud, for some customers there is an even more challenging requirement and problem: proving data provenance—not just proving the integrity of the data, but the more specific provenance of the data. There is an important difference between the two terms. Integrity of data refers to data that has not been changed in an unauthorized manner or by an unauthorized person. Provenance means not only that the data has integrity, but also that it is computationally accurate; that is, the data was accurately calculated. For example, consider the following financial equation: SUM((((2*3)*4)/6)−2) = $2.00

Data Provenance

- With that equation, the expected answer is $2.00. If the answer were different, there would be an integrity problem. Of course, the assumption is that the $2.00 is in U.S. dollars, but the assumption could be incorrect if a different dollar is used with the following associated assumptions:
- The equation is specific to the Australian, Bahamian, Barbadian, Belize, Bermudian, Brunei, Canadian, Cayman Islands, Cook Islands, East Caribbean, Fijian, Guyanese, Hong Kong, Jamaican, Kiribati, Liberian, Namibian, New Zealand, Samoan, Singapore, Solomon Islands, Surinamese, New Taiwan, Trinidad and Tobago, Tuvaluan, or Zimbabwean dollar.
- The dollar is meant to be converted from another country's dollars into U.S. dollars.
- The correct exchange rate is used and the conversion is calculated correctly and can be proven

Data Remanence

- Various techniques have been developed to counter data remanence.
- Clearing: Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information.

Sanitizing is the process of deliberately ,permanently and irreversible removing or destroying the data stored on a memory device to make it unrecoverable. A device that has been sanitized has no usable forensic tools, the data will not ever be recovered.

Data Security Mitigation

- Although data-in-transit can and should be encrypted, any use of that data in the cloud, beyond simple storage, requires that it be decrypted. Therefore, it is almost certain that in the cloud, data will be unencrypted. And if you are using a PaaS-based application or SaaS, customer unencrypted data will also almost certainly be hosted in a multitenancy environment (in public clouds).
- Add to that exposure the difficulties in determining the data's lineage, data provenance—where necessary—and even many providers' failure to adequately address such a basic security concern as data remanence, and the risks of data security for customers are significantly increased. So, what should you do to mitigate these risks to data security? The only viable option for mitigation is to ensure that any sensitive or regulated data is not placed into a public cloud (or that you encrypt data placed into the cloud for simple storage only)

Provider Data and Its Security

- In addition to the security of customers own data, customers should also be concerned about what data the provider collects and how the CSP protects that data.
- Specifically with regard to your customer data, what metadata does the provider have about your data, how is it secured, and what access do you, the customer, have to that metadata? As your volume of data with a particular provider increases, so does the value of that metadata.
- Additionally, your provider collects and must protect a huge amount of security-related data.

Provider Data and Its Security

- For example, at the network level, your provider should be collecting, monitoring, and protecting firewall, intrusion prevention system (IPS), security incident and event management (SIEM), and router flow data.
- At the host level your provider should be collecting system logfiles,
- and at the application level SaaS providers should be collecting application log data, including authentication and authorization information

Provider Data and Its Security

- What data your CSP collects and how it monitors and protects that data is important to the provider for its own audit purposes

- Additionally, this information is important to both providers and customers in case it is needed for incident response and any digital forensics required for incident analysis.

Storage Security

- For data stored in the cloud (i.e., storage-as-a-service), we are referring to IaaS and not data associated with an application running in the cloud on PaaS or SaaS. The same three information security concerns are associated with this data stored in the cloud
- (e.g., Amazon's S3) as with data stored elsewhere: confidentiality, integrity, and availability. .

Confidentiality

- When it comes to the confidentiality of data stored in a public cloud, you have two potential concerns. First, what access control exists to protect the data?
- Access control consists of both authentication and authorization.
- The second potential concern is: How is the data that is stored in the cloud actually protected? For all practical purposes, protection of data stored in the cloud involves the use of encryption.

Confidentiality

- So, is a customer's data actually encrypted when it is stored in the cloud? And if so, what encryption algorithm, and with what key strength? It depends, and specifically, it depends on which CSP you are using. For example, EMC's MozyEnterprise does encrypt a customer's data.
- However, AWS S3 does not encrypt a customer's data. Customers are able to encrypt their own data themselves prior to uploading, but S3 does not provide encryption. Another confidentiality consideration for encryption is key management

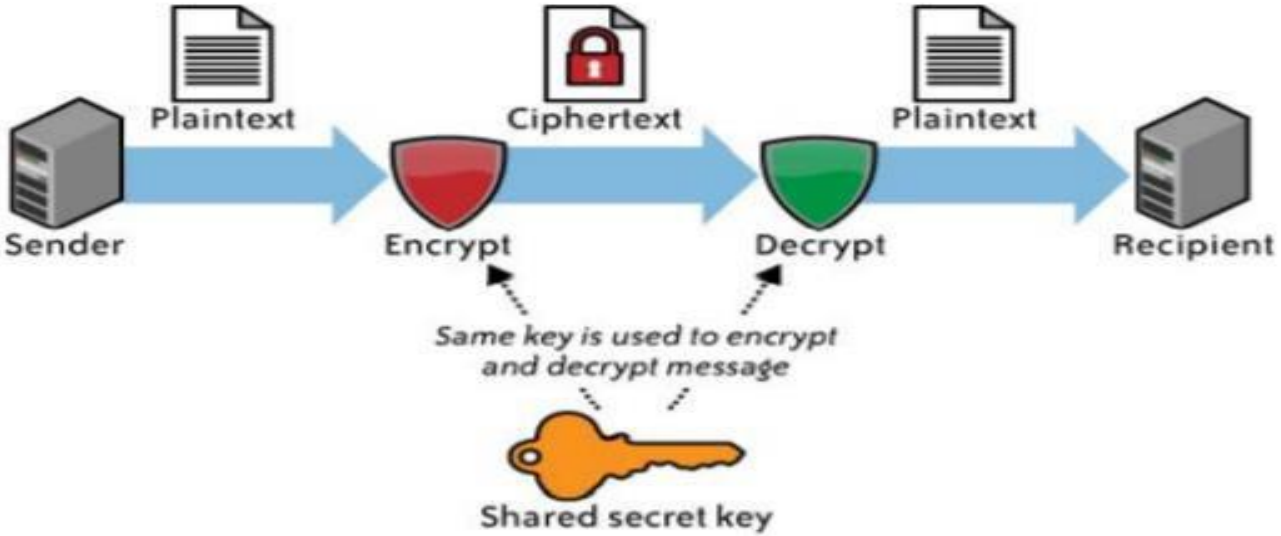
Confidentiality

- If a CSP does encrypt a customer's data, the next consideration concerns what encryption algorithm it uses. Not all encryption algorithms are created equal. Cryptographically, many algorithms provide insufficient security.

- How are the encryption keys that are used going to be managed—and by whom? Are you going to manage your own keys? Hopefully, the answer is yes, and hopefully you have the expertise to manage your own keys

Symmetric encryption

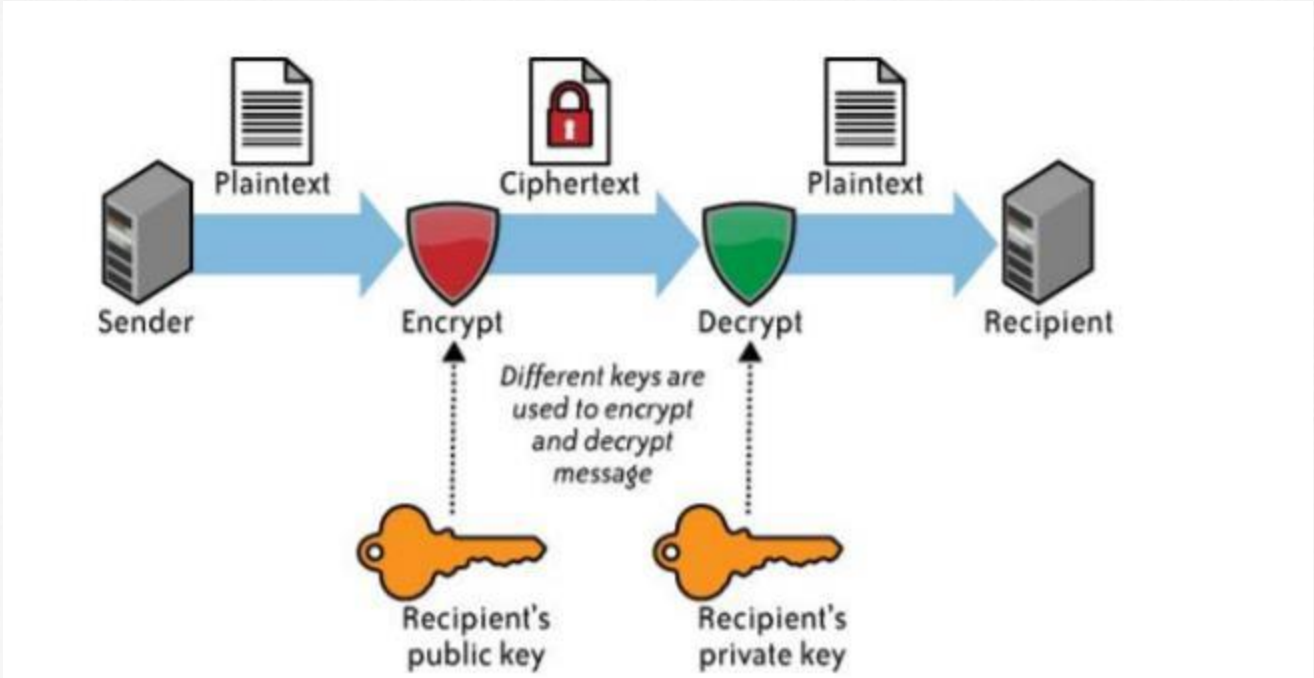
- Symmetric encryption (see Figure 1) involves the use of a single secret key for both the encryption and decryption of data. Only symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data



. Symmetric encryption

Asymmetric encryption

- Although the example in Figure -2 is related to email, the same concept (i.e., a public key and a private key) is not used in data storage encryption



Asymmetric encryption

what key length is used?

- The next consideration for you is what key length is used. With symmetric encryption, the longer the key length (i.e., the greater number of bits in the key), the stronger the encryption. Although long key lengths provide more protection, they are also more computationally intensive, and may strain the capabilities of computer processors.
- What can be said is that key lengths should be a minimum of 112 bits for Triple DES (Data Encryption Standard) and 128- bits for AES (Advanced Encryption Standard)—both NIST-approved algorithms

Integrity

- In addition to the confidentiality of your data, you also need to worry about the integrity of your data. Confidentiality does not imply integrity; data can be encrypted for confidentiality purposes, and yet you might not have a way to verify the integrity of that data. Encryption alone is sufficient for confidentiality, but integrity also requires the use of message authentication codes (MACs).

Integrity

- Once a customer has several gigabytes (or more) of its data up in the cloud for storage, how does the customer check on the integrity of the data stored there? There are IaaS transfer costs associated with moving data into and back down from the cloud. What a customer really wants to do is to validate the integrity of its data while that data remains in the cloud—without having to download and re upload that data.
- This task is even more difficult because it must be done in the cloud without explicit knowledge of the whole data set. Customers generally do not know on which physical machines their data is stored, or where those systems are located. Additionally, that data set is probably dynamic and changing frequently. Those frequent changes obviate the effectiveness of traditional integrity insurance technique

Availability

- Availability Assuming that a customer's data has maintained its confidentiality and integrity, you must also be concerned about the availability of your data. There are currently three major threats in this regard—none of which are new to computing, but all of which take on increased importance in cloud computing because of increased risk. The first threat to availability is network-based attacks(DoS,DDoS)

Availability

- A number of high-profile cloud provider outages have occurred.
- For example, Amazon's S3 suffered a 2.5-hour outage in February 2008 and an eight-hour outage in July 2008. AWS is one of the more mature cloud providers, so imagine the difficulties that other, smaller or less mature cloud providers are having.
- These Amazon outages were all the more apparent because of the relatively large number of customers that the S3 service supports—and whom are highly (if not totally) reliant on S3's availability for their own operations. In addition to service outages, in some cases data stored in the cloud has actually been lost.

Availability

- For example, in March 2009, “cloud-based storage service provider Carbonite Inc. filed a lawsuit charging that faulty equipment from two hardware providers caused backup failures that resulted in the company losing data for 7,500 customers two years ago.

23/09/2020

IAM

Identity & Access Management

Trust Boundaries and IAM

- In a typical organization where applications are deployed within the organization's perimeter the "trust boundary" is mostly static and is monitored and controlled by the IT department. In that traditional model, the trust boundary encompasses the network, systems, and applications hosted in a private data center managed by the IT department (sometimes third-party providers under IT supervision). And access to the network, systems, and applications is secured via network security controls including virtual private networks (VPNs), intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and multifactor authentication.

IAM

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

OR

AWS (AMAZON WEB SERVICES) IAM is a web services that helps you securely control access to resources. You use IAM to control who is authenticated(signed-in) and authorized(has permission) to use resources.

Why have enterprises started to implement IAM?

- **IAM** has emerged as a critical foundation for realizing the business benefits in terms of cost savings, management control, operational efficiency and business growth of enterprises. Enterprises need to manage access to information and applications scattered across internal and external application systems. Moreover, they must provide this access for a growing number of identities, both inside and outside the organization, without compromising security or exposing sensitive information. In addition, they shall have to ensure the correctness of data in order for the **IAM** Framework to function properly.

What is an IAM Framework?

- An **IAM** Framework /Component can be divided into four major areas:
- **Authentication**,**--**(Signed in)
- **Authorization**,**--(has Permission)**
- **User Management &**

a. Creating new user
b. Adding user to the required access group
c. Maintaining Password policies, privileges

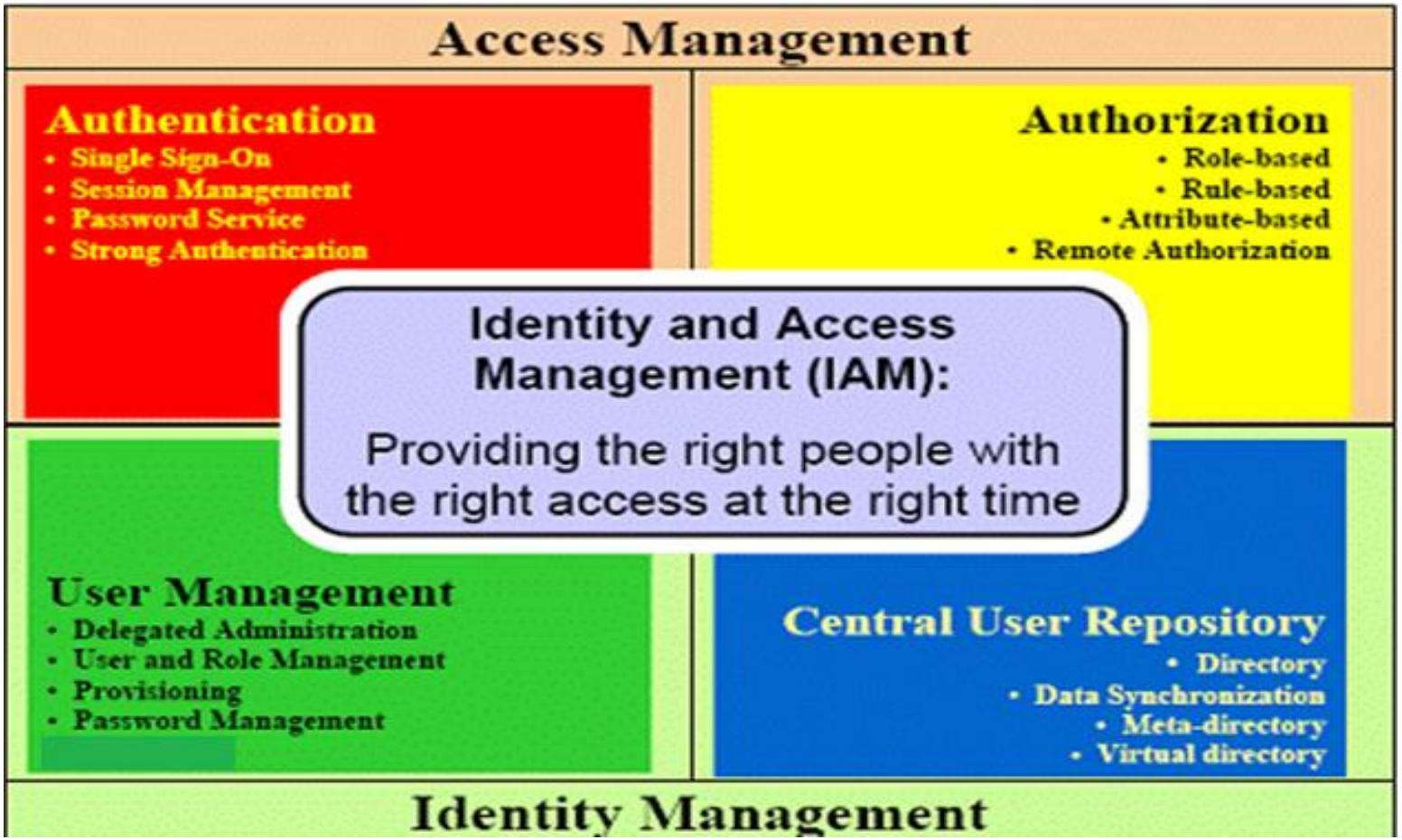
- Central User Repository. It establishes identity and access control rules for user.

- Database of users

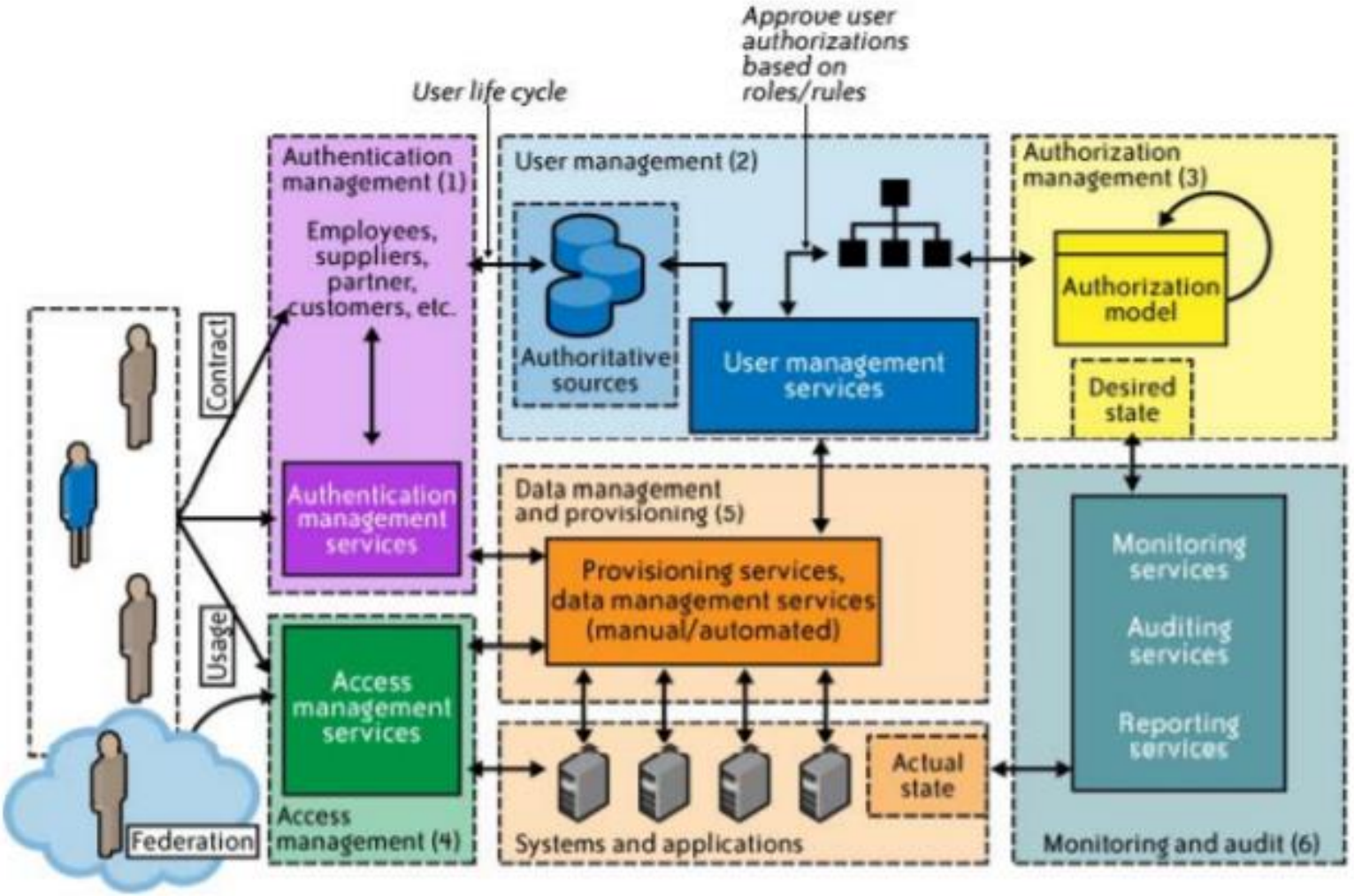
-

Goal IAM

To provide the right people with the right access at the right time



IAM Architecture



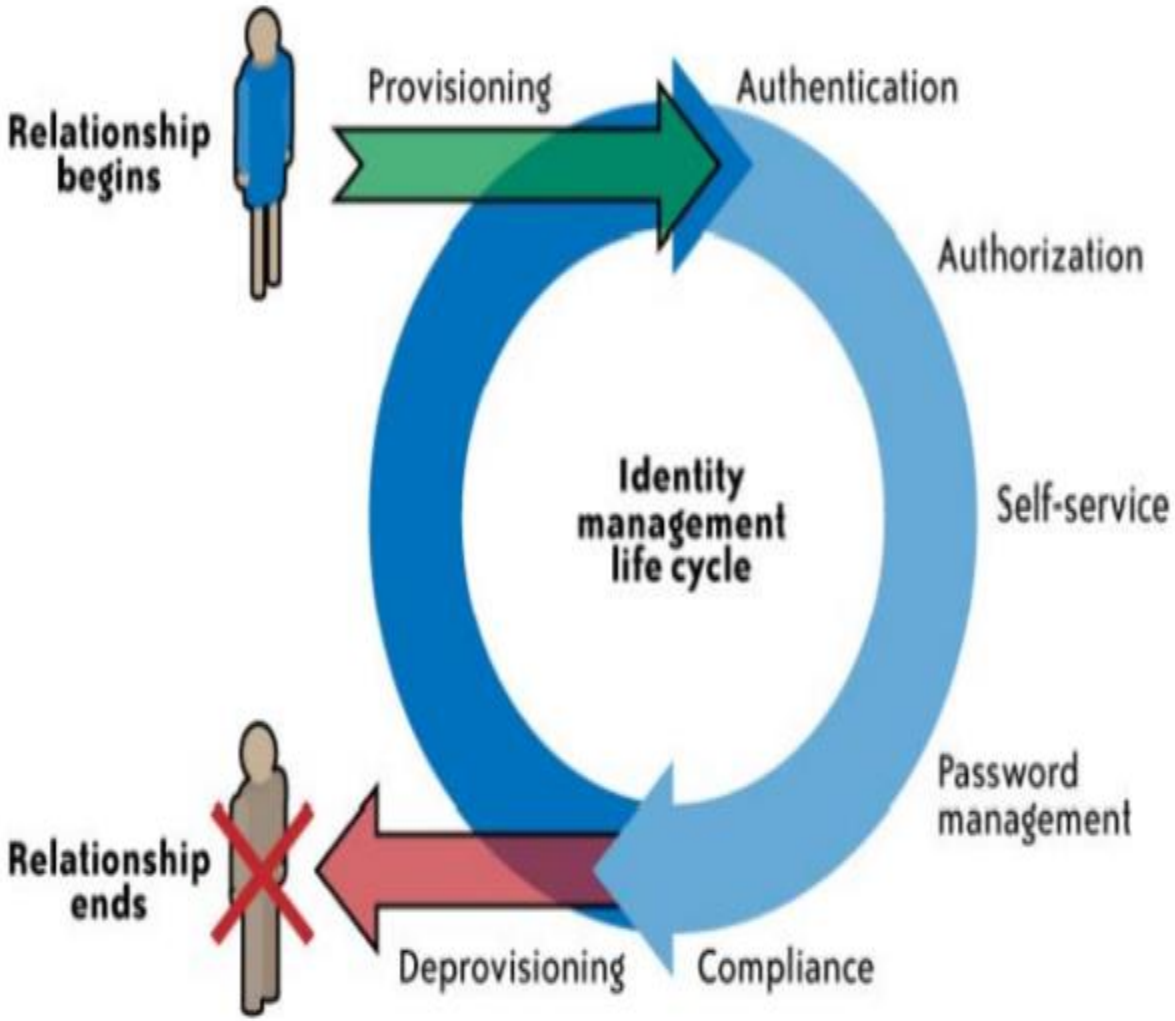
. *Enterprise IAM functional architecture*

IAM

- The IAM processes to support the business can be broadly categorized as follows:
- User management : Activities for the effective governance and management of identity life cycles
- Authentication management : Activities for the effective governance and management of the process for determining that an entity is who or what it claims to be
- Authorization management : Activities for the effective governance and management of the process for determining entitlement rights that decide what resources an entity is permitted to access in accordance with the organization's policies
- Access management : Enforcement of policies for access control in response to a request from an entity (user, services) wanting to access an IT resource within the organization
- Data management and provisioning : Propagation of identity and data for authorization to IT resources via automated or manual processes
- Monitoring and auditing : Monitoring, auditing, and reporting compliance by users regarding access to resources within the organization based on the defined policies

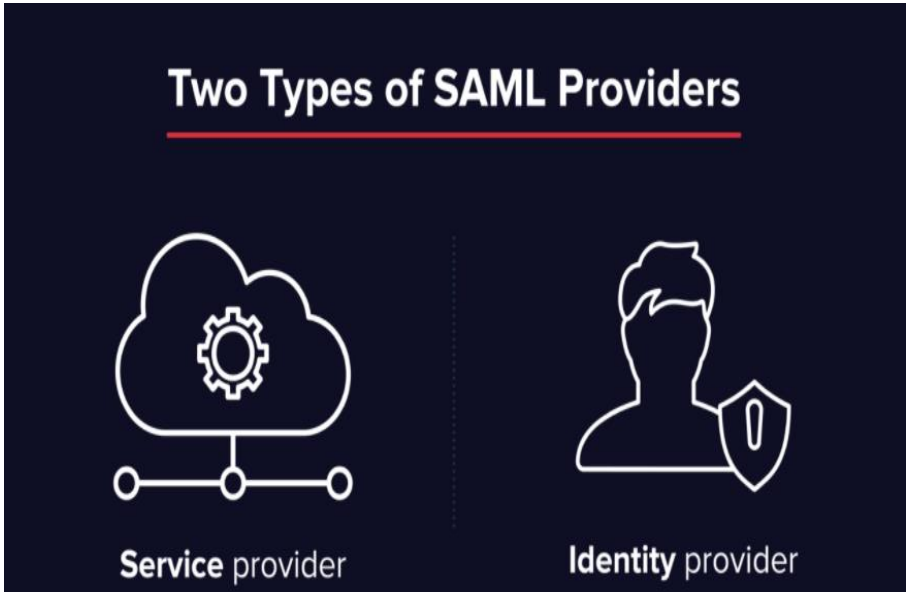
IAM processes support the following operational activities:

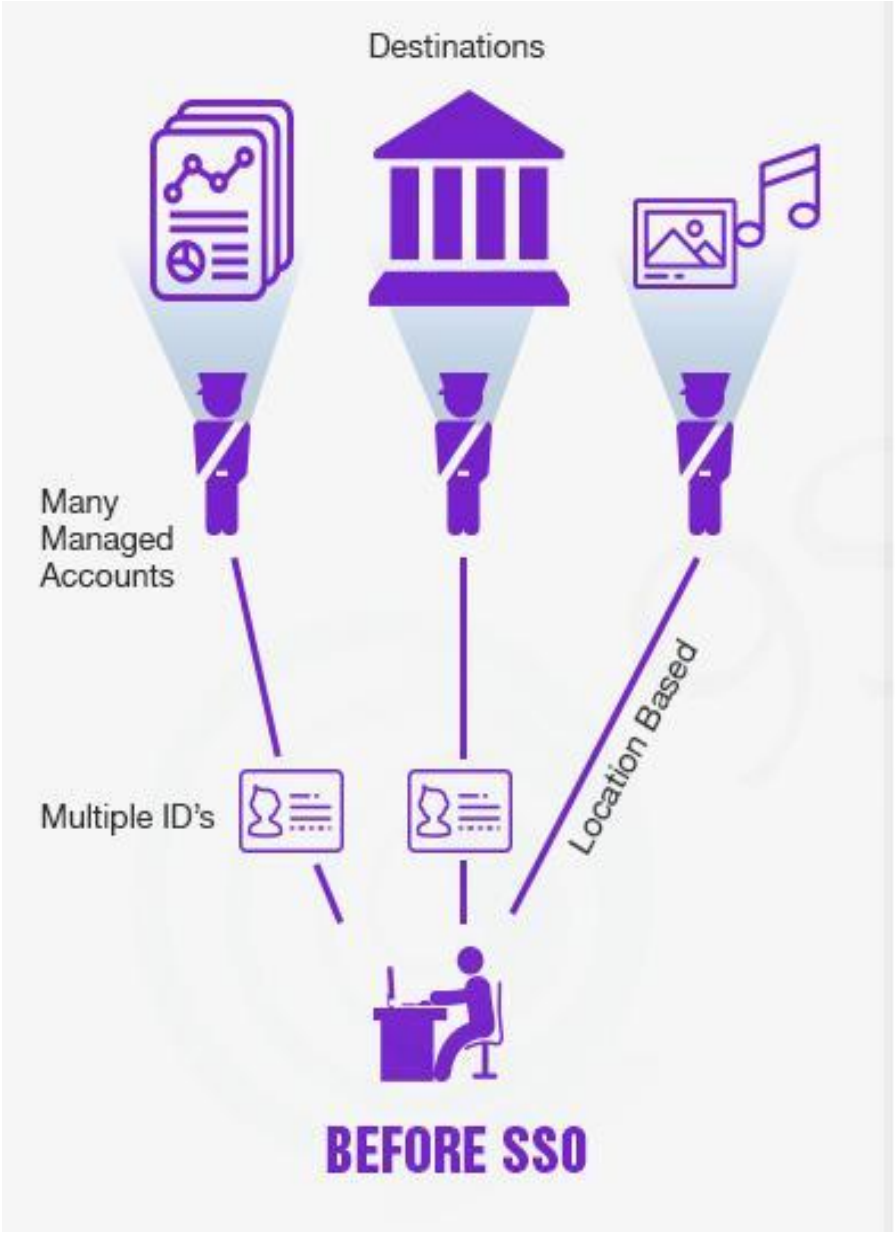
- Provisioning
- Credential and attribute management
- Entitlement management
- Compliance management
- Identity federation management

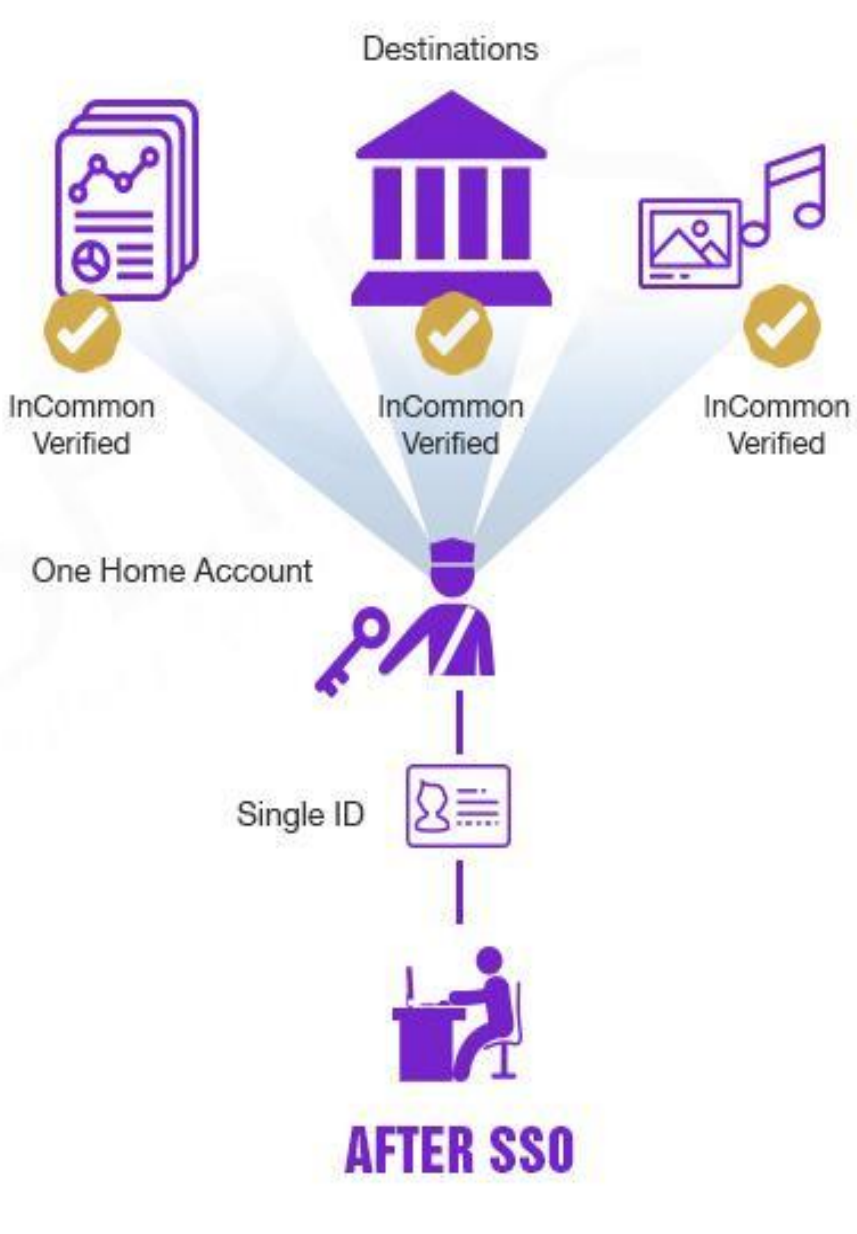

Relationship begins
Provisioning
Authentication
Authorization
Identity management life cycle
Self-service
Password management
Compliance
Deprovisioning
Relationship ends

IAM standard

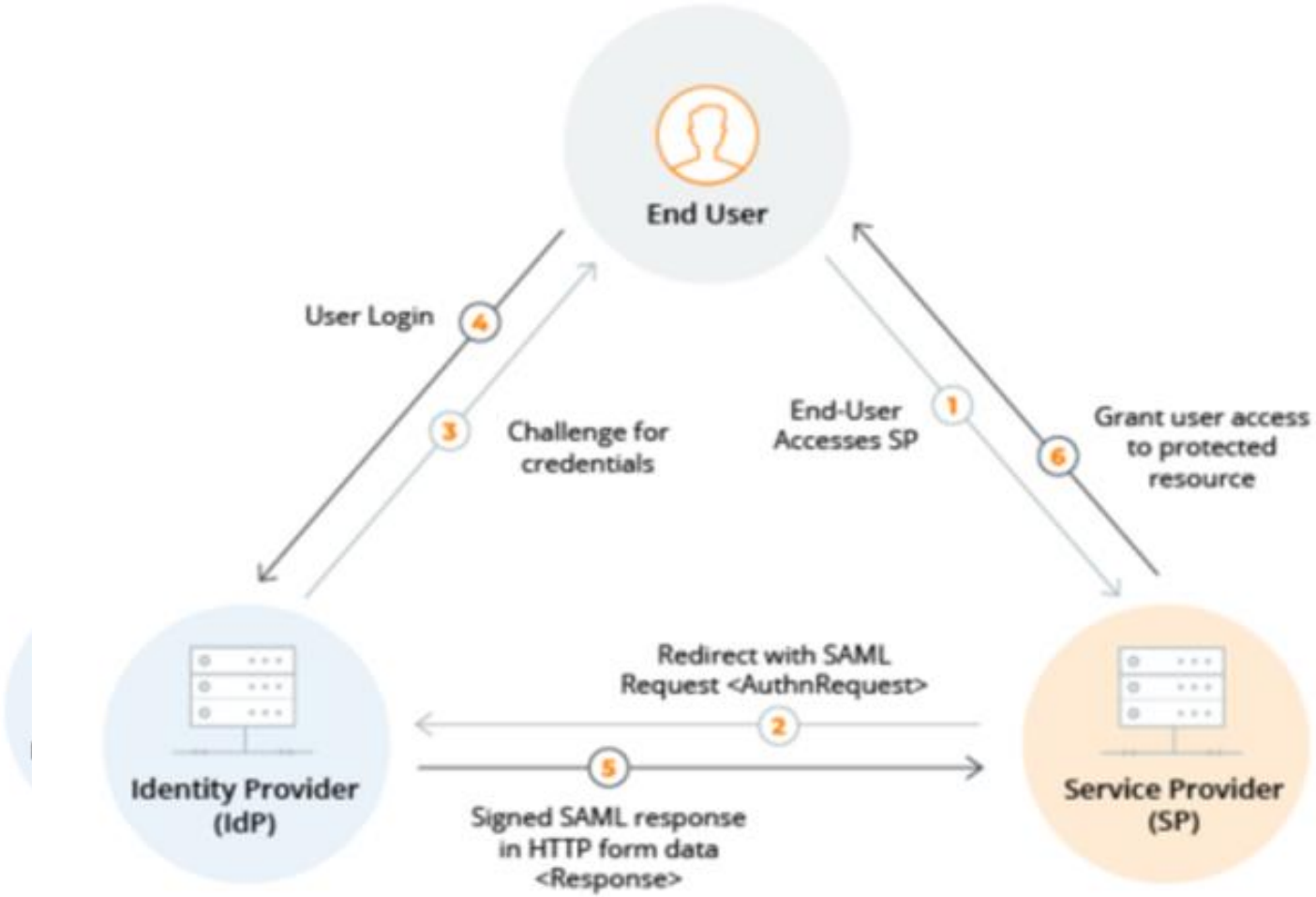
- **SAML Security Assertion Markup Language** is an XML-based open standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.
- Security Assertion Markup Language (SAML) is a type of Single Sign-On (SSO) standard.



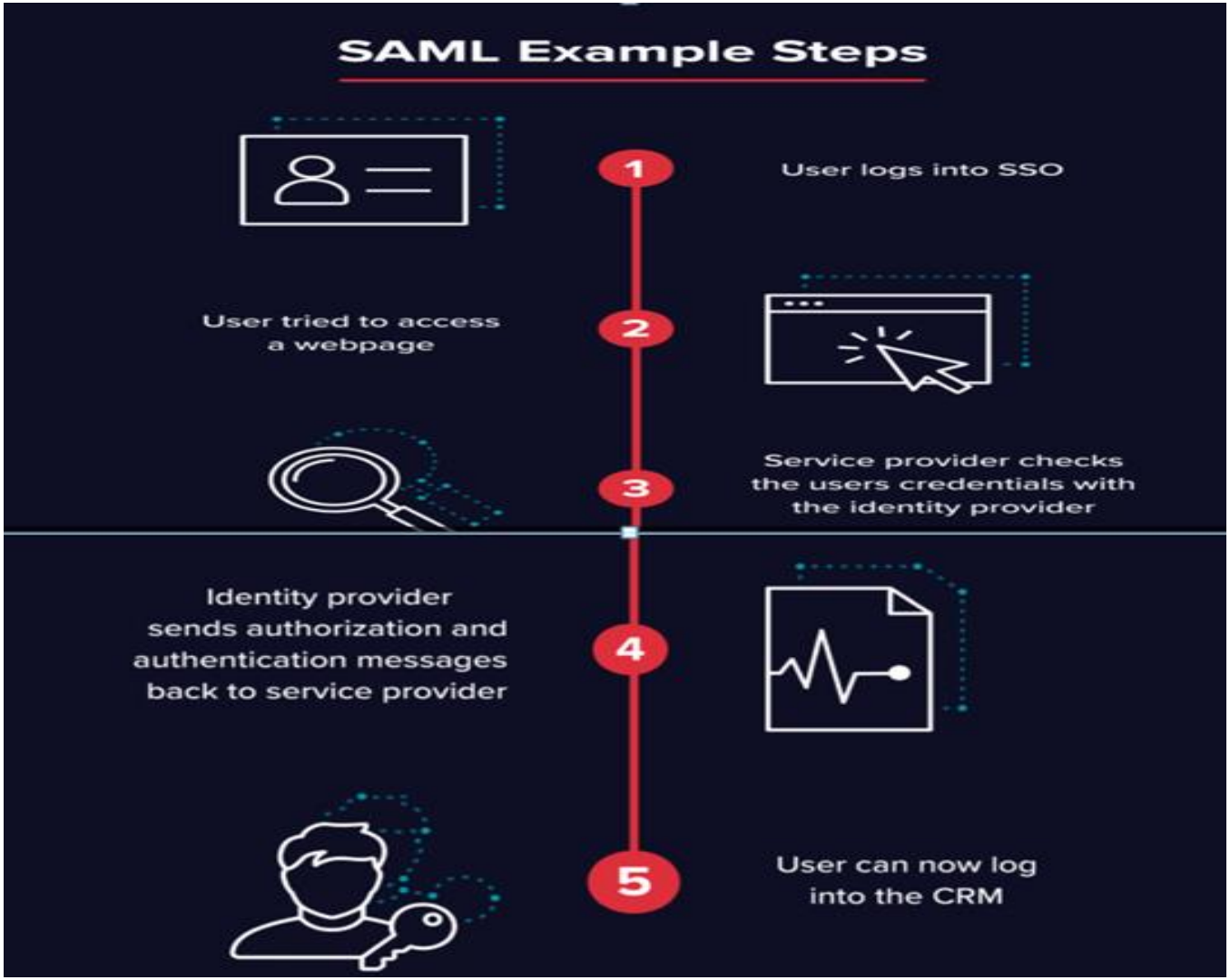

Destinations
Many Managed Accounts
Multiple ID's
Location Based
BEFORE SSO


Destinations
InCommon Verified
InCommon Verified
InCommon Verified
One Home Account
Single ID
AFTER SSO

For eg. Authenticating in your Gmail account doesn't require to do the same in youtube, google drive, and other google services.

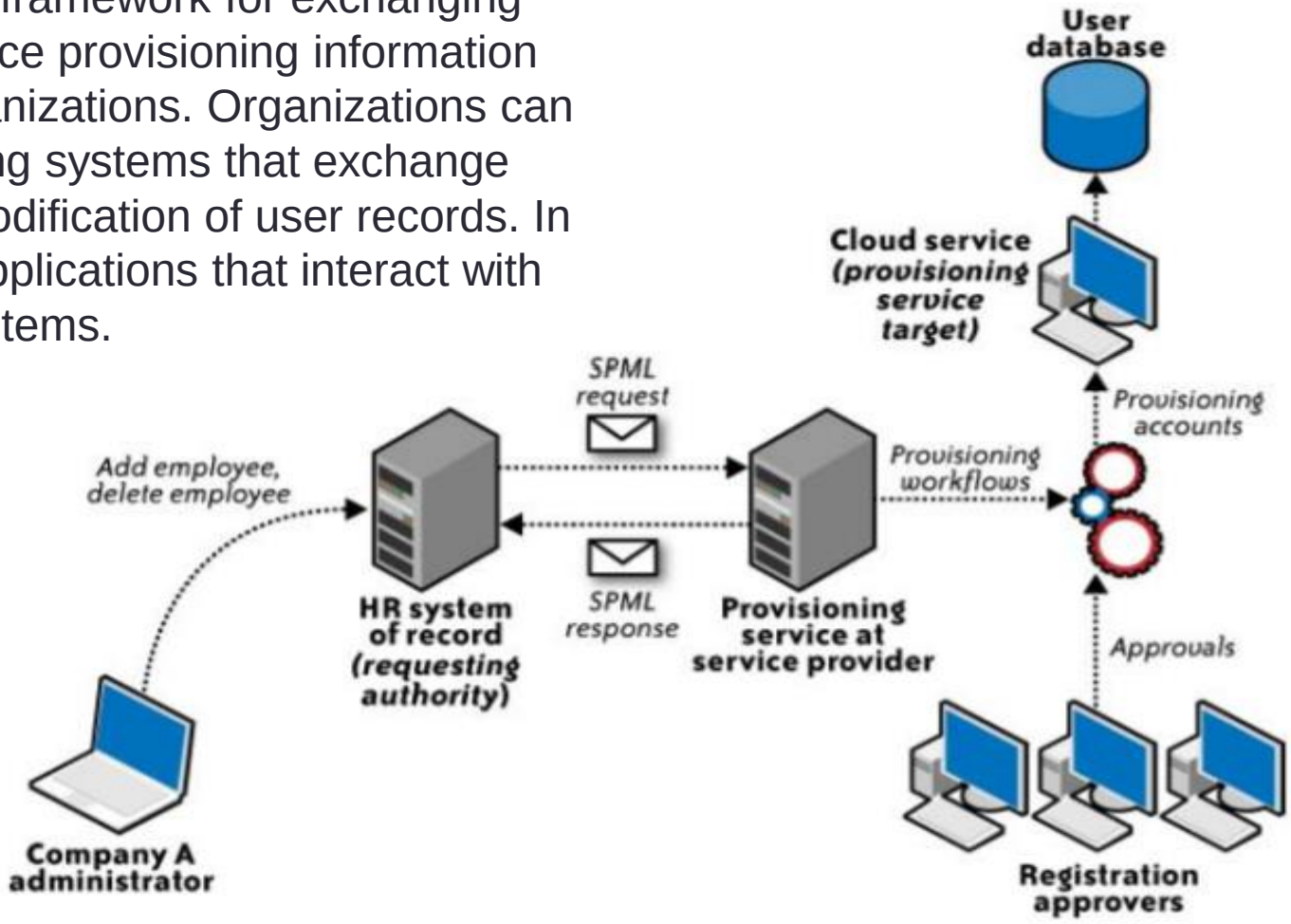

End User
User Login
4
3
Challenge for credentials
End-User Accesses SP
1
6
Grant user access to protected resource
Redirect with SAML Request <AuthnRequest>
2
5
Signed SAML response in HTTP form data <Response>
Identity Provider (IdP)
Service Provider (SP)

SAML


SAML Example Steps
1
User logs into SSO
User tried to access a webpage
2
3
Service provider checks the users credentials with the identity provider
Identity provider sends authorization and authentication messages back to service provider
4
5
User can now log into the CRM

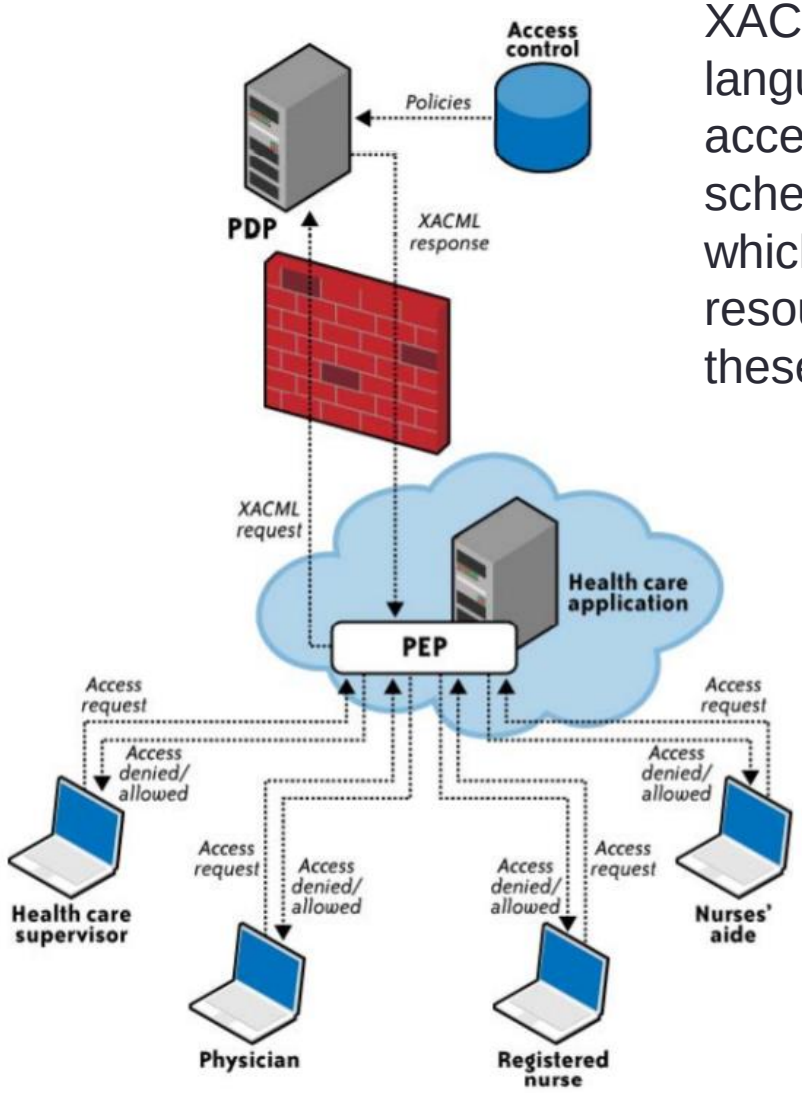
Service Provisioning Markup Language (SPML)

SPML is an XML-based framework for exchanging user, resource,and service provisioning information among cooperating organizations. Organizations can have multiple provisioning systems that exchange information about the modification of user records. In addition, there can be applications that interact with multiple provisioning systems.



SPML use case

eXensible Access Control Markup Language (XACML)



XACML XML-based access control language for policy management and access decisions. It provides an XML schema for a general policy language which is used to protect any kind of resource and make access decisions over these resources.

User---resource, req…….PEP—PDP ----PIP (Policy information point)

A1
Rakesh
Id—p1001

PEP(Policy Enforcement Point)

- It is the interface of the application environment.
- It is network device on which policy decisions are carried out.
- When user tries to access a file or other resources on the computer network, the PEP will describe the user`s attribute to the other entities on the system

PDP(Policy decision Point)

- It collects all the necessary information from available information sources and concludes with a decision on what access to grant.
- PDP should be located in trusted network with strong access control policies ,e.g., in a corporate trusted network protected by a corporate firewall

IAM Protocol

OpenID
OpenID is a protocol for **authentication** while OAuth is for **authorization**

OpenID is about verifying a person's **identity** (authentication).
OAuth is about **accessing** a person's resource (authorization).

OpenID Connect **does both**.

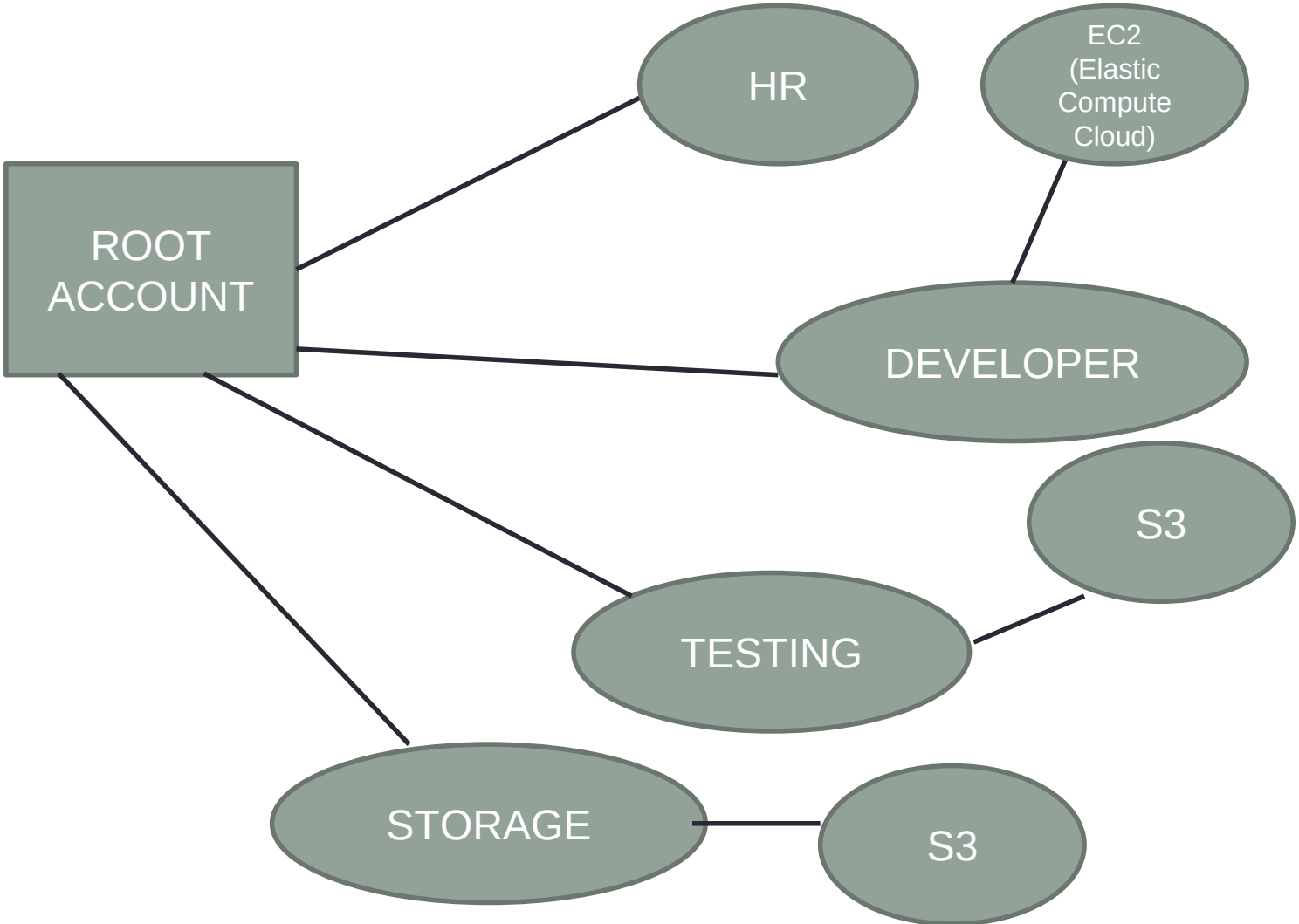
IAM Protocol

Information cards

ROOT ACCOUNT IN AWS

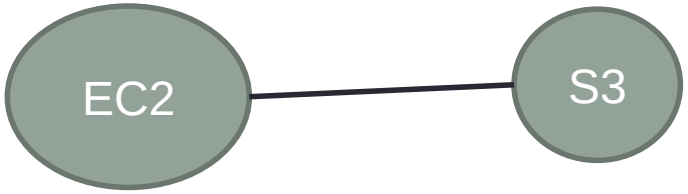
- There are two different types of users in AWS. You are either the account owner (root user) or you are an AWS Identity and Access Management (IAM) user.
- The root user is created when the AWS account is created and IAM users are created by the root user
- All AWS users have security credentials.

AWS


HR
EC2
(Elastic
Compute
Cloud)
ROOT
ACCOUNT
DEVELOPER
S3
TESTING
STORAGE
S3

IAM Features

1. Shared access to your AWS account
2. Granular Permission
3. Secure access to AWS resources for application that run on EC2.
4. Multifactor Authentication
5. Identity federation
6. Identity information for assurance
7. PCI-DSS Compliance(Payment Card Industry Data Security Standards)
8. Eventually consistent



IAM Challenges

- One critical challenge of IAM concerns managing access for diverse user populations (employees, contractors, partners, etc.) accessing internal and externally hosted services. IT is constantly challenged to rapidly provision appropriate access to the users whose roles and responsibilities often change for business reasons.
- Another issue is the **turnover of users** within the organization. Turnover varies by industry and function—seasonal staffing fluctuations in finance departments, for example—and can also arise from changes in the business, such as mergers and acquisitions, new product and service releases, business process outsourcing, and changing responsibilities. As a result, sustaining IAM processes can turn into a persistent challenge.

IAM Practices in the Cloud

30/09/2020

IAM Practices in the Cloud

- When compared to the traditional applications deployment model within the enterprise, IAM practices in the cloud are still evolving. In the current state of IAM technology, standards support by CSPs (SaaS, PaaS, and IaaS) is not consistent across providers. Although large providers such as Google, Microsoft, and Salesforce.com seem to demonstrate basic IAM capabilities.

CONTD....

- Although the principles and purported benefits of established enterprise IAM practices and processes are applicable to cloud services, they need to be adjusted to the cloud environment. Broadly speaking, user management functions in the cloud can be categorized as follows:

1. Cloud identity administration
2. Federation or SSO
3. Authorization management
4. Compliance management

Cloud Identity Administration

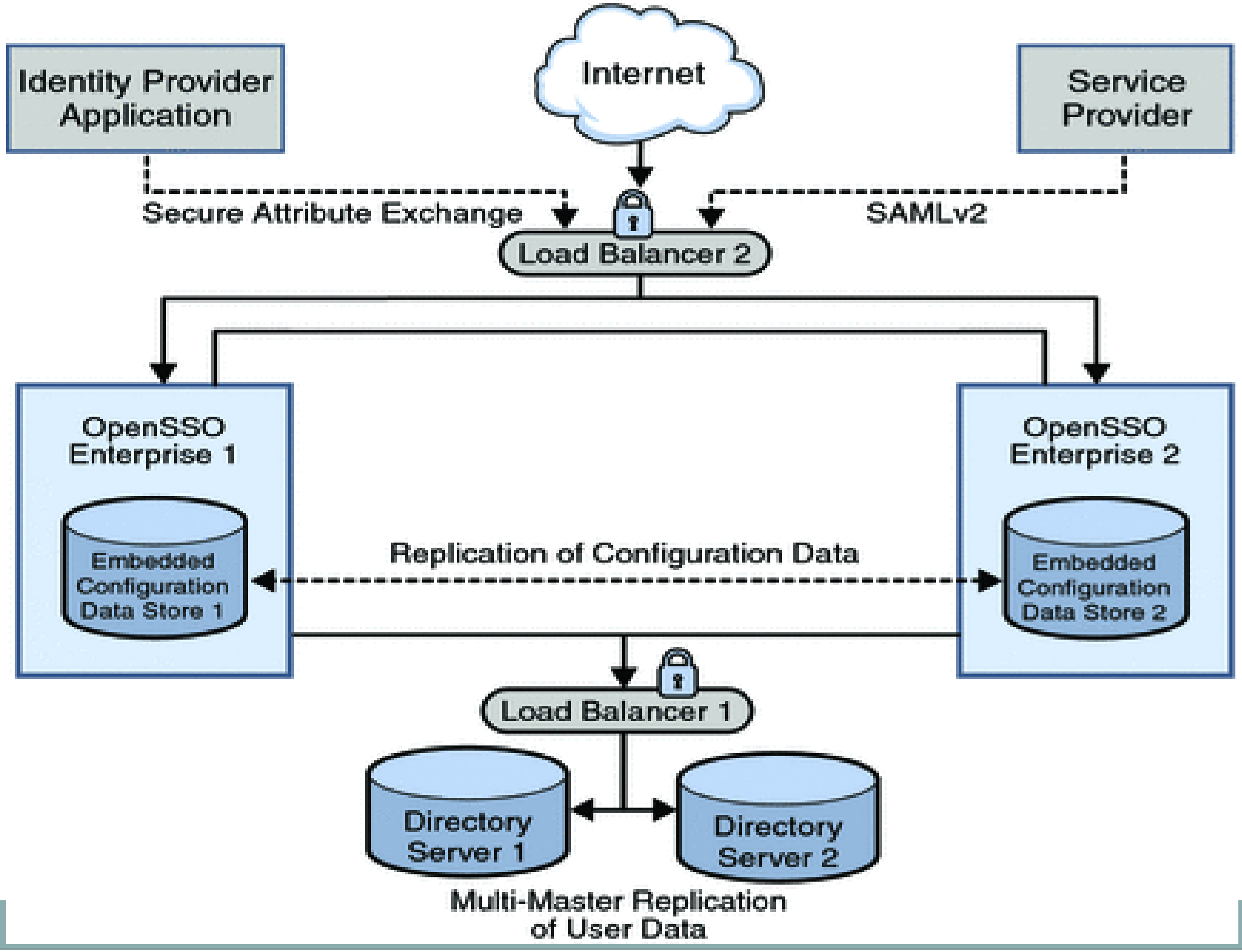
- Cloud identity administrative functions should focus on life cycle management of user identities in the cloud-

1. provisioning,
2. deprovisioning,
3. identity federation, SSO,
4. password or credentials management, profile management,
5. and administrative management

Federated Identity (SSO)

- Organizations planning to implement identity federation that enables SSO for users can take one of the following two paths (architectures):

1. Implement an enterprise IdP within an organization perimeter.
2. Integrate with a trusted cloud-based identity management service provider.


Identity Provider Application
Internet
Service Provider
Secure Attribute Exchange
SAMLv2
Load Balancer 2
OpenSSO Enterprise 1
OpenSSO Enterprise 2
Embedded Configuration Data Store 1
Replication of Configuration Data
Embedded Configuration Data Store 2
Load Balancer 1
Directory Server 1
Directory Server 2
Multi-Master Replication of User Data

Contd....

- An identity provider specializes in providing authentication services. As the administrating service for authentication, an identity provider maintains and manages identity information. It establishes trust with a service provider in order to exchange user credentials, enabling single sign-on between the providers. Authentication by an identity provider is honored by all service providers with whom the identity provider is partnered. The identity provider domain is idp-example.com. The following image illustrates the identity provider architecture in this deployment.

Contd.....

- The identity provider domain in this deployment is idp-example.com. The identity provider application represents a legacy system which relies on OpenSSO Enterprise to act as a secure gateway through which identity information can be transferred to another application in a different domain. This functionality is provided by the Secure Attribute Exchange feature of OpenSSO Enterprise which uses SAML v2 without having to deal with federation protocol and processing

Cloud Authorization Management

- Medium-size and large organizations usually have specific requirements for authorization features for their cloud users (i.e., assignment of privileges, or entitlements, to users based on their job functions). In some cases, a business application may require role-based access control (RBAC), in which case authorization is structured to suit the organization's functional role requirements

Contd…

- Most cloud services support at least dual roles (privileges): administrator and end user. It is a normal practice among CSPs to provision the administrator role with administrative privileges. These privileges allow administrators to provision and deprovision identities, basic attribute profiles, and, in some cases, to set access control policies such as password strength and trusted networks from which connections are accepted.
- XACML is the preferred standard for expressing and enforcing authorization and user authentication policies.

IAM Support for Compliance Management

- As much as cloud IAM architecture and practices impact the efficiency of internal IT processes, they also play a major role in managing compliance within the enterprise. Properly implemented IAM practices and processes can help improve the effectiveness of the controls identified by compliance frameworks. For example, by automating the timely provisioning and deprovisioning of users and entitlements, organizations can reduce the risk of unauthorized users accessing cloud services and meet your privacy and compliance requirements.

Contd…

- IAM standards such as SAML (federation), SPML (provisioning), and XACML (authorization) by the CSP, you should assess the CSP capabilities on a case-by-case basis and institute process

Cloud Service Provider IAM Practice

- From the CSP's (SaaS, PaaS, or IaaS) perspective, IAM features should be included in the cloud service's design criteria, with the goal of delegating user authentication and authorization to the customer using user management and federation standards. Support for IAM features has integration implications for both customers (e.g., single sign-on, user provisioning) and CSPs (e.g., billing, accounting resource utilization)

Contd…

- From a cloud customer perspective, the application's IAM capabilities (or lack thereof), such as identity federation, will impact the cloud service governance, integration, and user experience (e.g., barriers to adopt the cloud service).

Enterprise IAM requirements include:

- Provisioning of cloud service accounts to users, including administrators.
- Provisioning of cloud services for service-to-service integration (e.g., private [internal] cloud integration with a public cloud).
- SSO support for users based on federation standards (e.g., SAML support).

Security Management in the Cloud

Security Management in the Cloud

Security management in the cloud is a set of strategies designed to allow a business to use cloud applications and networks to their greatest potential

- **Identifying and assessing cloud services.** First, you need to spend time identifying which cloud products and services are being used in your organization, and which ones might be considered in the future. Then, you'll need to assess and audit those items, analyzing their security.
- **Auditing and adjusting native security settings.** Within each application, you'll have full control of your own privacy and security settings. It's on your cloud security team to understand which settings are available, and take full advantage of them to grant your organization the highest possible level of security.
- **Encrypting data.** In many cases, you'll need to take extra efforts to prevent data loss and preserve data integrity by encrypting your data and securing your connections. It's your responsibility to allow legitimate network traffic and block suspicious traffic.
- **Managing devices.** Cloud applications allow you to reduce the amount of physical infrastructure you maintain, but you and your employees will still be accessing data and services with specific devices. You'll need some way to manage and monitor those devices to ensure only authorized devices can access your data.
- **Managing users.** Similarly, you'll need to consider user-level controls. Establish varying levels of user permissions, to restrict access to your most valuable or sensitive information, and change user permissions as necessary to allow secure access.
- **Reporting.** It's also important to monitor cloud activity from a high level, and report on that activity so you can better understand your risks and ongoing operations.

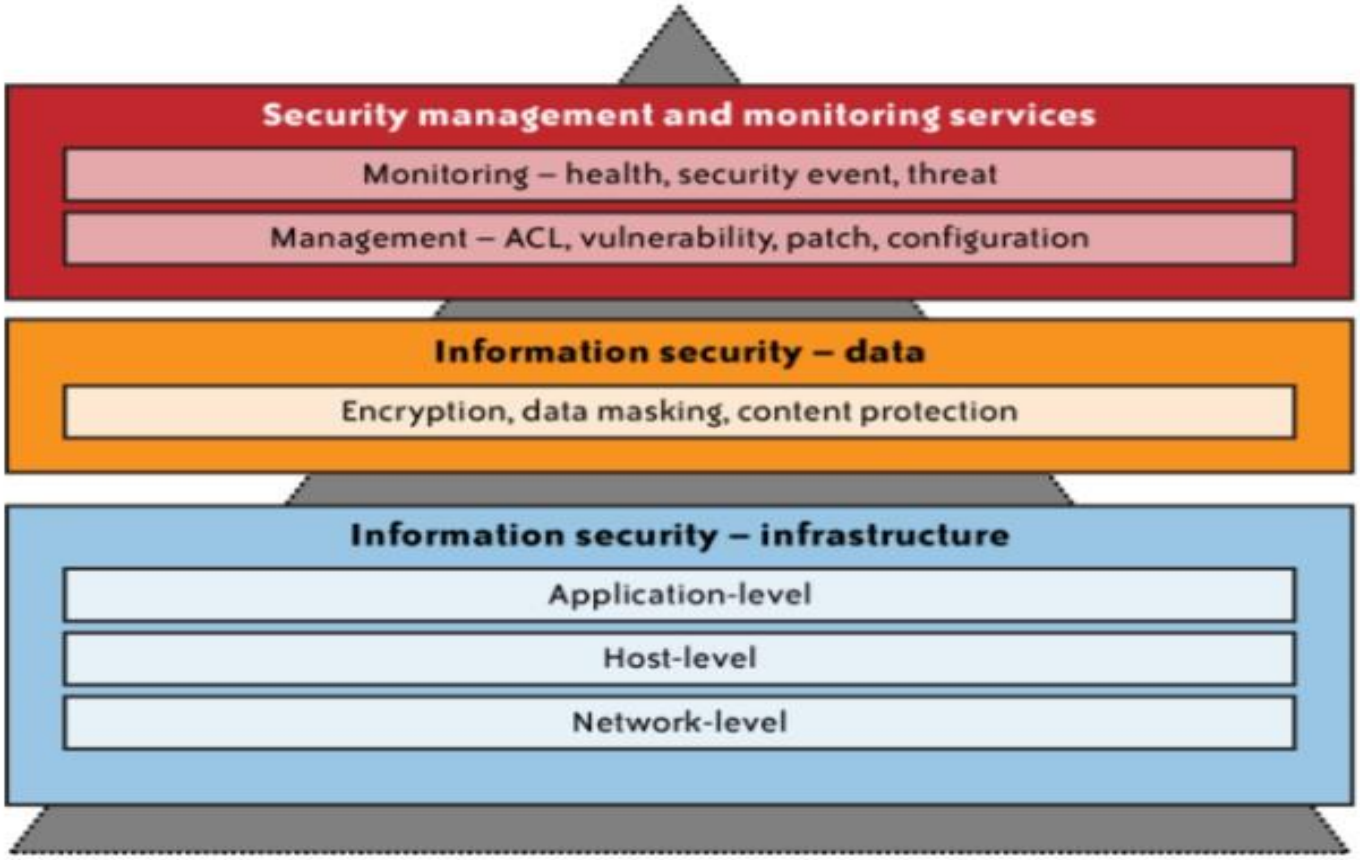
Introduction

- **WITH THE ADOPTION OF PUBLIC CLOUD SERVICES, A LARGE PART OF YOUR NETWORK,** system, applications, and data will move under third-party provider control.
- security model with responsibilities shared between the customer and the cloud service provider (CSP).
- This shared responsibility model will bring new security management challenges to the organization's IT operations staff.

Contd…

- As a customer of the cloud, you should start with the exercise of understanding the trust boundary of your services in the cloud. You should understand all the layers you own, touch, or interface with in the cloud service—network, host, application, database, storage, and web services including identity services . You also need to understand the scope of IT system management and monitoring responsibilities that fall on your shoulders, including access, change, configuration, patch, and vulnerability management.

Contd..



Security management and monitoring scope

Contd…

- Although you may be transferring some of the operational responsibilities to the provider, the level of responsibilities will vary and will depend on a variety of factors, including the service delivery model (SPI), provider service-level agreement (SLA), and provider-specific capabilities to support the extension of your internal security management processes and tools.
- IT organizations are known to employ security management frameworks, such as ISO27000 and the Information Technology Infrastructure Library (ITIL) service management framework.

Contd…

- In short, security management is a constant process and will be very relevant to cloud security management. The goal of the ITIL Security Management framework is divided into two parts:
- Realization of security requirements
- Realization of a basic level of security

Security Management Standards

- Security Management has to be carried out in the cloud.
- Standards include ITIL(Information Technology Infrastructure Library) and ISO 27001/27002
- What are the policies, procedures, processes and work instruction for

Information Technology Infrastructure Library(ITIL)

- The ITIL (Information Technology Infrastructure Library) is a framework designed to standardize the selection, planning, delivery and maintenance of IT services within a business. The goal is to improve efficiency and achieve predictable service delivery.

Set of guidelines with instructions for
how you can provide the best service
possible

ITIL

ITIL an approach of how to do IT service management. Not the only method but it`s certainly the most popular one.
ITIL is used most of the biggest companies worldwide across all industries the works for them it will probably work for you

ITIL v4

"A means of enabling value co-creation by facilitating outcomes that customers want to achieve, without the customer having to manage specific costs and risks"

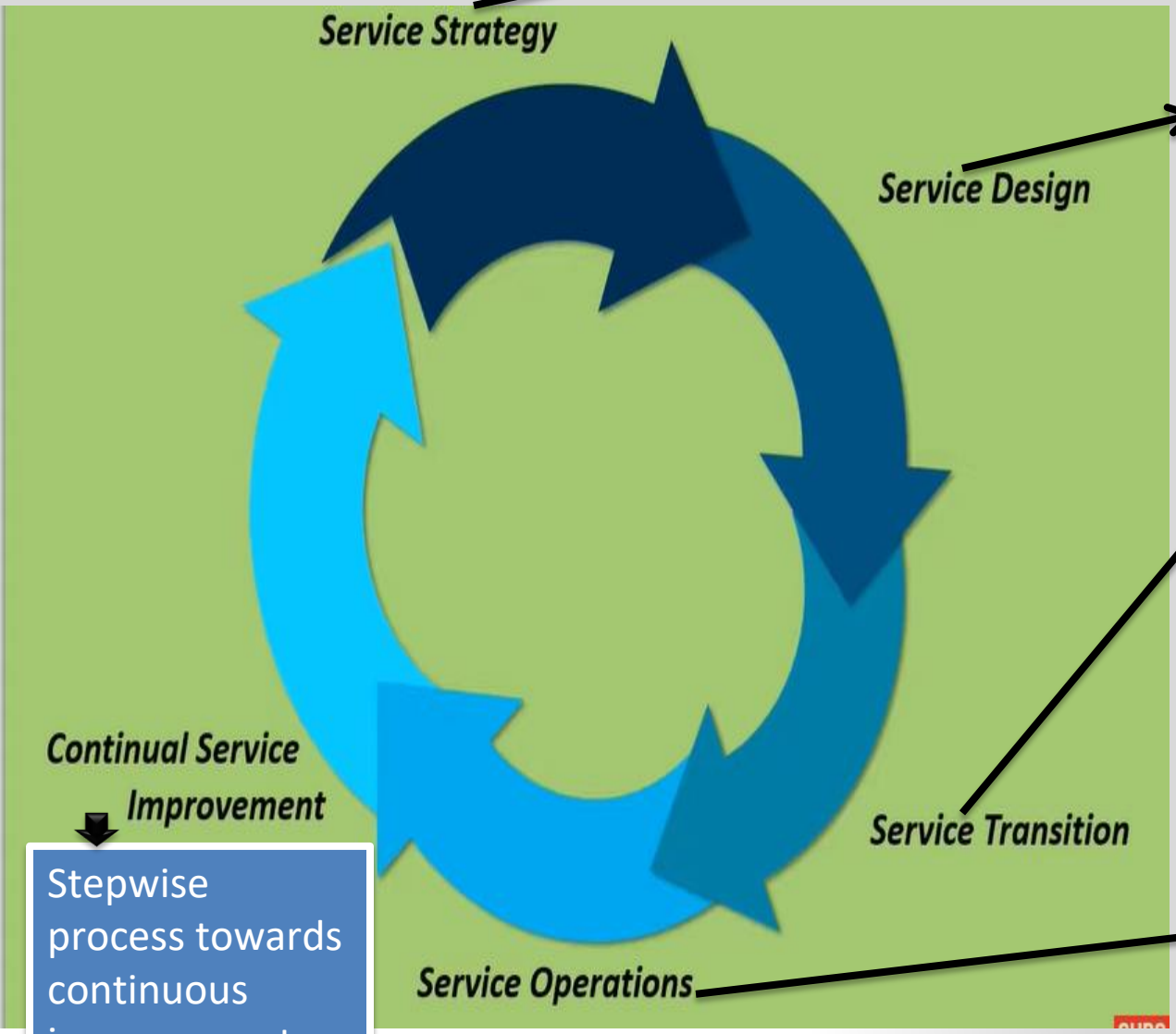
Information Technology Infrastructure Library(ITIL)

- The Information Technology Infrastructure Library (ITIL) is a set of best practices and guidelines that define an integrated, process-based approach for managing information technology services. ITIL can be applied across almost every type of IT environment including cloud operating environment. ITIL seeks to ensure that effective information security measures are taken at strategic, tactical, and operational levels. Information security is considered an iterative process that must be controlled, planned, implemented, evaluated, and maintained

Information Technology Infrastructure Library(ITIL)

- ITIL breaks information security down into:
- **Policies :**The overall objectives an organization is attempting to achieve
- **Processes :**What has to happen to achieve the objectives **Procedures :**Who does what and when to achieve the objectives Work instructions Instructions for taking specific actions

ITIL Process Stages



Vision and mission of an organization

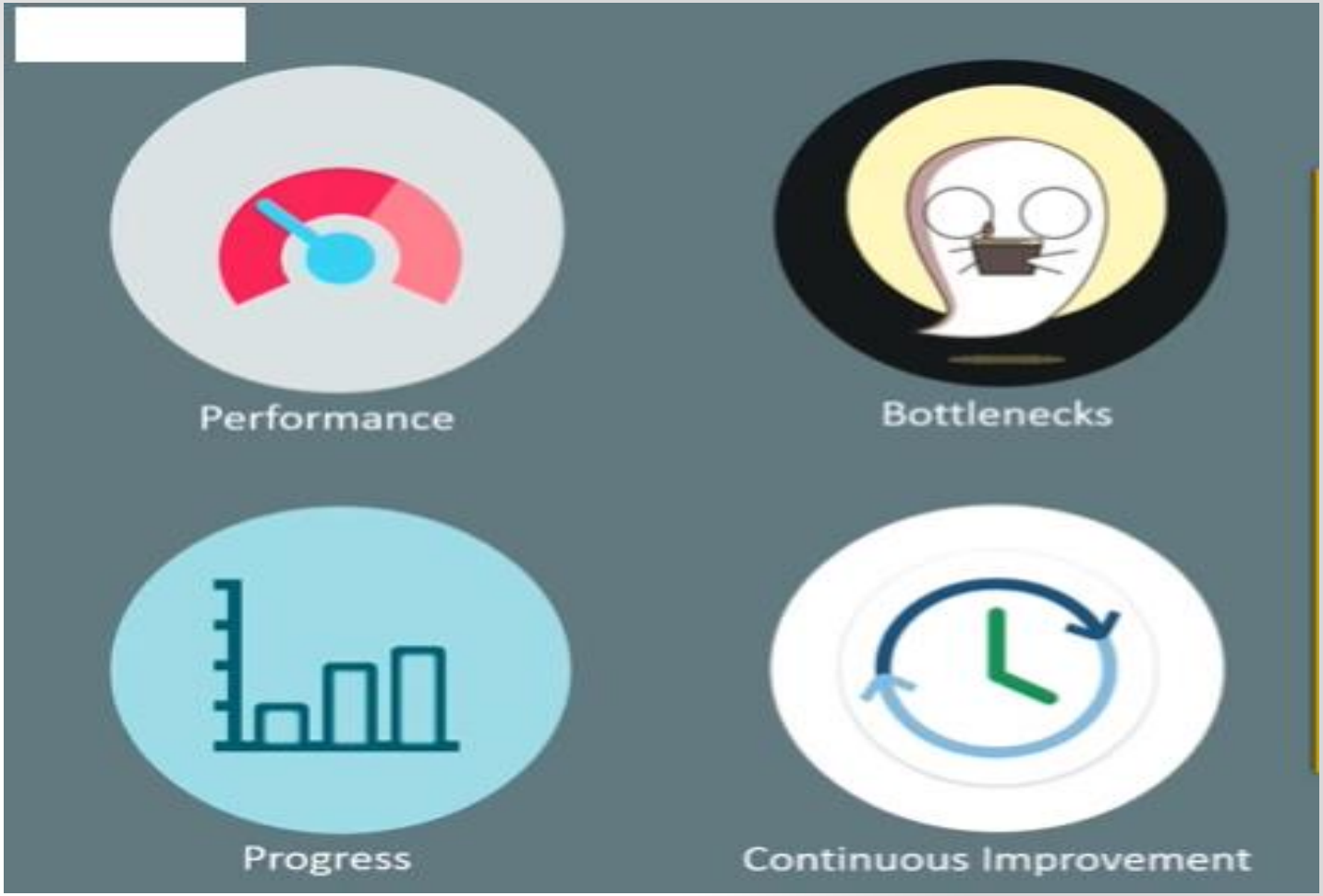
Handle the current issues

Process of project management

Day to day activities

Stepwise process towards continuous improvement

ITIL Function




HONDA
SONY
VISA
Walmart
Microsoft
NASA
BOEING
IBM
JPMorganChase
hp

ISO &IEC

- **ISO** stands for **International Organization for standardization**
  - founded in 1947
  - develop and publish International Standards.
  - published 21578 International Standards
  - reach up-to 162 countries and have 3923 technical bodies to take care of standards development
- **IEC** stands for **International Electro Technical Commission**Founded in 1906
- prepare and publish International Standards for all electrical, electronic and related technologies. These are known collectively as “electrotechnology”.

ISO27001/ 27002-information security control

- Its is the international standard that sets out the specification for an information security management system (ISMS).
- Its best-practice approach helps organisations manage their information security by addressing people and processes as well as technology.
- ISO 27001 is a framework that helps organisations “establish, implement, operate, monitor, review, maintain and continually improve an ISMS.
- ISO 27001 is an auditable standard.
- It ensure selection of adequate security controls (114 controls) to protect information assets from various threats and risks.

example

Information Security Management System (ISMS)

- ISO/IEC(the Internal Organization for Standardization) and(the Internationl Electrotechnical Commission) together write interdisciplinary standards which are valid in all the industries. ISO 27001 is the standard for 'Information Security' which is called as '**Information Security Management System**'
- An Information Security Management System (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems.
- **An Information Security Management System (ISMS) is a management system based on a systematic business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.**
- It is a quality standard that explains the different requirements to implement an information security management system. This is to make sure there are security parameters in place to protect the most vital data of any organization.


Design, Build
& Maintain
the ISMS

how does it help your organization?

- It is a quality standard that explains the different requirements to implement an information security management system. This is to make sure there are security parameters in place to protect the most vital data of any organization.
- When you have ISO/27001 standard implemented, you can be rest assured that your data will be protected from any possible security threat. There would be different processes and procedures that are implemented in your organization that would help your employees understand how data must be protected. These changes in the system and the certification too would give a lot of confidence to employees, clients and possible customers.

Benefits of ISMS

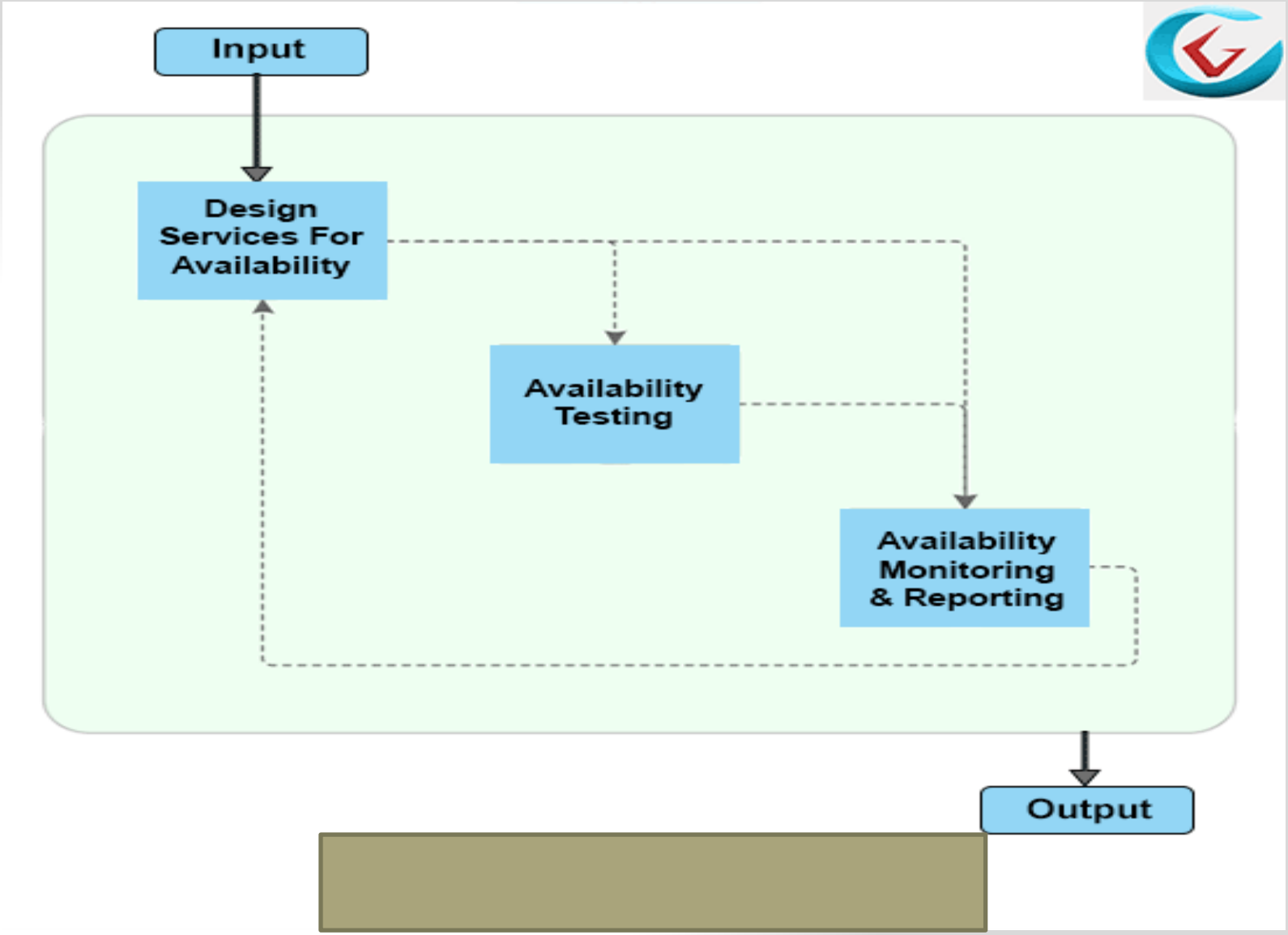
- Ability to market more: Because more people in the industry want to work with companies that protect data better, you would be able to market yourself quite easily. There would always be potential clients you can approach .They would potentially never have to worry about data loss or theft with a certification like this with their vendor.
- Confidence of clients: Having the confidence of your clients is of critical importance in any field of business. The moment your clients know they have the right vendor; they would renew your contracts with ease.

Security Management in the cloud

- After analyzing the management process disciplines across the ITIL and ISO frameworks, identified the following relevant processes as the recommended security management focus areas for securing services in the cloud:
- Availability management (ITIL)
- Access control (ISO/IEC 27002, ITIL)
- Vulnerability management (ISO/IEC 27002)
- Patch management (ITIL)
- Configuration management (ITIL)
- Incident response (ISO/IEC 27002)
- System use and access monitoring (ISO/IEC 27002)

Availability management

- The Goal of Availability Management is to ensure that level of service availability is delivered in all services is matched to or exceeds the current and future agreed needs of the business in a cost-effective manner.
- Availability is one of the most critical parts of the warranty of a service. If a service does not deliver the levels of availability required, then the business will not experience the value that has been promised.
- Without availability the utility of the service cannot be accessed. Availability management process activity extends across the service lifecycle.


Input
Design Services For Availability
Availability Testing
Availability Monitoring & Reporting
Output

The Objectives

- Produce and maintain an appropriate and up to date availability Plan, that reflects the current and future needs of the business.
- Provide advice and guidance to all other areas on availability related issues.
- Assist with diagnosis and resolution of availability related incidents and problems.
- Asses the impact of all changes on the Availability Plan, and the performance, and capacity of services and resources.
- Availability management should always ensure that the agreed level of availability is provided. The measurement and monitoring of IT availability is a key activity to ensure availability levels are being met.

Few key concepts of Availability Management

- **Availability:** In simplest terms, the ability of a service, component to perform its agreed function when required. This term answer the question, is it available to use when needed?
- **Reliability:** A measure of how long a service, component can perform its agreed function without interruption. When we understood the availability, the questions comes, how long the service will be available? This can be answered by reliability.
- **Maintainability:** A measure of how quickly and effectively a service, component can be restored to normal after a failure. The emphasis is on how soon or how quickly the services can be back ..

Availability management (ITIL)

- Cloud services are not immune to outages,
- Cloud Computing Incidents Database (CCID), which tracks cloud service outages, major CSPs have suffered downtime ranging from a few minutes to a few hours. In one case, a service outage lasted more than 24 hours!
- on December 20, 2005 Salesforce.com (the on-demand customer relationship management service) said it suffered from a system outage that prevented users from accessing the system during business hours.

SaaS Availability Management

- SaaS service providers are responsible for business continuity, application, and infrastructure security management processes. This means the tasks your IT organization once handled will now be handled by the CSP. Some mature organizations that are aligned with industry standards, such as ITIL, will be faced with new challenges of governance of SaaS services as they try to map internal service-level categories to a CSP
- **Customer Responsibility** Customers should understand the SLA and communication methods to stay informed on service outages.
- When possible, customers should use automated tools such as Nagios(Nagios offers monitoring and alerting services for servers, switches, applications and services.) or Siteuptime.com to verify the availability of the SaaS service.

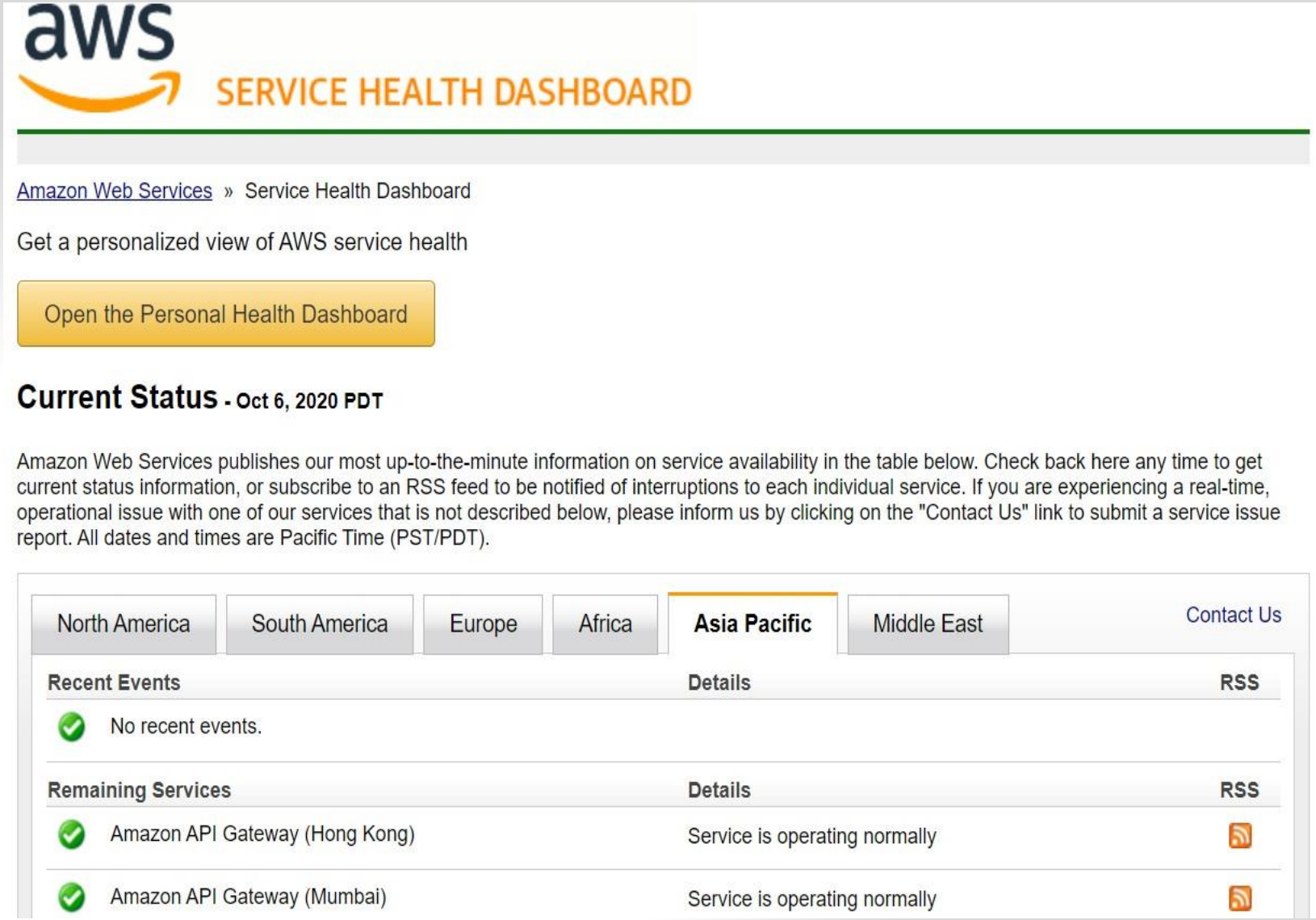
SaaS Availability Management

- SaaS Health Monitoring The following options are available to customers to stay informed on the health of their service:

• Service health dashboard published by the CSP. Usually SaaS providers, such as Salesforce.com, publish the current state of the service, current outages that may impact customers, and upcoming scheduled maintenance services on their website

• Customer mailing list that notifies customers of occurring and recently occurred outages.

• Internal or third-party-based service monitoring tools that periodically check SaaS provider health and alert customers when service becomes unavailable (e.g., Nagios monitoring tool).


aws
SERVICE HEALTH DASHBOARD
Amazon Web Services » Service Health Dashboard
Get a personalized view of AWS service health
Open the Personal Health Dashboard
Current Status - Oct 6, 2020 PDT
Amazon Web Services publishes our most up-to-the-minute information on service availability in the table below. Check back here any time to get current status information, or subscribe to an RSS feed to be notified of interruptions to each individual service. If you are experiencing a real-time, operational issue with one of our services that is not described below, please inform us by clicking on the "Contact Us" link to submit a service issue report. All dates and times are Pacific Time (PST/PDT).
North America
South America
Europe
Africa
Asia Pacific
Middle East
Contact Us
Recent Events
Details
RSS
No recent events.
Remaining Services
Details
RSS
Amazon API Gateway (Hong Kong)
Service is operating normally
Amazon API Gateway (Mumbai)
Service is operating normally

PaaS Availability Management

- Manage this activity for applications deployed in the PaaS platform (the provider is responsible for runtime engine and services).
- For example, a social network application on the Google App Engine that depends on a Facebook application for a contact management service.
- For example, Force.com is responsible for the management of the AppExchange platform, and customers are responsible for managing the applications developed and deployed on that platform.

PaaS Availability Management

- **Customer Responsibility:**the PaaS application customer should carefully analyze the dependencies of the application on the third-party web services (components).
- The following considerations are for PaaS customers:
- **PaaS platform service levels Customers** should carefully review the terms and conditions of the CSP's SLAs and understand the availability constraints.
- **Third-party web services provider service levels:** When your PaaS application depends on a third-party service, it is important to understand the SLA of that service

PaaS Availability Management

- PaaS Health Monitoring: customers should monitor their application, as well as the third-party web component services.
- Service health dashboard published by the CSP
- CSP customer mailing list that notifies customers of occurring and recently occurred outages
- RSS feed for RSS readers with availability and outage information
- Internal or third-party-based service monitoring tools that periodically check your PaaS application, as well as third-party web services that monitor your application (e.g., Nagios monitoring tool)

IaaS Availability Management

- Availability considerations for the IaaS delivery model should include both a computing and storage (persistent and ephemeral) infrastructure in the cloud.
- IaaS providers may also offer other services such as account management, a message queue service, an identity and authentication service, a database service, a billing service, and monitoring services.
- Hence, availability management should take into consideration all the services that you depend on for your IT and business needs.
- Customers are responsible for all aspects of availability management since they are responsible for provisioning and managing the life cycle of virtual servers

IaaS Availability Management

- **IaaS Health Monitoring:**
- Service health dashboard published by the CSP.
- CSP customer mailing list that notifies customers of occurring and recently occurred outages.
- Internal or third-party-based service monitoring tools (e.g., Nagios) that periodically check the health of your IaaS virtual server. For example, Amazon Web Services (AWS) is offering a cloud monitoring service called CloudWatch. This web service provides monitoring for AWS cloud resources, including Amazon's Elastic Compute Cloud (EC2). It also provides customers with visibility into resource utilization, operational performance, and overall demand patterns, including metrics such as CPU utilization, disk reads and writes, and network traffic.
-

Access Control

At a high level, access control is about restricting access to a resource. Any access control system, whether physical or logical, has five main components:

- **Authentication:** The act of proving an assertion, such as the identity of a person or computer user. It might involve validating personal identity documents, verifying the authenticity of a website with a digital certificate, or checking login credentials against stored details.
- **Authorization:** The function of specifying access rights or privileges to resources. For example, human resources staff are normally authorized to access employee records and this policy is usually formalized as access control rules in a computer system.
- **Access:** Once authenticated and authorized, the person or computer can access the resource.
- **Manage:** Managing an access control system includes adding and removing authentication and authorization of users or systems. Some systems will sync with G Suite or Azure Active Directory, streamlining the management process.
- **Audit:** Frequently used as part of access control to enforce the principle of least privilege. Over time, users can end up with access they no longer need, e.g. when they change roles. Regular audits minimize this risk.

Access Control

- The access control management functions should address the following:
- Who should have access to what resource? (Assignment of entitlements to users)
- Why should the user have access to the resource? (Assignment of entitlements based on the user's job functions and responsibilities)
- How should you access the resource? (What authentication method and strength are required prior to granting access to the resource)
- Who has access to what resource? (Auditing and reporting to verify entitlement assignments)

Access Control: SaaS

- In the SaaS delivery model, the CSP is responsible for managing all aspects of the network, server, and application infrastructure.
- In that model, since the application is delivered as a service to end users, usually via a web browser, network-based controls are becoming less relevant and are augmented or superseded by user access controls, e.g., authentication using a one-time password.
- Hence, customers should focus on user access controls (authentication, federation, privilege management, deprovisioning, etc.) to protect the information hosted by SaaS.

Access Control: PaaS

- In the PaaS delivery model, the CSP is responsible for managing access control to the network, servers, and application platform infrastructure.
- However, the customer is responsible for access control to the applications deployed on a PaaS platform.
- Access control to applications manifests as end user access management, which includes provisioning and authentication of users

Access Control: IaaS

- IaaS customers are entirely responsible for managing all aspects of access control to their resources in the cloud. Access to the virtual servers, virtual network, virtual storage, and applications hosted on an IaaS platform will have to be designed and managed by the customer. In an IaaS delivery model, access control management falls into one of the following two categories:
- **CSP infrastructure access control:** Access control management to the host, network, and management applications that are owned and managed by the CSP
- **Customer virtual infrastructure access control :**Access control management to your virtual server (virtual machines or VMs), virtual storage, virtual networks, and applications hosted on virtual servers

Vulnerability and Patch Management

- Vulnerability management and patch management are not products. They are processes – and the products are tools used to enable the process.
- Vulnerability management and patch management products are often lumped together and assumed to be part of the same product.
- While they have a compatible relationship, they are not the same. Vulnerability and patch management products are distinct products with different purposes and goals that are used to support these processes.

Patch management

A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bugfixes or bug fixes

- Patch management is the process that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing patches and determining which patches are the appropriate ones. Managing patches thus becomes easy and simple.
- Patching is a process to repair a vulnerability or a flaw that is identified after the release of an application or a software. Newly released patches can fix a bug or a security flaw, can help to enhance applications with new features, fix security vulnerability.
- Unpatched software can make the device a vulnerable target of exploits. Patching a software as and when the patch is released is critical to deny malware access.

Patch management

Patch management is the process of distributing and applying updates to software. These patches are often necessary to correct errors (also referred to as “vulnerabilities” or “bugs”) in the software.
When a vulnerability is found after the release of a piece of software, a patch can be used to fix it.

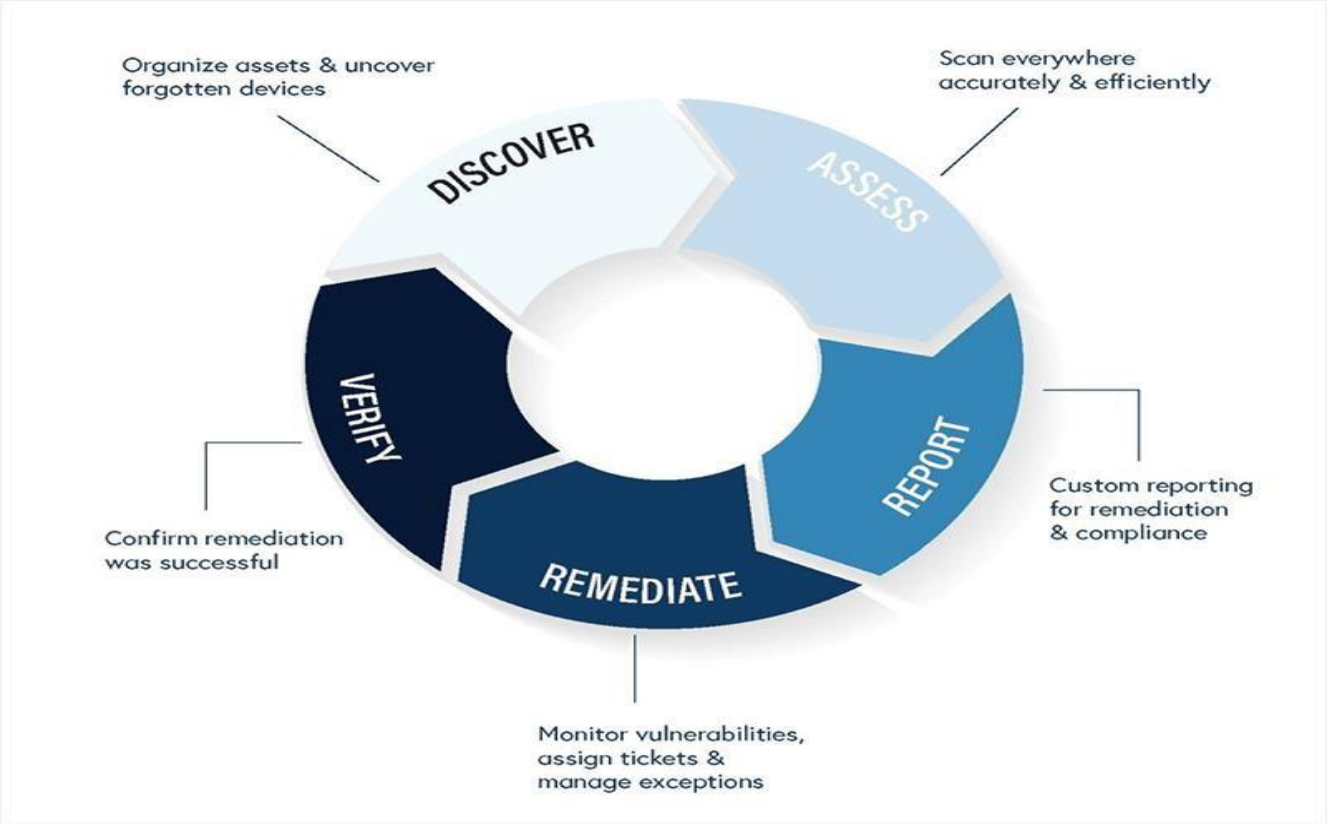
- Patch management is a process used to update the software, operating systems and applications on an asset in a logical manner. The purpose of a patch management system is to highlight, classify and prioritize any missing patches on an asset.
- For the purpose of specificity, patches are updates from the vendor; they can contain anything from security fixes to new features. The vendor sets their policy for what can be in a patch, and they should document all changes and additions in a readme file.
- Not all patches contain security fixes, and not all patches will fix the security issues listed. This is why just having a patch management tool will not make you secure.

Vulnerability management

- Vulnerability management is a continual process, not only to detect risks on your network but to create a plan to prevent those vulnerabilities from causing future damage. A good vulnerability management system combines technology and a team of security experts to proactively detect and act upon security risk.
- A vulnerability is a weakness in your system that leaves you open to attacks. It can be caused by a flaw in hardware, software, or in the implementation of either one, which leaves your system open to potential risk.

- Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimizing their "attack surface."
- Security vulnerabilities, in turn, refer to technological weaknesses that allow attackers to compromise a product and the information it holds. This process needs to be performed continuously in order to keep up with new systems being added to networks, changes that are made to systems, and the discovery of new vulnerabilities over time.

The Stages of Vulnerability Management



Stage 1: Discover

- The initial stage of the vulnerability management process is all about preparing for the vulnerability scans and tests and making sure your bases are covered. This means organizing all your company assets and uncovering any forgotten devices.
- Compile all of the assets you need to test, determine their importance and who can access them (whether just administrators or your whole team). Work to maintain a continuously updated inventory so you can provide a map of the vulnerabilities throughout your network.

Stage 2: Assess

- Once you've compiled all of your devices and inventory, the next stage involves the tests to make sure every device is scanned, both accurately and efficiently.
- It's not just about knowing the vulnerabilities, but gaining timely, efficient access to the information. If you aren't receiving the data from a credible source, you might be wasting your time on false positives.
- Once you're aware of the potential risks on your devices, the next step is to prioritize those vulnerabilities. With the large number of vulnerabilities disclosed every day, it can seem impossible to manage them all, making it all the more significant to prioritize the biggest risks and resolve those first.

Stage 3: Report

- All this data is then compiled into a custom report, giving details on the vulnerabilities and how to prioritize them. These reports will include recommendations as well as the best plan to triage the risks quickly and seamlessly.
- It should include the actions to take and give step-by-step instructions to fix the problem. The purpose of the report is to significantly decrease the security risk that these vulnerabilities present in a practical way.

Stage 4: Remediate

- In the stage of remediation, the goal is to monitor vulnerabilities, assign tickets, and manage exceptions.
- As vulnerabilities are detected and reported, the next step in the vulnerability management process is to correct, monitor, or remove those vulnerabilities. This can be accomplished through the necessary updates and patches or workarounds to avoid the threat.
- This stage is then repeated as new vulnerabilities are discovered. The network and its devices need to be continuously monitored to detect and find new vulnerabilities that might lead to potential, future threats.

Stage 5: Verify

- The final step is to verify the success of the entire process. This step not only helps you see that the mitigation was successful but also maintains transparency and accountability across the company. The whole goal is to reduce the attack surface of a company, findings ways to minimize the threat of an attack by decreasing vulnerabilities.

- With an ever-growing number of vulnerabilities, it's challenging to know how to detect them on your own, let alone prioritize and remediate them. Equip your team to fight back by investing in a vulnerability management tool and team to minimize the risk and potential threats.