

WEEK 2. Introduction to Cloud Computing

Objective of the study

At the end of this unit, you should be able to:

1. Define Cloud computing
2. Understand the basic concepts of the cloud
3. Know the deployments models and types

Introduction

Cloud Computing provides us a means by which we can access the applications as utilities, over the Internet. It allows us to create, configure, and customize applications online. What is Cloud? The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud.

What is Cloud Computing? Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application.

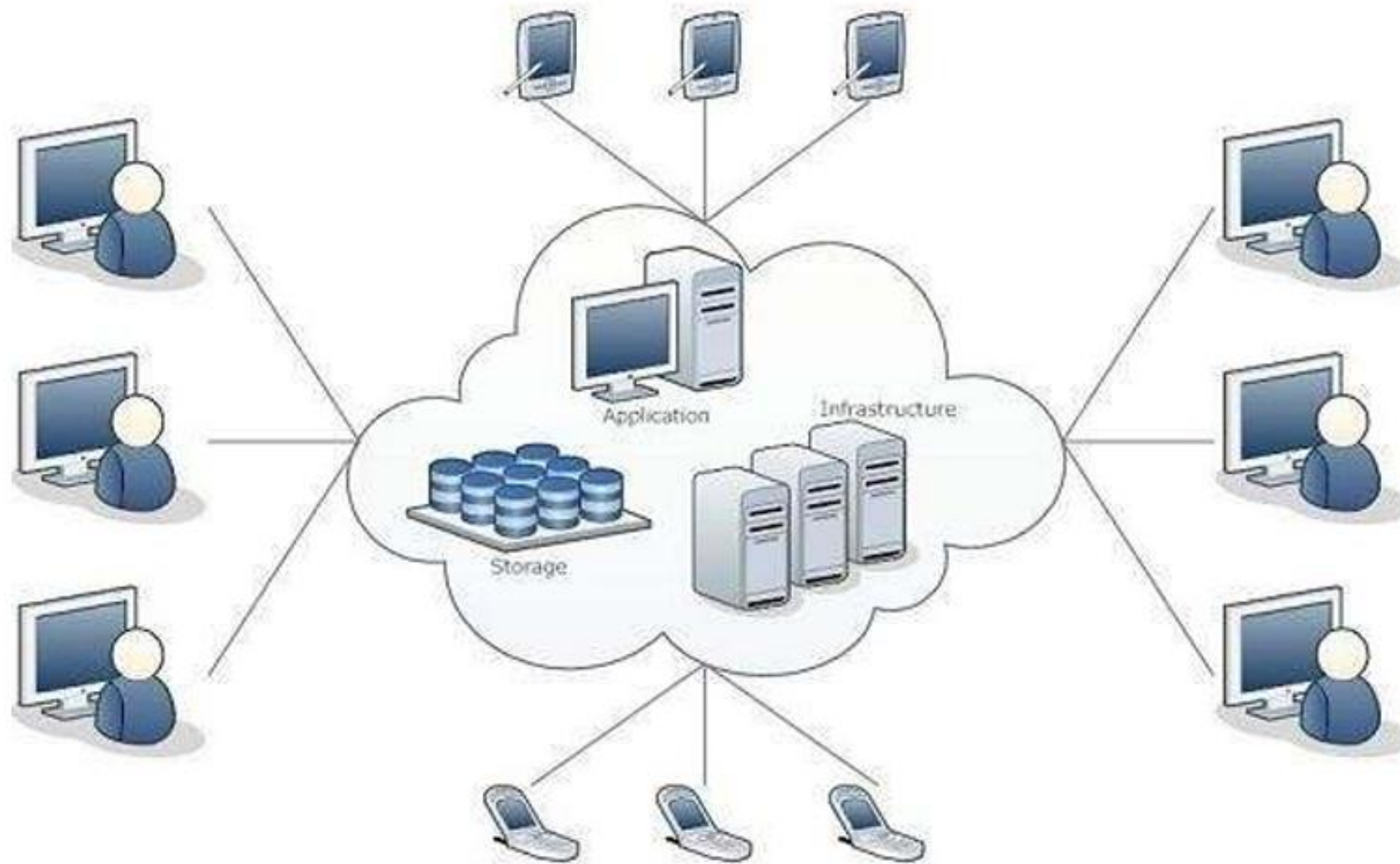


Figure 1 showing the cloud diagram

Basic Concepts

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

- Deployment Models
- Service Models

Deployment models

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access:

- Public,
- Private,
- Hybrid
- and Community.

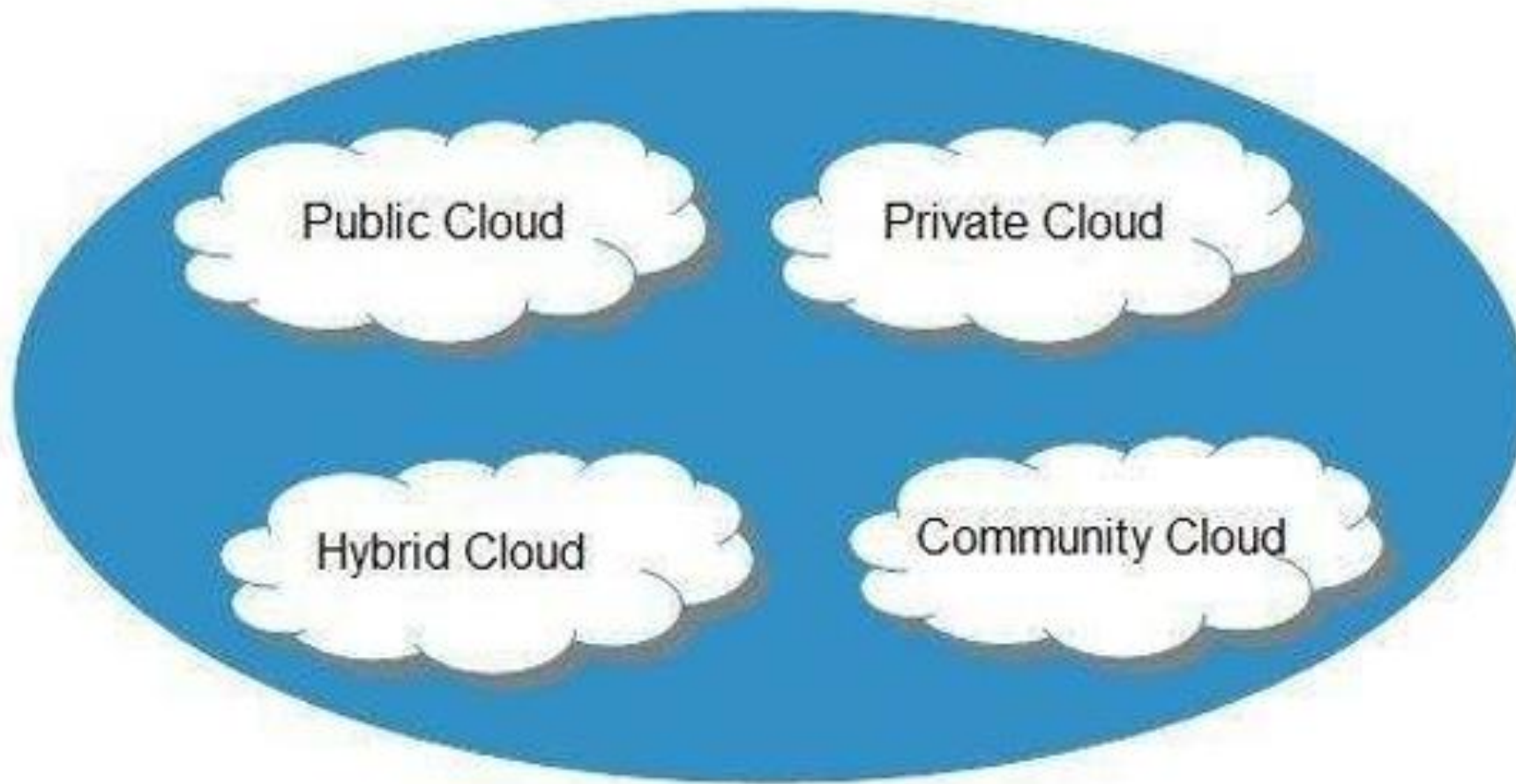


Figure 2. Types of deployment models

Public Cloud

The Public Cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness, e.g., e-mail.

Private Cloud

The Private Cloud allows systems and services to be accessible within an organization. It offers increased security because of its private nature.

Community Cloud

The Community Cloud allows systems and services to be accessible by group of organizations.

Hybrid Cloud

The Hybrid Cloud is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

Assignment

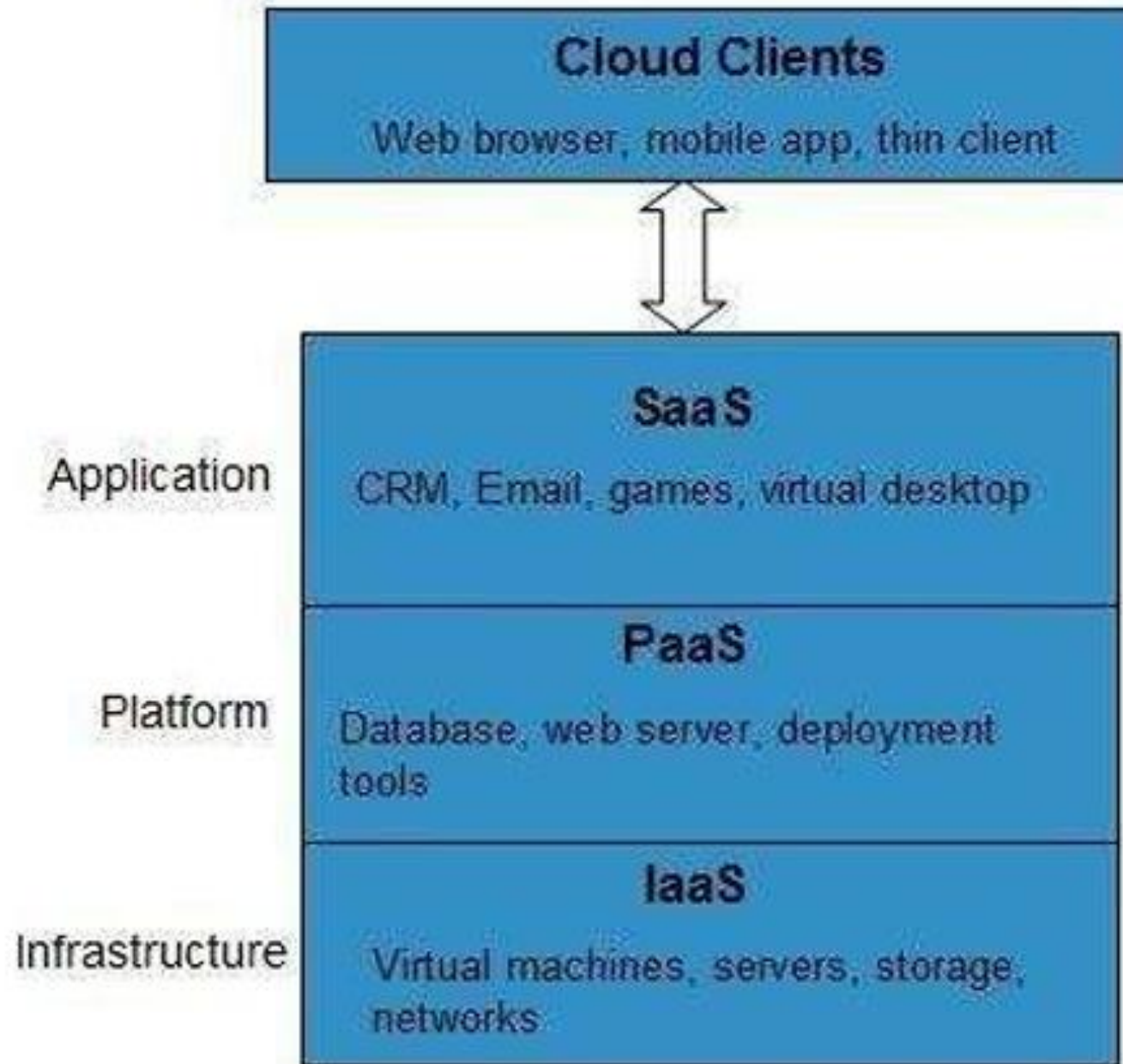
Write short notes on the deployment models stating where they can be used. Avoid copying and pasting. Submit in the next class.

Service Models

Service Models are the reference models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

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

There are many other service models all of which can take the form like XaaS, i.e., Anything as a Service. This can be Network as a Service, Business as a Service, Identity as a Service, Database as a Service or Strategy as a Service. The Infrastructure as a Service (IaaS) is the most basic level of service. Each of the service models make use of the underlying service model, i.e., each inherits the security and management mechanism from the underlying model, as shown in the following diagram:



Infrastructure as Service (IAAS)

IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

Platform as a service (PAAS)

PAAS provides the runtime environment for applications, development & deployment tools, etc.

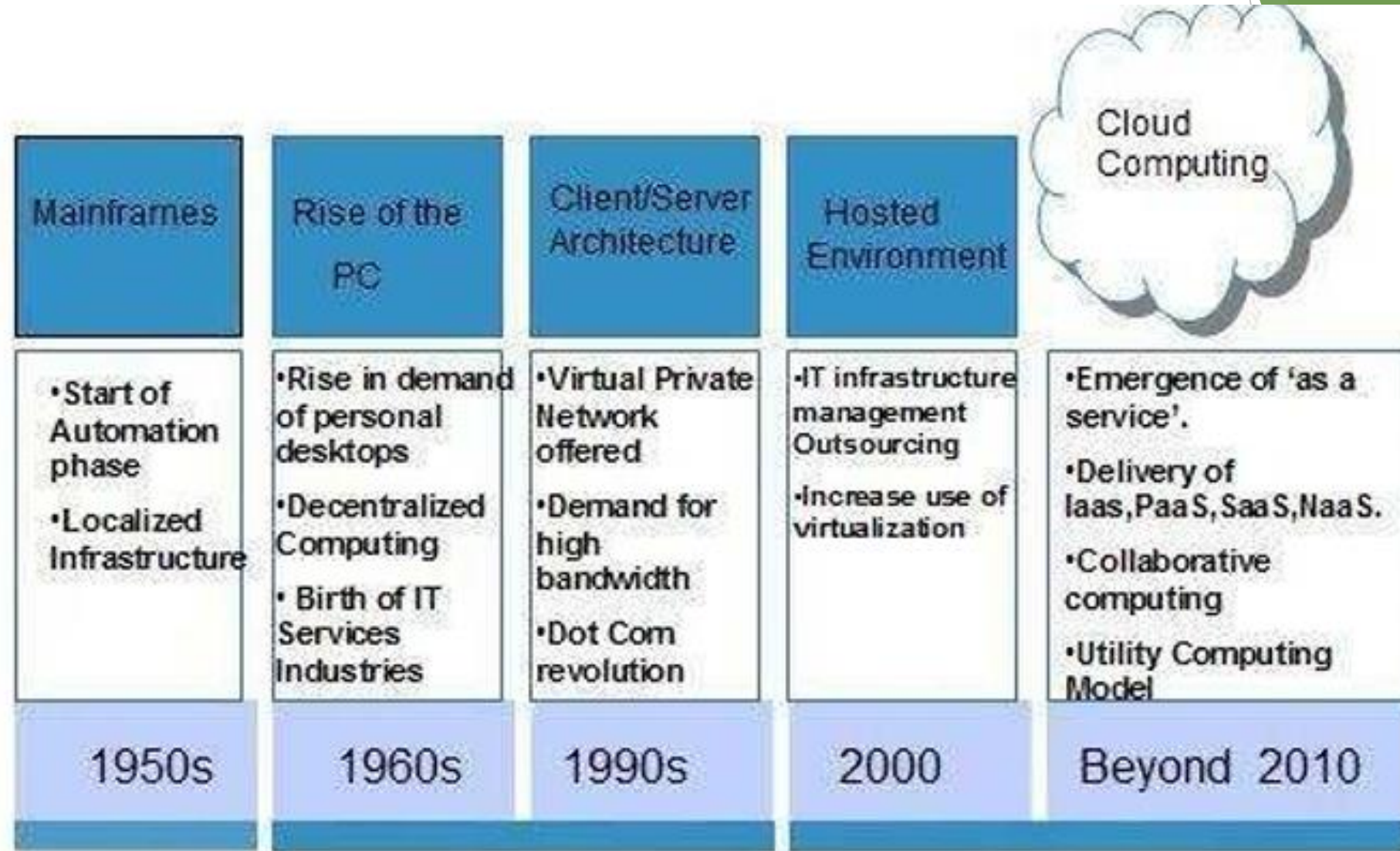
Software as a service (SAAS)

SAAS model allows to use software applications as a service to end users.

History of Cloud Computing

History

The concept of Cloud Computing came into existence in 1950 with implementation of mainframe computers, accessible via thin/static clients. Since then, cloud computing has been evolved from static clients to dynamic ones from software to services. The following diagram explains the evolution of cloud computing:



Benefits of the Cloud

Computing has numerous advantages. Some of them are listed below:

- One can access applications as utilities, over the Internet.
- Manipulate and configure the application online at any time.
- It does not require to install a specific piece of software to access or manipulate cloud application.
- Cloud Computing offers online development and deployment tools, programming runtime environment through Platform as a Service model.
- Cloud resources are available over the network in a manner that provides platform independent access to any type of clients.
- Cloud Computing offers on-demand self-service. The resources can be used without interaction with cloud service provider.
- Cloud Computing is highly cost effective because it operates at higher efficiencies with greater utilization. It just requires an Internet connection.
- Cloud Computing offers load balancing that makes it more reliable.

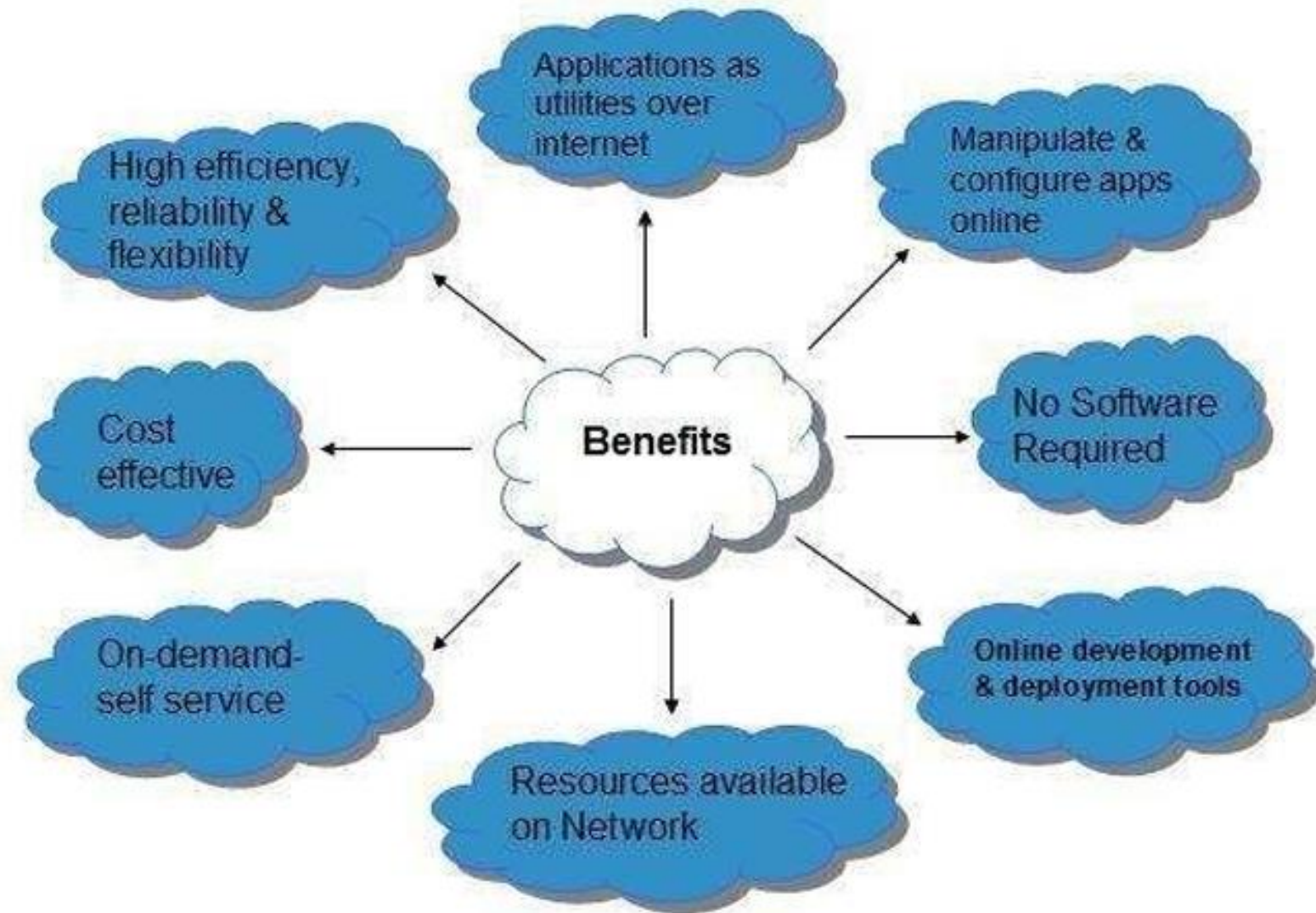


Figure 3. Benefits of the cloud

Risk of the cloud

- ▶ Risks Although Cloud Computing is a great innovation in the world of computing, there also exist downsides of cloud computing. Some of them are discussed below:

- ▶ **Security & privacy**

It is the biggest concern about cloud computing. Since data management and infrastructure management in cloud is provided by third-party, it is always a risk to handover the sensitive information to such providers. Although the cloud computing vendors ensure more secure password protected accounts, any sign of security breach would result in loss of clients and businesses.

Lock-IN. It is very difficult for the customers to switch from one Cloud Service Provider (CSP) to another. It results in dependency on a particular CSP for service.

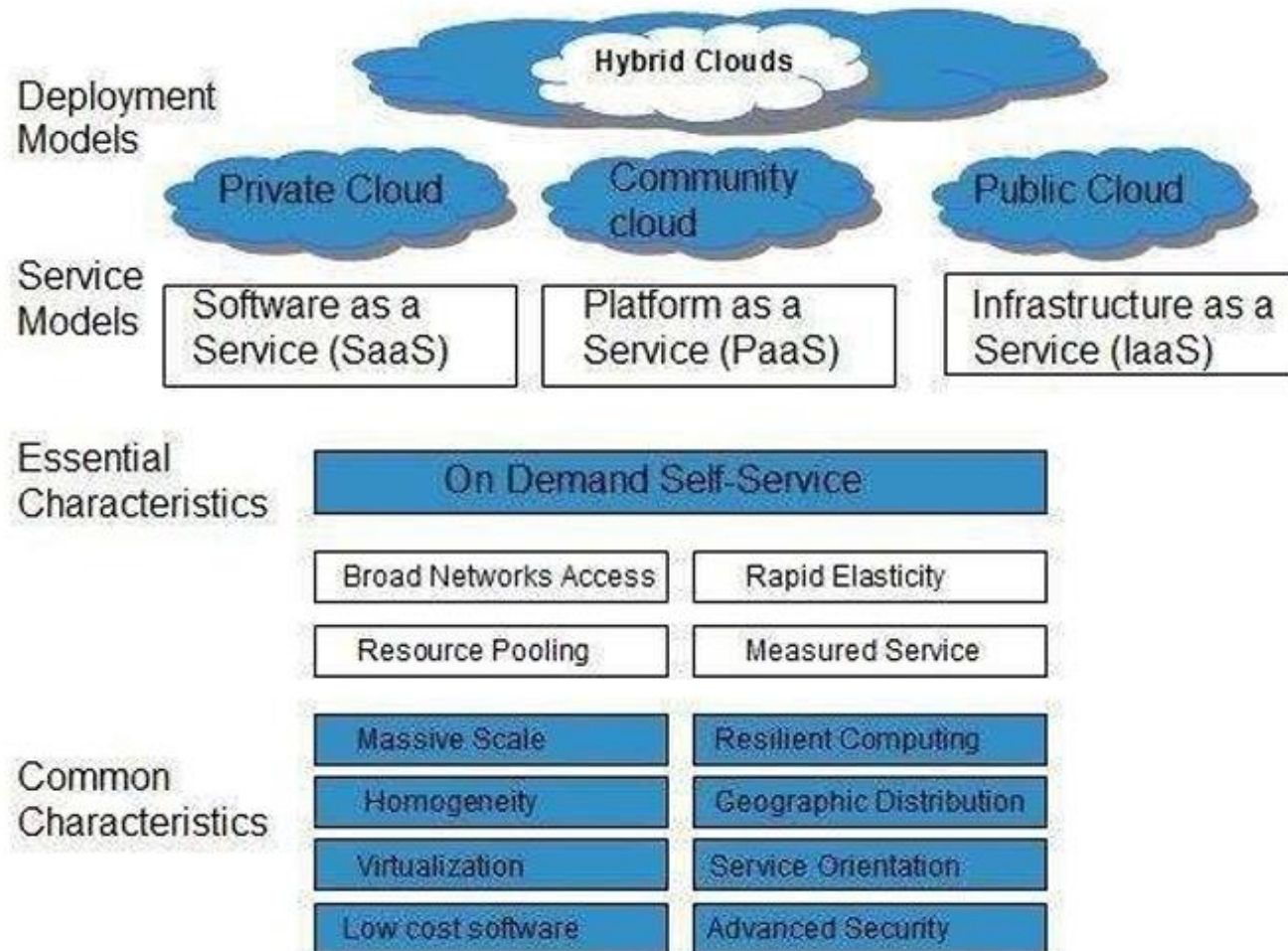
Isolation failure. This risk involves the failure of isolation mechanism that separates storage, memory, routing between the different tenants.

Management interface compromise. In case of public cloud provider, the customer management interfaces are accessible through the Internet.

Insecure or incomplete data deletion. It is possible that the data requested for deletion may not get deleted. It happens either because extra copies of data are stored but are not available or disk destroyed also stores data from other tenants.

Characteristics

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



On demand self-service

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

Broad network access

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

Resource pooling

Cloud Computing allows multiple tenants to share a pool of resources. One can share single physical instance of hardware, database and basic infrastructure.

Rapid elasticity

It is very easy to scale up or down the resources at any time. Resources used by the customers or currently assigned to customers are automatically monitored and resources.

Measured service

Service Models & Deployment Models will be discussed by next class.

Objectives of the study:

At the end of this lesson, you must be able to:

1. List the cloud computing migration planning stages
2. Reflection of the fundamentals of Azure

Quiz

1. List and explain the deployment and service models

CLOUD COMPUTING -PLANNING

Before deploying applications to cloud, it is necessary to consider your business requirements.

The Following are the issues one must have to think about:

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

Reflection on Azure Fundamentals

.

100

Chapter 1:- Opening Azure Devops account and creating project.

Chapter 2:- Devops Fundamentals and EIGHT structure life cycle of Devops.

Chapter 3:- Accessing Azure devops project from Azure portal.

Chapter 4:- Understanding Organization, Project structure.

Chapter 5:- Understanding Private and Public project.

dev.azure.com/devopsquestpond/test123

HMS How To Isolate Tren... Seasonal-Trend dec... IT – Software has b... Forecasting throug... In this notebook I ill... 3 ways to solve the... Blog: SIL calcul

Azure DevOps devopsquestpond / test123 / Overview / Summary

Search

test123

Private

Overview

Boards

Work items

Boards

Backlogs

Sprints

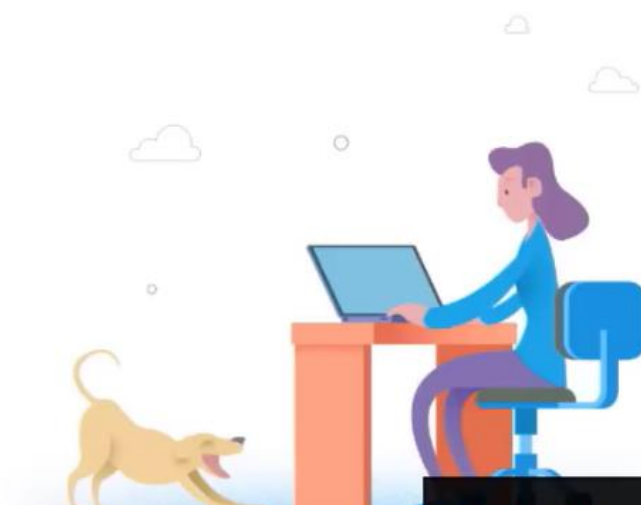
Queries

Delivery Plans

Repos

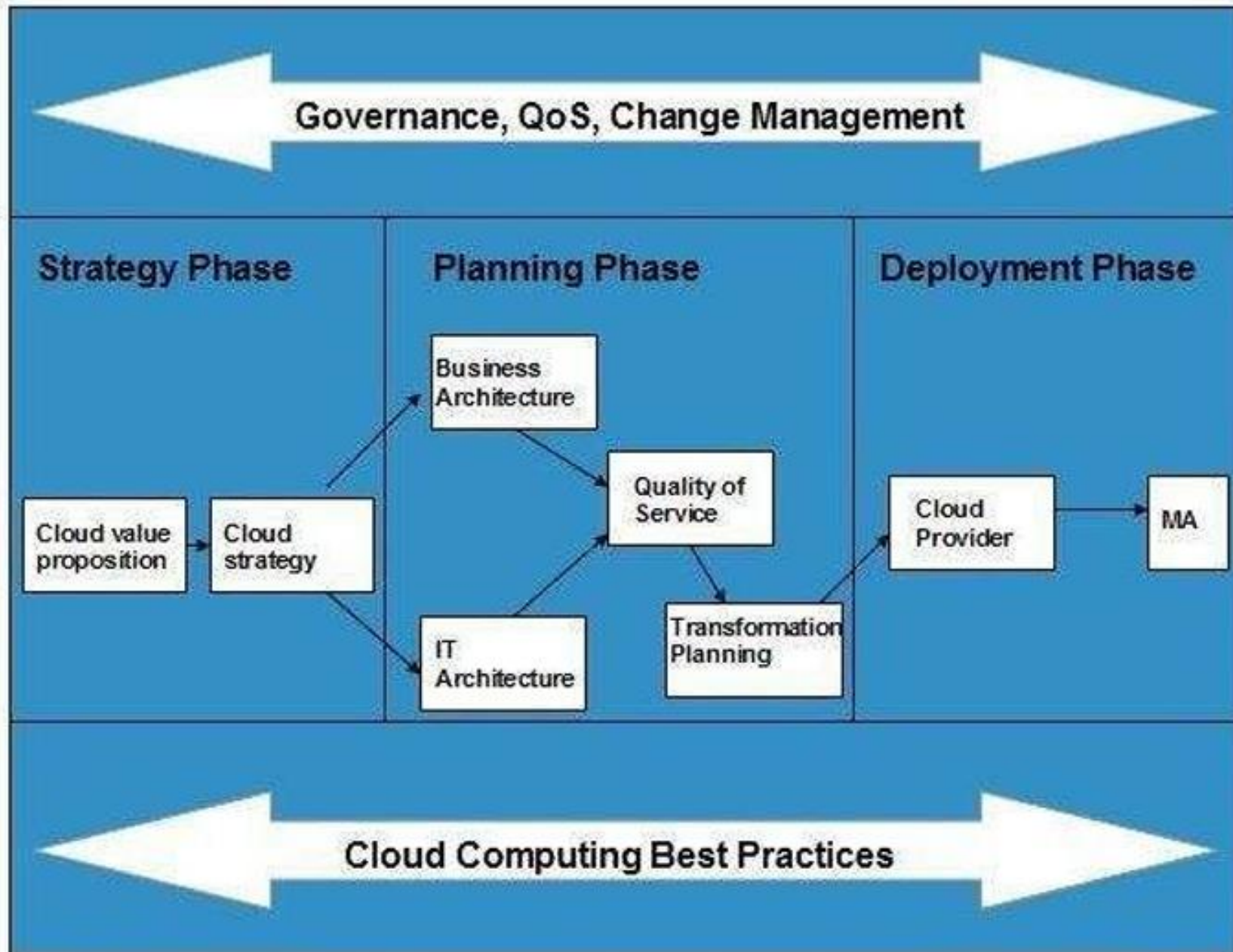
Pipelines

test123



www.questpond.com

Figure 3.1 Planning Stages



Strategy Planning Phase

In this, we analyze the strategy problems that customer might face. There are two steps to perform this analysis:

- Cloud Computing Value Proposition
- Cloud Computing Strategy Planning

Cloud computing value proposition

In this, we analyze the factors influencing the customers when applying cloud computing mode and target the key problems they wish to solve.

These key factors are:

- IT management simplification
- Operation and maintenance cost reduction
- Business mode innovation
- Low cost outsourcing hosting
- High service quality outsourcing hosting.

Cloud computing strategy planning

The strategy establishment is based on the analysis result of the above step. In this step, a strategy document is prepared according to the conditions a customer might face when applying cloud computing mode.

This step performs analysis of problems and risks in the cloud application to ensure the customers that the cloud computing successfully meet their business goals. This phase involves the following planning steps:

- Business architecture development
- It architecture development
- Requirements on quality of service development
- Transformation plan development

► **Business architecture development** In this step, we recognize the risks that might be caused by cloud computing application from a business perspective.

► **IT architecture development**

In this step, we identify the applications that support the business processes and the technologies required to support enterprise applications and data systems.

► **Requirements on quality of service development**

Quality of service refers to the non-functional requirements such as reliability, security, disaster recovery, etc. The success of applying cloud computing mode depends on these non-functional factors.

► **Transformation plan development**

In this step, we formulate all kinds of plans that are required to

Cloud computing deployment phase

This phase focuses on both of the above two phases. It involves the following two steps:

- Cloud computing provider
- Maintenance and technical service

► Cloud computing provider

This step includes selecting a cloud provider on basis of service level agreement (SLA), which defines the level of service the provider will meet.

► Maintenance and technical service

Maintenance and technical services are provided by the cloud provider. They must have to ensure the quality of services.

Week 4

CLOUD COMPUTING-TECHNOLOGIES/Architecture

At the end of this topic, you should be able to;

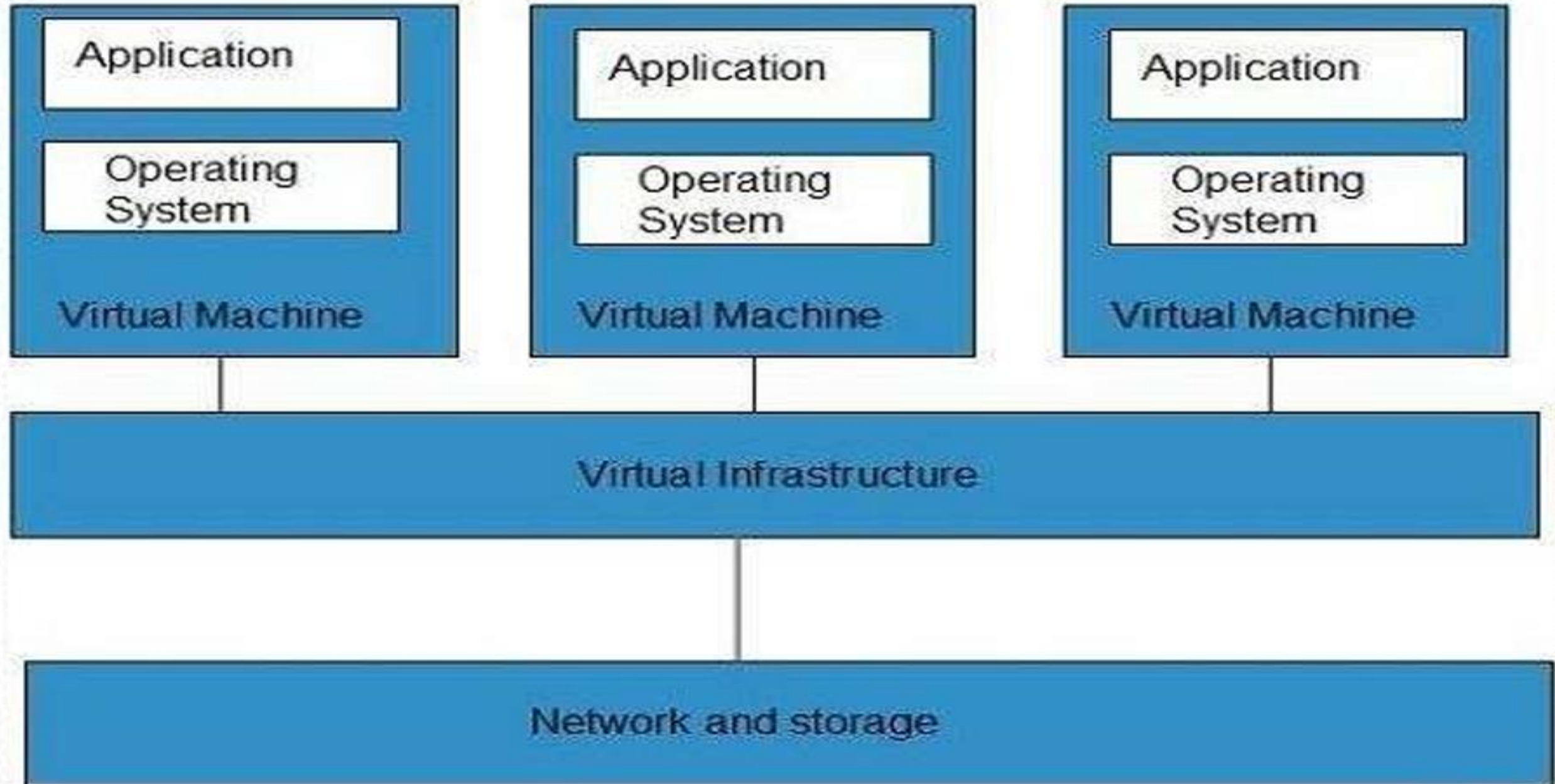
- ▶ explain the virtualization technique
- ▶ list few stages of activities in the Service-oriented architecture (SOA)
- ▶ explain the concept of Grid computing
- ▶ explain the utility concept as related to the cloud
- ▶ explain the concept of cloud computing architecture.

Virtualization

Virtualization is a technique, which allows to share single physical instance of an application or resource among multiple organizations or tenants (customers). It does so by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded.

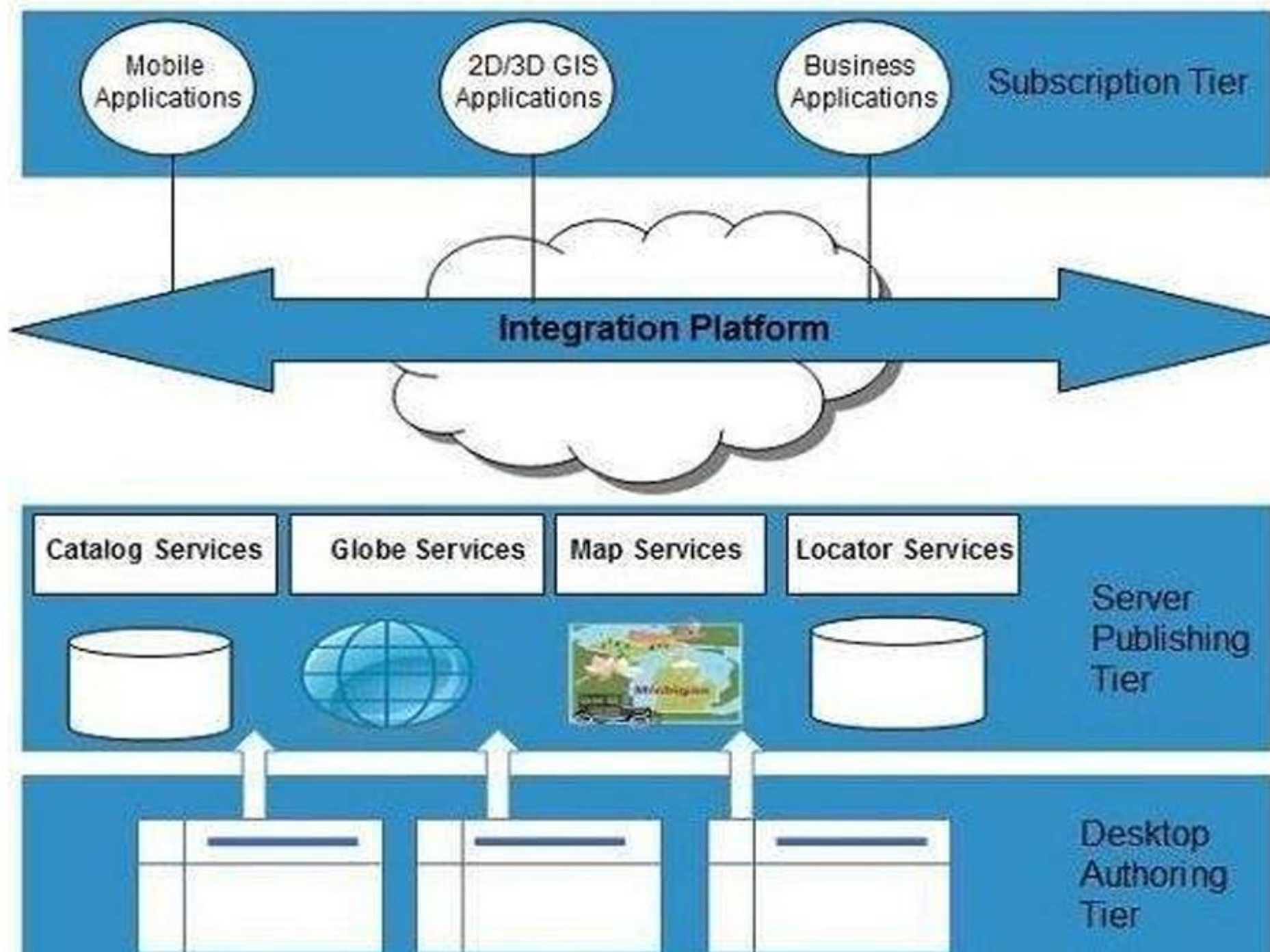


Virtualized Cloud Model



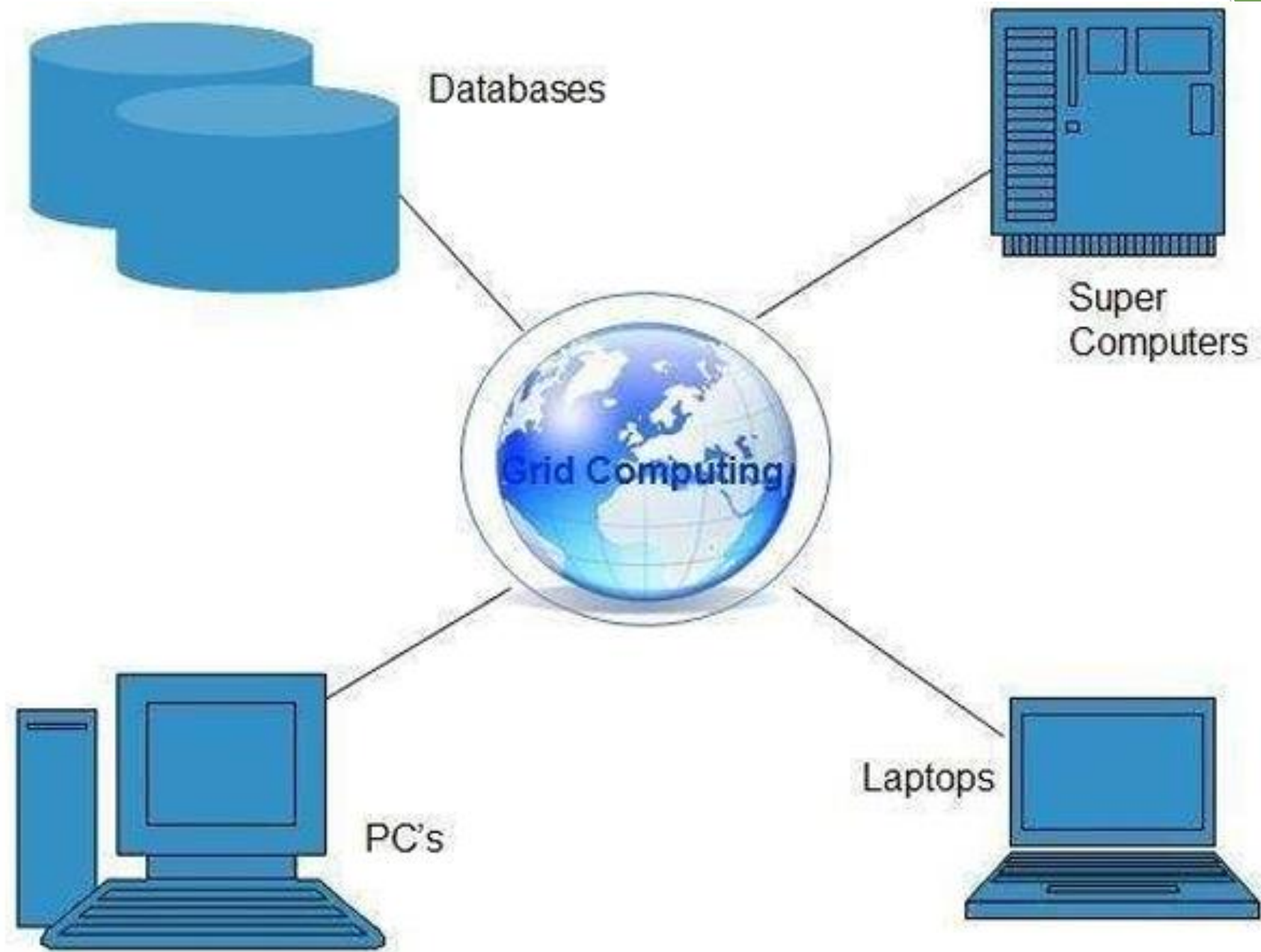
Service-oriented architecture (SOA)

Service-oriented architecture helps to use applications as a service for other applications regardless the type of vendor, product or technology. Therefore, it is possible to exchange of data between applications of different vendors without additional programming or making changes to services.



Grid computing

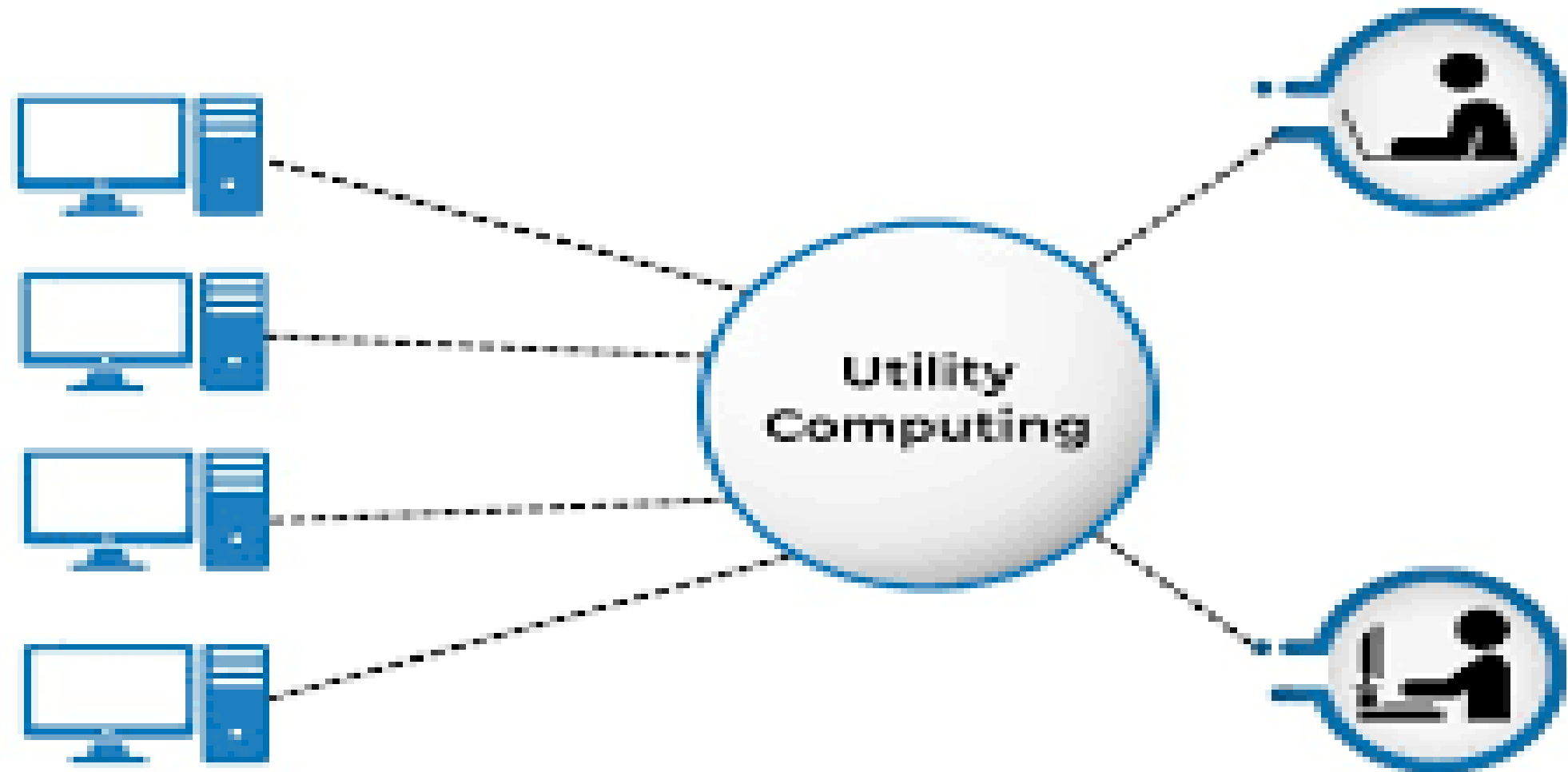
- ▶ Grid computing refers to distributed computing in which a group of computers from multiple locations are connected with each other to achieve common objective. These computer resources are heterogeneous and geographically dispersed. Grid computing breaks complex task into smaller pieces. These smaller pieces are distributed to cpus that reside within the grid.



Utility computing

Utility computing is based on pay per use model. It offers computational resources on demand as a metered service. Cloud computing, grid computing, and managed it services are based on the concept of utility computing.

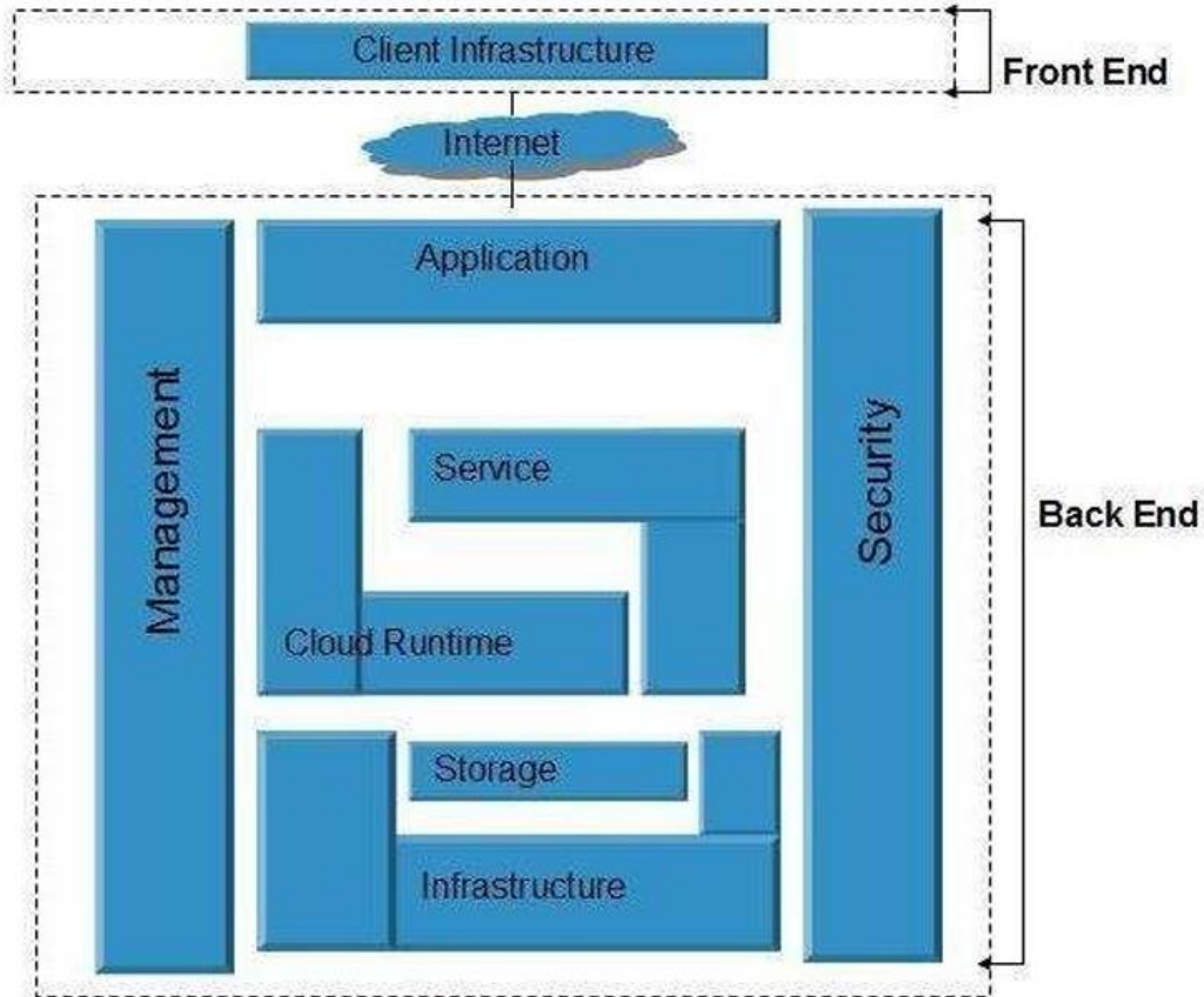
Utility Computing



CLOUD COMPUTING-ARCHITECTURE

The cloud computing architecture comprises many cloud components, each of them are loosely coupled. We can broadly divide the cloud architecture into two parts:

- Front end
 - Back end
- Each of the ends are connected through a network, usually via internet. The following diagram shows the graphical view of cloud computing architecture:



► Front end

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, e.g., web browser.

► Back end

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.

Important points

- 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, helps the connected devices to communicate with each other.

Week 5 CLOUD COMPUTING INFRASTRUCTURE & MODELS

Objectives:

At the end of this unit, you should be able to:

- List and explain the six cloud infrastructure components
- Explain the cloud models with respect to the use
- Discuss about the Azure cloud fundamental and AWS

CLOUD COMPUTING INFRASTRUCTURE

► Cloud infrastructure components

Cloud infrastructure consists of servers, storage, network, management software, deployment software and platform virtualization.

1. **Hypervisor** is a firmware or low-level program that acts as a virtual machine manager. It allows to share the single physical instance of cloud resources between several tenants.

Management Software

Deployment Software

Hypervisor

Network

Server

Storage

Cloud Infrastructural Components

2. Management software

Management software helps to maintain and configure the infrastructure.

3. Deployment software

Deployment software helps to deploy and integrate the application on the cloud.

4. Network

Network is the key component of cloud infrastructure. It allows to connect cloud services over the internet. It is also possible to deliver network as a utility over the internet, i.e., the consumer can customize the network route and protocol.

5. Server

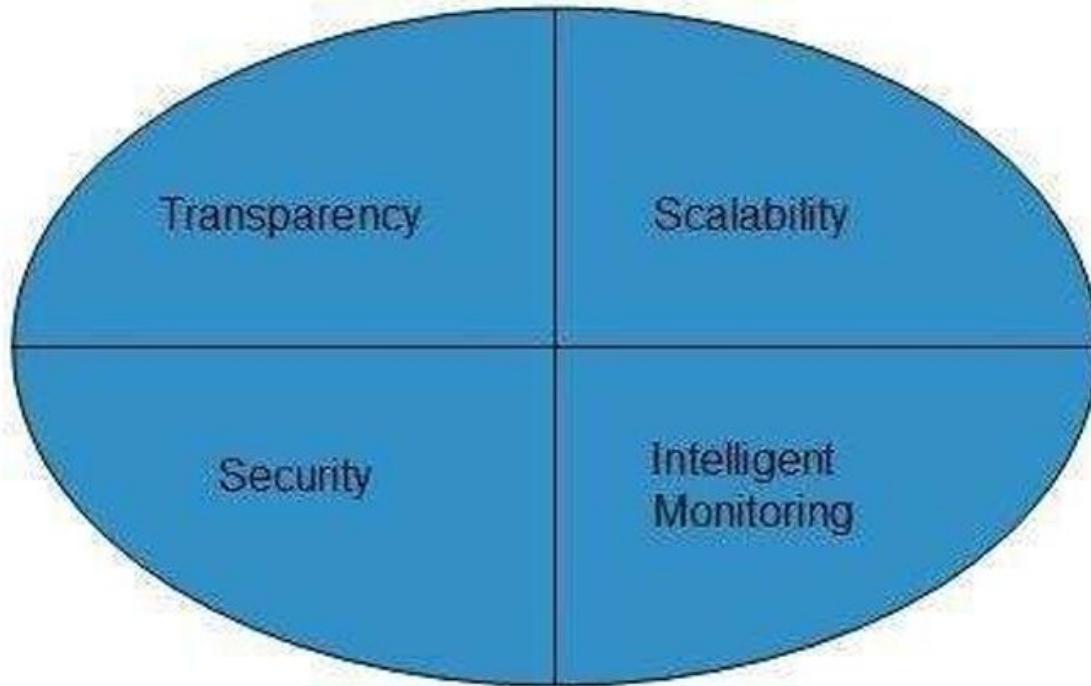
Server helps to compute the resource sharing and offer other services such as resource allocation and deallocation, monitoring resources, security, etc.

6. Storage

Cloud uses distributed file system for storage purpose. If one of the storage resource fails, then it can be extracted from another one which makes cloud computing more reliable.

► Infrastructural constraints

Fundamental constraints that cloud infrastructure should implement are shown in the following diagram:



► Transparency

Since virtualization is the key to share resources in cloud environment. But it is not possible to satisfy the demand with single resource or server. Therefore, there must be transparency in resources, load balancing and application, so that we can scale them on demand.

► Scalability

Scaling up an application delivery solution is not that easy as scaling up an application because it involves configuration overhead or even re-architecting the network. So, application delivery solution is need to be scalable which will require the virtual infrastructure such that resource can be provisioned and de-provisioned easily.

► Intelligent monitoring

To achieve transparency and scalability, application solution delivery will need to be capable of intelligent monitoring.

► Security

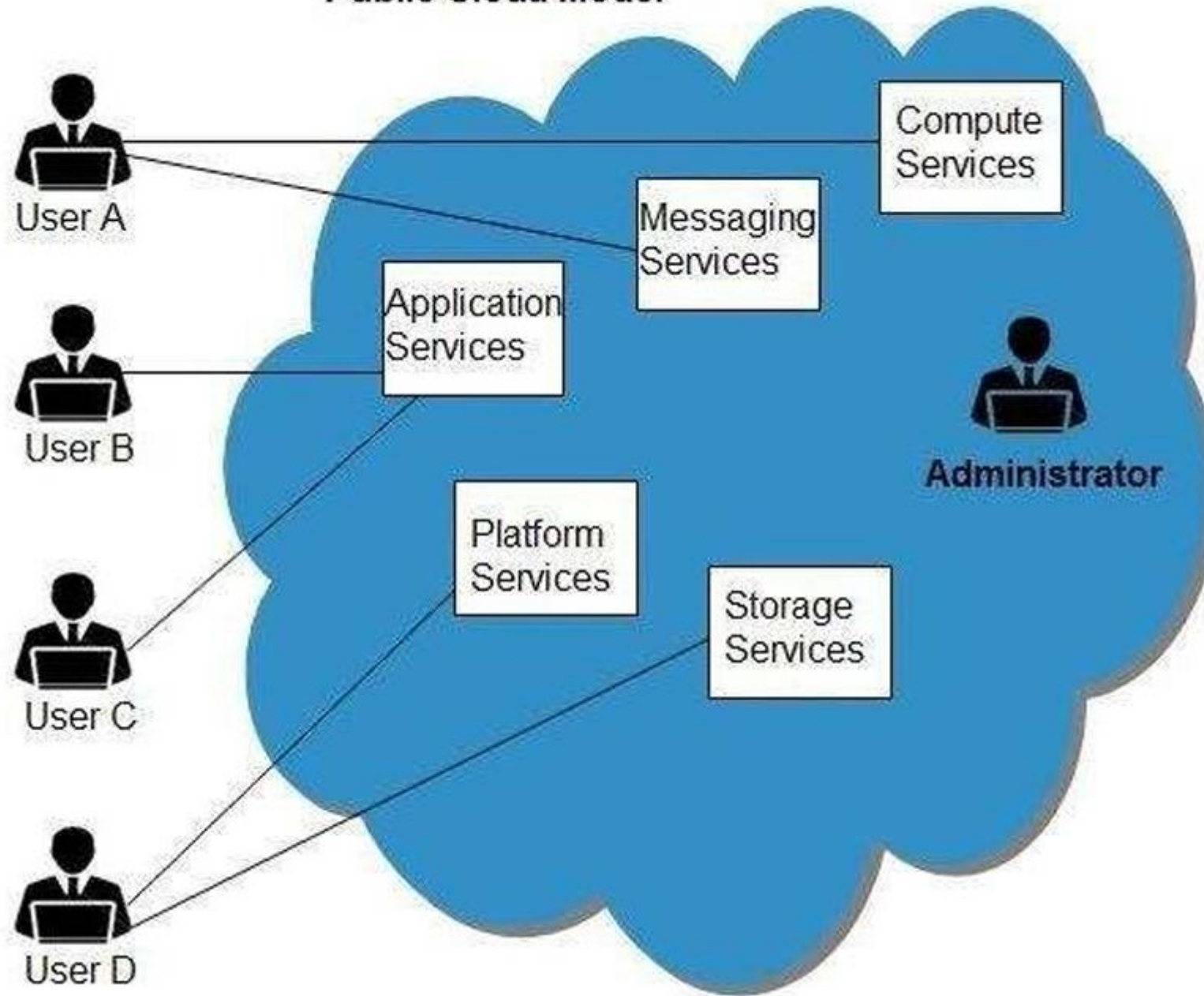
The mega data center in the cloud should be securely architected. Also the control node, a entry point in mega data center also needs to be secure.

CLOUD MODELS

► Public cloud

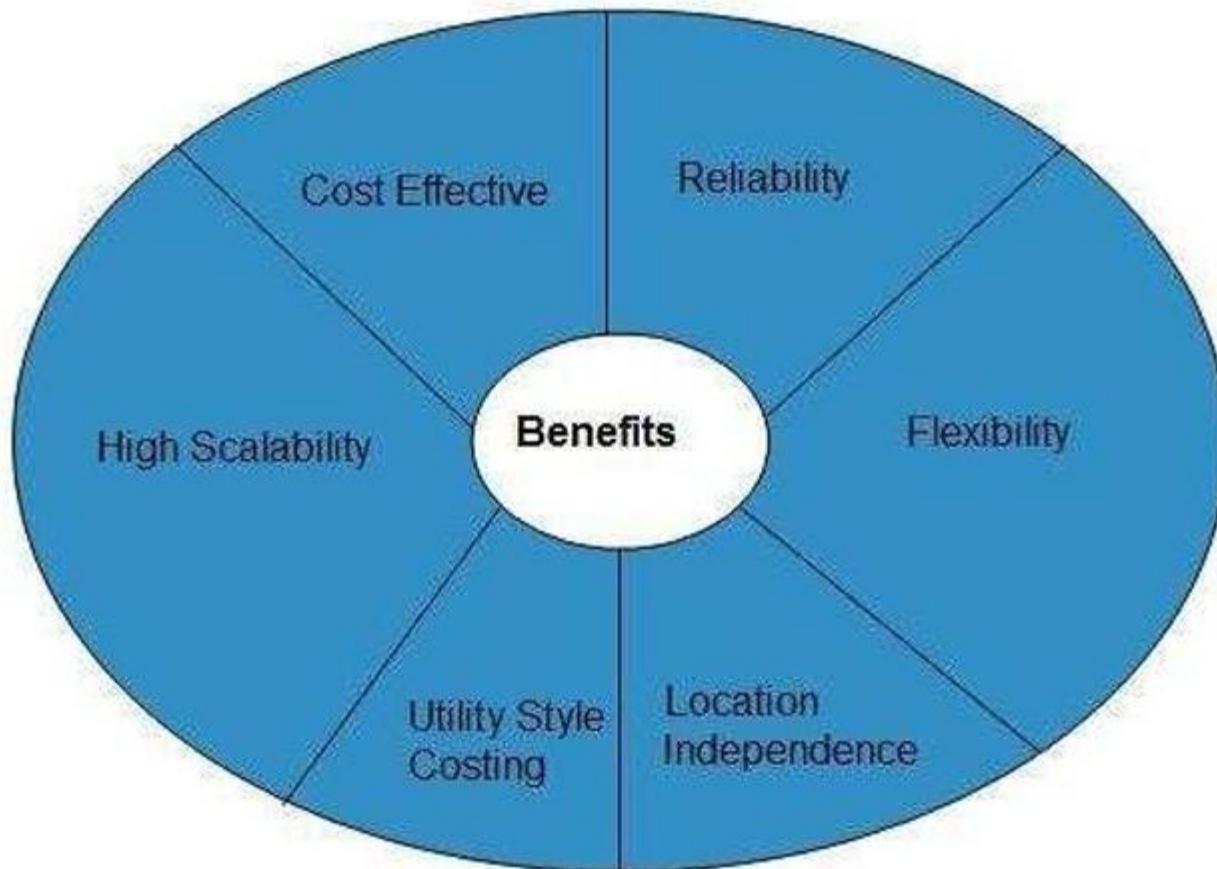
The public cloud allows systems and services to be easily accessible to general public, e.g., google, amazon, Microsoft offers cloud services via internet

Public Cloud Model



► Benefits

There are many benefits of deploying cloud as public cloud model. The following diagram shows some of those benefits:



► **Cost effective**

Since public cloud share same resources with large number of consumer, it has low cost.

► **Reliability**

Since public cloud employs large number of resources from different locations, if any of the resource fail, public cloud can employ another one.

► **Flexibility**

It is also very easy to integrate public cloud with private cloud, hence gives consumers a flexible approach.

► **Location independence**

Since, public cloud services are delivered through internet, therefore ensures location independence.

► **Utility style costing**

Public cloud is also based on pay-per-use model and resources are accessible whenever consumer needs it.

► **High scalability**

Cloud resources are made available on demand from a pool of resources, i.e., they can be scaled up or down according the requirement.

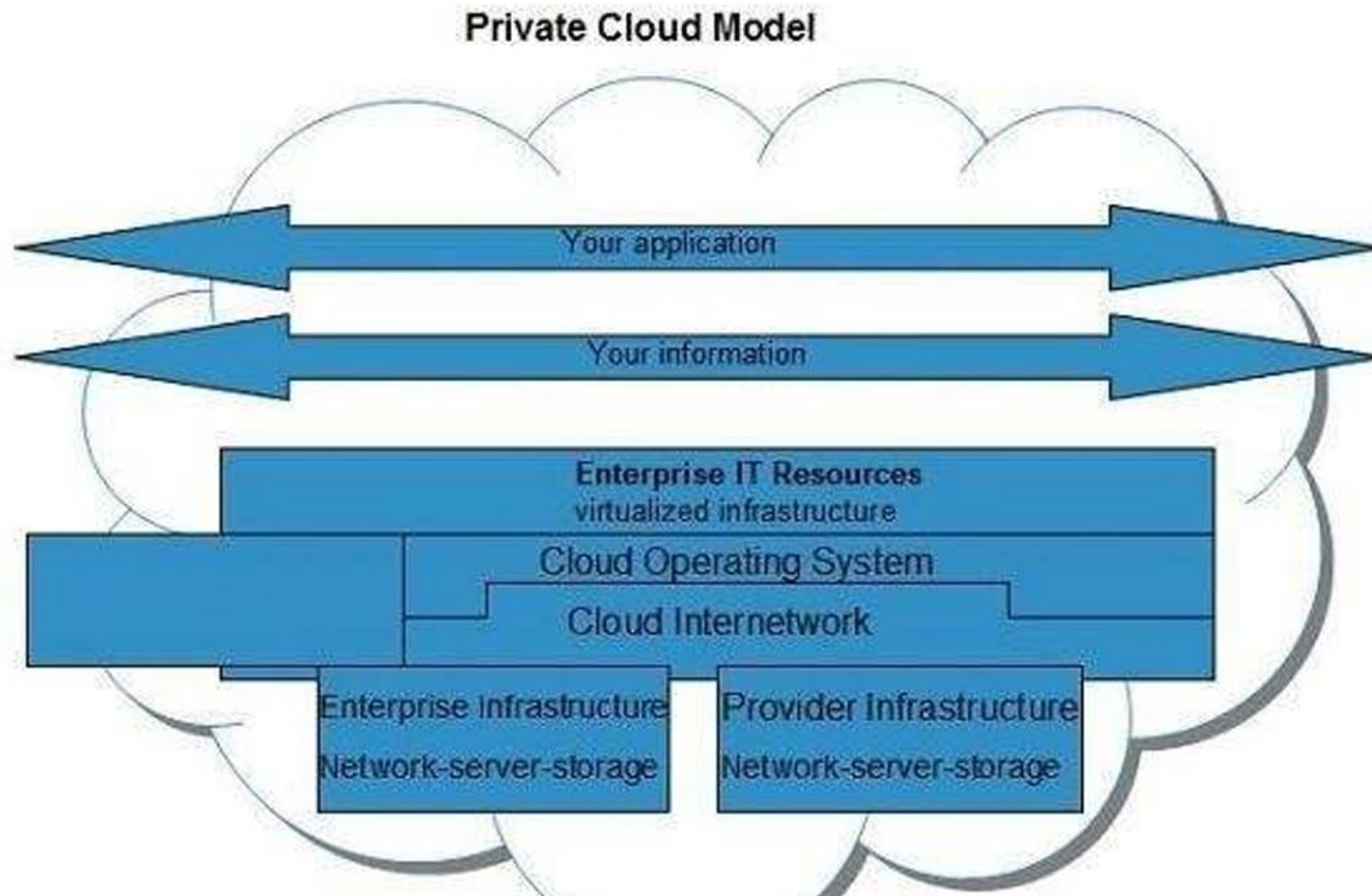
DISADVANTAGES

Here are the disadvantages of public cloud model:

- ▶ Low security In public cloud model, data is hosted off-site and resources are shared publicly, therefore does not ensure higher level of security.
- ▶ Less customizable It is comparatively less customizable than private cloud

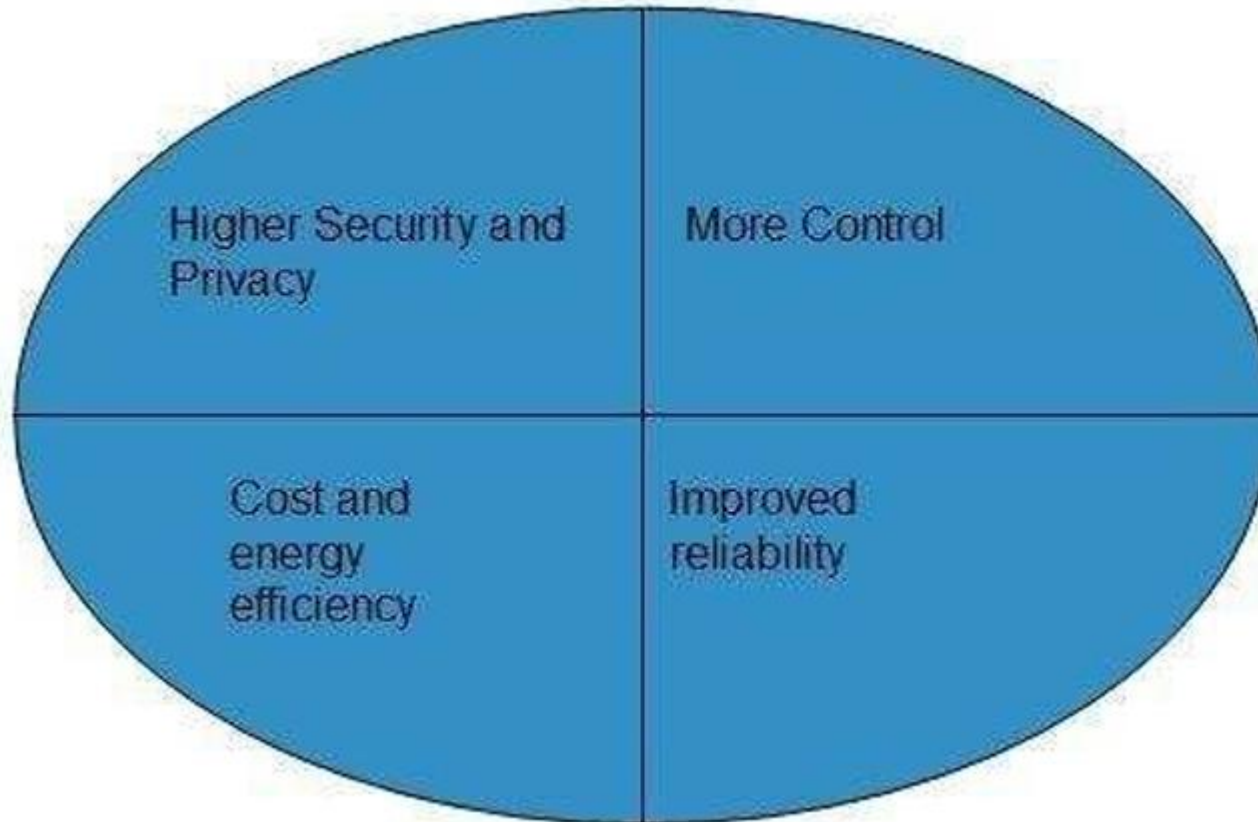
PRIVATE CLOUD


The private cloud allows systems and services to be accessible within an organization. The private cloud is operated only within a single organization. However, it may be managed internally or by third-party.



BENEFITS

There are many benefits of deploying cloud as private cloud model. The following diagram shows some of those benefits:



- 
- The background of the slide features an abstract design with overlapping green triangles and polygons of various shades, ranging from light lime green to dark forest green. The shapes are layered, creating a sense of depth and movement. The overall aesthetic is modern and tech-oriented.
- ▶ **Higher security and privacy:** Private cloud operations are not available to general public and resources are shared from distinct pool of resources, therefore, ensures high security and privacy.
 - ▶ **More control** Private clouds have more control on its resources and hardware than public cloud because it is accessed only within an organization.
 - ▶ **Cost and energy efficiency** Private cloud resources are not as cost effective as public clouds but they offer more efficiency than public cloud.

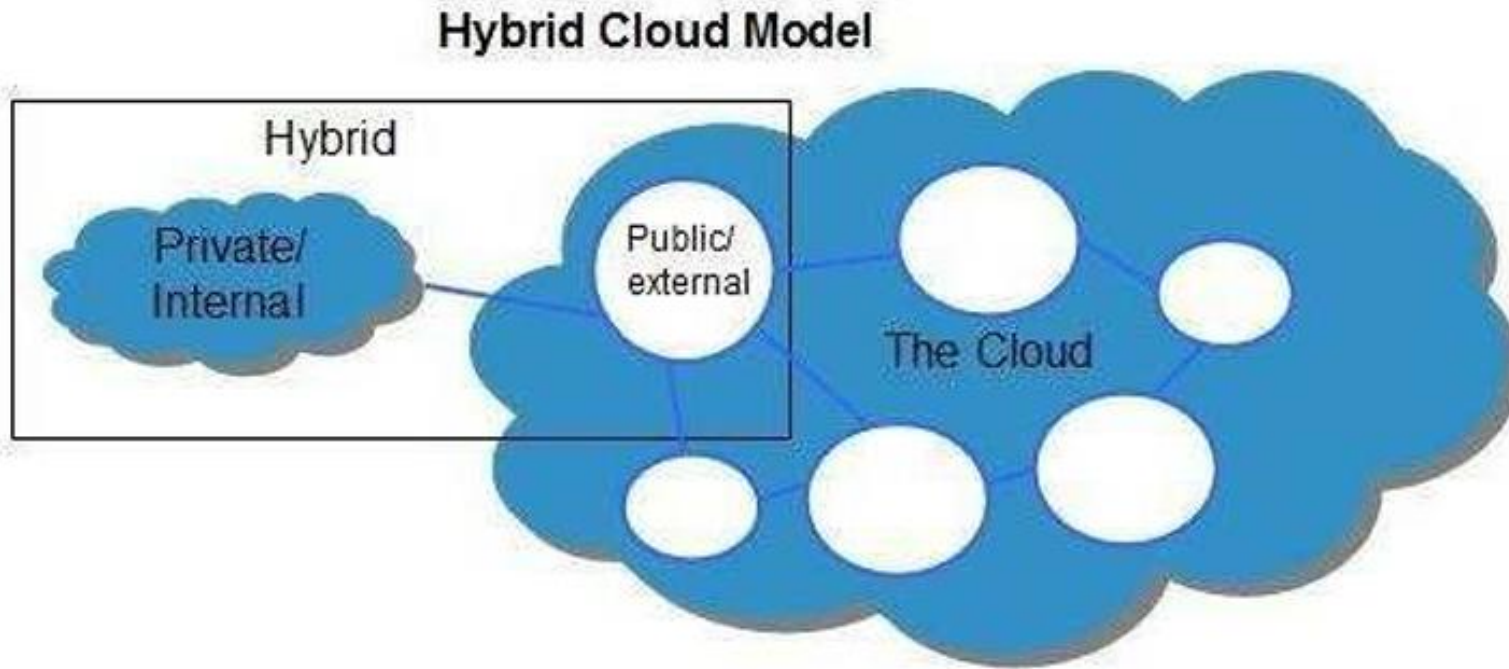
DISADVANTAGES

Here are the disadvantages of using private cloud model:

- ▶ **Restricted area** Private cloud is only accessible locally and is very difficult to deploy globally.
- ▶ **Inflexible pricing** In order to fulfill demand, purchasing new hardware is very costly.
- ▶ **Limited scalability** Private cloud can be scaled only within capacity of internal hosted resources.
- ▶ **Additional skills** In order to maintain cloud deployment, organization requires more skilled and expertise

HYBRID

The hybrid cloud is a mixture of public and private cloud. Non-critical activities are performed using public Cloud while the critical activities are performed using private cloud.



BENEFITS

There are many benefits of deploying cloud as hybrid cloud model. The following diagram shows some of those benefits:

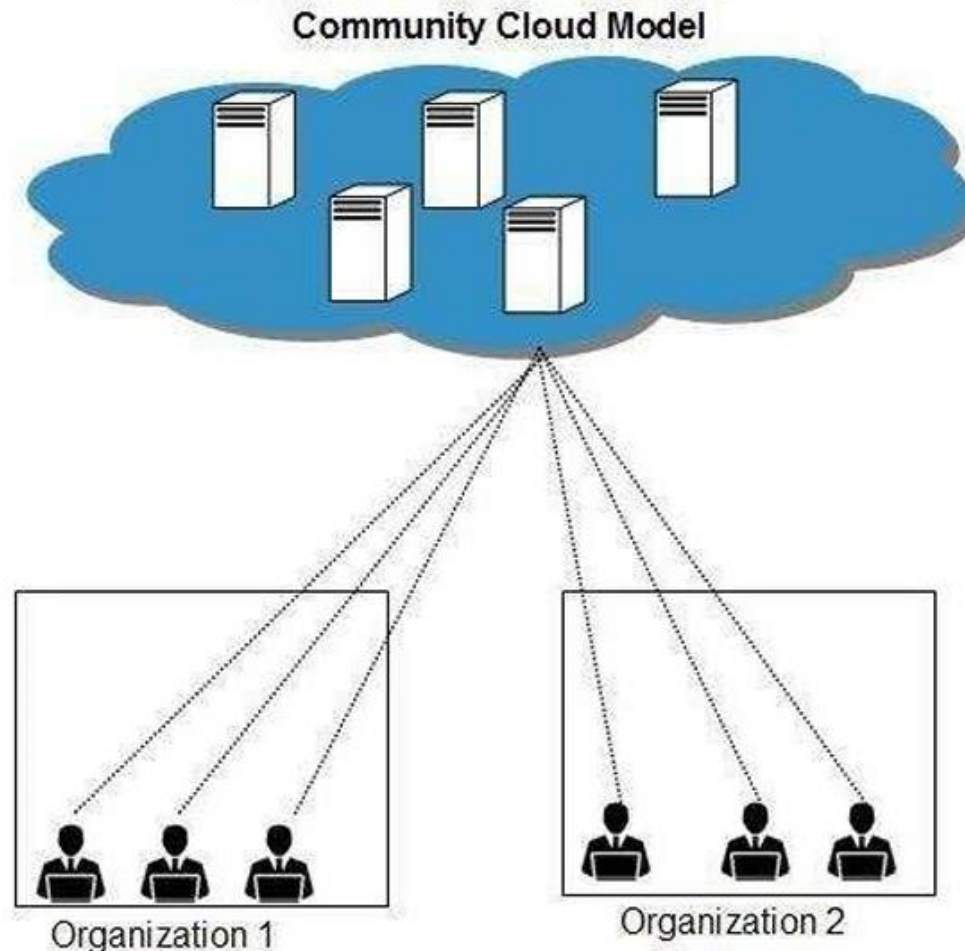
- ▶ **Scalability** It offers both features of public cloud scalability and private cloud scalability.
- ▶ **Flexibility** It offers both secure resources and scalable public resources.
- ▶ **Cost efficiencies** Public cloud are more cost effective than private, therefore hybrid cloud can have this saving.
- ▶ **Security** Private cloud in hybrid cloud ensures higher degree of security.

Disadvantages

- ▶ **Networking issues** Networking becomes complex due to presence of private and public cloud.
- ▶ **Security compliance** It is necessary to ensure that cloud services are compliant with organization's security policies.
- ▶ **Infrastructural dependency** The hybrid cloud model is dependent on internal it infrastructure, therefore it is necessary to ensure redundancy across data centers.

COMMUNITY CLOUD

The community cloud allows system and services to be accessible by group of organizations. It shares the infrastructure between several organizations from a specific community. It may be managed internally or by the third party.



BENEFITS

There are many benefits of deploying cloud as community cloud model. The following diagram shows some of those benefits:

- ▶ Cost effective Community cloud offers same advantage as that of private cloud at low cost. Sharing between organizations Community cloud provides an infrastructure to share cloud resources and capabilities among several organizations.
- ▶ Security Community cloud is comparatively more secure than the public cloud.

Disadvantages

- Since all data is housed at one location, one must be careful in storing data in community cloud because it might be accessible by others.
- It is also challenging to allocate responsibilities of governance, security and cost.

Week 6-SERVICE MODELS

► Objectives

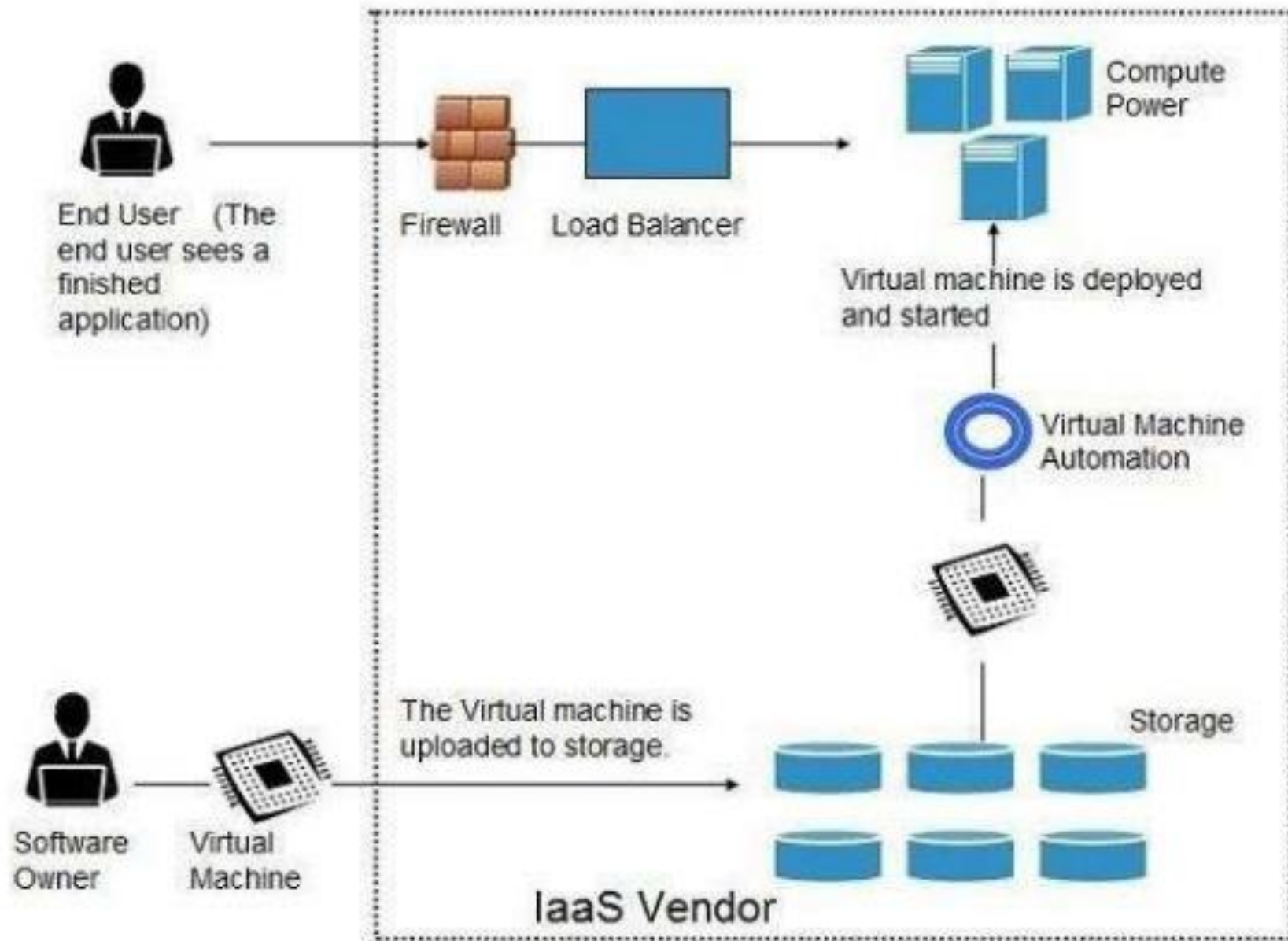
At the end of this unit, you should be able to;

1. Know the infrastructure as a service
2. Understand the xtics, benefits and security issues
3. Know the Platform as a service
4. Understand the xtics, benefits and security issues

Infrastructure-as-a-service

IAAS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc., apart from these resources, the IAAS also offers:

- ▶ Virtual machine disk storage
- ▶ Virtual local area network (VLANs)
- ▶ Load balancers
- ▶ IP addresses
- ▶ Software bundles All of the above resources are made available to end user via server virtualization. Moreover, these resources are accessed by the customers as if they own them.



Benefits

IAAS allows the cloud provider to freely locate the infrastructure over the internet in a cost-effective manner. Some of the key benefits of IAAS are listed below:

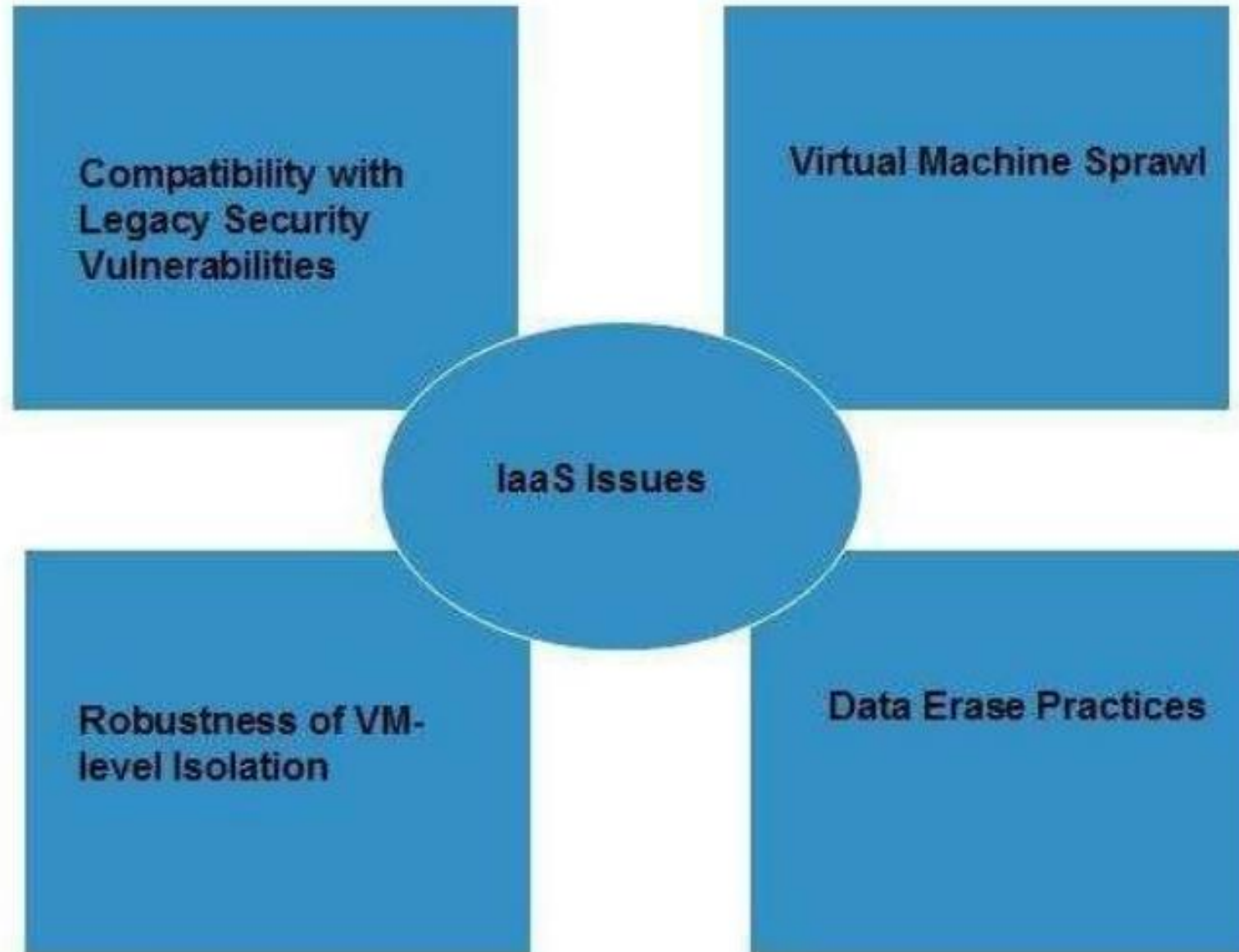
- Full control of the computing resources through administrative access to VMS.
- Flexible and efficient renting of computer hardware.
- Portability, interoperability with legacy applications.

Full control over computing resources through administrative access to VMS IAAS allows the consumer to access computing resources through administrative access to virtual machines in the following manner:

- Consumer issues administrative command to cloud provider to run the virtual machine or to save data on cloud's server.
- Consumer issues administrative command to virtual machines they owned to start web server or installing new applications.

- ▶ Flexible and efficient renting of computer hardware IAAS resources such as virtual machines, storages, bandwidth, IP addresses, monitoring services, firewalls, etc., all are made available to the consumers on rent. The consumer has to pay based the length of time a consumer retains a resource. Also with administrative access to virtual machines, the consumer can also run any software, even a custom operating system.
- ▶ Portability, interoperability with legacy applications It is possible to maintain legacy between applications and workloads between IAAS clouds. For example, network applications such as web server, e-mail server that normally runs on consumer-owned server hardware can also be run from VMS in IAAS cloud.

Issues of Challenges



- ▶ **Compatibility with legacy security vulnerabilities** Because IAAS offers the consumer to run legacy software in provider's infrastructure, therefore it exposes consumers to all of the security vulnerabilities of such legacy software.
- ▶ **Virtual machine sprawl** The VM can become out of date with respect to security updates because IAAS allows the consumer to operate the virtual machines in running, suspended and off state. However, the provider can automatically update such VMS, but this mechanism is hard and complex.
- ▶ **Robustness of VM-level isolation** IAAS offers an isolated environment to individual consumers through hypervisor. Hypervisor is a software layer that includes hardware support for virtualization to split a physical computer into multiple virtual machines.
- ▶ **Data erase practices** The consumer uses virtual machines that in turn uses the common disk resources provided by the cloud provider. When the consumer releases the resource, the cloud provider must ensure that next consumer to rent the resource does not observe data residue from previous consumer.

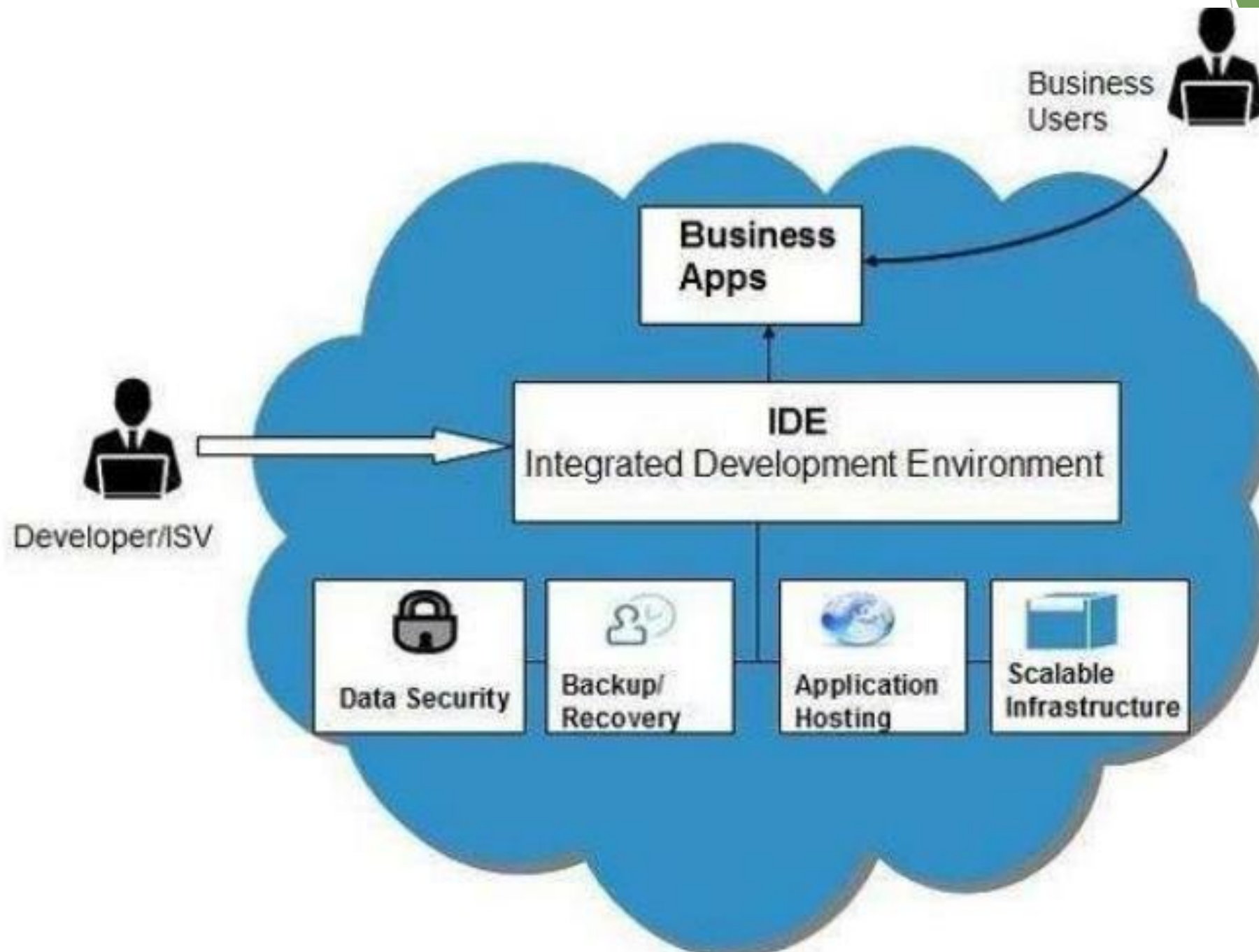
Characteristics

Here are the characteristics of iaas service model:

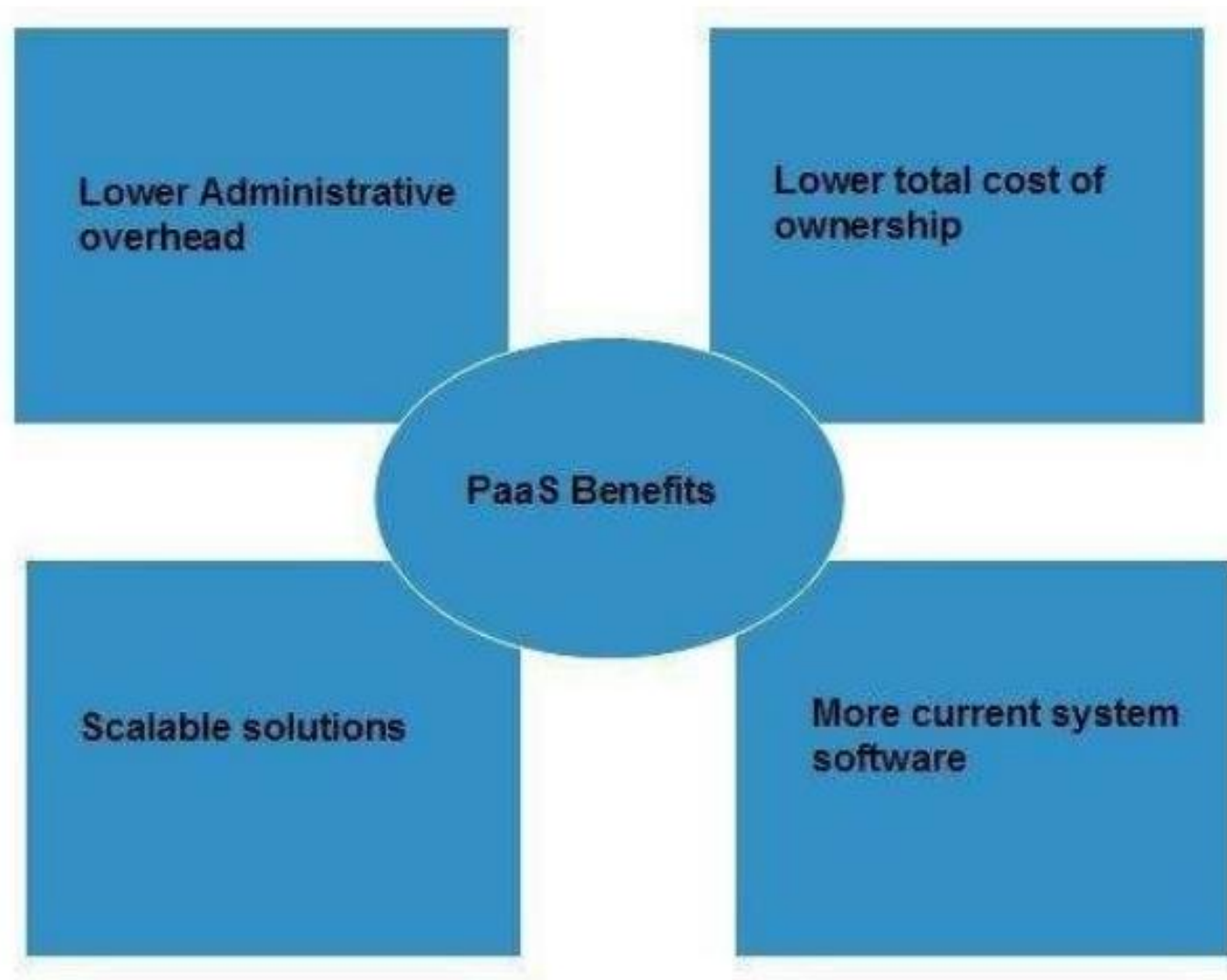
- ▶ Virtual machines with pre-installed software.
- ▶ Virtual machines with pre-installed operating systems such as windows, linux, and solaris.
- ▶ On-demand availability of resources.
- ▶ Allows to store copies of particular data in different locations.
- ▶ The computing resources can be easily scaled up and down.

Platform-as-a-service

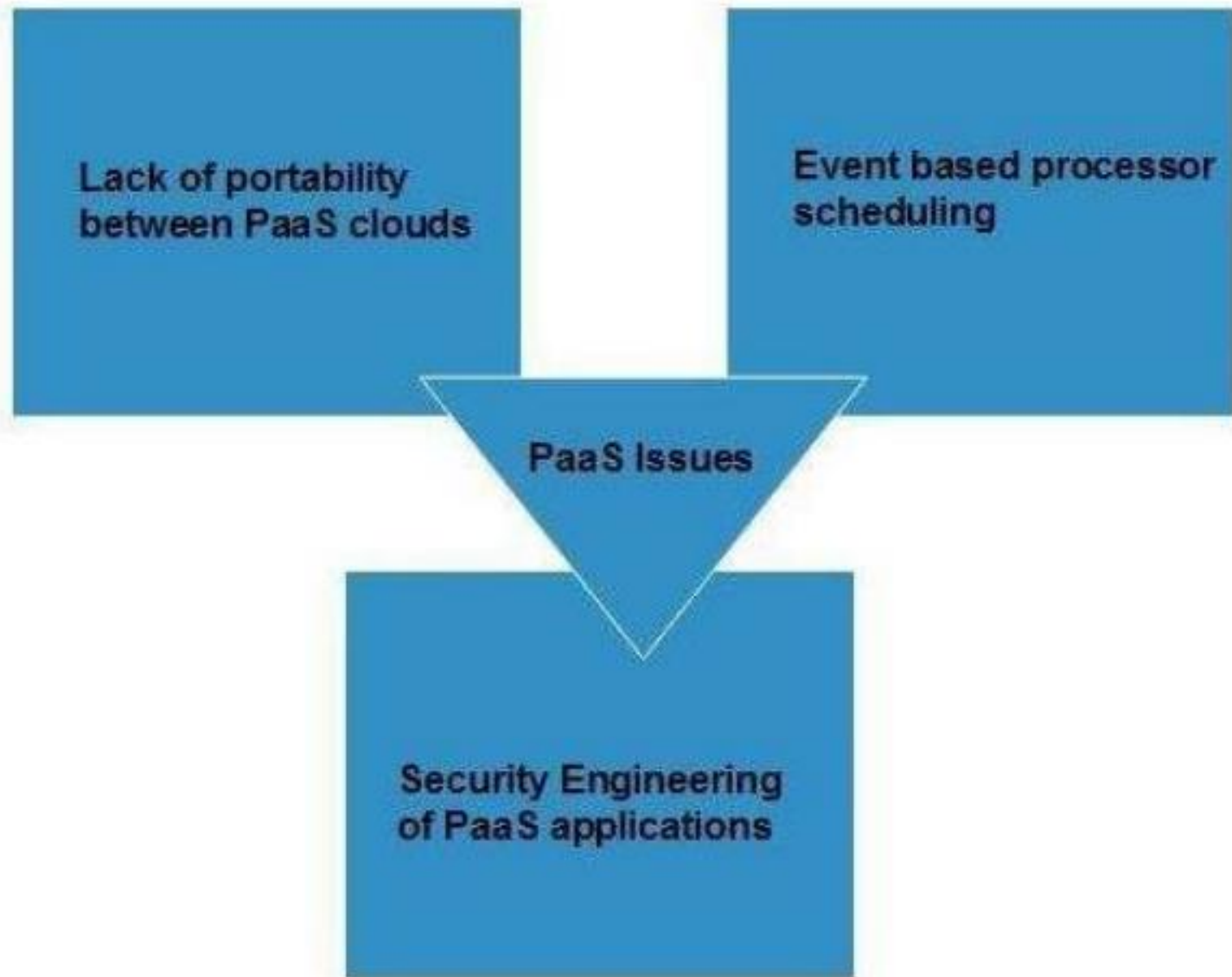
- ▶ PAAS offers the runtime environment for applications. It also offers development & deployment tools, required To develop applications.
- ▶ PAAS has a feature of point-and-click tools that enables non-developers to create web applications. Google's app engine, force.com are examples of PAAS offering vendors. Developer may log on to these websites and use the built-in API to create web-based applications. But the disadvantage of using PAAS is that the developer lock-in with a particular vendor. For example, an application written in python against Google's API using Google's app engine is likely to work only in that environment. Therefore, the vendor lock-in is the biggest problem in PAAS.
- ▶ The following diagram shows how PAAS offers an API and development tools to the developers and how it helps the end user to access business applications.



Benefits



Issues



Characteristics

- ▶ • PAAS offers browser based development environment. It allows the developer to create database and edit the application code either via application programming interface or point-and-click tools.
- ▶ • PAAS provides built-in security, scalability, and web service interfaces.
- ▶ • PAAS provides built-in tools for defining workflow and approval processes and defining business rules.
- ▶ • It is easy to integrate with other applications on the same platform.
- ▶ • PAAS also provides web services interfaces that allow us to connect the applications outside the platform.

Week 7-SERVICE MODELS

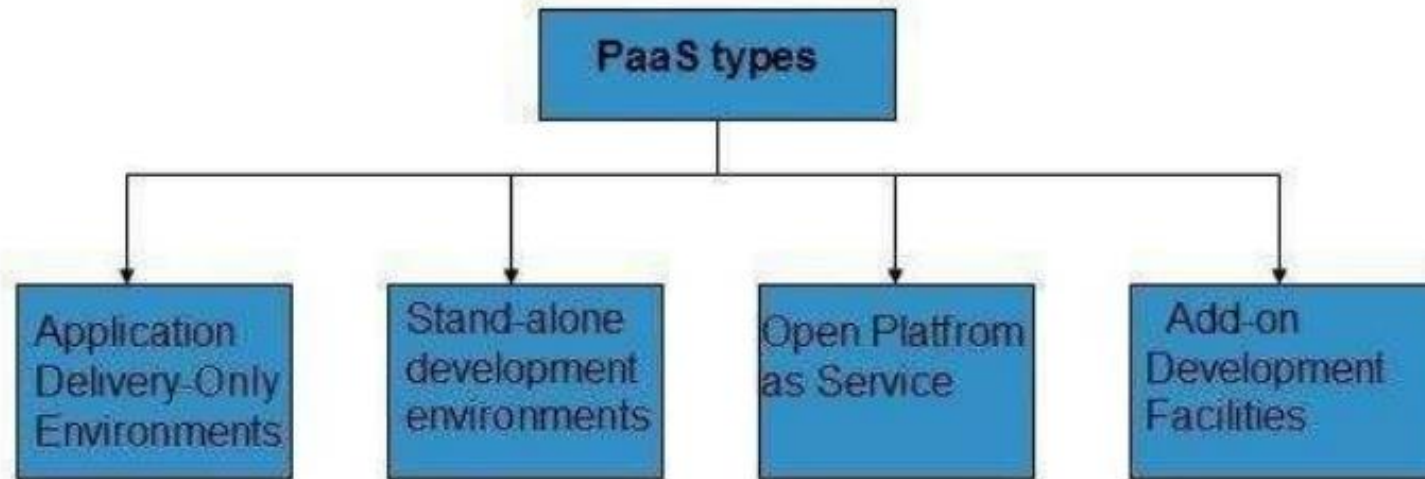
► Objectives

At the end of this unit, you should be able to;

1. Know the Software as a service
2. Understand the xtics, benefits and security issues
3. Know the identity as a service
4. Understand the xtics, benefits and security issues
5. Know the Network as a service
6. Understand the xtics, benefits and security issues
7. Understand the concept of Cloud Computing Management

PAAS types

Based on the functions, the PAAS can be classified into four types as shown in the following diagram:



Stand-alone development environments

The **stand-alone PAAS** works as an independent entity for a specific function. It does not include licensing, technical dependencies on specific SAAS applications.

Application delivery-only environments

The application delivery PAAS includes on-demand scaling and application security.

Open platform as a service

Open PAAS offers an **open source software** that helps a PAAS provider to run applications.

Add-on development facilities

The **add-on PAAS** allows to customize the existing SAAS platform.

Software-as-a-service

Software as a service (SAAS) model allows to provide software application as a service to the end users. It Refers to a software that is deployed on a hosted service and is accessible via internet. There are several SAAS applications, some of them are listed below:

- Billing and invoicing system
- Customer relationship management (CRM) applications
- Help desk applications
- Human resource (HR) solutions

Some of the SAAS applications are not customizable such as an **office suite**. But SAAS provides us **application programming interface (api)**, which allows the developer to develop a customized application.

Characteristics

Here are the characteristics of SAAS service model:

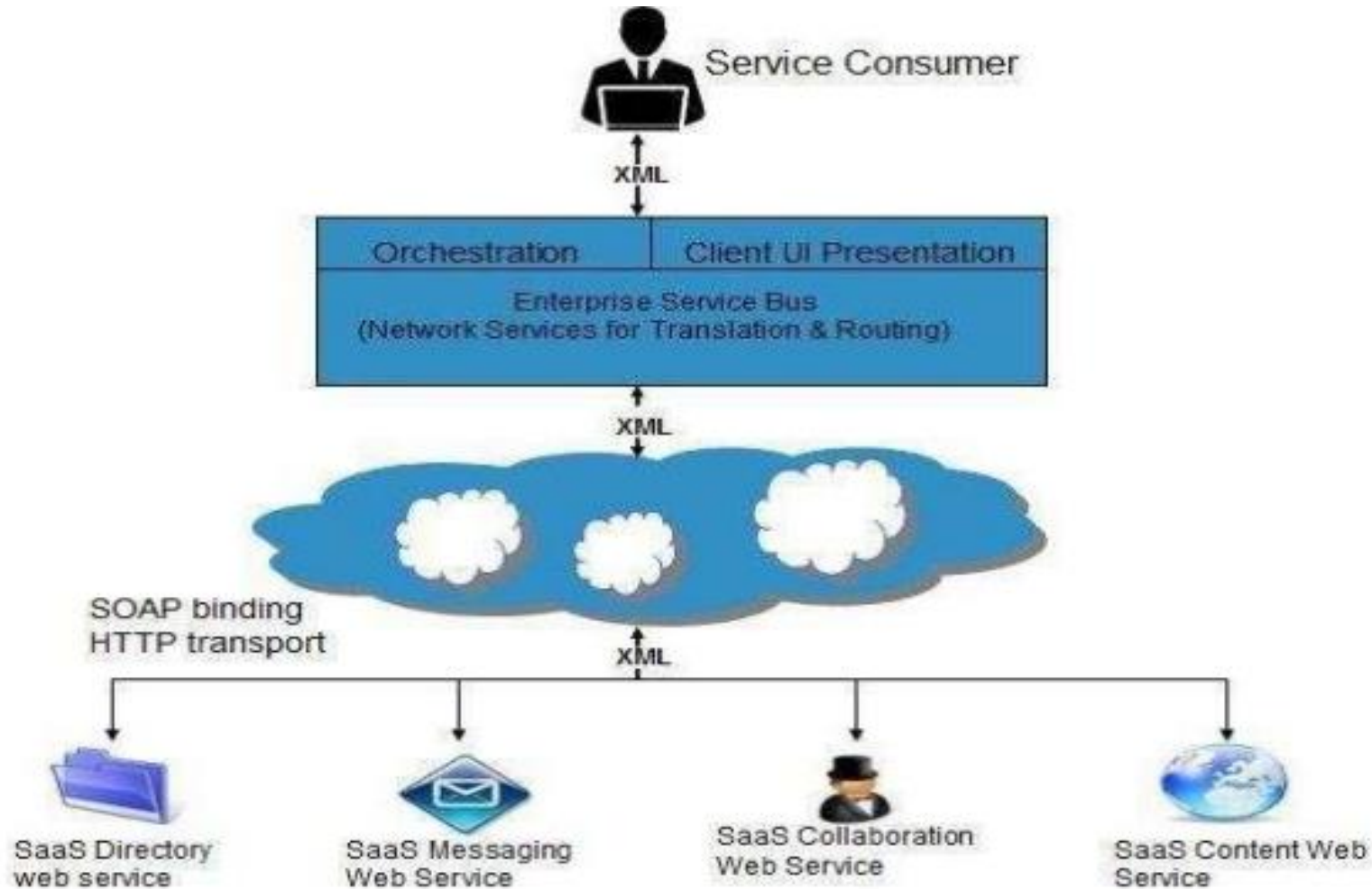
- SAAS makes the software available over the internet.
- The software are maintained by the vendor rather than where they are running.
- The license to the software may be subscription based or usage based. And it is billed on recurring basis.
- SAAS applications are cost effective since they do not require any maintenance at end user side.
- They are available on demand.
- They can be scaled up or down on demand.
- They are automatically upgraded and updated.
- SAAS offers share data model. Therefore, multiple users can share single instance of infrastructure. It is not required to hard code the functionality for individual users.
- All users are running same version of the software.

Benefits

Using SAAS has proved to be beneficial in terms of scalability, efficiency, performance and much more. Some of the benefits are listed below:

- Modest software tools
- Efficient use of software licenses
- Centralized management & data
- Platform responsibilities managed by provider
- Multitenant solutions

The following diagram shows the SAAS implementation based on SOA:



Identity-as-a-service

Employees in a company require to login into system to perform various tasks. These systems may be based on local server or cloud based. Following are the problems that an employee might face:

- Remembering different username and password combinations for accessing multiple servers.
- If an employee leaves the company, it's required to ensure that each of the user's account has been disabled. This increases workload on it staff.

To solve above problems, a new technique emerged which is known as **identity as a service (IDAAS)**. IDAAS offers management of identity (information) as a digital entity. This identity can be used during electronic transactions.

Identity

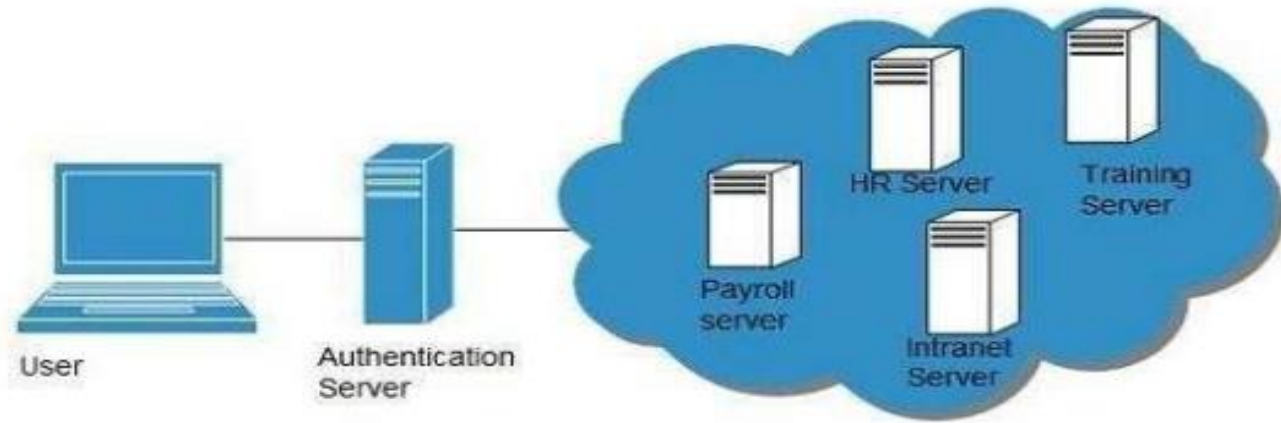
Identity refers to set of attributes associated with something and make it recognizable. All objects may have same attributes, but their identity cannot be the same. This unique identity is assigned through unique identification attribute.

There are several **identity services** that have been deployed to validate services such as validating web sites, transactions, transaction participants, client, etc. Identity as a service may include the following:

- Directory services
- Federated services
- Registration
- Authentication services
- Risk and event monitoring
- Single sign-on services
- Identity and profile management

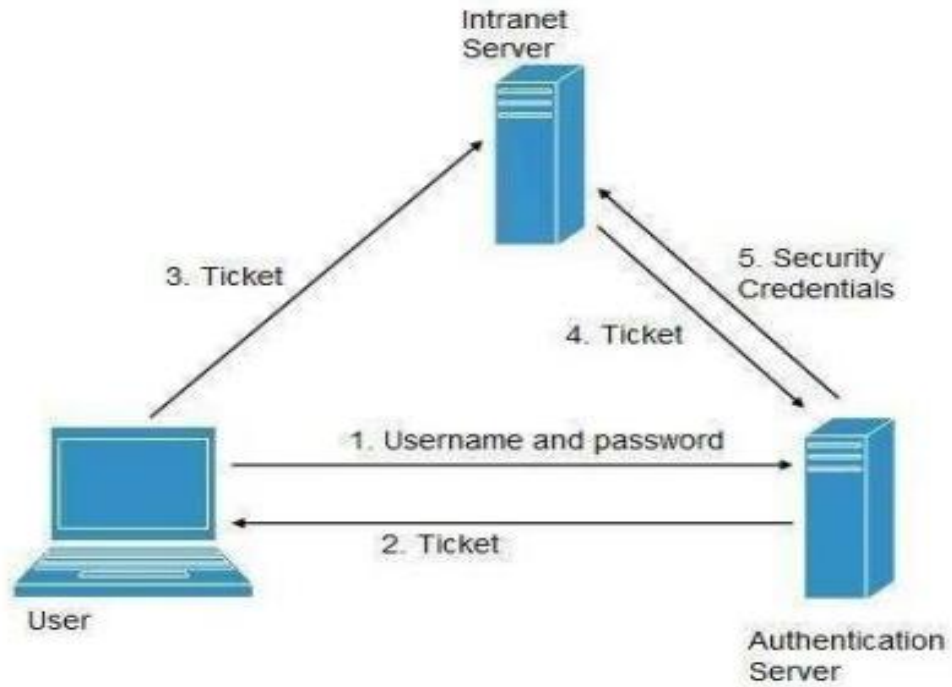
► Single sign-on (SSO)

To solve the problem of using different username & password combination for different servers, companies now employ single sign-on software, which allows the user to login only one time and manages the user's access to other systems. SSO has single authentication server, managing multiple accesses to other systems, as shown in the following diagram.



SSO working

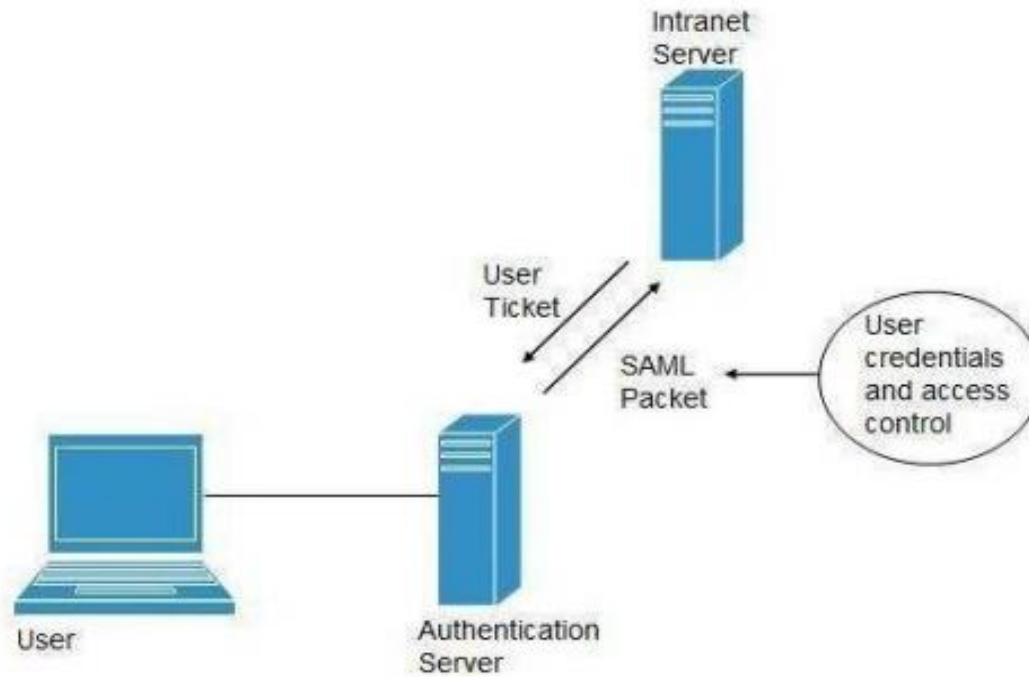
There are several implementations of SSO. Here, we will discuss the common working of SSO:



- ▶ The following steps explain the working of single sign-on software:
- ▶ 1. User logs into the authentication server using a username and password.
- ▶ 2. The authentication server returns the user's ticket.
- ▶ 3. User sends the ticket to intranet server.
- ▶ 4. Intranet server sends the ticket to the authentication server.
- ▶ 5. Authentication servers ends the user's security credentials for that server back to the intranet server. If an employee leaves the company, then it just required to disable the user at the authentication server, which in turn disables the user's access to all the systems.

Federated identity management (FIDM)

- ▶ FIDM describes the technologies and protocols that enable a user to package security credentials across security domains. It uses security markup language (SAML) to package a user's security credentials as shown in the following diagram:



Openid

It offers users to login into multiple websites with single account. Google, yahoo!, flickr, myspace, wordpress.com are some of the companies that support openid.

Benefits

- Increased site conversation rates.
- Access to greater user profile content.
- Fewer problems with lost passwords.
- Ease of content integration into social networking sites.

Network-as-a-service

Overview

Network as a service allows us to access to network infrastructure directly and securely. NaaS makes it Possible to deploy custom routing protocols.

NaaS uses virtualized network infrastructure to provide network services to the consumer. It is the responsibility of NaaS provider to maintain and manage the network resources which decreases the workload from the consumer. Moreover, NaaS offers network as a utility.

NaaS is also based on pay-per-use model.

How NaaS is delivered?

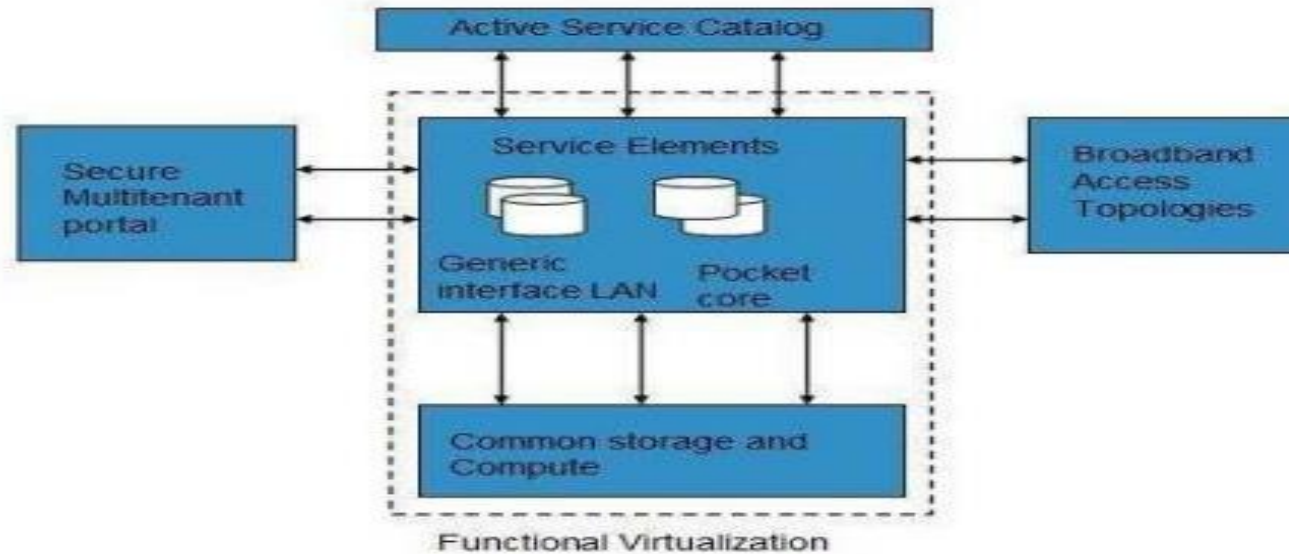
To use NaaS model, the consumer is required to logon to the web portal, where he can get online api. Here, the consumer can customize the route.

In turn, consumer has to pay for the capacity used. It is also possible to turn off the capacity at any time.

Mobile NaaS

Mobile NaaS offers more efficient and flexible control over mobile devices. It uses virtualization to simplify the architecture to create more efficient processes.

Following diagram shows the mobile NaaS service elements:



NaaS benefits

NaaS offers a number of benefits, some of them are discussed below:



- ▶ • **Independence:** Each consumer is independent and can segregate the network.
- ▶ • **Bursting:** Customers have to pay for high-capacity network only when needed.
- ▶ • **Resilience:** There exists reliability treatments that can be applied for critical applications.
- ▶ • **Analytics:** There exists data protection solution for highly sensitive applications.
- ▶ • **Ease of adding new service elements:** It is very easy to integrate new service elements to the network.
- ▶ • **Support models:** There exists more open support models, which help to reduce the operation cost.
- ▶ • **Isolation of customer traffic:** The customer traffic is logically isolated.

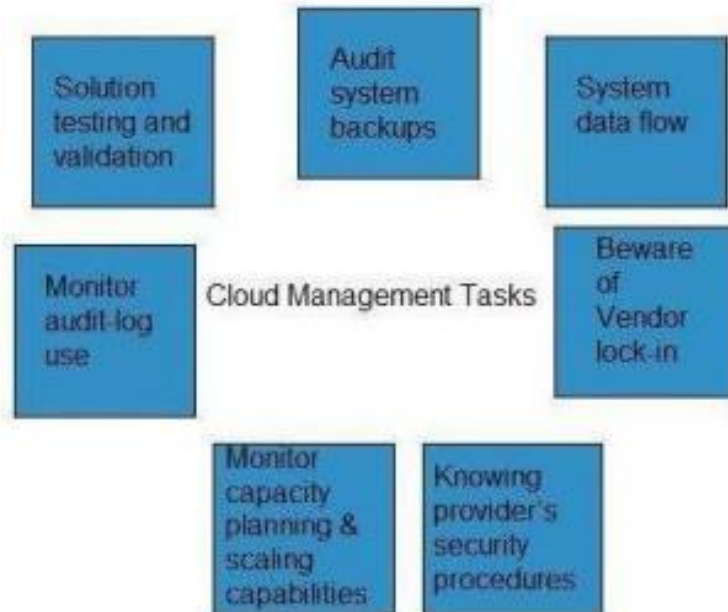
CLOUD COMPUTING MANAGEMENT

Overview

It is the responsibility of cloud provider to manage resources and their performance. Management may include several aspects of cloud computing such as load balancing, performance, storage and backups, capacity, deployment, etc. Management is required to access full functionality of resources in the cloud.

Cloud management tasks

Cloud management involves a number of tasks to be performed by the cloud provider to ensure efficient use of cloud resources. Here, we will discuss some of these tasks:



Audit system backups

It is required to timely audit the backups to ensure you can successfully restore randomly selected files of different users. Backups can be performed in following ways:

- Backing up files by the company, from on-site computers to the disks that reside within the cloud.
- Backing up files by the cloud provider.

It is necessary to know if cloud provider has encrypted the data, who has access to that data and if the backup is taken at different locations, you must know where.

System's data flow

The managers should develop a diagram describing a detailed process flow. This process flow will describe the movement of company's data throughout the cloud solution.

Beware of vendor lock-in

The managers must know the procedure to exit from services of a particular cloud provider. There must exist procedures, enabling the managers to export company's data to a file and importing it to another provider.

Knowing provider's security procedures

The managers should know the security plans of the provider for different services:

- Multitenant use
- E-commerce processing

- Employee screening
- Encryption policy

Monitor capacity planning and scaling capabilities

The managers should know the capacity planning in order to ensure whether the cloud provider will meet the future capacity requirement for his business or not.

It is also required to manage scaling capabilities in order to ensure services can be scaled up or down as per the user need.

Monitor audit-log use

In order to identify the errors in the system, managers must audit the logs on a regular basis.

Solution testing and validation

It is necessary to test the solutions provided by the provider in order to validate that it gives the correct result and is error-free. This is necessary for a system to be robust and reliable.

END OF 414 LECTURE FOR THE SEMESTER

