Cloud Computing

By

K. Bhaskara Rao

Asst. Prof.

IT Dept.

BEC

DEFINITION, 5-4-3 PRINCIPLES OF CLOUD COMPUTING, CLOUD ECO SYSTEM, FEATURES OF CLOUD SERVICE, BENEFITS AND DRAWBACKS, CLOUD ARCHITECTURE, ANATOMY OF CLOUD, NETWORK CONNECTIVITY IN CLOUD COMPUTING, APPLICATIONS ON THE CLOUD, MANAGING THE CLOUD, MIGRATING APPLICATION TO CLOUD.

Cloud Computing

- Cloud computing, also on-demand computing, is a kind of Internet-based computing that **provides shared processing resources and data** to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources" .

- A style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies."
- **Elasticity** is the ability of an IT infrastructure to quickly expand or cut back capacity and **services** without hindering or jeopardizing the infrastructure's stability, performance, security, governance or compliance protocols.

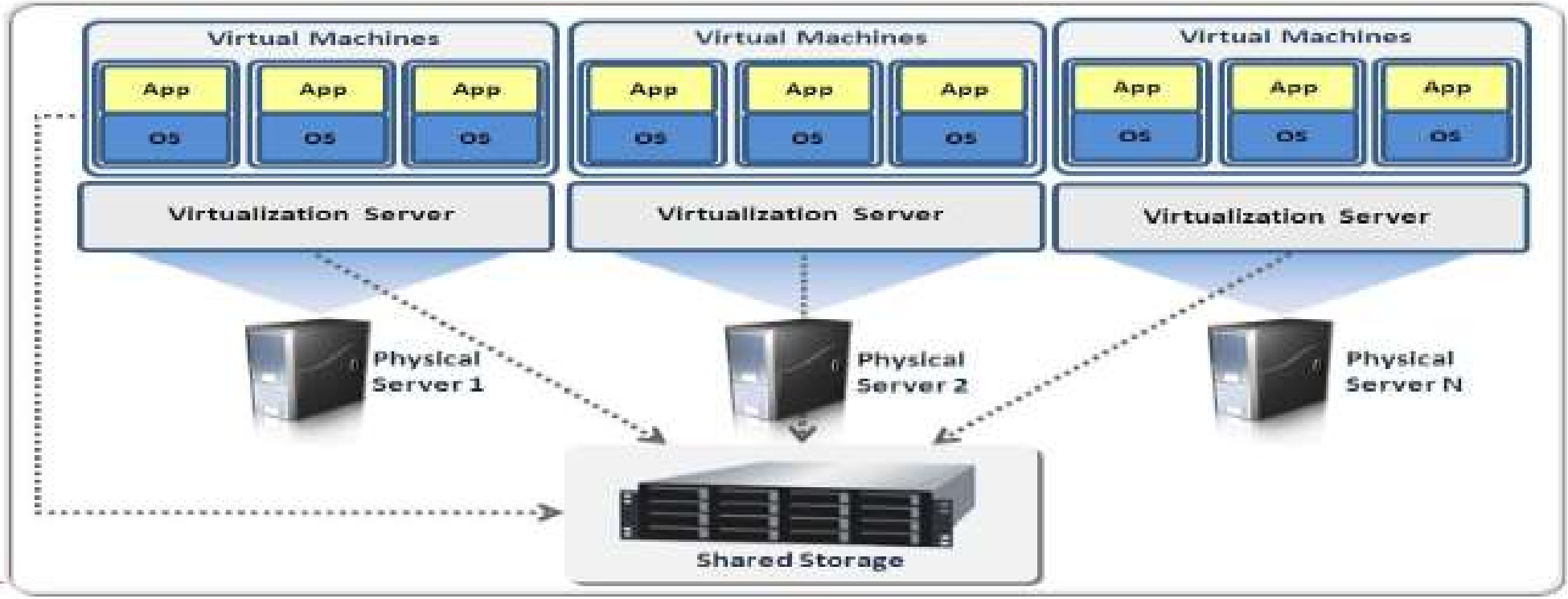
- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- In cloud computing, the IT and business resources, such as servers, storage, network, applications, and processes, can be dynamically provisioned to the user needs and workload.
- cloud computing is a mechanism of *bringing–hiring or getting the services of the computing power or infrastructure* to an organizational or individual level to the extent required and paying only for the consumed services. (similar to consuming electric power in homes)

Cloud Computing

- Cloud computing encompasses the subscription-based or pay-per-use service model of offering computing to end users or customers over the Internet and thereby extending the IT's existing capabilities.

Major Technology Innovations that made the cloud possible (2)

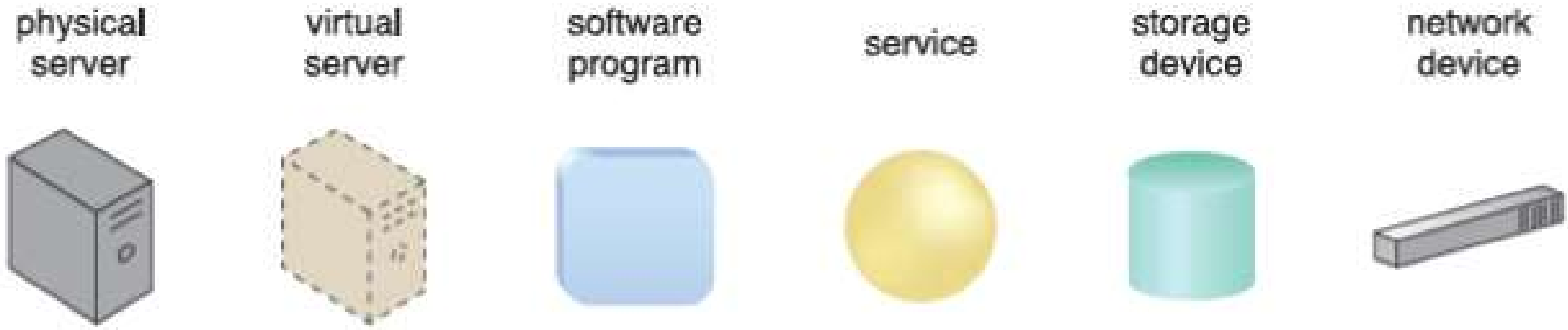
- Virtualization
  - allows physical IT resources to provide multiple virtual images of themselves so that their underlying processing capabilities can be shared by multiple users.



Cloud

- IT Resource that is delivered can be a a physical or virtual IT-related artifact that can be either software-based, or hardware-based.

IT Resources:



Approaches to Cloud Computing
(Cloud Delivery Models)

The three approaches to cloud computing are Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Differ in what is provided to the consumer.

- Iaas → Infrastructure as a Service (Servers , Disk, RAM, Network Stack etc…)
- PaaS → Platform as a Service (Runtime, DB platform, Frameworks..)
- SaaS → Software as a Service (Application, Data)

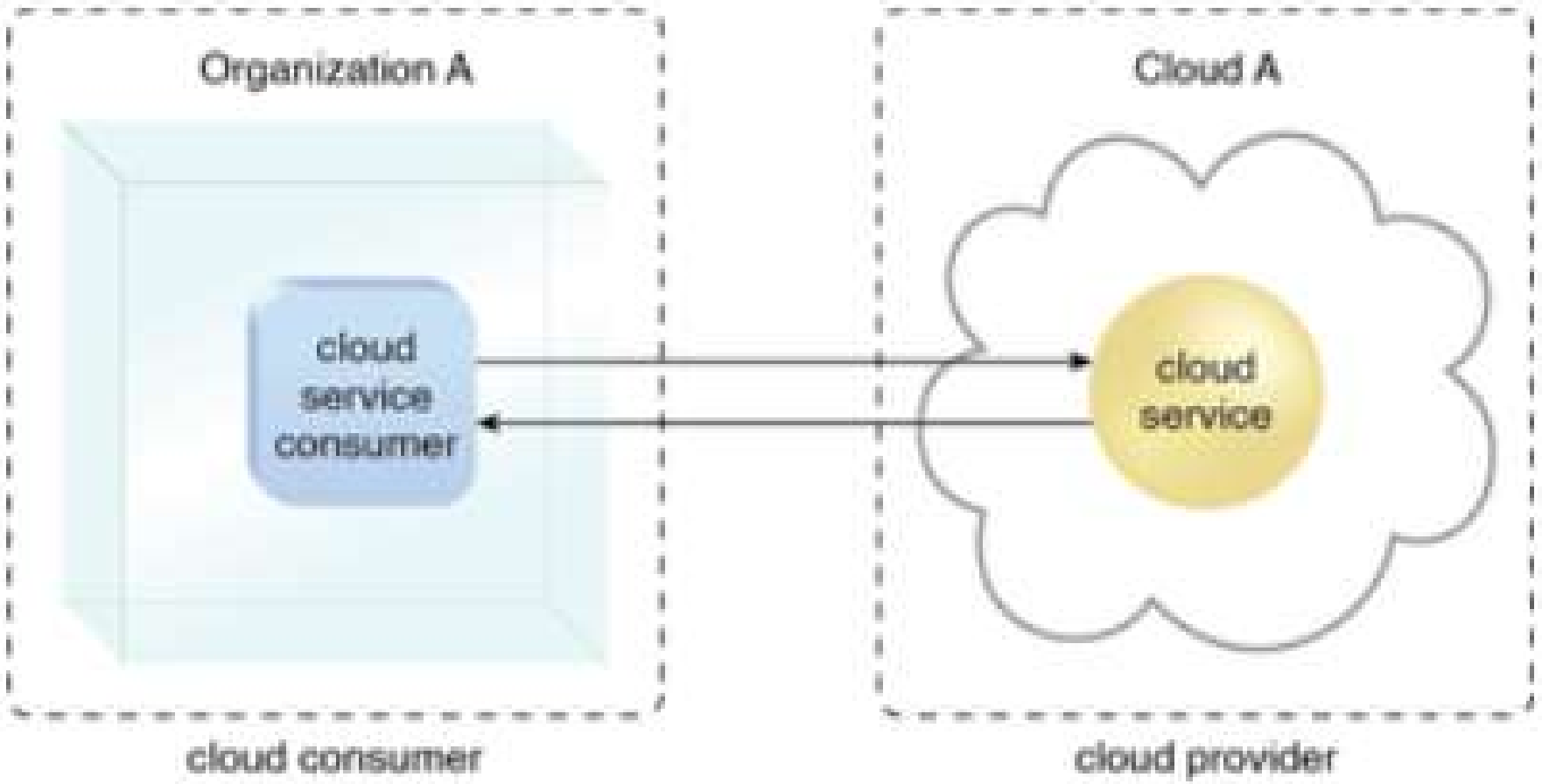
Infrastructure: Include hardware, network, connectivity, operating systems, and other "raw" IT resources.

- IaaS provides IT resources that are virtualized and packaged into bundles that simplify up-front runtime scaling and customization of the infrastructure
- **Cloud Consumer:** The party that uses cloud-based IT resources.
- **Cloud Provider:** The party that provides the IT resources.

Many specialized variations of the three base cloud delivery models have emerged:

- Storage-as-a-Service
- Database-as-a-Service
- Security-as-a-Service
- Communication-as-a-Service
- Integration-as-a-Service
- Testing-as-a-Service
- Process-as-a-Service

Introduction



Cloud Characteristics

- **On-Demand Usage**
  - Automated ability of a cloud to transparently scale IT resources.

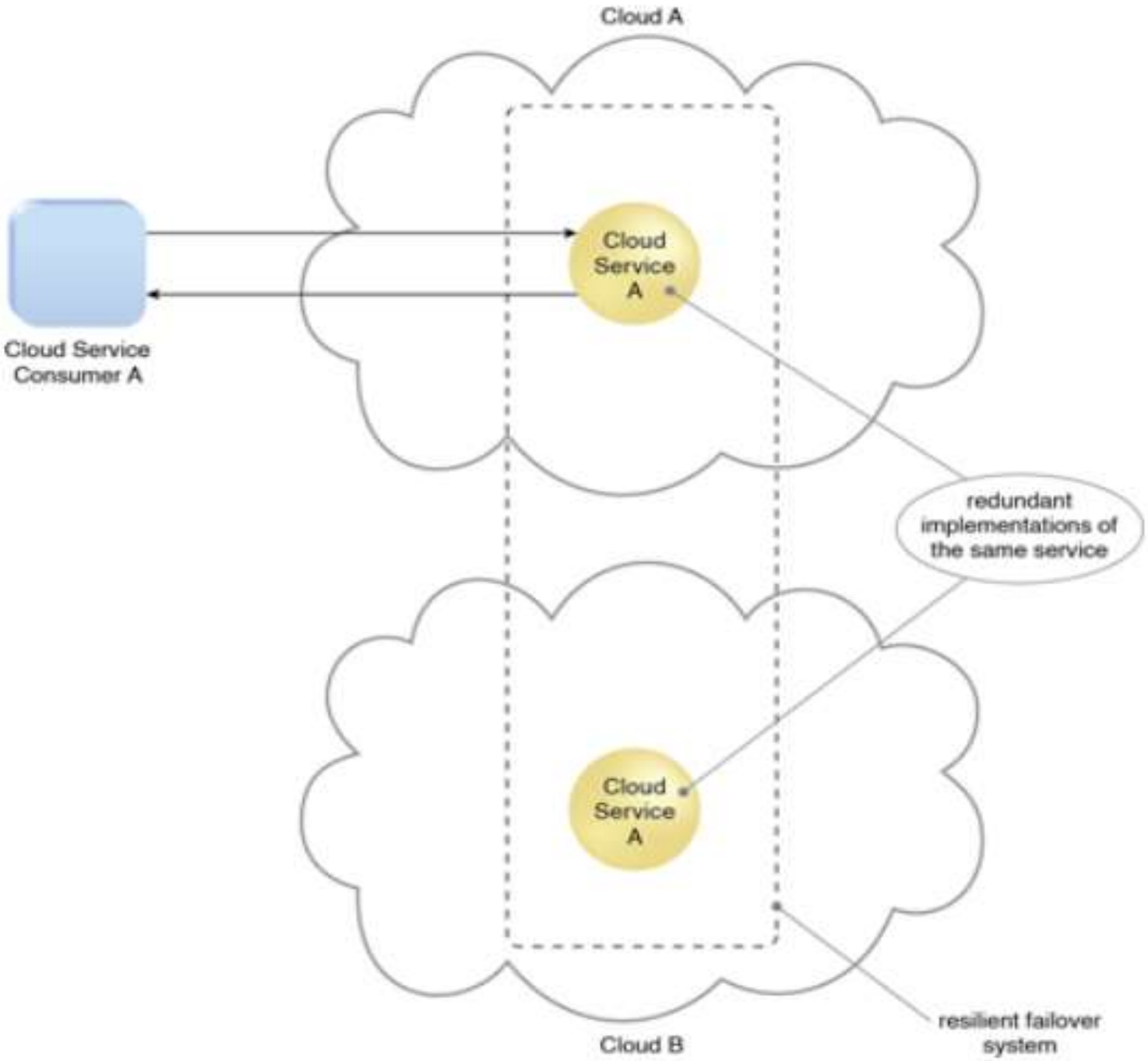
- **Ubiquitous Access** → *Ubiquitous Access* represents the ability for a cloud service to be widely accessible. Establishing ubiquitous access for a cloud service can require support for a range of devices, transport protocols, interfaces, and security technologies.

- **Multitenancy** → One instance serves different customers.
- **Elasticity** → automated ability of a cloud to transparently scale IT resources as required in response to runtime conditions or as pre-determined by the cloud consumer or cloud provider.

- **Measured Usage** → ability of a cloud platform to keep track of the usage of its IT resources, primarily by cloud consumers . Based on what is measured, the cloud provider can charge a cloud consumer only for the IT resources actually used and/or for the timeframe during which access to the IT resources was granted.

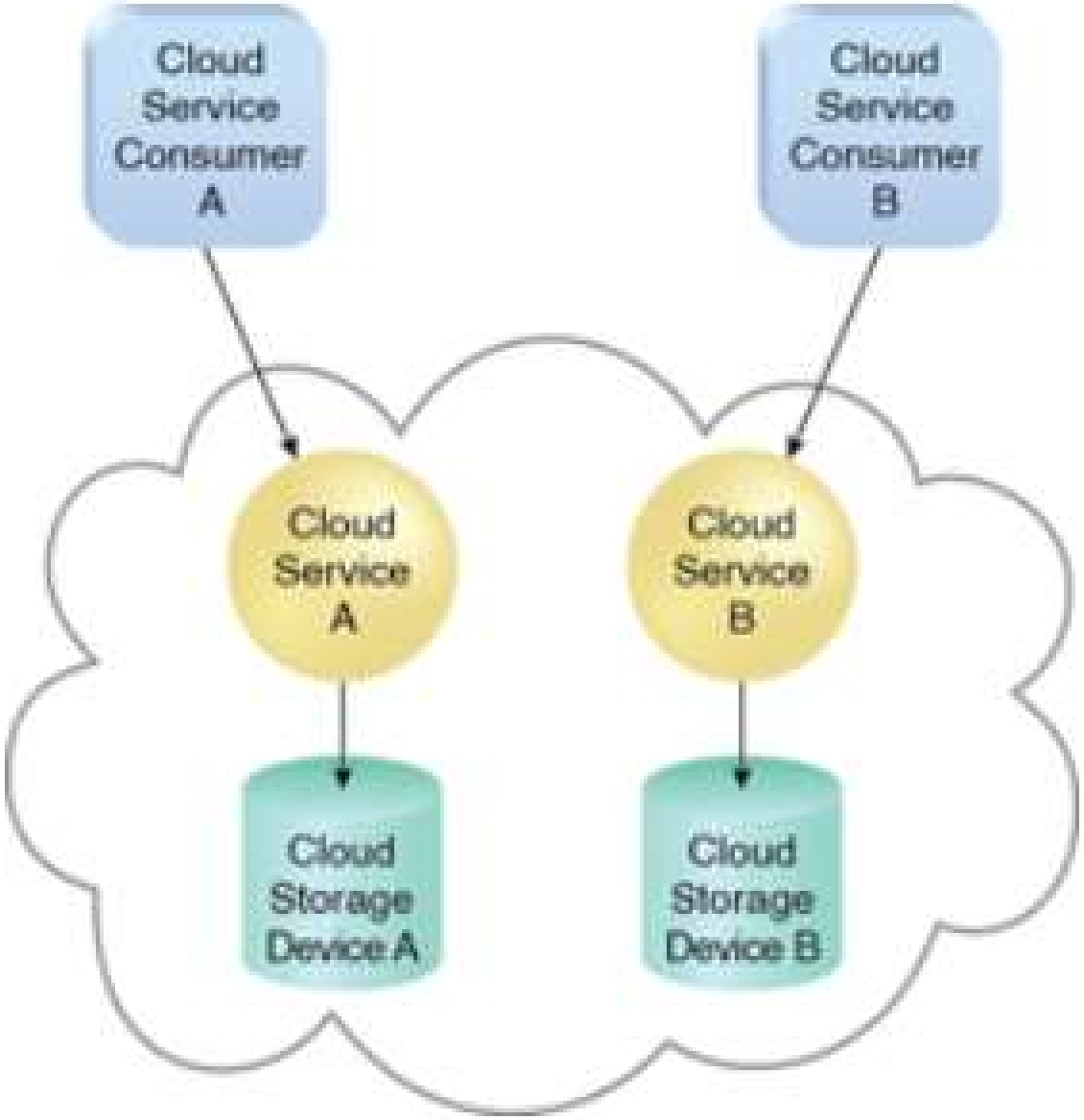
- **Resiliency:** (recovering readily): Distribution of redundant implementations of IT resources across physical locations. IT resources can be pre-configured so that if one becomes deficient, processing is automatically handed over to another redundant implementation.

A resilient cloud service



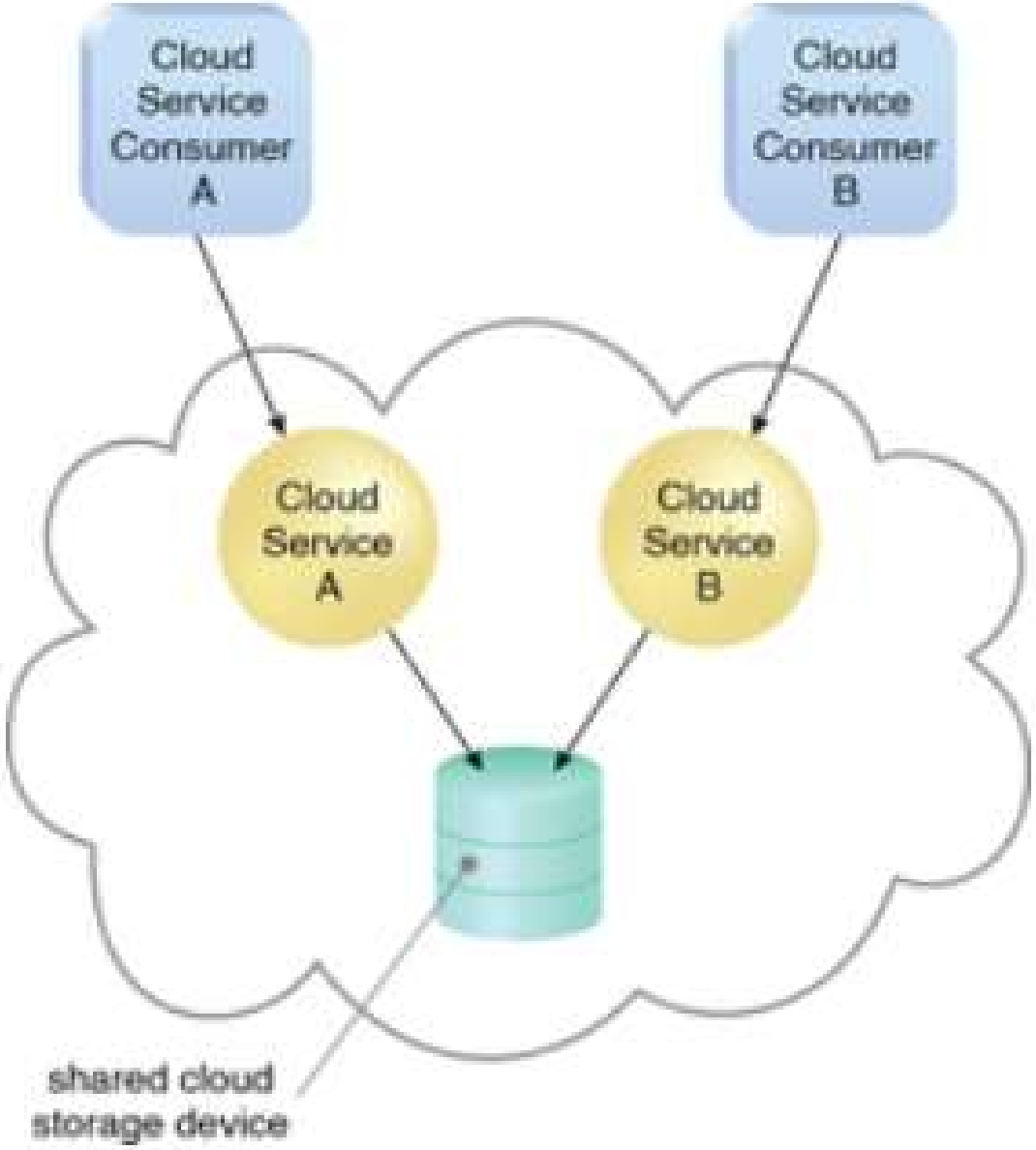
Single-tenant environment

- In a single-tenant environment, each cloud consumer has a separate IT resource instance.



multi-tenant environment

- a single instance of an IT resource, such as a cloud storage device, serves multiple consumers.



Introduction

cloud software environments:

Open source:

Eucalyptus and Nimbus

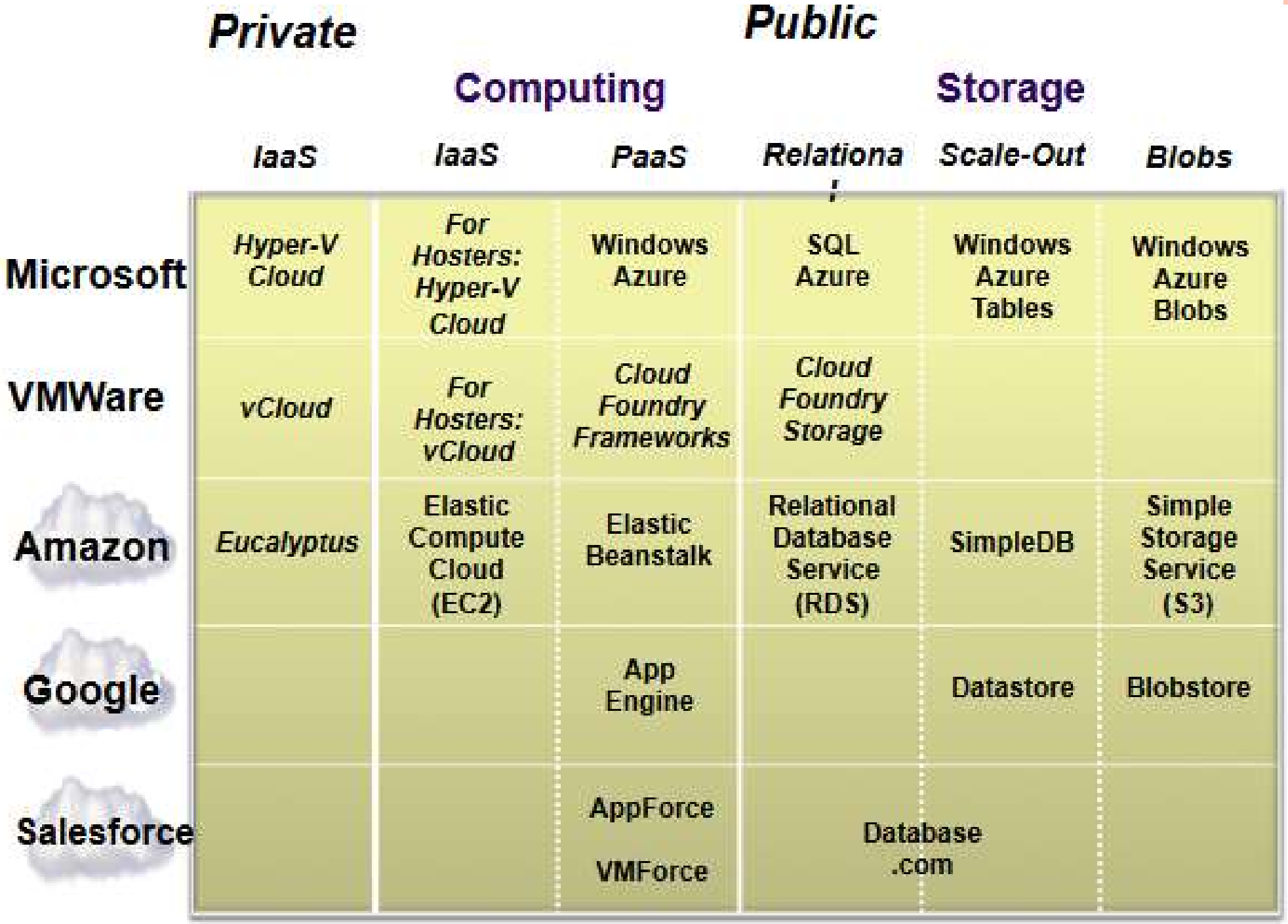
- Manjrasoft Aneka

OpenNebula

Google AppEngine,

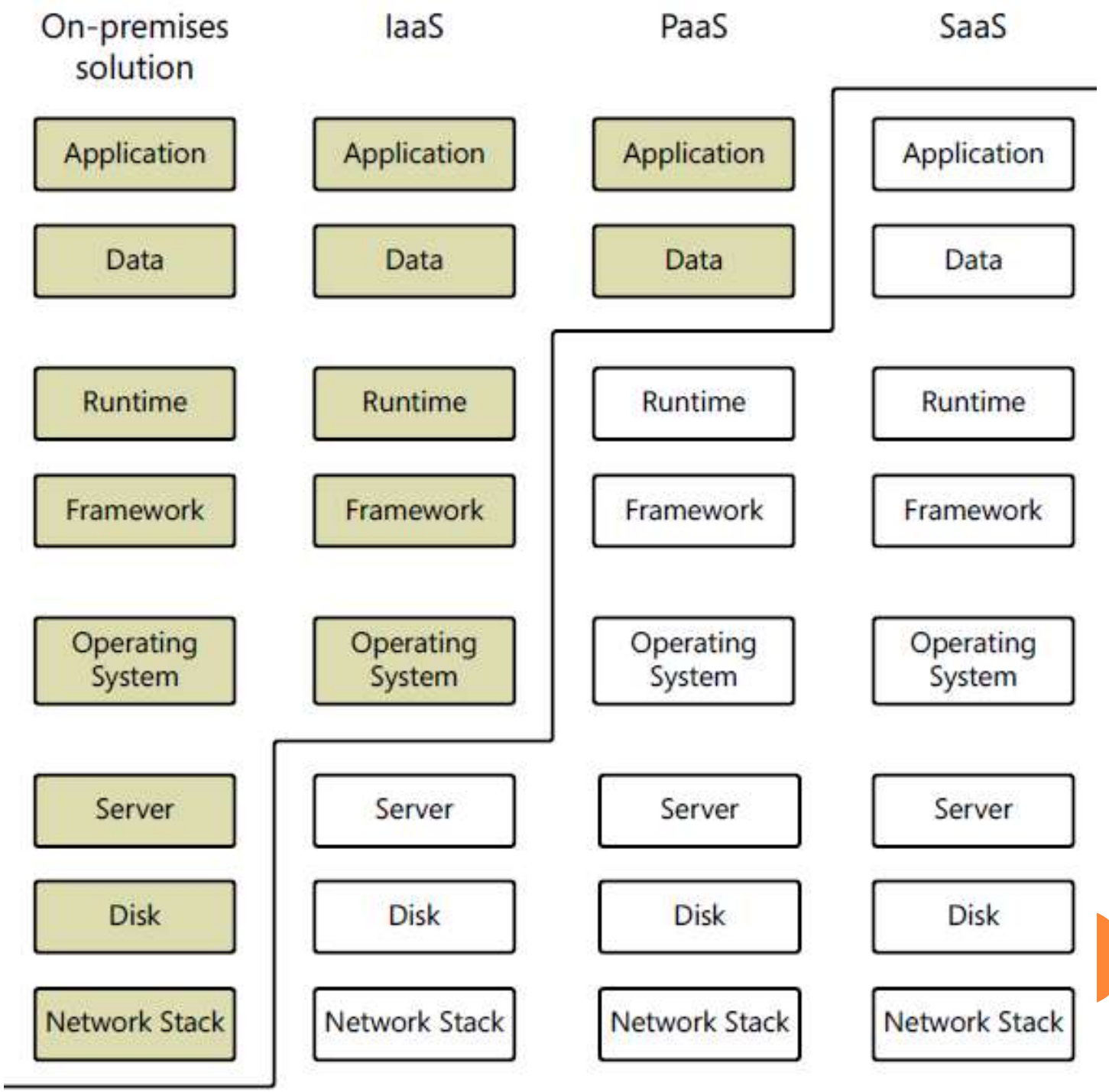
Google WebToolkit

OverView

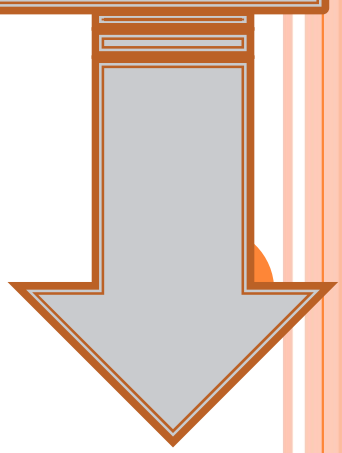

Private
Public
Computing
Storage
IaaS
IaaS
PaaS
Relationa
Scale-Out
Blobs
Microsoft
Hyper-V Cloud
For Hosters: Hyper-V Cloud
Windows Azure
SQL Azure
Windows Azure Tables
Windows Azure Blobs
VMWare
vCloud
For Hosters: vCloud
Cloud Foundry Frameworks
Cloud Foundry Storage
Amazon
Eucalyptus
Elastic Compute Cloud (EC2)
Elastic Beanstalk
Relational Database Service (RDS)
SimpleDB
Simple Storage Service (S3)
Google
App Engine
Datastore
Blobstore
Salesforce
AppForce
VMForce
Database .com

Cloud Services defined

Responsibility of you and the vendor is shown in the diagram



- ✓ 5-4-3 Principles of Cloud Computing
- ✓ Cloud Eco System
- ✓ Features of Cloud Service



5-4-3 Principles of Cloud Computing

5-4-3 principles

5 Essential Characteristics

4 Cloud Deployment Models

3 Service Offering Models

5 Essential Characteristics:

1. On-demand self-service
2. Broad network access
3. Elastic resource pooling
4. Rapid elasticity
5. Measured service

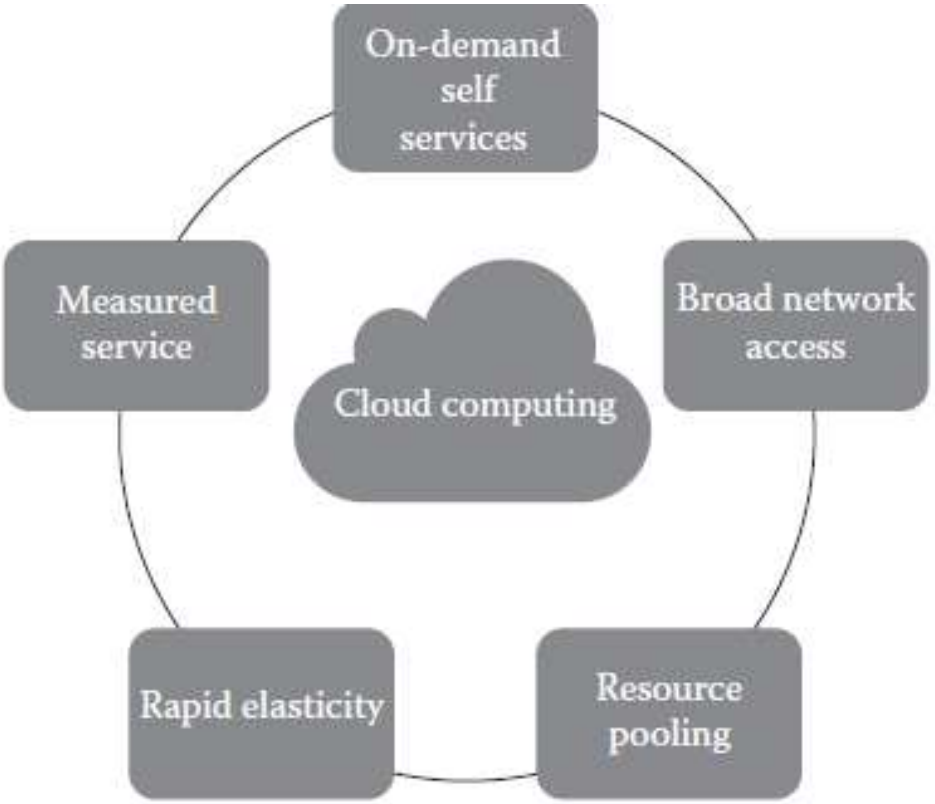
4 Cloud Deployment Models

1. Private
2. Public
3. Community
4. Hybrid

3 Service Offering Models → SaaS, PaaS, IaaS

5-4-3 principles

5 Essential Characteristics:



On-demand self-service:

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

5-4-3 principles - 5 Essential Characteristics

5 Essential Characteristics:

2. Broad network access:

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants [PDAs]).

3. Elastic resource pooling:

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

5-4-3 principles - 5 Essential Characteristics

5 Essential Characteristics:

4. Rapid elasticity:

- Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.
- To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

5. Measured service:

Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

5-4-3 principles - 4 Cloud Deployment models

4 Cloud Deployment Models

Deployment models describe the ways with which the cloud services can be deployed or made available to its customers, depending on the organizational structure and the provisioning location.

1. Private Cloud:

- The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

2. Public Cloud:

- The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

5-4-3 principles - 4 Cloud Deployment models

4 Cloud Deployment Models

3. Community Cloud:

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

4. Hybrid Cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public).

5-4-3 principles- 3 Service Offerings

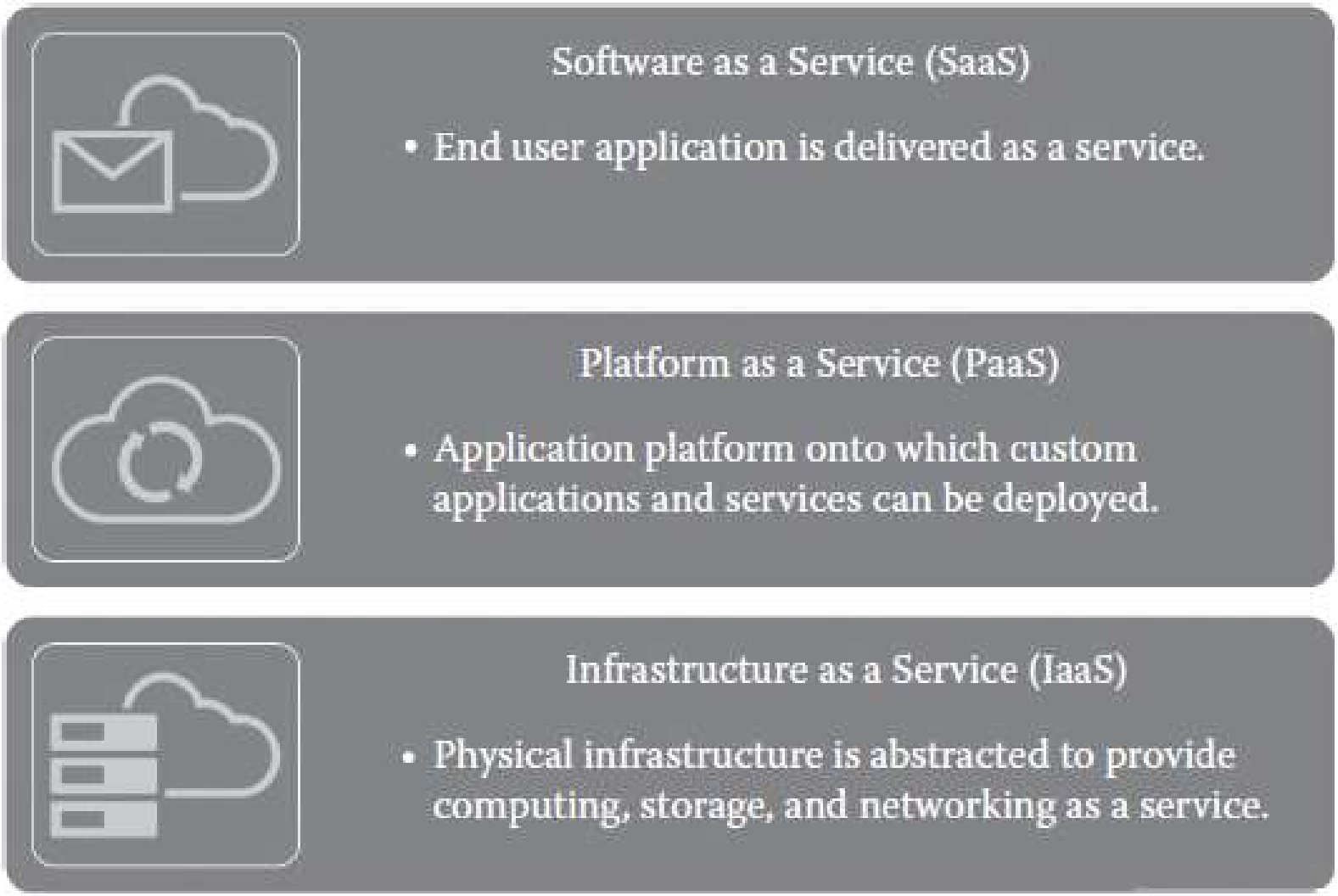
3 Service Offering Models:

The three kinds of services with which the cloud-based computing resources are available to end customers are as follows: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). It is also known as the service–platform–infrastructure (SPI) model of the cloud

- SaaS (Software As A Service)
- PaaS (Platform As A Service)
- IaaS (Infrastructure As A Service)

5-4-3 principles- 3 Service Offerings

SPI (Service-Platform-Infrastructure) Model of Cloud:



Introduction

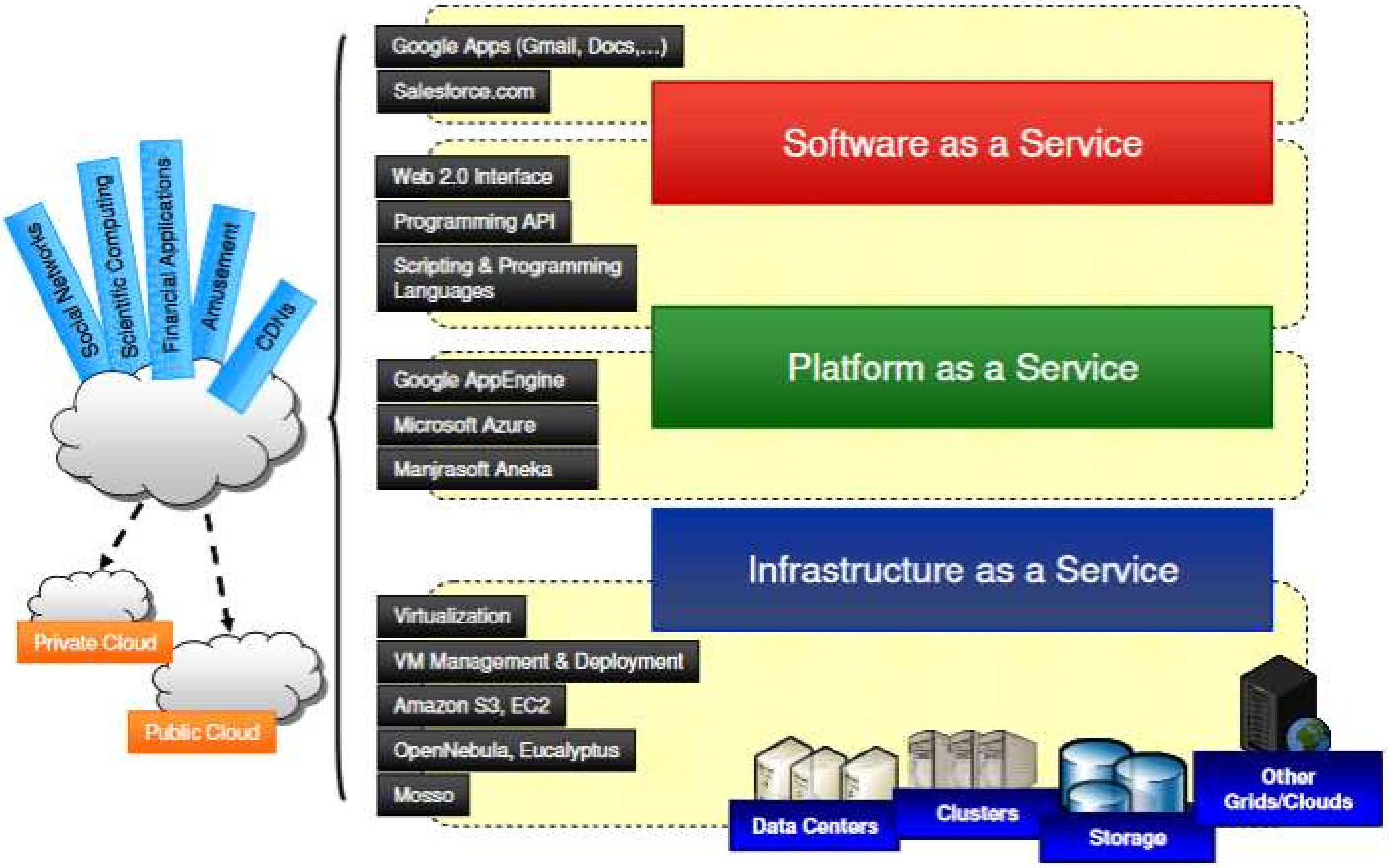
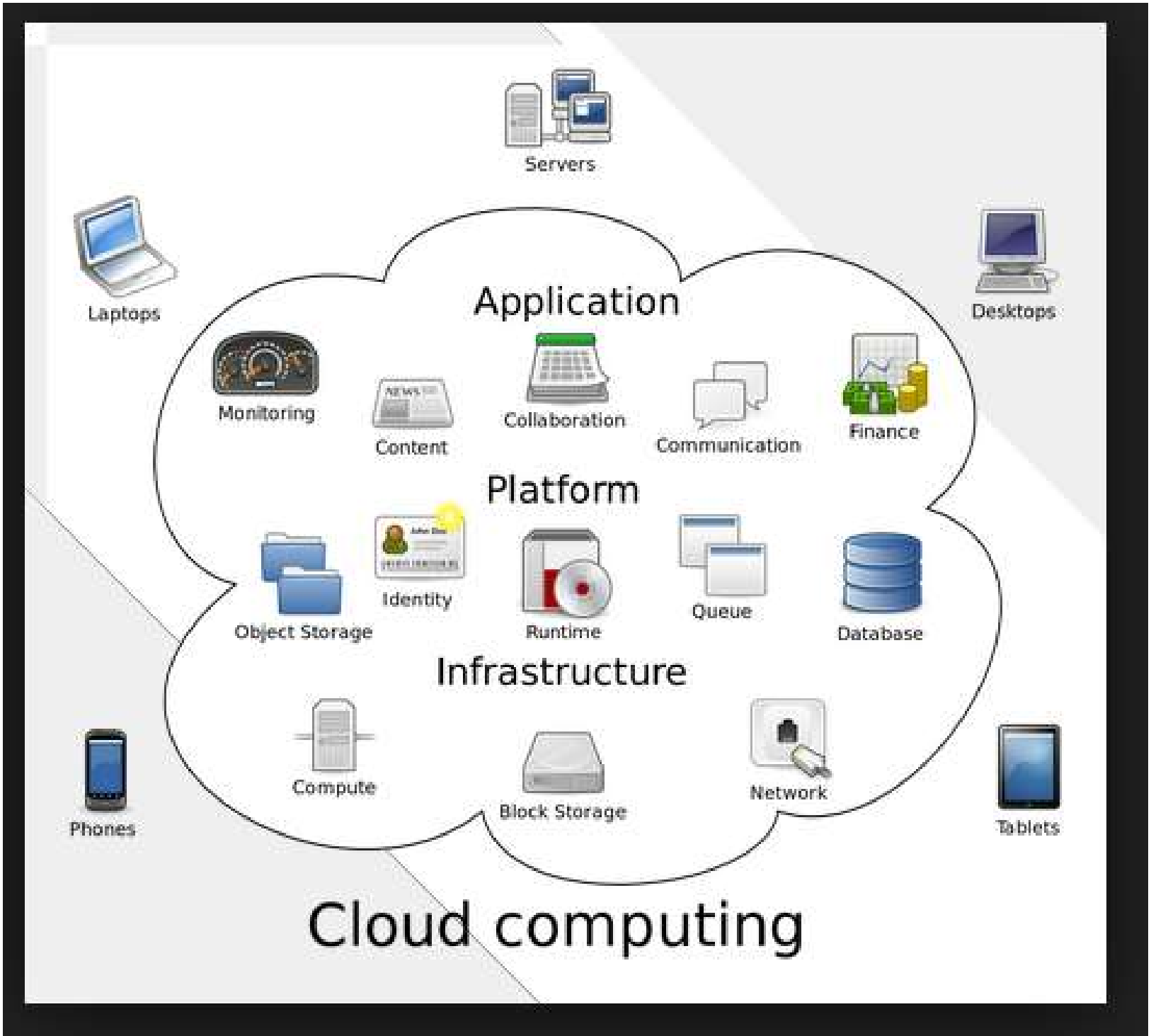


Figure 1. Cloud Computing architecture.


Servers
Laptops
Desktops
Application
Monitoring
Content
Collaboration
Communication
Finance
Platform
Identity
Object Storage
Runtime
Queue
Database
Infrastructure
Compute
Block Storage
Network
Phones
Tablets
Cloud computing

5-4-3 principles- 3 Service Offerings

3 Service Offering Models:

SaaS is a software distribution model in which applications (software, which is one of the most important computing resources) are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

PaaS is a paradigm for delivering operating systems and associated services (e.g., computer aided software engineering [CASE] tools, integrated development environments [IDEs] for developing software solutions) over the Internet without downloads or installation.

IaaS involves outsourcing the equipment used to support operations, including storage, hardware, servers, and networking components.

5-4-3 principles- 3 Service Offerings

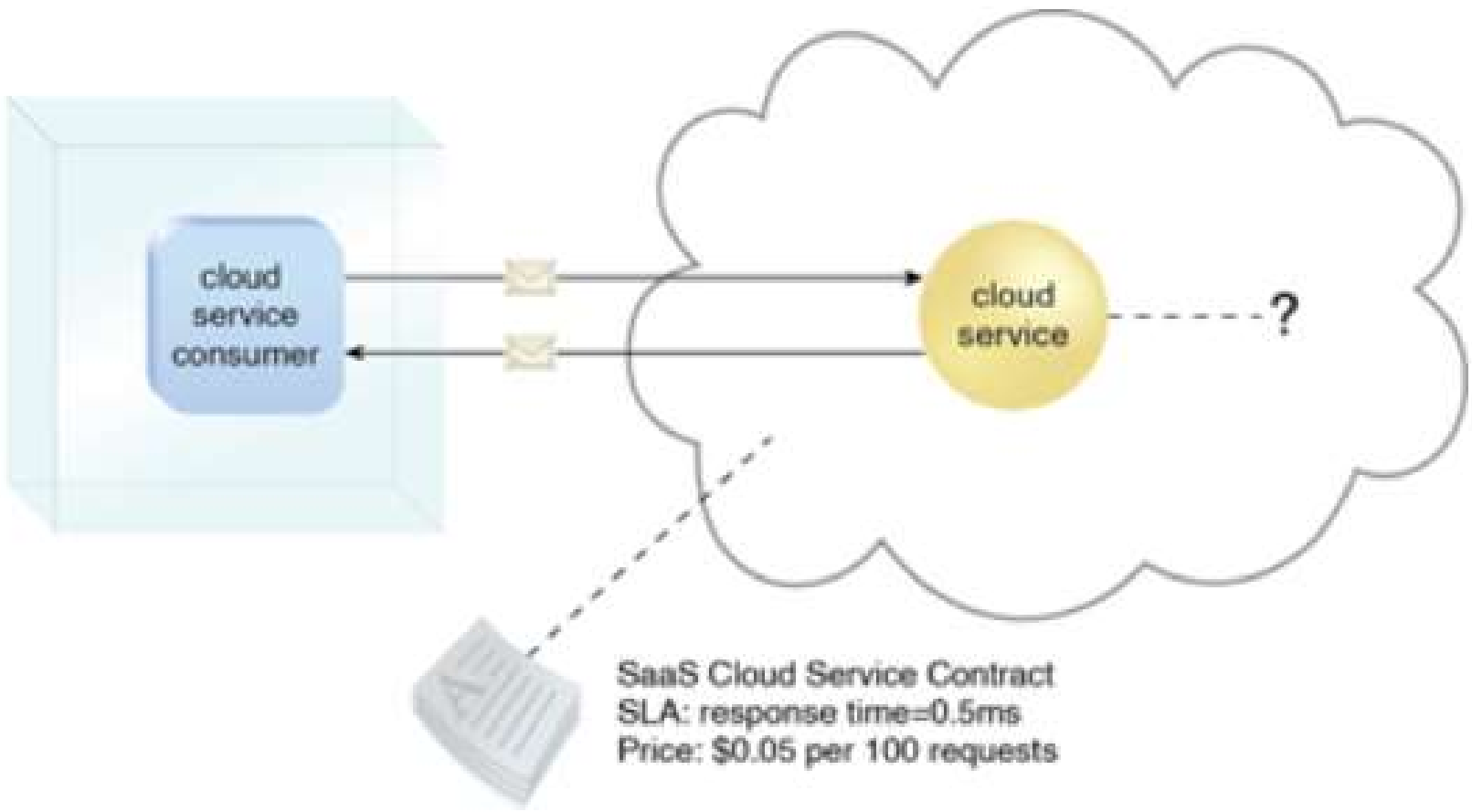
3 Service Offering Models:

1. Cloud SaaS: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure, including network, servers, operating systems, storage, and even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The consumer does not manage or control the underlying cloud infrastructure.
- Typical applications offered as a service include customer relationship management (CRM), business intelligence analytics, and online accounting software.

SaaS

- A software program positioned as a shared, reusable cloud service.
- Google Docs, Yahoo Mail, Google Maps.



5-4-3 principles- 3 Service Offerings

3 Service Offering Models:

Cloud PaaS:

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

The consumer does not manage or control the underlying cloud infrastructure but has control over the deployed applications and possibly configuration settings for the application-hosting environment. In other words, it is a packaged and ready-to-run development or operating framework.

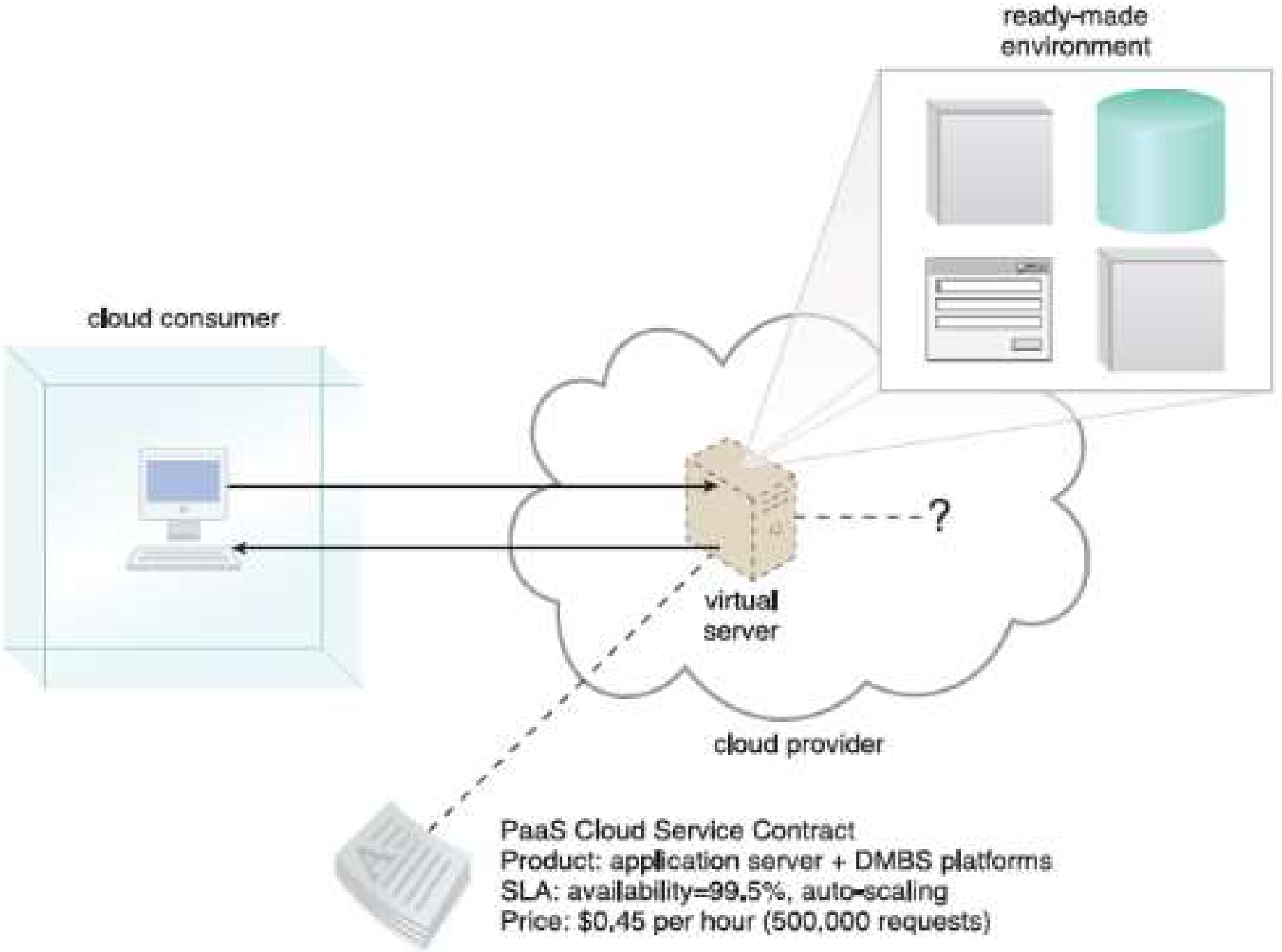
The PaaS vendor provides the networks, servers, and storage and manages the levels of scalability and maintenance.

The client typically pays for services used. Examples of PaaS providers include Google App Engine and **Microsoft Azure Services.**

PaaS

- PaaS represents a pre-defined "ready-to-use" environment typically comprised of already deployed and configured IT resources.
  - predefined Network, Storage, Computing services
  - predefined ways of using them
  - predefined development environments. (Java Runtime, .NET Runtime, DBMS platforms, IIS Server, Tomcat Server)
  -

PaaS


ready-made
environment
cloud consumer
?
virtual
server
cloud provider
PaaS Cloud Service Contract
Product: application server + DMBS platforms
SLA: availability=99,5%, auto-scaling
Price: $0,45 per hour (500.000 requests)

5-4-3 principles- 3 Service Offerings

3 Service Offering Models:

Cloud IaaS:

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources on a pay-per-use basis where he or she is able to deploy and run arbitrary software, which can include operating systems and applications.

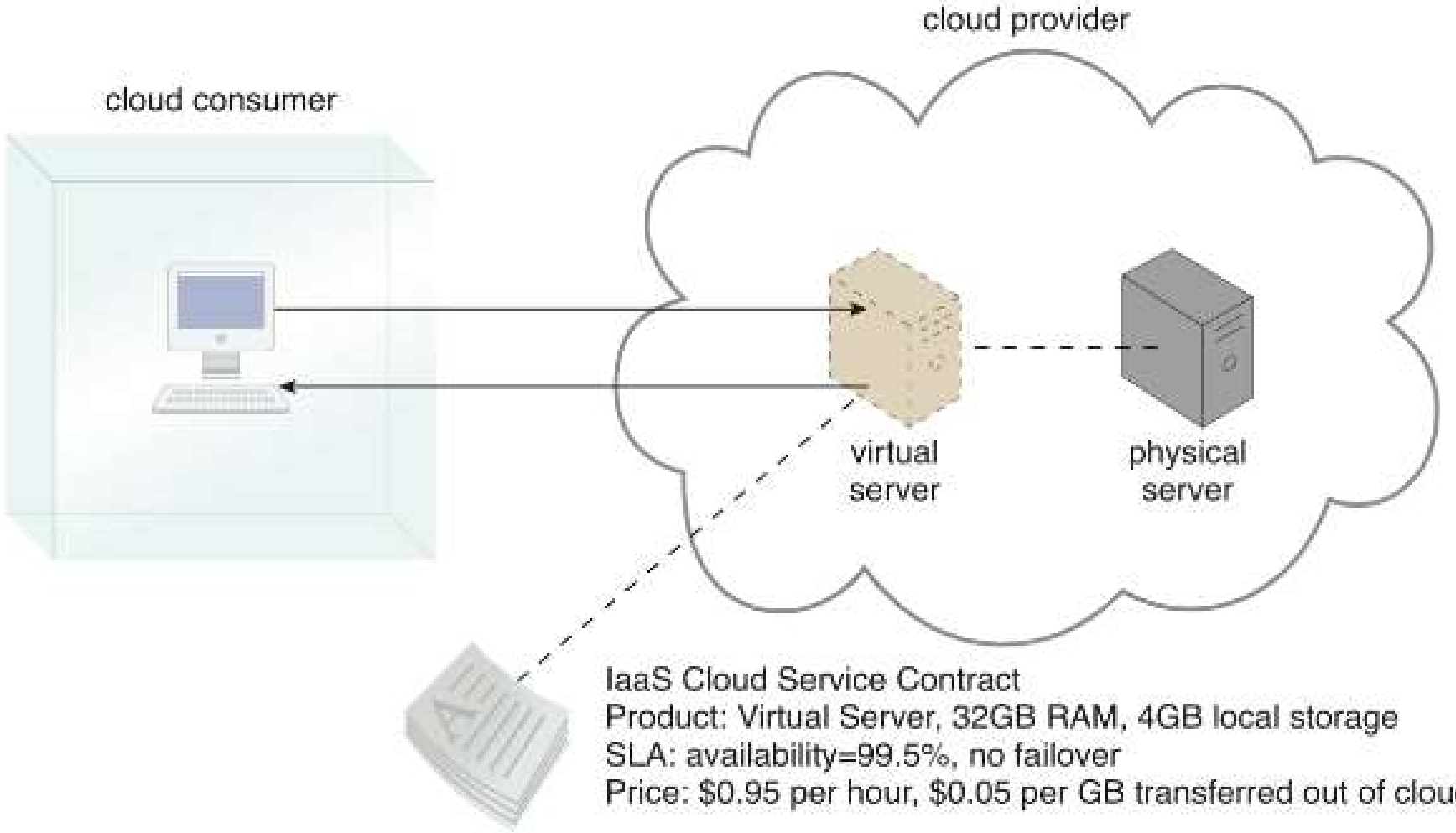
The consumer does not manage or control the underlying cloud infrastructure but has control over the operating systems, storage, and deployed applications and possibly limited control of select networking components (e.g., host firewalls).

The service provider owns the equipment and is responsible for housing, cooling operation, and maintenance.

Amazon Web Services (AWS) is a popular example of a large IaaS provider.

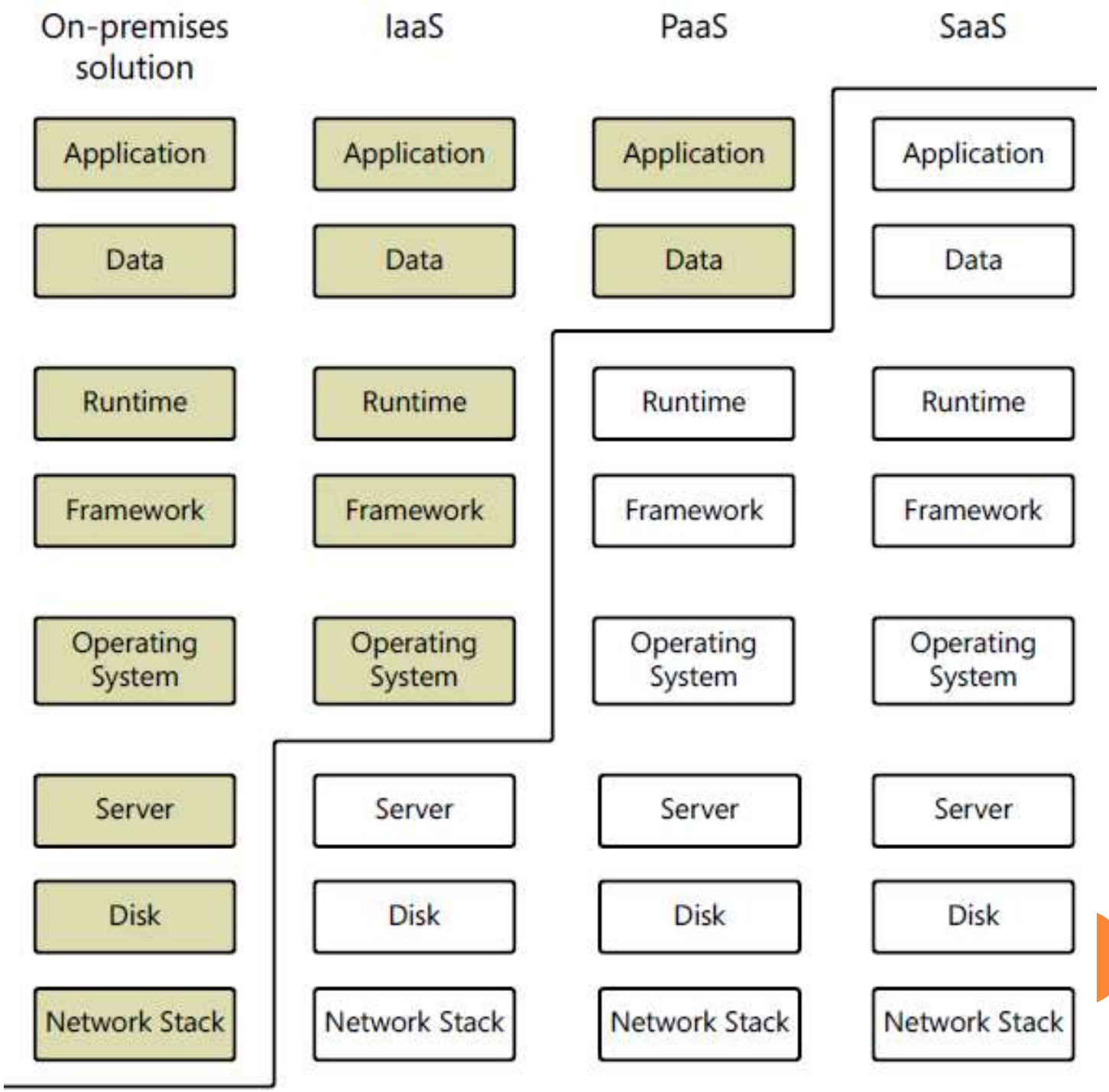
The major difference between PaaS and IaaS is the amount of control that users have. In essence, PaaS allows vendors to manage everything, while IaaS requires more management from the customer side. (see next slide ..)

Iaas


cloud provider
cloud consumer
virtual
server
physical
server
IaaS Cloud Service Contract
Product: Virtual Server, 32GB RAM, 4GB local storage
SLA: availability=99.5%, no failover
Price: $0.95 per hour, $0.05 per GB transferred out of cloud

Cloud Services defined

Responsibility of you and the vendor is shown in the diagram



Cloud Ecosystem

Cloud Eco System

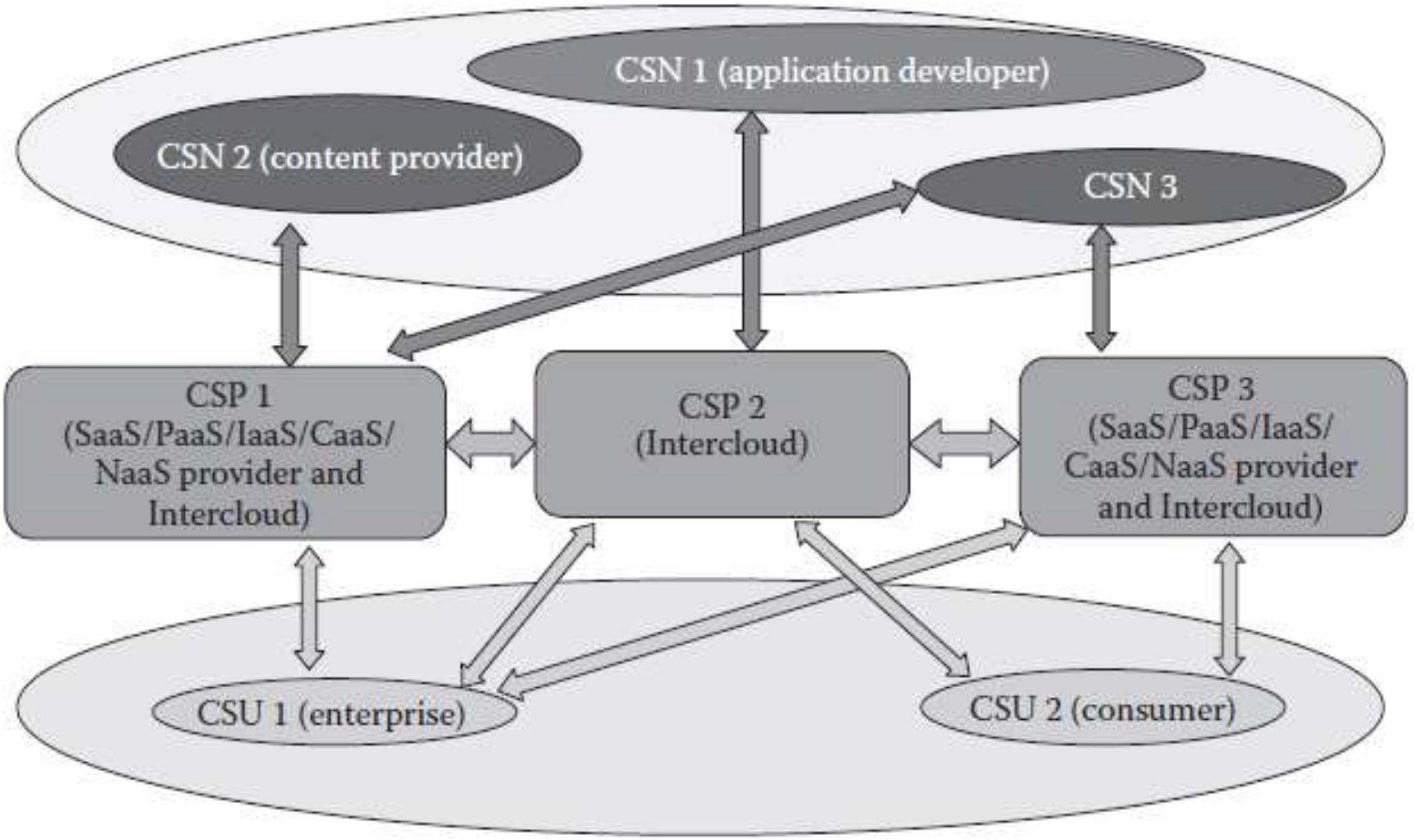


FIGURE 2.4
Actors with some of their possible roles in a cloud ecosystem.

Requirements for Cloud Service

Requirements for Cloud Service

- ***Multitenancy***
  - *Maximizes the resource sharing,*
  - *Supports horizontal scaling*
- ***Service life cycle management***
  - Automatic service provisioning with metering and charging or billing settlement needs to be provided for services that are dynamically created, modified, and then released in virtual environments.
- ***Security***
  - The security of each individual service needs to be protected in the multitenant cloud environment.
  - Cloud provides strict control for tenants' service access to different resources
- ***Responsiveness***
  - The cloud ecosystem is expected to enable early detection, diagnosis, and fixing of service-related problems in order to help the customers use the services faithfully.
- ***Intelligent service deployment***
  - It is expected that the cloud enables efficient use of resources in service deployment, that is, maximizing the number of deployed services while minimizing the usage of resources and still respecting the SLAs (Service Level Agreement)

Requirements for Cloud Service contd…

- ***Portability***
  - It is expected that a cloud service supports the portability of its features over various underlying resources and that CSPs should be able to accommodate cloud workload portability (e.g., **VM portability**) with limited service disruption.
- ***Interoperability***
- It is expected to have available well-documented and well-tested specifications that allow heterogeneous systems in cloud environments to work together

- ***Regulatory aspects***
- All applicable regulations shall be respected, including privacy protection.

- ***Environmental sustainability***
- optimizing energy consumption
- Accessing on-demand shared pools of configurable resources that can be rapidly provisioned and released from different devices with minimal energy consumption.

Requirements for Cloud Service contd…

- ***Service reliability, service availability, and quality assurance***
- CSUs demand for their services end-to-end quality of service (QoS) assurance, high levels of reliability, and continued availability to their CSPs.

- ***Service access***
- A cloud infrastructure is expected to provide CSUs with access to cloud services from any user device. It is expected that CSUs have a consistent experience when accessing cloud services.

- ***Flexibility***
- It is expected that the cloud service be capable of supporting multiple cloud deployment models and cloud service categories
- ***Accounting and charging***
- It is expected that a cloud service be capable to support various accounting and charging models and policies.
- ***Massive data processing***
- It is expected that a cloud supports mechanisms for massive data processing (e.g., extracting, transforming, and loading data). It is worth to note in this context that distributed and/

Cloud Service Requirements

IaaS service requirements:

- **Computing hardware requirements** (including processing, memory, disk, network interfaces, and virtual machines)
- **Computing software requirements** (including OS and other preinstalled software)
- **Storage requirements** (including storage capacity)
- **Network requirements** (including QoS specifications, such as bandwidth and traffic volumes)
- **Availability requirements** (including protection/backup plan for computing, storage, and network resources)

PaaS service requirements:

- Requirements similar to those of the IaaS category
- Deployment options of user-created applications (e.g., scale-out options)

SaaS service requirements:

- Application-specific requirements (including licensing options)
- Network requirements (including QoS specifications such as bandwidth and traffic volumes)

Cloud Computing benefits

- *Achieve economies of scale*
- *Reduce spending on technology infrastructure*
- *Globalize the workforce*:
- *Streamline business processes*
- *Reduce capital costs*
- *Pervasive accessibility*
- *Monitor projects more effectively*
- *Less personnel training is needed*
- *Minimize maintenance and licensing software*
- *Improved flexibility*

Cloud Computing Drawbacks

- Dependency on Internet Connectivity
- *Security Concerns*
- Depending on the cloud vendor or provider, customers may face restrictions on the availability of applications, operating systems, and infrastructure options.
- All development platforms may not be available in the cloud due to the fact that the cloud vendor may not aware of such solutions.
- Interoperabebility of Applications

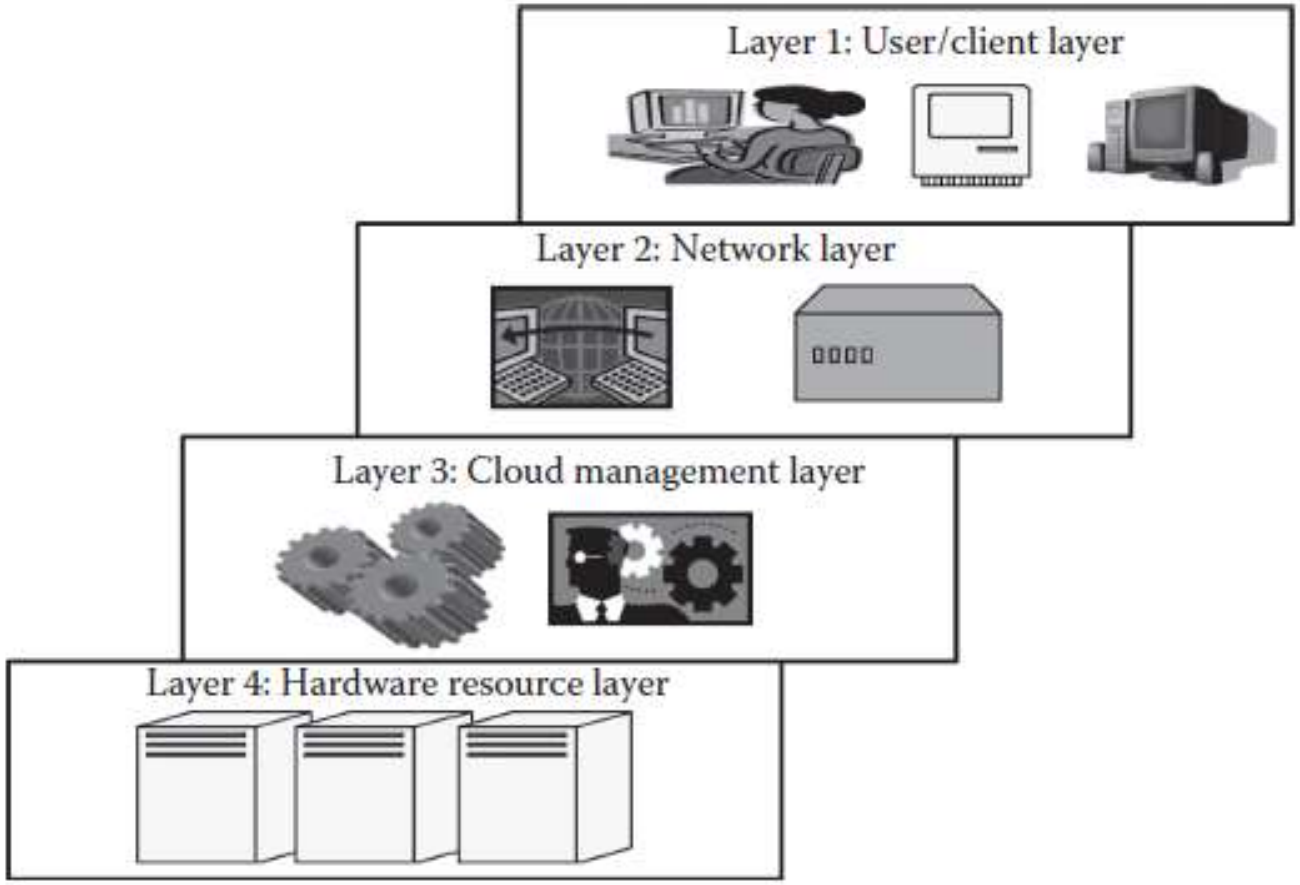
Cloud Architecture, Anatomy of the Cloud, Network Connectivity in Cloud, Applications on the Cloud, Managing the Cloud

Cloud Architecture

Cloud Architecture

- Is an hierarchical view of describing the technology.
- Describes its working mechanism of cloud
- Cloud Architecture includes the dependencies on which it works and the components that work over it.
- The cloud architecture can be divided into **four layers** based on the access of the cloud by the user.

Cloud Architectu



Thin & Thick Clients

A **thick client** is a computer in client–server architecture or networks that typically provides broad functionality independent of the central server. Originally known as just a "client" or "fat client", the name is contrasted to **thin client**, which describes a computer heavily dependent on a server's applications.

A Thick client still requires at least periodic connection to a network or central server, but is often characterised by the ability to perform many functions without that connection. In contrast, a thin client generally does as little processing as possible and relies on accessing the server each time input data needs to be processed or validated.

Cloud Architecture

- The cloud architecture can be divided into **four layers** based on the access of the cloud by the user.
- *Layer 1 (User / Client Layer)*
- Layer 2 (Network Layer)
- Layer 3 (Cloud Management Layer)
- Layer 4 (Hardware Resource Layer)

Layer 1 (User / Client Layer):

All the users or client belong to this layer. This is the place where the client/user initiates the connection to the cloud.

- The client can be any device such as a thin client, thick client, or mobile or any handheld device that would support basic functionalities to access a web application.
- **The thin client** here refers to a device that is completely dependent on some other system for its complete functionality. In simple terms, they have very low processing capability. (Ex: Browsers, Office 365, Google Docs etc…)
- **Thick clients** are general computers that have adequate processing capability. They have sufficient capability for independent work. Usually, a cloud application can be accessed in the same way as a web application.
- ***Note:*** A cloud application can be accessed in the same way as a web application. But internally, the properties of cloud applications are significantly different .

Cloud Architecture

Layer 2(Network Layer):

- This layer allows the users to connect to the cloud.
- The whole cloud infrastructure is dependent on this connection where the services are offered to the customers.
- This is primarily the Internet in the case of a public cloud.
- The public cloud usually exists in a specific location and the user would not know the location as it is abstract and the public cloud can be accessed all over the world.
- In the case of a private cloud, the connectivity may be provided by a local area network (LAN).
- When accessing the public or private cloud, the users require minimum bandwidth, which is sometimes defined by the cloud providers.

Layer 3 (Cloud Management Layer):

- This layer consists of softwares that are used in managing the cloud. The softwares can be **a cloud operating system (OS),** a software that acts as an interface between the data center (actual resources) and the user, **or a management software** that allows managing resources.
- These softwares usually allow resource management (scheduling, provisioning, etc.), optimization and internal cloud governance.
- **This layer comes under the scope of SLAs** (Service Level Agreement), that is, the operations taking place in this layer would affect the SLAs that are being decided upon between the users and the service providers.

Cloud Architecture

Layer 4 (Hardware Resource Layer):

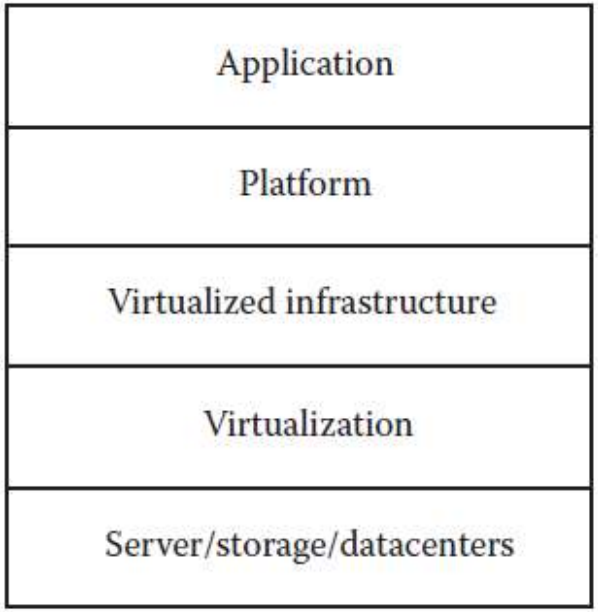
- Layer 4 consists of provisions for actual hardware resources.
- In the case of a public cloud, a data center is used in the back end. In private cloud, it can be a data center.
- **This layer comes under the scope of SLAs.**
- The data center consists of a high-speed network connection and a highly efficient algorithm to transfer the data from the data center to the manager. There can be a number of data centers.

Anatomy of Cloud

Anatomy of a cloud

- Cloud anatomy can be simply defined as the structure of the cloud. Cloud anatomy cannot be considered the same as cloud architecture.
- It may not include any dependency on which or over which the technology works,
- **whereas architecture wholly defines and describes the technology over which it is working.**
- Architecture is a hierarchical structural view that defines the technology as well as the technology over which it is dependent or/and the technology that are dependent on it.
- **anatomy can be considered as a part of architecture**

It depends on the person to choose the depth of description of the cloud. A different view of anatomy is given

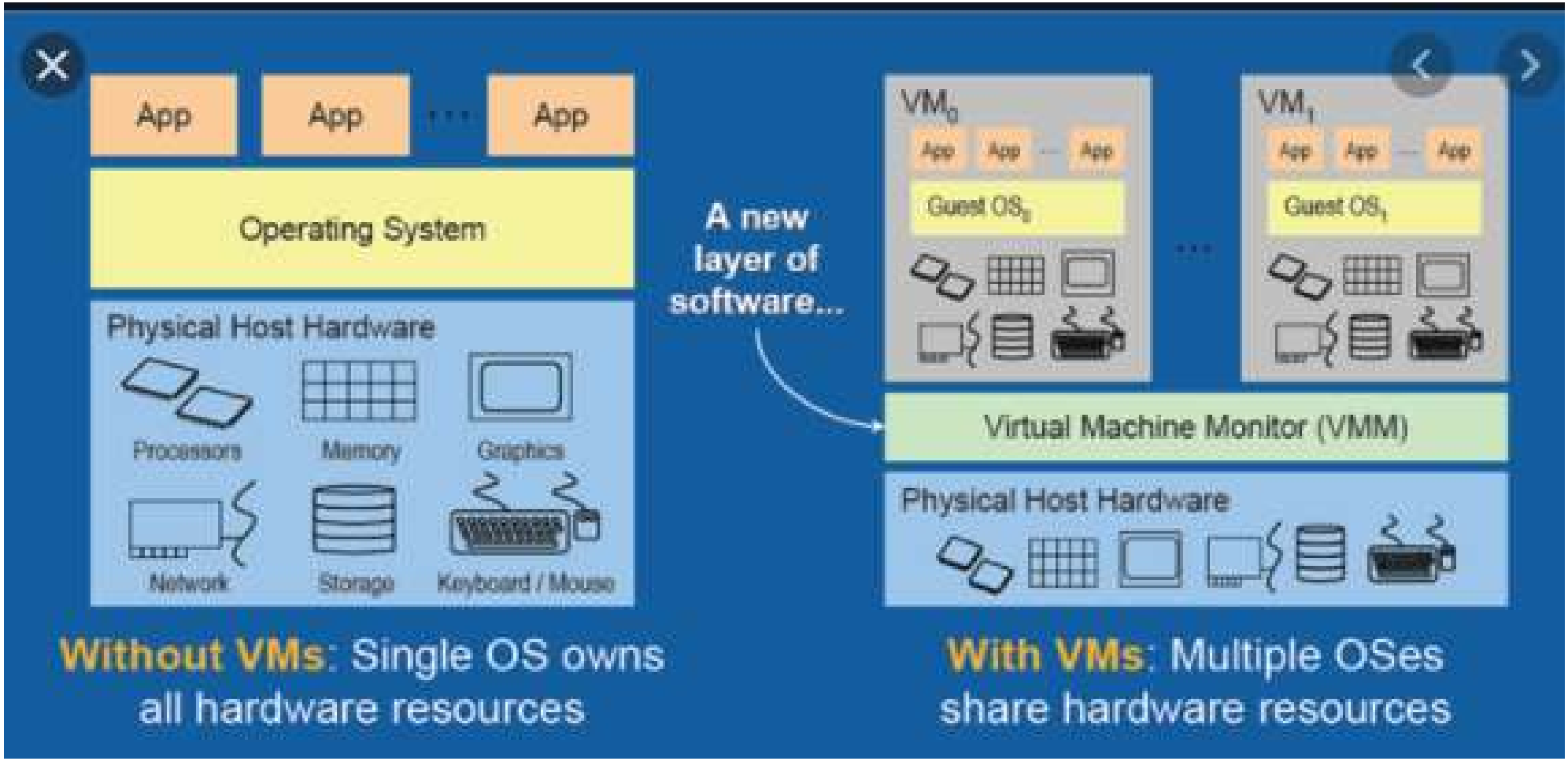


Anatomy of a cloud… contd
Cloud Components

- There are basically **five components of the cloud:**

- 1. *Application*: The upper layer is the application layer. In this layer, any applications are executed.
- 2. *Platform*: This component consists of platforms that are responsible for the execution of the application. This platform is between the infrastructure and the application.
- 3. *Infrastructure*: The infrastructure consists of resources over which the other components work. This provides computational capability to the user.
- 4. *Virtualization*: Virtualization is the process of making logical components of resources over the existing physical resources. The logical components are isolated and independent, which form the infrastructure.
- 5. *Physical hardware*: The physical hardware is provided by server and storage units.

Virtualization



Network Connectivity in Cloud Computing, Applications on the Cloud

Network Connectivity in CC

- Cloud computing is a technique of resource sharing where servers, storage, and other computing infrastructure in multiple locations are connected by networks.
- For many cloud computing applications, network performance will be the key issue to cloud computing performance.
- Based on different deployment models, options for networking are:
  - Public Cloud Access Networking
  - Private Cloud Access Networking
  - Intracloud Networking for Public Cloud Services
  - Private Intracloud Networking

Public Cloud Access Networking:

- In this option, the connectivity is often through the Internet, though some cloud providers may be able to support virtual private networks (VPNs) for customers.
- Accessing public cloud services will always create issues related to security, which in turn is related to performance.
- If we want to reduce the delay without compromising security, then we have to select a suitable routing method such as the one reducing the delay by minimizing transit *hops* in the end-to-end connectivity between the cloud provider and cloud consumer.

Network Connectivity in CC

Private Cloud Access Networking:

In the private cloud deployment model, since the cloud is part of an organizational network, the technology and approaches are local to the in-house network structure.

This may include an Internet VPN or VPN service from a network operator.

Intracloud Networking for Public Cloud Servi:ce:

- Here, the resources of the cloud provider and thus the cloud service to the customer are based on the resources that are geographically apart from each other but still connected via the Internet.
- Public cloud computing networks details are internal to the service provider and thus not visible to the user/customer

Private Intracloud Networking:

- Private intracloud networking is usually supported over connectivity between the major data center sites owned by the company.
- At a minimum, all cloud computing implementations will rely on intracloud networking to link users with the resource to which their application was assigned.

Applications on the Cloud

1. **Stand Alone Applications**
2. **Web Applications**
3. **Cloud Applications**

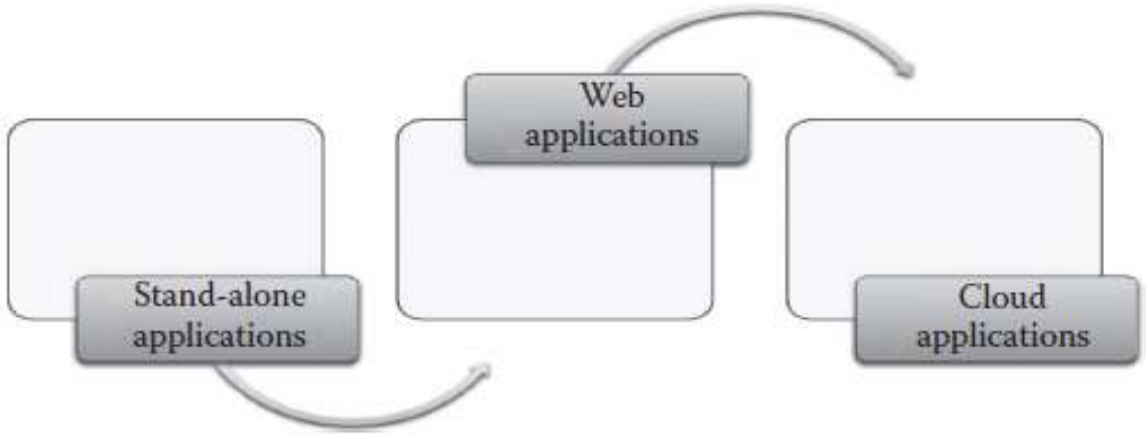
Stand Alone Applications:

- A stand-alone application is developed to be run on a single system that does not use network for its functioning.
- These stand-alone applications use only the machine in which they are installed.
- The functioning of these kinds of systems is totally dependent on the resources or features available within the system.
- These systems do not need the data or processing power of other systems; they are self-sustaining

Applications on the Cloud

Web Applications:

- client server architecture is followed by the web applications
- Unlike stand-alone applications, these systems were totally dependent on the network for its working.
- Here, there are basically two components, called as the client and the server.
- The server is a high-end machine that consists of the web application installed.
- This web application is accessed from other client systems.
- The client can reside anywhere in the network. It can access the web application through the Internet.



Applications on the Cloud

Web Applications defects:

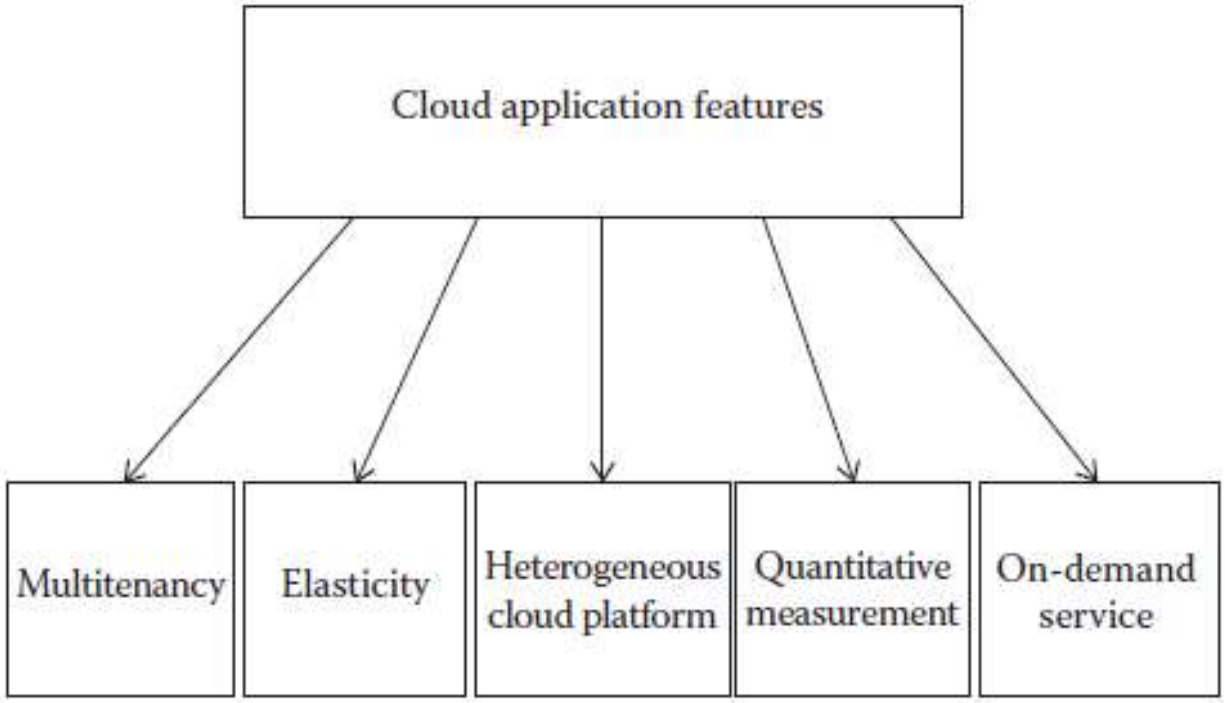
1. The web application is not elastic and cannot handle very heavy loads, that is, it cannot serve highly varying loads.
2. The web application is not multitenant.
3. The web application does not provide a quantitative measurement of the services that are given to the users, though they can monitor the user.
4. The web applications are usually in one particular platform.
5. The web applications are not provided on a pay-as-you-go basis; thus, a particular service is given to the user for permanent or trial use and usually the timings of user access cannot be monitored.
6. Due to its nonelastic nature, peak load transactions cannot be handled.

Cloud Applications

3. Cloud Applications:

to solve the mentioned problems with web applications, the cloud applications were developed.

- A cloud application is different from other applications; they have unique features.
- A cloud application usually can be accessed as a web application but its properties differ.



Cloud Application Features

- *Multitenancy*
- *Elasticity*
- *Heterogeneous cloud platform*
- *Quantitative measurement*
- *On-demand service*

Multitenancy: *The software can be shared by different users with full independence. Here, independence refers to logical independence.*

Elasticity: *Elasticity can be defined as the degree to which a system is able to adapt to workload changes by provisioning and deprovisioning resources in an autonomic manner such that at each point in time, the available resources match the current demand as closely as possible.*

Heterogeneous cloud platform: *The cloud platform supports heterogeneity, wherein any type of application can be deployed in the cloud.*

Quantitative measurement: *The services provided can be quantitatively measured. The user is usually offered services based on certain charges. the application or resources are given as a utility on a pay-per-use basis.*

On-demand service: *The cloud applications offer service to the user, on demand, that is, whenever the user requires it.*

Managing the Cloud

Managing the Cloud

- Cloud management is aimed at efficiently managing the cloud so as to maintain the QoS.
- The whole cloud is dependent on the way it is managed. Cloud management can be divided into two parts:
  1. Managing the infrastructure of the cloud
  2. Managing the cloud application

1. Managing the Cloud infrastructure :

- A cloud infrastructure is a very complex system that consists of a lot of resources. These resources are usually shared by several users.
- The infrastructure of the cloud is considered to be the backbone of the cloud. This component is mainly responsible for the QoS factor. If the infrastructure is not properly managed, then the whole cloud can fail and QoS would be adversely affected.
- The core of cloud management is resource management. Resource management involves several internal tasks such as resource **scheduling, provisioning, and load balancing**. These tasks are performed by cloud OS.

1. Managing the Cloud Infrastructure

- Poor resource management may lead to several inefficiencies in terms of **performance, functionality, and cost.**
- **Performance:** is the most important aspect of the cloud, because everything in the cloud is dependent on the SLAs and the SLAs can be satisfied only if performance is good.
- The basic **functionality** of the cloud should always be provided and considered at any cost. Even if there is a small discrepancy in providing the functionality, the whole purpose of maintaining the cloud will not serve the purpose. A partially functional cloud would not satisfy the SLAs.
- **Cost:** The cost is a very important criterion as far as the business prospects of the cloud are concerned.
- If the cost of resource management is high, then definitely the cost of accessing the resources would be high and there is never a lossy business from any organization and so the service provider would not bear the cost and hence the users have to pay more.
- Efficient resource management with less cost is required.
- **Power consumption and optimization:** consolidation of server and storage workloads. Consolidation would reduce the energy consumption and in some cases would increase the performance of the cloud.
- **Load fluctuation:** predictable and unpredictable workload fluctuations
  - The cloud can be preconfigured for handling such kind of fluctuations.

2. Managing the Cloud Application

- Business companies are increasingly looking to move or build their corporate applications on cloud platforms to improve agility or to **meet dynamic requirements** that exist in the globalization of businesses and responsiveness to market demands
- Shifting or moving the applications to the cloud environment brings new complexities. Applications become more composite and complex, which requires leveraging not only capabilities like ***storage and database*** offered by the cloud providers but also **third-party SaaS capabilities like e-mail and messaging.**
- So, understanding the availability of an application requires inspecting the infrastructure, the services it consumes, and the upkeep of the application.
- The composite nature of cloud applications requires visibility into all the services to determine the **overall availability and uptime.**
- Cloud application management is to address these issues and propose solutions to make it possible to have insight into the application that runs in the cloud, as well as implement or **enforce enterprise policies** like governance and auditing and environment management while the application is deployed in the cloud.
- These **cloud-based monitoring and management services** can collect a multitude of events, analyze them, and identify critical information that requires additional remedial actions like adjusting capacity or provisioning new services.
- Application management has to be supported with **tools and processes** required for managing other environments that might coexist, enabling efficient operations.

Migrating Application to Cloud

1. phases
2. approaches

MIGRATING APPLICATION TO CLOUD

- Cloud migration encompasses moving one or more enterprise applications and their IT environments from the traditional hosting type to the cloud environment, either public, private, or hybrid.
- Cloud migration presents an opportunity to significantly reduce costs incurred on applications. This activity comprises, of different phases like **evaluation, migration strategy, prototyping, provisioning, and testing.**

Phases of Cloud Migration:

1. *Evaluation*
2. *Migration strategy*
3. *Prototyping*
4. *Provisioning*
5. *Testing*

Phases of Cloud Migration

1. Evaluation: Evaluation is carried out for all the components like

- Current infrastructure and
- Application Architecture,
- Environment in terms of Compute, Storage, Monitoring, and Management,
- SLAs,
- Operational Processes,
- Financial Considerations,
- Risk,
- Security,
- Compliance, and
- Licensing needs

are identified to build a business case for moving to the cloud.

2. Migration strategy: Based on the evaluation, a migration strategy is drawn—a hotplug strategy is used where the applications and their data and interface dependencies are isolated and these applications can be operationalized all at once.

OR

An application is partially migrated.

Phases of Cloud Migration

3. Prototyping:

Migration activity is preceded by a prototyping activity to validate and ensure that a **small portion of the applications are tested** on the cloud environment with test data setup.

4. Provisioning: **Premigration optimizations** identified are implemented.

- ✓ **Cloud servers** are provisioned for all the identified environments
- ✓ **Necessary platform softwares** and applications are deployed
- ✓ **Configurations** are tuned to match the new environment sizing
- ✓ **Databases and files** are replicated
- ✓ **All internal and external integration points** are properly configured
- ✓ **Web services, batch jobs, and operation and management software** are set up in the new environments

5. Testing: **Postmigration tests** are conducted to ensure that migration has been successful.

- ✓ Performance and Load testing
- ✓ Failure and Recovery testing
- ✓ Scale-out testing are conducted against the expected traffic load and resource utilization levels.

Approaches for Cloud Migration

Four Approaches for cloud migration:

1) *Migrate existing applications*
2) *Start from scratch*
3) *Separate company*
4) *Buy an existing cloud vendor*

1. Migrate existing applications:

Rebuild or rearchitect some or all the applications, taking advantage of some of the virtualization technologies around to accelerate the work.

2. Start from scratch:

Rather than confuse customers with choice, and tie up engineers trying to rebuild existing application, it may be easier to start again.

3. Separate company:

One may want to create a whole new company with separate brand, management, R&D, and sales. The investment and internet protocol (IP) may come from the existing company, but many of the conflicts disappear once a new *born in the cloud* company is established.

Approaches for Cloud Migration

4. Buy an existing cloud vendor:

For a large established vendor, buying a cloud-based competitor achieves two things. Firstly, it removes a competitor, and secondly, it enables the vendor to hit the ground running in the cloud space.

Chapter 2:
Cloud Deployment Models & Service Models

Chapter 2.1
Cloud Deployment Models

CLOAD DEPLOYMENT MODELS

- **The deployment models** are the different ways in which the cloud computing environment can be set up, that is, the several ways in which the cloud can be deployed.

- It is important to have an idea about the deployment models because setting up a cloud is the most basic requirement prior to starting any further study about cloud computing. Cloud computing is business oriented.

- A model should be selected based on the **needs, requirements, budget, and security.**
- A wrong decision in the deployment model may affect the organization heavily.
- There are many users of the cloud, and each user has different needs. One deployment model will not suite all the cloud users. Based on the cloud setup, the properties of the cloud change.

CLOAD DEPLOYMENT MODELS

4 types of Deployment Models:

1. Private cloud
2. Public cloud
3. Community cloud
4. Hybrid cloud

Private Cloud:

- According to the National Institute of Standards and Technology (NIST), private cloud can be defined as the cloud infrastructure that is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).
- It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises
- The private cloud in simple terms is the cloud environment created for a single organization. It is usually private to the organization but can be managed by the organization or any other third party.
- Private cloud can be deployed using Opensource tools such as Openstack, Eucalyptus.
- The private cloud is small in size as compared to other cloud models. Here, the cloud is deployed and maintained by the organizations itself.

CLOAD DEPLOYMENT MODELS

1. Private cloud

a) Characteristics

b) Suitability

c) On-Premise Private Cloud

- ✓ Issues

d) Outsourced Private Cloud

- ✓ Issues

e) Advantages

f) Disadvantages

Cloud Deployment Models - Private Cloud

Private Cloud

Characteristics:

1. Secure

The private cloud is secure. This is because usually the private cloud is deployed and managed by the organization itself, and hence there is least chance of data being leaked out of the cloud.

2. Central control

The organization mostly has full control over the cloud as usually the private cloud is managed by the organization itself. Thus, when managed by the organization itself, there is no need for the organization to rely on anybody.

3. Weak SLAs

Formal SLAs may or may not exist in a private cloud. But if they exist they are weak as it is between the organization and the users of the same organization. Thus, high availability and good service may or may not be available. This depends on the organization that is controlling the cloud.

Private Cloud

Advantages:

- The cloud is small in size and is easy to maintain.
- It provides a high level of security and privacy to the user.
- It is controlled by the organization.

Disadvantages:

- For the private cloud, budget is a constraint.
- The private clouds have loose SLAs.

Private Cloud

Suitability:

Suitability refers to the instances where this cloud model can be used. It also signifies the most **suitable conditions and environment where this cloud model can be used**, such as the following:

- The organizations or enterprises that require a separate cloud for their personal or official use.
- The organizations or enterprises that have a sufficient amount of funds as managing and maintaining a cloud is a costly affair.
- The organizations or enterprises that consider data security to be important.
- The organizations that want autonomy and complete control over the cloud.
- The organizations that have a less number of users.
- The organizations that have prebuilt infrastructure for deploying the cloud and are ready for timely maintenance of the cloud for efficient functioning.
- Special care needs to be taken and resources should be available for troubleshooting.

Private Cloud

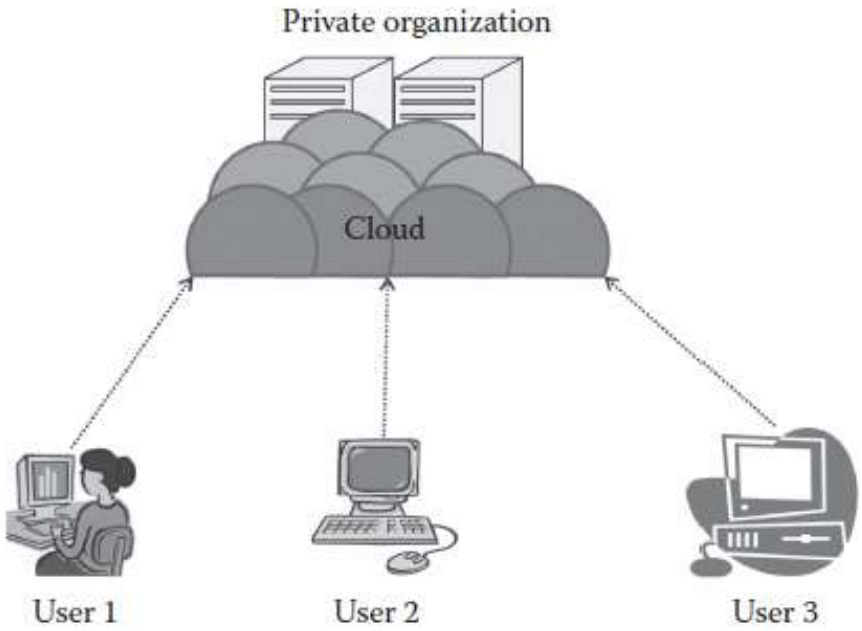
Not suitable conditions:

- The organizations that have high user base
- The organizations that have financial constraints
- The organizations that do not have prebuilt infrastructure
- The organizations that do not have sufficient manpower to maintain and manage the cloud

Private Cloud

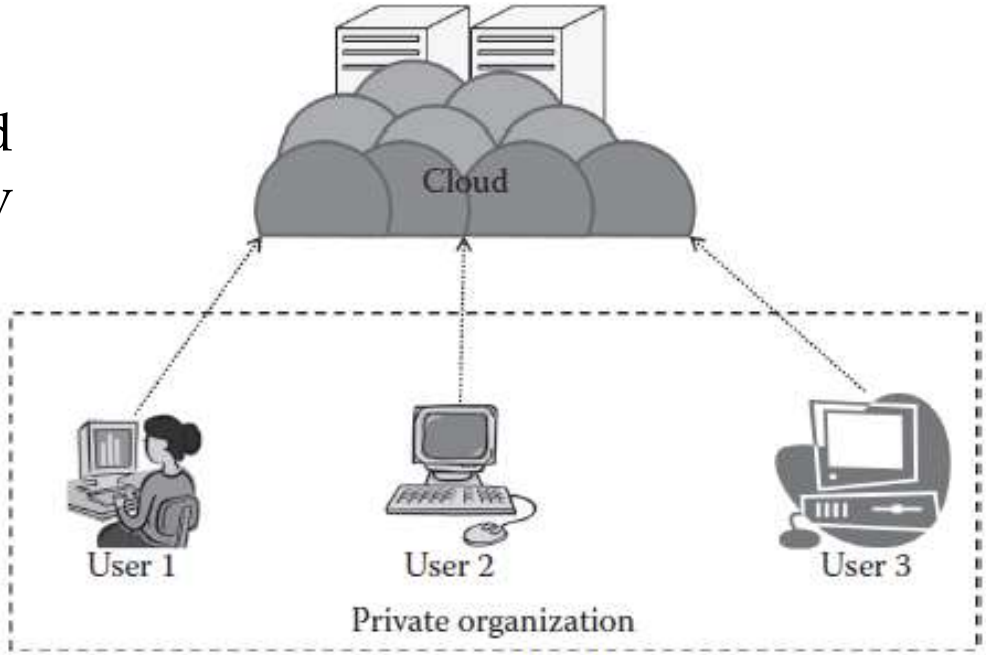
On primises private cloud:

On-premise private cloud is a typical private cloud that is managed by a single organization. Here, the cloud is deployed in organizational premises and is connected to the organizational network.



Outsourced private cloud:

The outsourced private cloud has a cloud outsourced to a third party. A third party manages the whole cloud.



Private Cloud - Issues

Issues: handling in Private Cloud:

SLAs:

- For any cloud to operate, there must be certain agreements between the user and the service provider. The service provider will agree upon certain terms and conditions regarding the service delivery.

- These terms and conditions need to be strictly followed; if not, there will be a penalty on the part of the defaulting party. If the service provider fails to provide services as per the SLA, then he has to pay a penalty to the user;

Network:

- The cloud is totally dependent on the network that is laid out. The network usually consists of a high bandwidth and has a low latency.

Performance:

- The performance of a cloud delivery model primarily depends on the network and resources. Since here the networks are managed internally, the performance can be controlled by the network management team, and mostly this would have good performance as the number of resources is low.

Private Cloud - Issues

Issues : handling in Private Cloud:

Security and Data Privacy:

- *Security and data privacy*: Security and data privacy, though a problem with every type of service model, affect the private cloud the least.
- As the data of the users are solely managed by the company and most of the data would be related to the organization or company, here there is a lesser chance that the data will be leaked to people outside as there are no users outside the organization.

- Hence, comparatively, the private cloud is more resistant to attacks than any other cloud type purely because of the type of users and local area network. But, security breaches are possible if an internal user misuses the privileges.

Location:

- The private cloud does not have any problems related to the location of data being stored. In a private cloud, the data are internal and are usually stored in the same geographical location where the cloud users, that is, organization, are present (on-premise cloud).

Cloud Management:

- This involves several tasks such as resource scheduling, resource provisioning, and resource management.
- The network is small, and the numbers of users and the amount of resources are less.

Private Cloud - Issues

Issues: handling in Private Cloud:

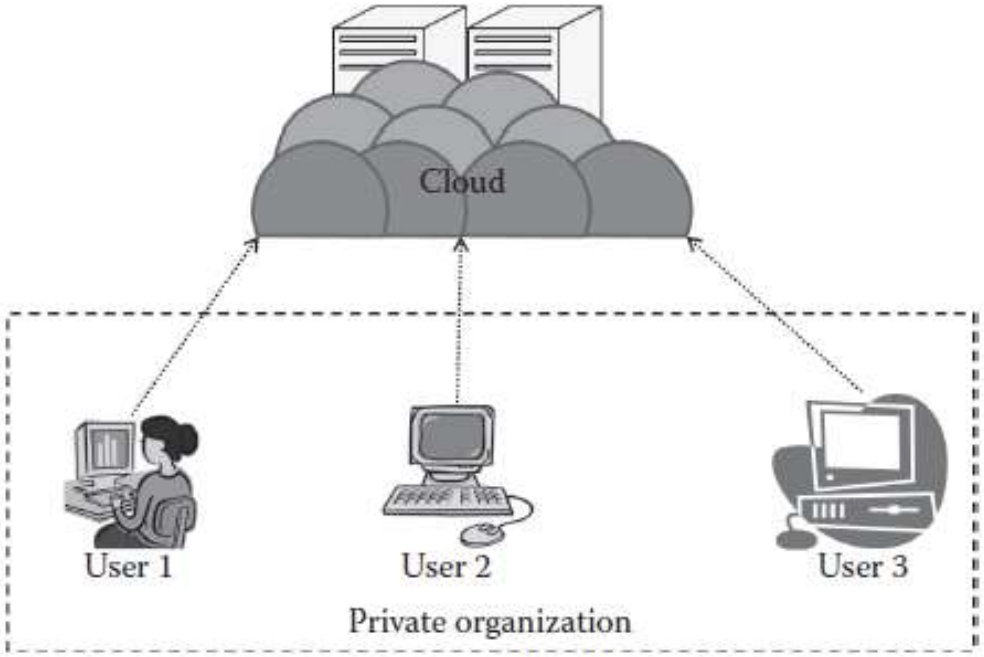
Multitenancy: As multitenant architecture supports multiple tenants with the same physical or software resource, there is a chance of unwanted access of data, and it will have less effect in the private cloud as all the issues will be intraorganizational.

Maintenance:

The cloud is maintained by the organization where the cloud is deployed. The defective resources (drives and processors) are replaced with the good resources. The number of resources is less in the private cloud, so maintenance is comparatively easier.

Outsourced Private Cloud

Outsourced private cloud:



The outsourced private cloud has a cloud outsourced to a third party. A third party manages the whole cloud.

Outsourced Private Cloud - Issues

ISSUES:

SLAs:

The SLA is between the third party and the outsourcing organization. Here, the whole cloud is managed by the third party that will be usually not available on premise. The SLAs are usually followed strictly as it is a third-party organization

Network:

The cloud is fully deployed at the third-party site. The cloud's internal network is managed by a third party, and the organizations connect to the third party by means of either a dedicated connection or through the Internet. The internal network of the organization is managed by the organization, and it does not come under the purview of the SLA.

Security and privacy:

Security and privacy need to be considered when the cloud is outsourced. Here, the cloud is less secure than the on-site private cloud. The privacy and security of the data mainly depend on the hosting third party as they have the control of the cloud. But, basically the security threat is from the third party and the internal employee.

Outsourced Private Cloud - Issues

Laws and conflicts:

If this cloud is deployed outside the country, then the security laws pertaining to that will apply upon the data and the data are still not fully safe. Usually, private clouds are not deployed outside, but if the off-site location is outside the country's boundary, then several problems may arise.

Location:

The private cloud is usually located off site here. When there is a change of location, the data need to be transmitted through long distances. In few cases, it might be out of the country, which will lead to certain issues regarding the data and its transfer.

Performance:

The performance of the cloud depends on the third party that is outsourcing the cloud.

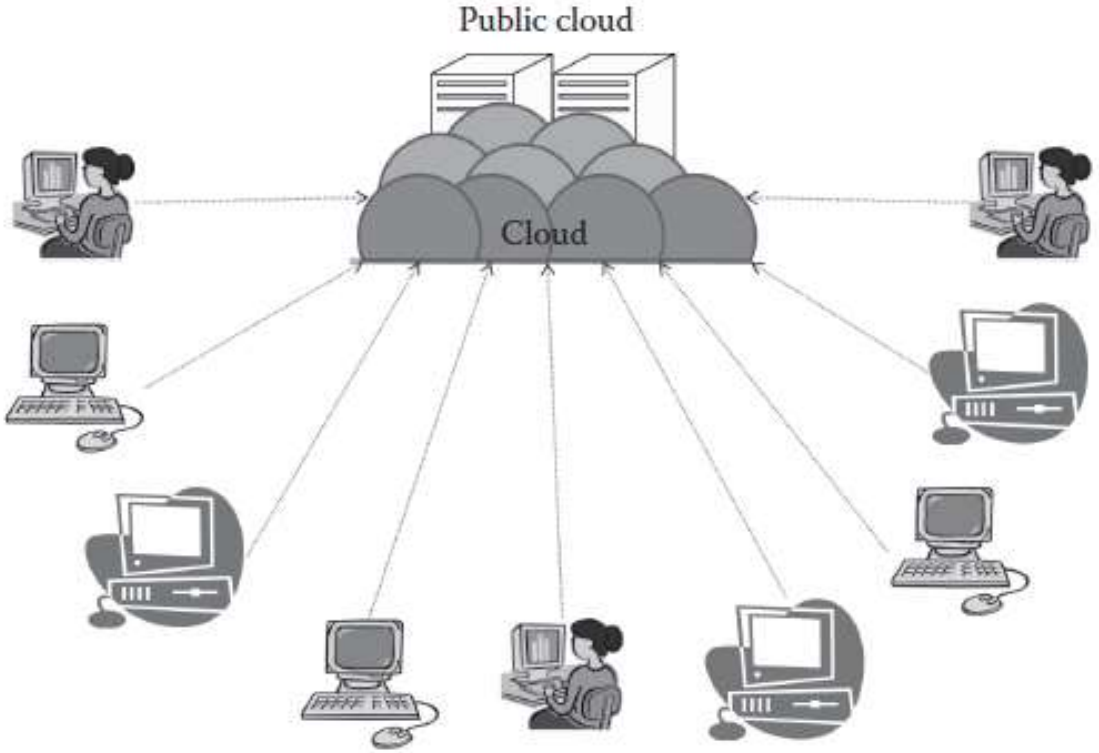
Maintenance:

The cloud is maintained by a third-party organization where the cloud is deployed. As mentioned, the defective resources (drives and processors) are replaced with the good resources. Here, again the process is less complex compared to the public cloud. The cost of maintenance is a big issue. If an organization owns a cloud, then the cost related to the cloud needs to be borne by the organization and this is usually high.

Cloud Deployment Models - Public Cloud

Public Cloud

- According to NIST, the public cloud is the cloud infrastructure that is provisioned for open use by the general public.
- It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- Public cloud consists of users from all over the world. A user can simply purchase resources on an hourly basis and work with the resources.
- There is no need of any prebuilt infrastructure for using the public cloud. These resources are available in the cloud provider's premises.
- Usually, cloud providers accept all the requests, and hence, the resources in the service providers' end are considered *infinite* in one aspect. Some of the well-known examples of the public cloud are Amazon AWS, Microsoft Azure, etc.



Public Cloud

Characteristics:

1. *Highly scalable*
2. *Affordable*
3. *Less secure*
4. *Highly available*
5. *Strict SLAs*

Highly scalable:

The public cloud is highly scalable. The resources in the public cloud are large in number and the service providers make sure that all the requests are granted. Hence, the public cloud is considered to be scalable.

***Affordable*:**

The public cloud is offered to the public on a pay-as-you-go basis; hence, the user has to pay only for what he or she is using (usually on a per-hour basis). And, this does not involve any cost related to the deployment.

***Less secure*:** The public cloud is less secure out of all the four deployment models. This is because the public cloud is offered by a third party and they have full control over the cloud. Though the SLAs ensure privacy, still there is a high risk of data being leaked.

***Highly available*:** The public cloud is highly available because anybody from any part of the world can access the public cloud with proper permission, and this is not possible in other models as geographical or other access restrictions might be there.

Public Cloud

Characteristics:

***Strict SLAs*:** SLA is very strict in the case of the public cloud. As the service provider's business reputation and customer strength are totally dependent on the cloud services, they follow the SLA strictly and violations are avoided. These SLAs are very competitive.

Suitability:

There are several occasions and environments where the public cloud is **suitable**. Following are some:

- ✓ The requirement for resources is large, that is, there is large user base.
- ✓ The requirement for resources is varying.
- ✓ There is no physical infrastructure available.
- ✓ An organization has financial constraints.

The public cloud is **not suitable**, where the following applies:

- ✓ Security is very important.
- ✓ Organization expects autonomy.
- ✓ Third-party reliability is not preferred.

Public Cloud

Issues:

SLA:

- Unlike the private cloud, here the number of users is more and so are the numbers of service agreements. The service provider is answerable to all the users.
- The SLA will cover all the users from all parts of the world. The service provider has to guarantee all the users a fair share without any priority. Having the same SLA for all users is what is usually expected, but it depends on the service provider to have the same SLA for all the users irrespective of the place they are.

Network:

- The network plays a major role in the public cloud. Each and every user getting the services of the cloud gets it through the Internet. The services are accessed through the Internet by all the users, and hence, the service delivery wholly depends on the network.

- Here the service provider is not responsible for the network. The service provider is responsible for providing proper service to the customer, and once the services are given from the service provider, it goes on in transit to the user. The user will be charged for even if he or she has problem due to the network. The network usually consists of a high bandwidth and has a low latency. This is because the connection is only inside the organization. Network management is easier in this case.

Performance:

- As mentioned, the performance of a cloud delivery model primarily depends on the network and the resources. The service provider has to adequately manage the resources and the network. As the number of users increases, it is a challenging task for the service providers to give good performance.

Public Cloud

Issues:

Multitenancy: The resources are shared, that is, multiple users share the resources, hence the term multitenant. Due to this property, there is a high risk of data being leaked or a possible unprivileged access.

Location:

The location of the public cloud is an issue. As the public cloud is fragmented and is located in different regions, the access to these clouds involves a lot of data transfers through the Internet. There are several issues related to the location. For example, a user from India might be using the public cloud and he might have to access his personal resources from other countries. This is not good as the data are being stored in some other country.

Security and data privacy:

Security and data privacy are the biggest challenges in the public cloud. As data are stored in different places around the globe, data security is a very big issue. A user storing the data outside his or her country has a risk of the data being viewed by other people as that does not come under the jurisdiction of the user's country. Though this might not always be true, but it may happen.

Laws and conflicts:

The data are stored in different places of the world in different countries. Hence, data centers are bound to laws of the country in which they are located. This creates many conflicts and problems for the service providers and the users.

Public Cloud

Issues:

Cloud management:

- Here, the number of users is more, and so the management is difficult. The jobs here are time critical, and as the number of users increases, it becomes more difficult. Inefficient management of resources will lead to resource shortage, and user service might be affected. It has a direct impact on SLA and may cause SLA violation.

Maintenance:

- Maintaining the whole cloud is another task. This involves continuous check of the resources, network, and other such parameters for long-lasting efficient delivery of the service.
- The resource provider has to continuously change the resource components from time to time. The task of maintenance is very crucial in the public cloud. The good the cloud is maintained, the better is the quality of service. Here, the cloud data center is where the maintenance happens; continuously, the disks are replaced from time to time.

Public Cloud

Advantages:

- There is no need of establishing infrastructure for setting up a cloud.
- There is no need for maintaining the cloud.
- They are comparatively less costly than other cloud models.
- Strict SLAs are followed.
- There is no limit for the number of users.
- The public cloud is highly scalable.

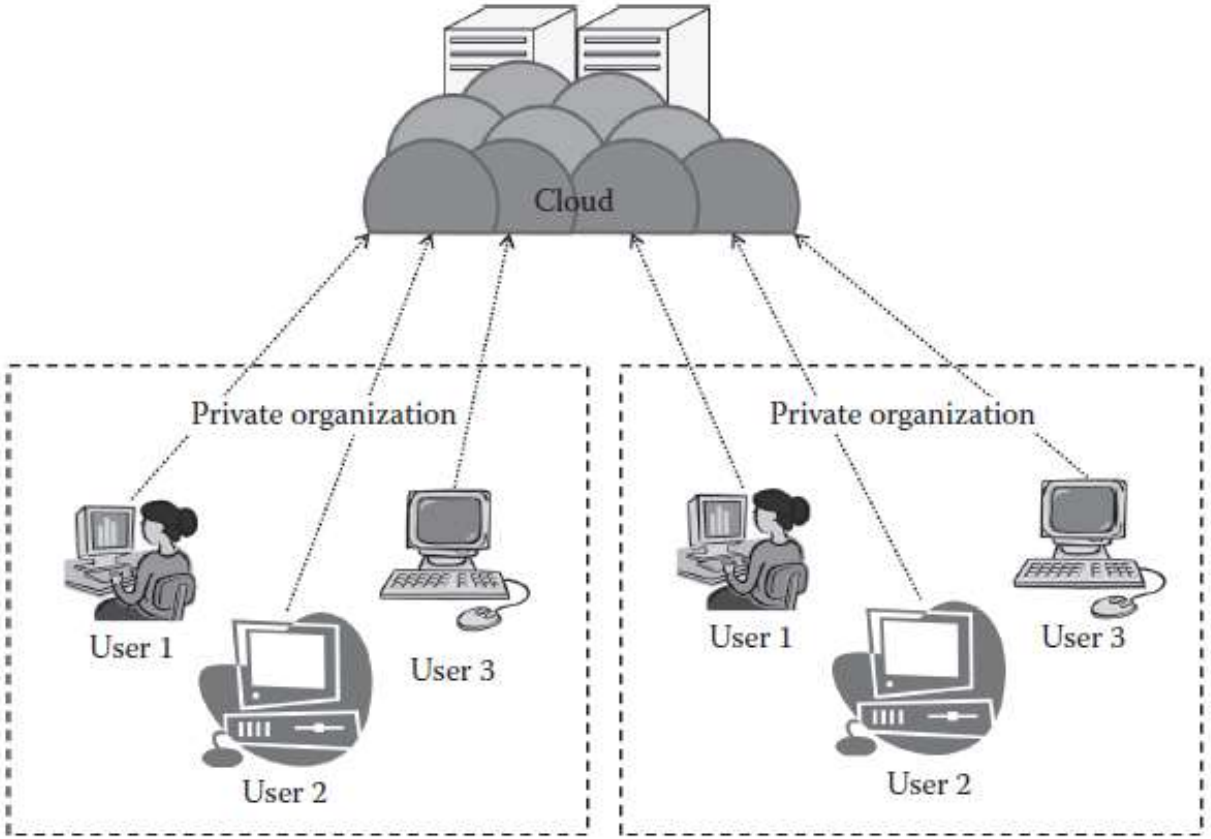
Dis Advantages:

- Security is an issue.
- Privacy and organizational autonomy are not possible.

Cloud Deployment Models - Community Cloud

Community Cloud

- According to NIST, the community cloud is the cloud infrastructure that is **provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).**
- It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them,
- it may exist on or off premises.
- It is a further extension of the private cloud.



Community Cloud

- Here the organizations are able to extract the power of the cloud, which is much bigger than the private cloud, and at the same time, they are able to use it at a usually less cost.
- The community is formed based on any common cause, but eventually, all the members of the community are benefitted.
- **This model is very suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either**

Characteristics:

***Collaborative and distributive maintenance*:**

- The community cloud is wholly collaborative, and usually no single party has full control over the whole cloud (in some cases, it may be controlled by one party).
- This is usually distributive, and hence, better cooperation gives better results.
- Even though it may be outsourced, collaboration based on purpose always proves to be beneficial.

***Partially secure*:**

Partially secure refers to the property of the community cloud where few organizations share the cloud, so there is a possibility that the data can be leaked from one organization to another, though it is safe from the outside world.

Community Cloud

Characteristics contd…

***Cost effective*:** The community cloud is cost effective as the whole cloud is being shared by several organizations or a community. Usually, not only cost but every other sharable responsibilities are also shared or divided among the groups.

Suitability:

This kind of cloud is **suitable for organizations that:**

- Want to establish a private cloud but have financial constraint
- **D**o not want to complete maintenance responsibility of the cloud
- Want to establish the cloud in order to collaborate with other clouds
- Want to have a collaborative cloud with more security features than the public cloud

This cloud is **not suitable for** organizations that:

- Prefer autonomy and control over the cloud
- Does not want to collaborate with other organizations

Community Cloud

Advantages:

- It allows establishing a low-cost private cloud.
- It allows collaborative work on the cloud.
- It allows sharing of responsibilities among the organization.
- It has better security than the public cloud.

Dis Advantages:

- Autonomy of an organization is lost.
- Security features are not as good as the private cloud.
- It is not suitable if there is no collaboration.

There are two types of **community cloud deployments:**

On-premise community cloud:

On-premise community cloud consists of the cloud deployed within the premises and is maintained by the organizations themselves.

Outsourced community cloud:

In the outsourced community cloud, the cloud is outsourced to a third party. The third party is responsible for maintenance and management of the cloud.

Community Cloud

Issues related to On-premise Community Cloud:

SLAs: SLAs are more compared to Private Cloud and Less compared to Public Cloud,.

- As more than one organization is involved, SLA has to be there to have a fair play among the users of the cloud and among the organizations themselves.

Network:

- ✓ The private cloud can be there in any location as this cloud is being shared by more than one organization. Here, each organization will have a separate network, and they will connect to the cloud. It is the responsibility of each organization to take care of their own network.
- ✓ **The service provider is not responsible for the network issues in the organization**. The network is not big and complex as in the public cloud.

Performance:

- ✓ In this type of deployment, more than one organization coordinate together and provide the cloud service. Thus, it is on the maintenance and management team that the performance depends.

Community Cloud

Issues related to On-premise Community Cloud:

Multitenancy:

- There is a moderate risk due to multitenancy. As this cloud is meant for several organizations, the unprivileged access into interorganizational data may lead to several problems

Location:

- The location of the cloud is very important in this case. Usually, the cloud is deployed at any one of the organizations or is maintained off site by any third party. In either case, the organizations have to access the cloud from another location.

Security and privacy:

- Security and privacy are issues in the community cloud since several organizations are involved in it.
- The privacy between the organizations needs to be maintained. As the data are collectively stored, the situation is more like that of a public cloud with less users.
- The organizations should have complete trust on the service provider, and as all other cloud models, this becomes the bottleneck.

Community Cloud

Issues related to On-premise Community Cloud:

Laws and conflicts:

This applies if organizations are located in different countries. If the organizations are located in the same country, then there is no issue, but if these organizations are located elsewhere, that is, in different countries, then they have to abide by the rules of the country in which the cloud infrastructure is present, thus making the process a bit more complex.

Cloud management:

- ✓ Cloud management is done by the service provider, here in this case by the organizations collectively.
- ✓ The organizations will have a management team specifically for this cloud and that is responsible for all the cloud management–related operations.

Cloud maintenance:

- ✓ Cloud maintenance is done by the organizations collectively. The maintenance team collectively maintains all the resources.
- ✓ It is responsible for continuous replacement of resources. In the community cloud, the number of resources is less than the public cloud but usually more than the private cloud.

Community Cloud

Issues related to Outsourced Community Cloud:

SLAs:

The SLA is between the group of organizations and the service provider. The SLA here is stringent as it involves a third party. The SLA here is aimed at a fair share of resources among the organizations. The service provider is not responsible for the technical problems within the organization.

Network:

The issues related to the network are same as the on-site community cloud, but here the service provider is outsourced and hence organizations are responsible for their own network and the service provider is responsible for the cloud network.

Performance:

The performance totally depends on the outsourced service provider. The service provider is responsible for efficient services, except for the network issue in the client side.

Community Cloud

Issues related to Outsourced Community Cloud:

Security and privacy: there are security and privacy issues as several organizations are involved in it, but in addition to that, the involvement of a third party as a service provider will create much more issues as the organizations have to completely rely on the third party.

Laws and conflicts:

In addition to the issues related to laws due to organizations' location, there is a major issue associated with the location of the cloud service provider. If the service provider is outside the country, then there is conflict related to data laws in that country

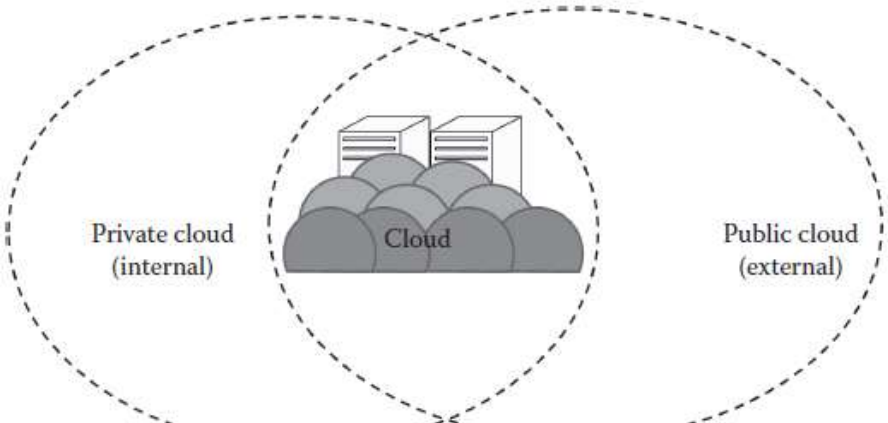
Cloud management & **Cloud maintenance:**

Cloud management and maintenance are done by the service provider. The complexity of managing and maintenance increases with the number of organizations in the community. But, this is less complex than the public cloud.

Cloud Deployment Models - Hybrid Cloud

Hybrid Cloud

- The hybrid cloud usually is a combination of both public and private clouds.
- According to NIST, the hybrid cloud can be defined as the cloud infrastructure that is a composition of two or more distinct cloud infrastructures **(private, community, or public)** that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.
- This is aimed at combining the advantages of private and public clouds.
- The usual method of using the hybrid cloud is to have a private cloud initially, and then for additional resources, the public cloud is used.
- There are several advantages of the hybrid cloud. The hybrid cloud can be regarded as a private cloud extended to the public cloud. This aims at utilizing the power of the public cloud by retaining the properties of the private cloud.
- One of the popular examples for the hybrid cloud is **Eucalyptus**. Eucalyptus was initially designed for the private cloud and is basically a private cloud, but now it also supports hybrid cloud.



Hybrid Cloud

Characteristics:

***Scalable*:** as the public cloud is scalable, the hybrid cloud with the help of its public counterpart is also scalable.

***Partially secure*:** The hybrid cloud usually is a combination of public and private. The private cloud is considered to be secured, but as the hybrid cloud also uses the public cloud, there is high risk of security breach. Thus, it cannot be fully termed as secure but as partially secure.

***Strict SLAs*:** As the hybrid cloud involved a public cloud intervention, the SLAs are stringent and might as per the public cloud service provider. But overall, the SLAs are more stringent than the private cloud.

Complex cloud management: Cloud management is complex and is a difficult task in the hybrid cloud as it involves more than one type of deployment models and also the numbers of users are high.

Suitability:

The hybrid cloud environment **is suitable for:**

- Organizations that want the private cloud environment with the scalability of the public cloud
- Organizations that require more security than the public cloud

The hybrid cloud **is not suitable for:**

- Organizations that consider security as a prime objective
- Organizations that will not be able to handle hybrid cloud management

Hybrid Cloud

Issues:

- ***SLA:*** SLA is one of the important aspects of the hybrid cloud as both private and public are involved. The private cloud does not have stringent agreements, whereas the public cloud has certain strict rules to be covered.
- ***Network:*** The network is usually a private network, and whenever there is a necessity, the public cloud is used through the Internet.
- ***Performance*:** switching from private to public for more performance
- ***Multitenancy:*** Multitenancy is an issue in the hybrid cloud as it involves the public cloud in addition to the private cloud. Thus, this property can be misused and the breaches will have adverse affects as some parts of the cloud go public.

Hybrid Cloud

Issues:

- ***Location:*** Like a private cloud, the location of these clouds can be on premise or off premise and they can be outsourced. They will have all the issues related to the private cloud; in addition to that, issues related to the public cloud will also come into picture whenever there is intermittent access to the public cloud.
- ***Security and privacy:*** Whenever the user is provided services using the public cloud, security and privacy become more strict. As it is the public cloud, the threat of data being lost is high.
- ***Laws and conflicts:*** Several laws of other countries come under the purview as the public cloud is involved, and usually these public clouds are situated outside the country's boundaries.
- ***Cloud management:***Here, everything is managed by the private cloud service provider.
- ***Cloud maintenance:*** Cloud maintenance is of the same complexity as the private cloud; here, only the resources under the purview of the private cloud need to be maintained. It involves a high cost of maintenance.

Hybrid Cloud

Advantages:

- It gives the power of both the private and public clouds.
- It is highly scalable.
- It provides better security than the public cloud.

Dis advantages:

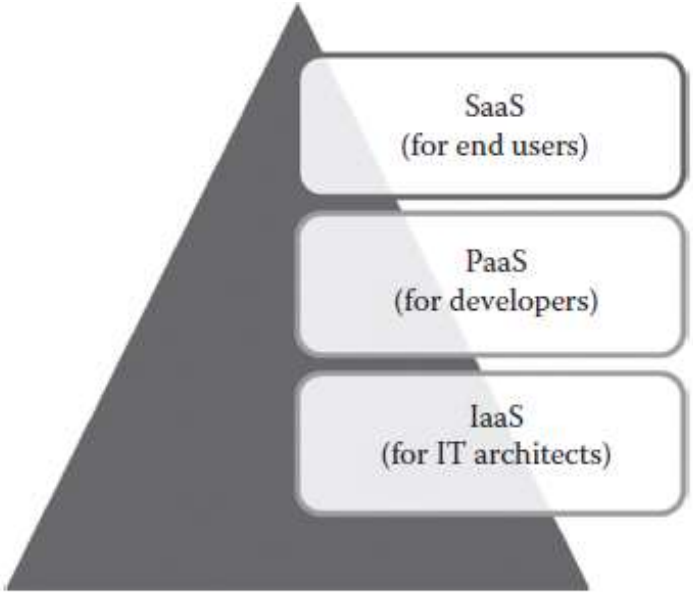
- The security features are not as good as the public cloud.
- Managing a hybrid cloud is complex.
- It has Strict SLAs.

Chapter 2.2
Cloud Service Models

Service Models

NIST (National Institute of Standards and Technology) defines three basic service models, namely, **IaaS, PaaS, and SaaS.**

- **IaaS**
- **PaaS**
- **SaaS**



Service Models

IaaS:

- In the IaaS case, Service provider provides Infrastructure such as compute, network, and storage etc as Service.
- The end users deploy or run their software on the computing resources provided by the service provider.
- The end users are responsible for managing applications that are running on top of the service provider cloud infrastructure.
- The end users can access the services from their devices through web command line interface (CLI) or application programming interfaces (APIs) provided by the service providers.
- Generally, the IaaS services are provided from the service provider cloud **Data Center.**
- Some of the popular IaaS providers include **Amazon Web Services (AWS), Google Compute Engine, OpenStack, and Eucalyptus, Microsoft Azure.**

Service Models

PaaS:

- The ability given to developers to develop and deploy an application on the development platform provided by the service provider.
- The developers are exempted from managing the development platform and underlying infrastructure.
- Here, the developers are responsible for managing the deployed application and configuring the development environment.
- PaaS services are provided by the service provider on an on-premise or dedicated or hosted cloud infrastructure.
- The developers can access the development platform over the Internet through web CLI, web user interface (UI), and integrated development environments (IDEs).
- Some of the popular PaaS providers **include Google App Engine, Microsoft Azure, Force.com, Red Hat OpenShift, Heroku, and Engine Yard.**

Service Models

SaaS:

- The ability given to the end users to access an application over the Internet that is hosted and managed by the service provider.
- Thus, the end users are exempted from managing or controlling an application, the development platform, and the underlying infrastructure.
- Generally, SaaS services are hosted in service provider–managed or service provider–hosted cloud infrastructure.
- The end users can access the services from any thin clients or web browsers.
- Some of the popular SaaS providers include **Saleforce.com, Google Apps, and Microsoft office 365, GoToMeeting etc…**

Service Models

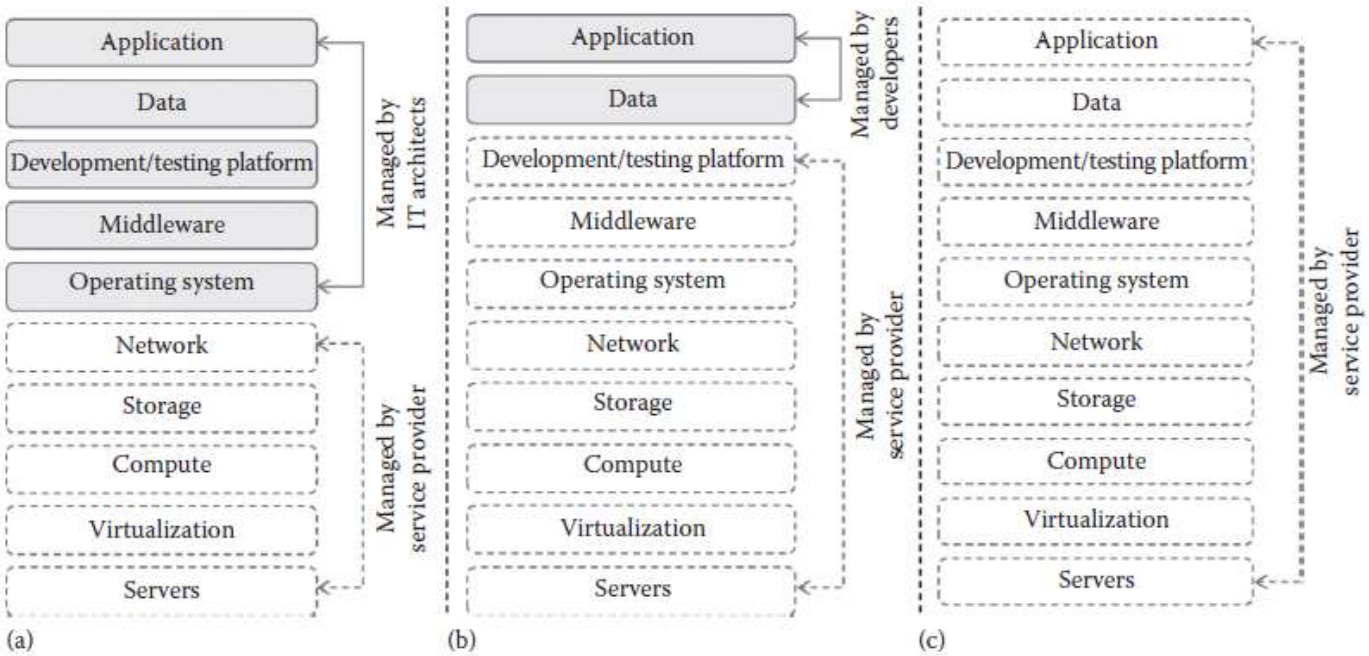
- The different cloud service models target different audiences.

For example:

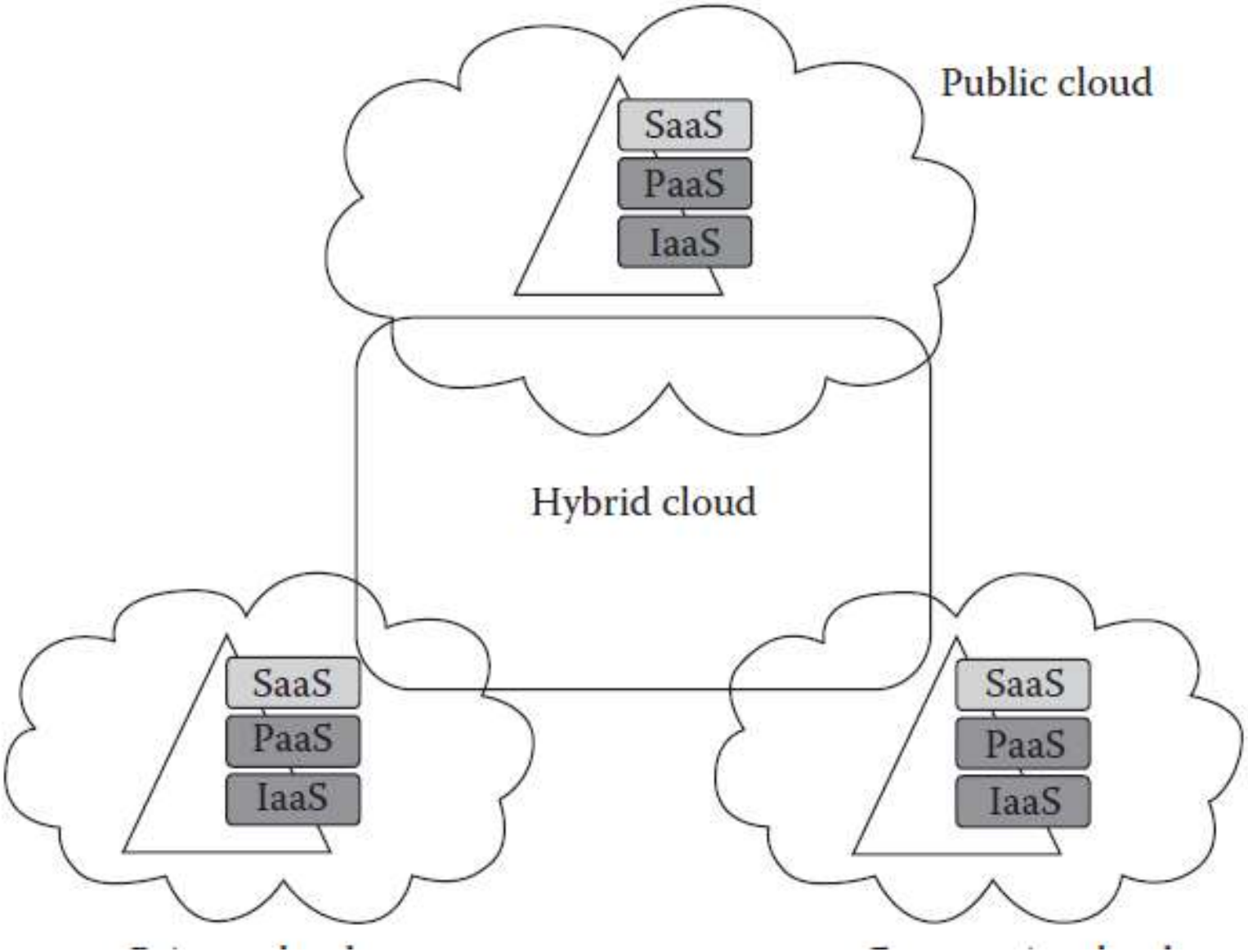
- the IaaS model targets the information technology (IT) architects
- PaaS targets the developers
- SaaS targets the end users

Service Models

- Based on the services subscribed, the responsibility of the targeted audience may vary.
- **In IaaS**, the end users are responsible for maintaining the development platform and the application running on top of the underlying infrastructure. The IaaS providers are responsible for maintaining the underlying hardware part (a) in below figure:
- **In PaaS,** the end users are responsible for managing the application that they have developed. The underlying infrastructure will be maintained by the infrastructure provider. (Fig. b)
- **In SaaS,** the end user is free from maintaining the infrastructure, development platform, and application that they are using. All the maintenance will be carried out by the SaaS p



Service Models



Deployment and delivery of different cloud service delivery models.

IaaS (Infrastructure As A Service)

IaaS

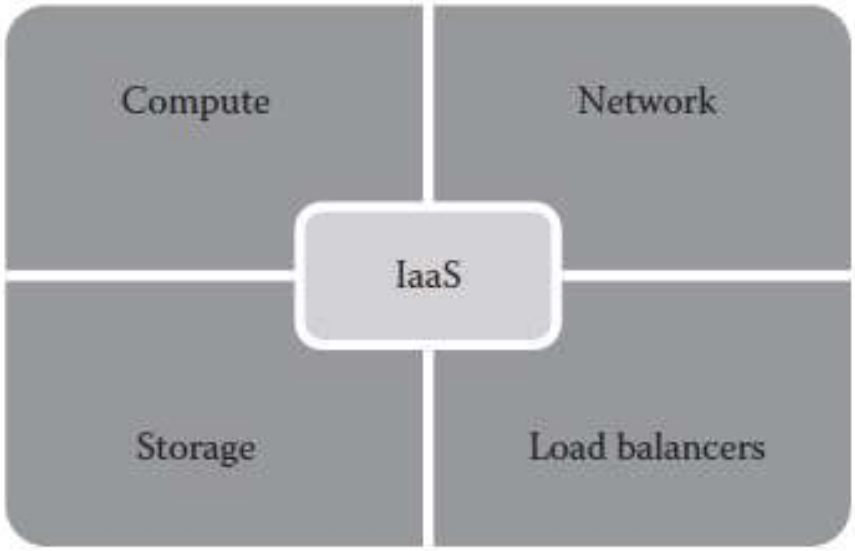
IaaS:

- In traditional data centers, the **computing power** is consumed by having physical access to the infrastructure.
- IaaS changes the computing from a physical infrastructure to a virtual infrastructure. IaaS provides virtual computing, storage, and network resources by abstracting the physical resources.
- Technology virtualization is used to provide the virtual resources. All the virtual resources are given to the virtual machines (VMs) that are configured by the service provider.
- The end users or IT architects will use the infrastructure resources in the form of VMs
- The targeted audience of IaaS is the IT architect. The IT architect can design virtual infrastructure, network, load balancers, etc., based on their needs. The IT architects need not maintain the physical servers as it is maintained by the service providers.
- The physical infrastructure can be maintained by the service providers themselves. Thus, it eliminates or hides the complexity of maintaining the physical infrastructure from the IT architects.

IaaS

IaaS:

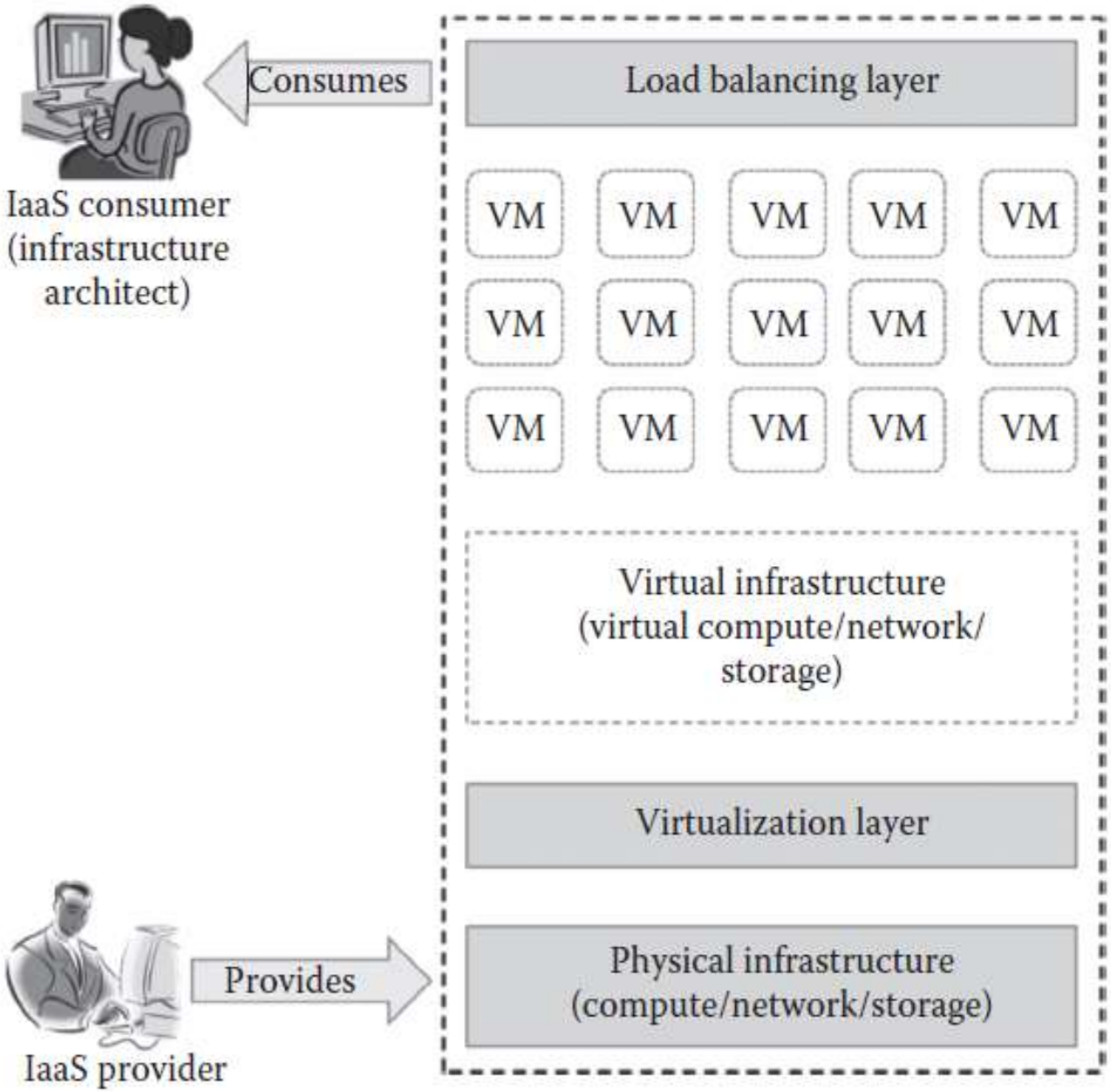
- A typical IaaS provider may provide the flowing services as shown in the following fig:



1. ***Compute*:** Computing as a Service includes virtual central processing units ***(CPUs) and virtual main memory*** for the VMs that are provisioned to the end users.
2. ***Storage*:** STaaS provides ***back-end storage*** for the VM images. Some of the IaaS providers also provide the back end for storing files.
3. ***Network*:** Network as a Service (NaaS) provides virtual networking components such as ***virtual router, switch, and bridge for the VMs***.
4. ***Load balancers*:** Load Balancing as a Service may provide load balancing capability at the infrastructure layer.

IaaS

IaaS:


Consumes
Load balancing layer
IaaS consumer
(infrastructure
architect)
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
Virtual infrastructure
(virtual compute/network/
storage)
Virtualization layer
Provides
Physical infrastructure
(compute/network/storage)
IaaS provider

IaaS

Characteristics:

Web access to the resources → The IaaS model enables the IT users to access infrastructure resources over the Internet. through Web Browser or Management Console.

Centralized management: Even though the physical resources are distributed, the management will be from a single place using management console.

Elasticity and dynamic scaling: IaaS provides elastic services where the usage of resources can be increased or decreased according to the requirements.

Shared infrastructure: IaaS follows a one-to-many delivery model and allows multiple IT users to share the same physical infrastructure.

Preconfigured VMs: IaaS providers offer preconfigured VMs with operating systems (OSs), network configuration, etc. The IT users can select any kind of VMs of their choice. The IT users are free to configure VMs from scratch. The users can directly start using the VMs as soon as they subscribed to the services.

Metered services: IaaS allows the IT users to rent the computing resources instead of buying it. The services consumed by the IT user will be measured, and the users will be charged by the IaaS providers based on the amount of usage.

IaaS

Suitability of IaaS:

Unpredictable spikes in usage: When there is a significant spike in usage of computing resources, IaaS is the best option for IT industries. If there is an unpredictable demand of infrastructure, then it is recommended to use IaaS services.

Limited capital investment: New start-up companies cannot invest more on buying infrastructure for their business needs. And so by using IaaS, start-up companies can reduce the capital investment on hardware. IaaS is the suitable option for start-up companies with less capital investment on hardware.

Infrastructure on demand: Some organizations may require large infrastructure for a short period of time. For this purpose, an organization cannot afford to buy more on-premise resources. Instead, they can rent the required resources.

IaaS

IaaS not Suitable when:

When regulatory compliance does not allow off-premise hosting: For some companies, its regulation may not allow the application and data to be hosted on third-party off-premise infrastructure.

When usage is minimal: When the usage is minimal and the available on-premise infrastructure itself is capable of satisfying their needs.

When better performance is required: Since the IaaS services are accessed through the Internet, sometimes the performance might be not as expected due to network latency

When there is a need for more control on physical infrastructure: Some organizations might require physical control over the underlying infrastructure. As the IaaS services are abstracted as virtual resources, it is not possible to have more control on underlying physical infrastructure.

IaaS

Pros (Advantages) of IaaS:

Pay-as-you-use model: The IaaS services are provided to the customers on a pay-per-use basis. This ensures that the customers are required to pay for what they have used. This model eliminates the unnecessary spending on buying hardware.

Reduced TCO(Total Cost of Ownership): Since IaaS providers allow the IT users to rent the computing resources, they need not buy physical hardware for running their business.

Elastic resources: IaaS provides resources based on the current needs. IT users can scale up or scale down the resources whenever they want. This dynamic scaling is done automatically using some load balancers.

Better resource utilization: Resource utilization is the most important criteria to succeed in the IT business. The purchased infrastructure should be utilized properly to increase the **ROI (Return On Investment).** IaaS ensures better resource utilization and provides high ROI for IaaS providers.

Supports Green IT: In traditional IT infrastructure, dedicated servers are used for different business needs. Since many servers are used, the power consumption will be high. This does not result in Green IT.

- In IaaS, the need of buying dedicated servers is eliminated as single infrastructure is shared between multiple customers, thus reducing the number of servers to be purchased and hence the power consumption that results in Green IT.

IaaS

Cons (Drawbacks) of IaaS:

Security issues: Since IaaS uses virtualization as the enabling technology, hypervisors play an important role. There are many attacks that target the hypervisors to compromise it. If hypervisors get compromised, then any VMs can be attacked easily.

Interoperability issues: There are no common standards followed among the different IaaS providers. It is very difficult to migrate any VM from one IaaS provider to the other. Sometimes, the customers might face the vendor lock-in problem.

Performance issues: IaaS is nothing but the consolidation of available resources from the distributed cloud servers. Here, all the distributed servers are connected over the network. Latency of the network plays an important role in deciding the performance. Because of latency issues, *sometimes* the VM contains issues with its performance.

IaaS

IaaS Providers summary:

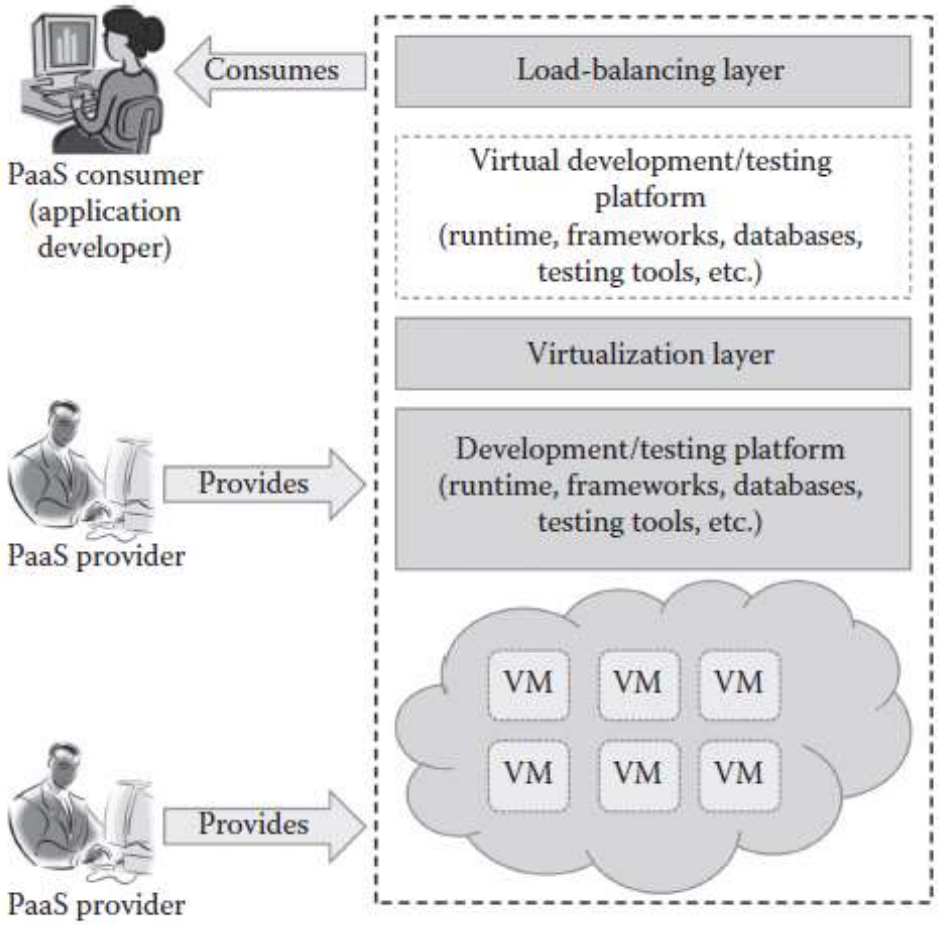
Summary of Popular IaaS Providers

Provider	License	Deployment Model	Host OS	Guest OS	Supported Hypervisor(s)
Amazon Web Services	Proprietary	Public	Not available	Red Hat Linux, Windows Server, SuSE Linux, Ubuntu, Fedora, Debian, CentOS, Gentoo Linux, Oracle Linux, and FreeBSD	Xen
Google Compute Engine	Proprietary	Public	Not available	Debian 7 Wheezy, CentOS 6, Red Hat Enterprise Linux, SUSE, Windows Server, CoreOS, FreeBSD, and SELinux	KVM
Microsoft Windows Azure	Proprietary	Public	Not available	Windows Server, CentOS, FreeBSD, openSUSE Linux, and Oracle Enterprise Linux	Windows Azure hypervisor
Eucalyptus	GPLv3	Private and hybrid	Linux	Linux and Windows	Xen, KVM, VMware
Apache CloudStack	Apache 2	Private	Linux	Windows, Linux, and various versions of BSD	KVM, vSphere, XenServer/ XCP
OpenNebula	Apache 2	Private, public, and hybrid	CentOS, Debian, and openSUSE	Microsoft Windows and Linux	Xen, KVM, VMware
OpenStack	Apache 2	Private and public	CentOS, Debian, Fedora, RHEL, openSUSE, and Ubuntu	CentOS, Ubuntu, Microsoft Windows, and FreeBSD	libvirt, Hyper-V, VMware, XenServer 6.2, baremetal, docker, Xen, LXC via libvirt

PaaS (Platform As A Service)

PaaS

- PaaS changes the application development from local machine to online.
- PaaS providers may provide programming languages, application frameworks, databases, and testing tools as a Service.
- The developers can consume the services over the Internet.



PaaS

PaaS provides the following as Service:

Programming Languages:

- PaaS providers provide a wide variety of programming languages for the developers to develop applications.
- Some of the popular programming languages provided by PaaS vendors are Java, Perl, PHP, Python, Ruby, Scala, Clojure, and Go.

Application Frameworks:

- PaaS vendors provide application frameworks that simplify the application development.
- Some of the popular application development frameworks provided by a PaaS provider include **Node.js, Rails, Drupal, Joomla, WordPress, Django, EE6, Spring, Play, Sinatra, Rack, and Zend.**

Databases:

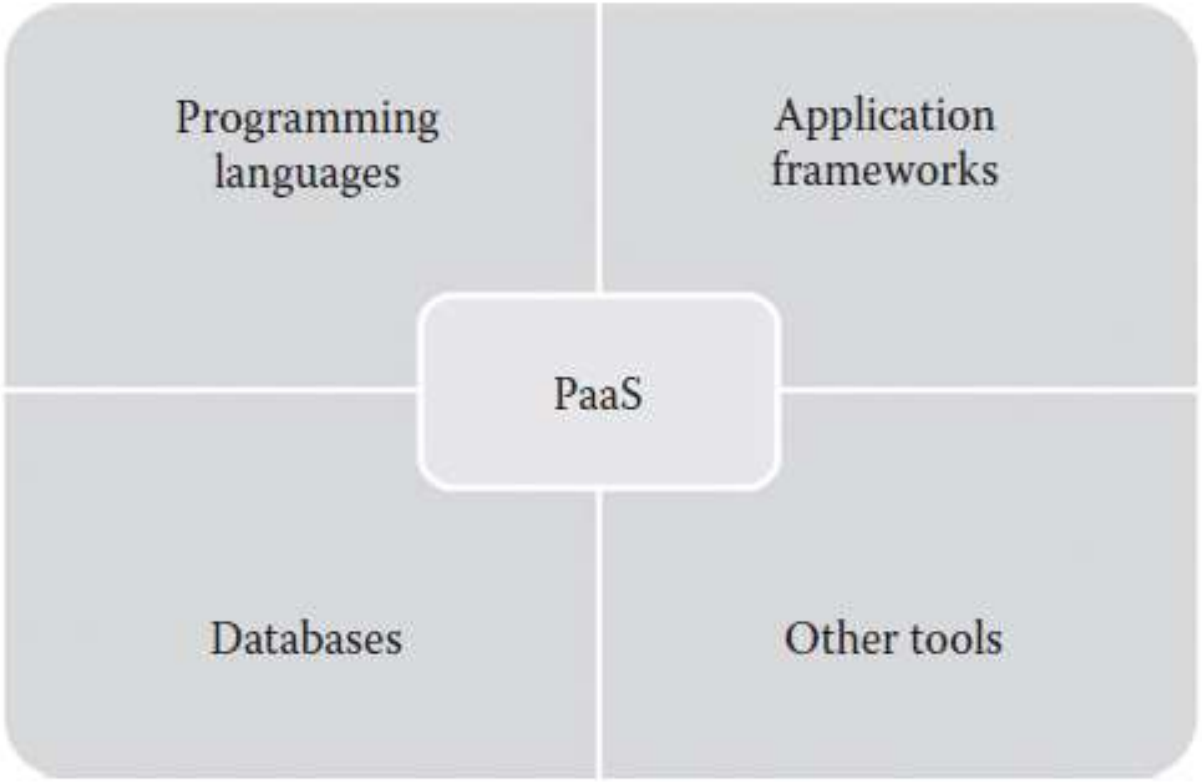
- Since every application needs to communicate with the databases, it becomes a must-have tool for every application.
- PaaS providers are providing databases also with their PaaS platforms.
- The popular databases provided by the popular PaaS vendors are **ClearDB, PostgreSQL, Cloudant, Membase, MongoDB, and Redis.**

PaaS

PaaS provides the following as Service:

Other Tools: PaaS providers provide all the tools that are required to develop, test, and deploy an application.

Services provided by the PaaS Providers:



PaaS - Characteristics

- **All in One:**
  - Most of the PaaS providers offer services to develop, test, deploy, host, and maintain applications in the same IDE.
  - Additionally, many service providers provide all the programming languages, frameworks, databases, and other development-related services that make developers choose from a wide variety of development platforms.
- **Web access to the development platform:**
- PaaS provides web access to the development platform. Using web UI, any developer can get access to the development platform. The web-based UI helps the developers create, modify, test, and deploy different applications on the same platform.
- **Offline access:** To enable offline development, some of the PaaS providers allow the developer to synchronize their local IDE with the PaaS services. The developers can develop an application locally and deploy it online whenever they are connected to the Internet.
- **Built-in scalability:**
  - PaaS services provide built-in scalability to an application that is developed using any particular PaaS. This ensures that the application is capable of handling varying loads efficiently.

PaaS - Characteristics

- **Collaborative platform:**

- ✓ Most of the PaaS services provide support for collaborative development. To enable collaboration among developers, most of the PaaS providers provide tools for project planning and communication.

- **Diverse client tools:**

- ✓ To make the development easier, PaaS providers provide a wide variety of client tools to help the developer. The client tools include CLI, web CLI, web UI, REST API, and IDE.
- ✓ The developers can choose any tools of their choice. These client tools are also capable of handling billing and subscription management.

PaaS - Suitability

- Most of the start-up SaaS development companies and independent software vendors (ISVs) widely use PaaS in developing an application.

PaaS is suitable for the following situations:

- ***Collaborative development*:**
- ✓ Since PaaS services provide a collaborative development environment, it is a suitable option for applications that need collaboration among developers and other third parties to carry out the development process.

- ***Automated testing and deployment:***
- ✓ Most of the PaaS services offer automated testing and deployment capabilities.
- ✓ The development team needs to concentrate more on development rather than testing and deployment.
- ✓ Thus, PaaS services are the best option where there is a need for automated testing and deployment of the applications.

- ***Time to market*:**
- ✓ The PaaS services follow the iterative and incremental development methodologies that ensure that the application is in the market as per the time frame given.

PaaS - non Suitability

PaaS is not suitable for the following situations:

- ***Frequent application migration*:**
- ✓ Since there are no common standards followed among PaaS providers, it is very difficult to migrate the application from one PaaS provider to the other.

- ***Customization at the infrastructure level*:**
- There are some application development platforms that need some configuration or customization of underlying infrastructure. In these situations, it is not possible to customize the underlying infrastructure with PaaS. If the application development platform needs any configuration at the hardware level, it is not recommended to go for PaaS.

- ***Flexibility at the platform level*:**
- PaaS provides template-based applications where all the different programming languages, databases, and message queues are predefined. It is an advantage if the application is a generic application.

- ***Integration with on-premise application*:**
- ✓ Since many PaaS services use their own proprietary technologies to define the application stack, it may not match with the on-premise application stack. This makes the integration of application hosted in on-premise platform and PaaS platform a difficult job.

PaaS - Pros and Cons

Adv of PaaS:

Quick development and deployment:

- ✓ PaaS provides all the required development and testing tools to develop, test, and deploy the software in one place.
- ✓ Most of the PaaS services automate the testing and deployment process as soon as the developer completes the development. This speeds up application development and deployment than traditional development platforms.

Reduces TCO (Total Cost of Ownership):

- ✓ The developers need not buy licensed development and testing tools if PaaS services are selected.
- ✓ PaaS allows the developers to rent the software, development platforms, and testing tools to develop, build, and deploy the application.
- ✓ PaaS does not require high-end infrastructure also to develop the application, thus reducing the TCO of the development company.

***Supports agile software development*:**

- ✓ Nowadays, most of the new-generation applications are developed using agile methodologies. Many ISVs(Independent Software Vendors) and SaaS development companies started adopting agile methodologies for application development.
- ✓ PaaS services support agile methodologies that the ISVs and other development companies are looking for.

PaaS - Pros and Cons

Adv of PaaS:

***Different teams can work together*:**

- ✓ The traditional development platform does not have extensive support for collaborative development.
- ✓ PaaS services support developers from different places to work together on the same project. This is possible because of the online common development platform provided by PaaS providers.

Ease of use:

The traditional development platform uses any one of CLI- or IDE-based interfaces for development. Some developers may not be familiar with the interfaces provided by the application development platform. This makes the development job a little bit difficult. But, PaaS provides a wide variety of client tools such as CLI, web CLI, web UI, APIs, and IDEs. The developers are free to choose any client tools of their choice. Especially, the web UI–based PaaS services increase the usability of the development platform for all types of developers.

Less maintenance overhead:

In on-premise applications, the development company or software vendor is responsible for maintaining the underlying hardware. They need to recruit skilled administrators to maintain the servers. This overhead is eliminated by the PaaS services as the underlying infrastructure is maintained by the infrastructure providers. This gives freedom to developers to work on the application development.

PaaS - Pros and Cons

Adv of PaaS:

Produces scalable applications:

- ✓ Most of the applications developed using PaaS services are web application or SaaS application. These applications require better scalability on the extra load.
- ✓ For handling extra load, the software vendors need to maintain an additional server. It is very difficult for a new start-up company to provide extra servers based on the additional load. But, PaaS services are providing built-in scalability to the application that is developed using the PaaS platform.

PaaS - Cons

Drawbacks of PaaS:

Vendor lock-in: The major drawback with PaaS providers are vendor lock-in. The main reason for vendor lock-in is lack of standards. There are no common standards followed among the different PaaS providers. The other reason for vendor lock-in is proprietary technologies used by PaaS providers. Most of the PaaS vendors use the proprietary technologies that are not compatible with the other PaaS providers. The vendor lock-in problem of PaaS services does not allow the applications to be migrated from one PaaS provider to the other.

***Security issues*:**

Since data are stored in off-premise third-party servers, many developers are afraid to go for PaaS services. Of course, many PaaS providers provide mechanisms to protect the user data, and it is not sufficient to feel the safety of on-premise deployment.

Less flexibility: Most of the PaaS providers provide many programming languages, databases, and other development tools. But, it is not extensive and does not satisfy all developer needs. Only some of the PaaS providers allow developers to extend the PaaS tools with the custom or new programming languages. Still most of the PaaS providers do not provide flexibility to the developers.

Depends on Internet connection: Since the PaaS services are delivered over the Internet, the developers should depend on Internet connectivity for developing the application. Even though some of the providers allow offline access, most of the PaaS providers do not allow offline access. With slow Internet connection, the usability and efficiency of the PaaS platform do not satisfy the developer requirements.

PaaS

PaaS Providers summary:

Summary of Popular PaaS Providers

Provider	License	Deployment Model	Supported Languages	Supported Frameworks	Supported Databases	Client Tools
Cloud Foundry	Open source and proprietary	Public	Python, PHP, Java, Groovy, Scala, and Ruby	Spring, Grails, Play, Node.js, Lift, Rails, Sinatra, and Rack	MySQL, PostgreSQL, MongoDB, and Redis	cf. CLI, IDEs, and build tools
Google App Engine	Proprietary	Public	Python, Java, Groovy, JRuby, Scala, Clojure, Go, and PHP	Django, CherryPy, Pyramid, Flask, web2py, and webapp2.	Google Cloud SQL, Datastore, BigTable, and Blobstore	APIs
Heroku	Proprietary	Public	Ruby, Java, Scala, Clojure and Python, PHP, and Perl	Rails, Play, Django, and Node.js.	ClearDB, PostgreSQL, Cloudant, Membase, MongoDB, and Redis	CLI and RESTful API
Microsoft Windows Azure	Proprietary	Public	.Net, PHP, Python, Ruby, and Java	Django, Rails, Drupal, Joomla, WordPress, DotNetNuke, and Node.js.	SQL Azure, MySQL, MongoDB, and CouchDB	RESTful API and IDEs

PaaS

PaaS Providers summary:

Red Hat OpenShift Online	Proprietary	Public	Java, Ruby, Python, PHP, and Perl	Node.js, Rails, Drupal, Joomla, WordPress, Django, EE6, Spring, Play, Sinatra, Rack, and Zend.	MySQL, PostgreSQL, and MongoDB	Web UI, APIs, CLI, and IDEs
ActiveState Stackato	Proprietary	Private	Java, Perl, PHP, Python, Ruby, Scala, Clojure, and Go	Spring, Node.js, Drupal, Joomla, WordPress, Django, Rails, and Sinatra.	MySQL, PostgreSQL, MongoDB, and Redis	CLI and IDE
Apprenda	Proprietary	Private	.Net and Java	Most of the frameworks form .Net.	SQL Server	REST APIs
CloudBees	Proprietary	Private	Java, Groovy, and Scala	Spring, JRails, JRuby, and Grails.	MySQL, PostgreSQL, MongoDB, and CouchDB	API, SDK, and IDEs
Cumulogic	Proprietary	Private	Java, PHP, and Python	Spring and Grails.	MySQL, MongoDB, and Couchbase	RESTful API
Gigaspaces Cloudify	Open source	Private	Any programming language specified by recipe	Rails, Play, and others.	MySQL, MongoDB, Couchbase, Cassandra, and others	CLI, web UI, and REST API

SaaS (Software As A Service)

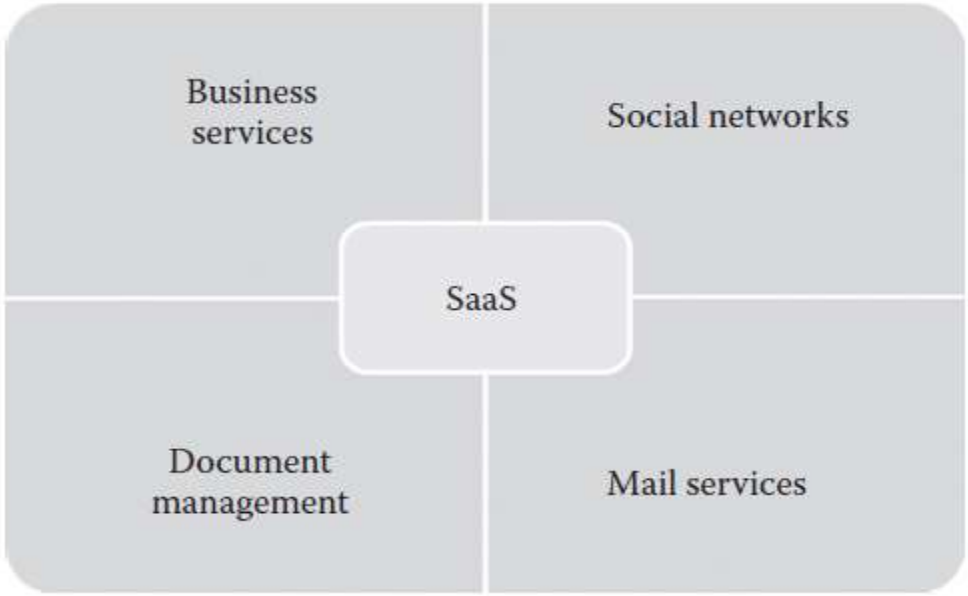
SaaS

SaaS:

- In the traditional software model, the software is delivered as a license-based product that needs to be installed in the end user device.
- Since SaaS is delivered as an on-demand service over the Internet, there is no need to install the software to the end user's devices.
- SaaS services can be accessed or disconnected at any time based on the end user's needs. SaaS services can be accessed from any lightweight web browsers on any devices such as laptops, tablets, and smartphones.
- Some of the SaaS services can be accessed from a thin client that does not contain much storage space and cannot run much software like the traditional desktop PCs.
- The important **benefits of using thin clients** for accessing the SaaS application are as follows:
  - less vulnerable to attack
  - has a longer life cycle
  - consumes less power
  - less expensive

SaaS:

- A SaaS provider may provide business services, social networks, document management, and mail services as shown in below diagram:



***Business services*:** Most of the SaaS providers started providing a variety of business services that attract start-up companies. The business SaaS services include ERP (Enterprise Resource Planning), CRM (Customer Relationship Mgt.), billing, sales, and human resources.

***Social networks*:** Since social networking sites are extensively used by the general public, many social networking service providers adopted SaaS for their sustainability.

***Document management*:** Since most of the enterprises extensively use electronic documents, most of the SaaS providers started providing services that are used to create, manage, and track electronic documents.

***Mail services*:** To handle the unpredictable number of users and the load on e-mail services, most of the e-mail providers started offering their services as SaaS services.

SaaS

Characteristics:

***One to many*:** SaaS services are delivered as a one-to-many model where a single instance of the application can be shared by multiple tenants or customers.

***Web access*:** SaaS services provide web access to the software. It allows the end user to access the application from any location if the device is connected to the Internet.

***Centralized management*:** Since SaaS services are hosted and managed from the central location, management of the SaaS application becomes easier. Normally, the SaaS providers will perform the automatic updates that ensure that each tenant is accessing the most recent version of the application without any user-side updates.

***Multidevice support*:** SaaS services can be accessed from any end user devices such as desktops, laptops, tablets, smartphones, and thin clients.

***Better scalability*:** Since most of the SaaS services leverage PaaS and IaaS for its development and deployment, it ensures a better scalability than the traditional software. The dynamic scaling of underlying cloud resources makes SaaS applications work efficiently even with varying loads.

***High availability*:** SaaS services ensure the 99.99% availability of user data as proper backup and recovery mechanisms are implemented at the back end.

***API integration*:** SaaS services have the capability of integrating with other software or service through standard APIs.

SaaS

Suitability of SaaS:

***On-demand software*:** The licensing-based software model requires buying full packaged software and increases the spending on buying software. Some of the occasionally used software does not give any ROI. Because of this, many end users are looking for a software that they can use as and when they needed.

***Software for start-up companies*:** When using any traditional software, the end user should buy devices with minimum requirements specified by the software vendor. This increases the investment on buying hardware for start-up companies. Since SaaS services do not require high-end infrastructure for accessing, it is a suitable option for start-up companies that can reduce the initial expenditure on buying high-end hardware

***Software compatible with multiple devices*:** Some of the applications like word processors or mail services need better accessibility from different devices. The SaaS applications are adaptable with almost all the devices.

***Software with varying loads*:** We cannot predict the load on popular applications such as social networking sites. The user may connect or disconnect from applications anytime. It is very difficult to handle varying loads with the traditional infrastructure. With the dynamic scaling capabilities, SaaS applications can handle varying loads efficiently without disrupting the normal behavior of the application.

SaaS

Not Suitable when:

***Real-time applications*:** Since SaaS applications depend on Internet connectivity, it may not work better with low Internet speed.

***Applications with confidential data*:** Data security, data governance, and data compliance are always issues with SaaS applications. Since data are stored with third-party service providers, there is no surety that our data will be safe.

***Better on-premise application*:** Some of the on-premise applications might fulfill all the requirements of the organization. In such situations, migrating to the SaaS model may not be the best option.

SaaS

Adv. Of SaaS:

***No client-side installation*:** SaaS services do not require client-side installation of the software. The end users can access the services directly from the service provider data center without any installation.

***Cost savings*:** Since SaaS services follow the utility-based billing or pay-as-you-go billing, it demands the end users to pay for what they have used. Most of the SaaS providers offer different subscription plans to benefit different customers.

***Less maintenance*:** SaaS services eliminate the additional overhead of maintaining the software from the client side. For example, in the traditional software, the end user is responsible for performing bulk updates. But in SaaS, the service provider itself maintains the automatic updates, monitoring, and other maintenance activities of the applications.

***Ease of access*:** SaaS services can be accessed from any devices if it is connected to the Internet. Accessibility of SaaS services is not restricted to any particular devices.

***Dynamic scaling*:** SaaS services are popularly known for elastic dynamic scaling. It is very difficult for on-premise software to provide dynamic scaling capability as it requires additional hardware.

***Disaster recovery*:** With proper backup and recovery mechanisms, replicas are maintained for every SaaS services. The replicas are distributed across many servers. If any server fails, the end user can access the SaaS from other servers.

Multitenancy: Multitenancy is the ability given to the end users to share a single instance of the application. Multitenancy increases resource utilization from the service provider side.

SaaS

Dis Adv. Of SaaS:

***Security*:** Security is the major concern in migrating to SaaS application. Since the SaaS application is shared between many end users, there is a possibility of data leakage. Here, the data are stored in the service provider data center.

***Connectivity requirements*:** SaaS applications require Internet connectivity for accessing it. Sometimes, the end user's Internet connectivity might be very slow. In such situations, the user cannot access the services with ease. The dependency on high-speed Internet connection is a major problem in SaaS applications.

***Loss of control*:** Since the data are stored in a third-party and off-premise location, the end user does not have any control over the data. The degree of control over the SaaS application and data is lesser than the on-premise application

SaaS

Summary of Popular SaaS Providers

Provider	Services Provided
Salseforce.com	On-demand CRM solutions
Google Apps	Gmail, Google Calendar, Talk, Docs, and Sites
Microsoft Office 356	Online office suite, software, plus services
NetSuite	ERP, accounting, order management, inventory, CRM, professional services automation (PSA), and e-commerce applications
Concur	Integrated travel and expense management solutions
GoToMeeting	Online meeting, desktop sharing, and video-conferencing software
Constant Contact	E-mail marketing, social-media marketing, online survey, event marketing, digital storefronts, and local deals tools
Workday, Inc.	Human capital management, payroll, and financial management
Oracle CRM	CRM applications
Intacct	Financial management and accounting software solutions

Other service offerrings

NaaS (Network as a Service)

DEaaS (Desktop as a Service)

STaaS (Storage as a Service)

DBaaS (Database as a Service)

DaaS (Data as a Service)

SECaaS (Security as a Service)

IDaaS (Identity as a Service)

XaaS (Everything as a Service):

XaaS may include Backup as a Service (BaaS), Communication as a Service (CaaS), Hadoop as a Service (HaaS), Disaster Recovery as a Service (DRaaS), Testing as a Service (TaaS), Firewall as a Service (FWaaS), Virtual Private Network as a Service (VPNaaS), Load Balancers as a Service (LBaaS), Message Queue as a Service (MQaaS), and Monitoring as a Service (MaaS).

Chapter 1.3
Introduction to AWS

Amazon Web Services (AWS)

AWS:

- ✓