

Cloud Computing & its Applications

Course Code: SWE4004

Dr Sunil Kumar Singh

Assistant Professor

School - SCOPE

VIT-AP University

sunil.singh@vitap.ac.in

Cabin - AB2 (124D)



Fundamental Concepts and Models

Outline

- Roles and boundaries
- Cloud characteristics
- Cloud delivery models
- Cloud deployment models.

Roles and Boundaries

Cloud Provider

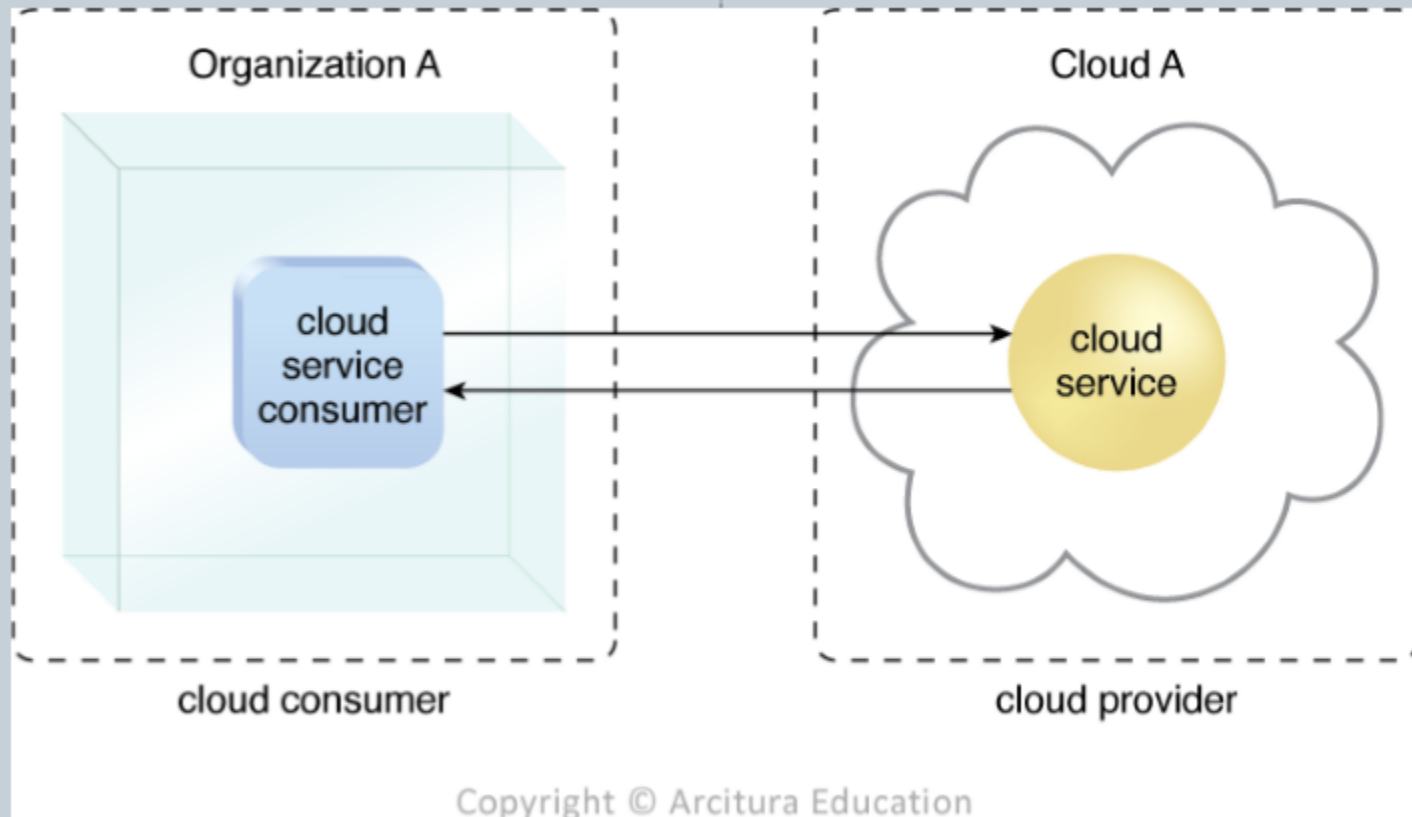
- The organization that provides cloud-based IT resources is the cloud provider.
- Cloud providers normally own the IT resources for lease by cloud consumers, and could also “resell” IT resources leased from other providers
- Responsible for cloud services available as per agreed upon SLA guarantees.

Roles and Boundaries (Cont..)

Cloud Consumer

- A cloud consumer is an organization (or a human) that has a formal contract or arrangement with a cloud provider to use IT ‘resources made available by the cloud provider.
- The cloud consumer uses a cloud service consumer to access a cloud service.

Roles and Boundaries (Cont..)



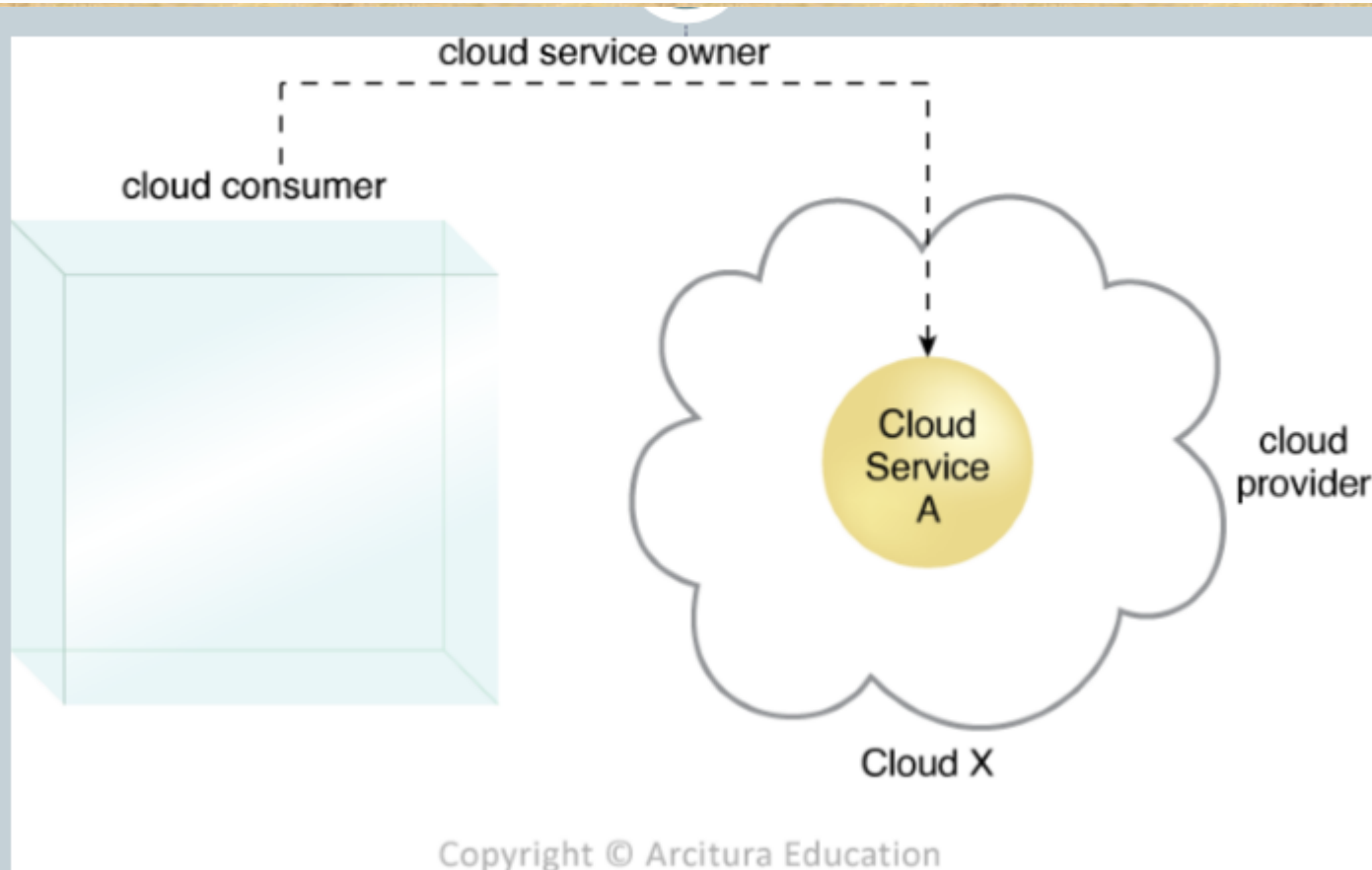
- *Figure 4.1 - A cloud consumer (Organization A) interacts with a cloud service from a cloud provider (that owns Cloud A). Within Organization A, the cloud service consumer is being used to access the cloud service.*

Roles and Boundaries (Cont..)

Cloud Service Owner

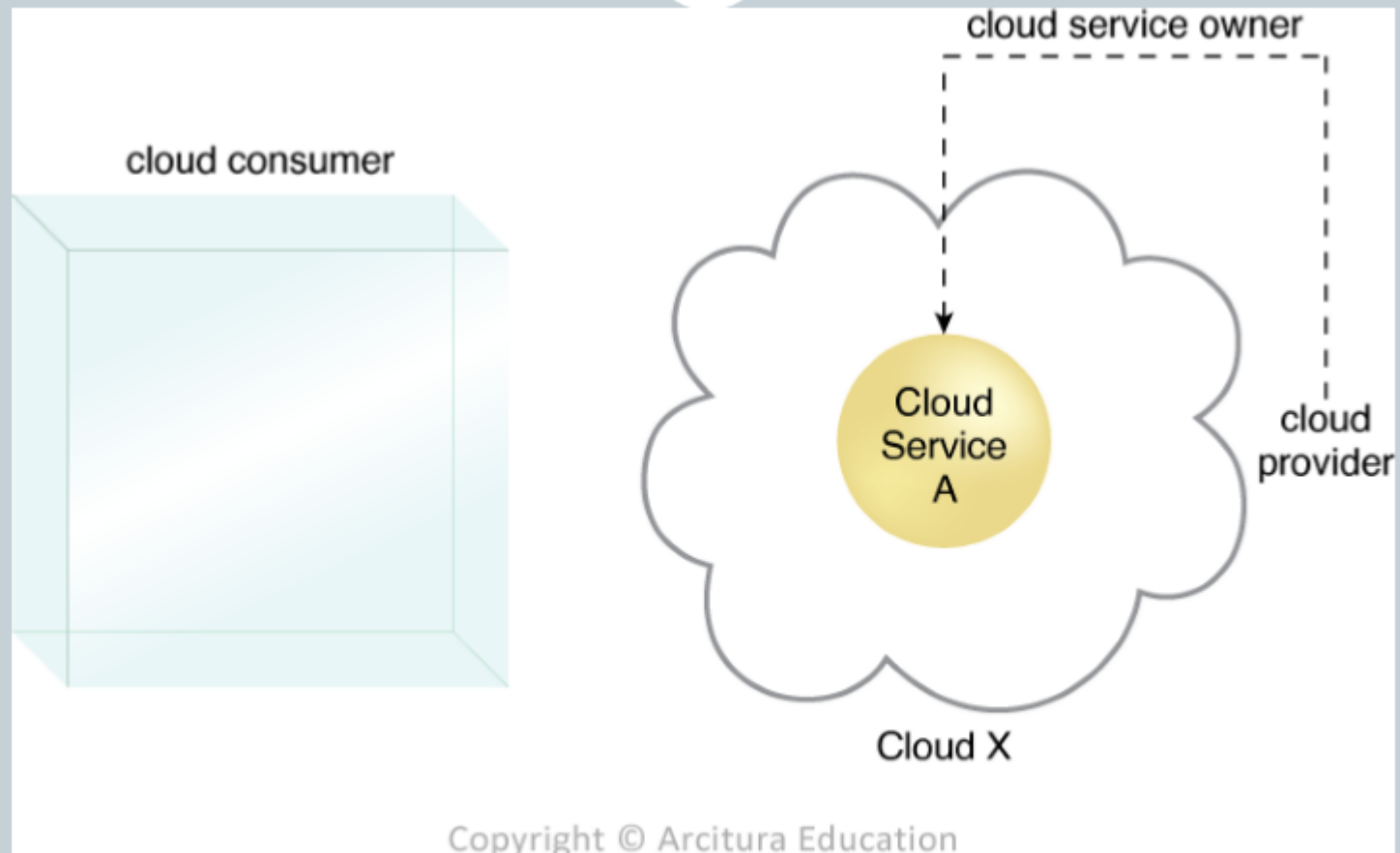
- The person organization that legally owns a cloud service is called a **cloud service owner**.
- The cloud service owner can be **cloud consumer**, or the cloud **provider** that owns the cloud within which the cloud service resides.
- A cloud consumer that owns a cloud service **hosted by a third party** cloud does not necessarily need to be the user of the cloud service.
- A cloud service owner \neq a cloud resource owner

Roles and Boundaries (Cont..)



- *Figure 4.2 - A cloud consumer can be a cloud service owner when it deploys its own service in a cloud.*

Roles and Boundaries (Cont..)



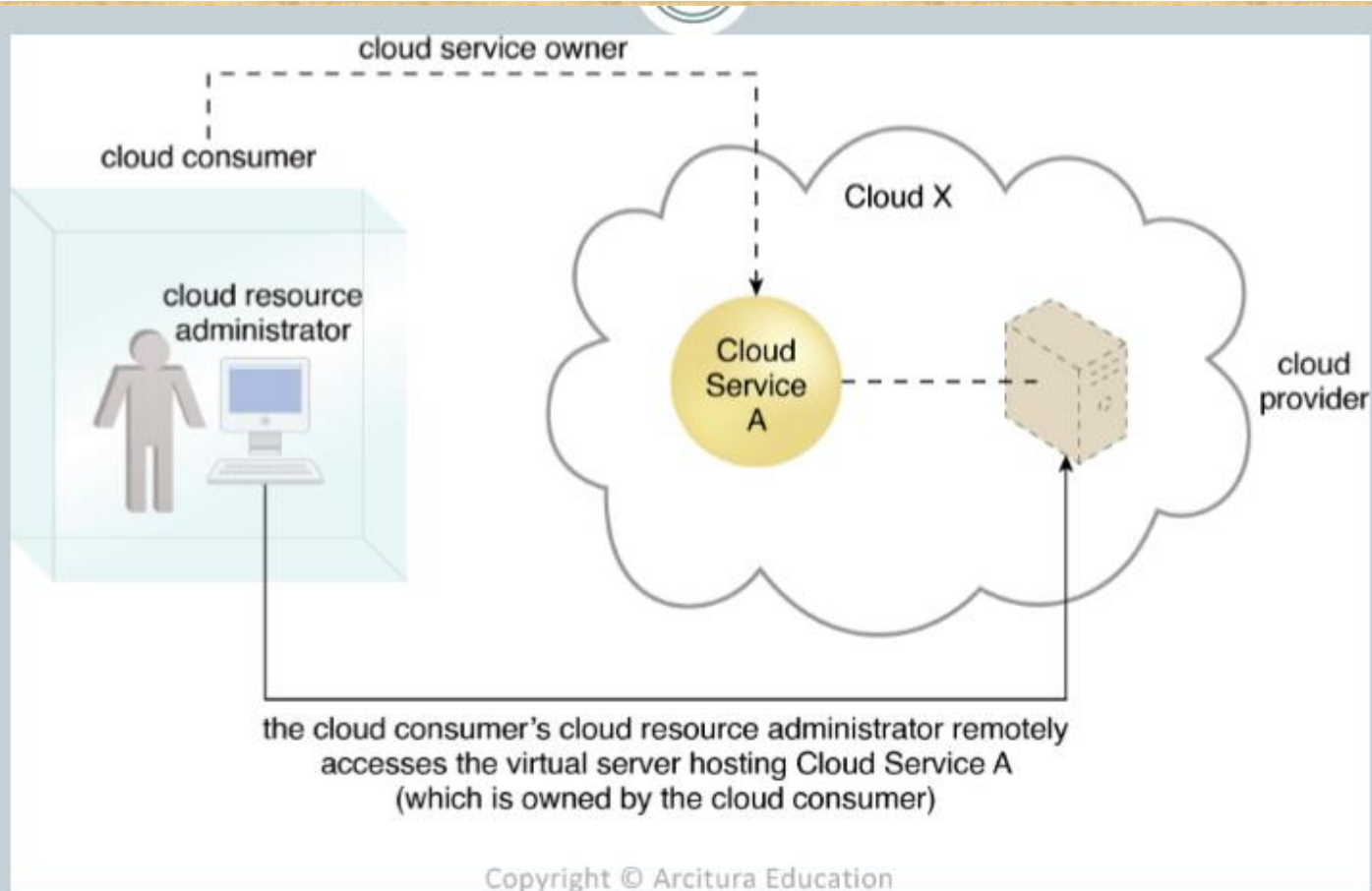
- *Figure 4.3 - A cloud provider becomes a cloud service owner if it deploys its own cloud service, typically for other cloud consumers to use.*

Roles and Boundaries (Cont..)

Cloud Resource Administrator

- A **cloud service administrator** is the person or organization responsible for administering a cloud-based IT resource (including IT services).
- The cloud consumer or cloud provider , or even third-party organization could be a cloud resource administrator.

Roles and Boundaries (Cont..)



- *Figure 4.4 - A cloud resource administrator can be with a cloud consumer organization and administer remotely accessible IT resources that belong to the cloud consumer.*

Roles and Boundaries (Cont..)

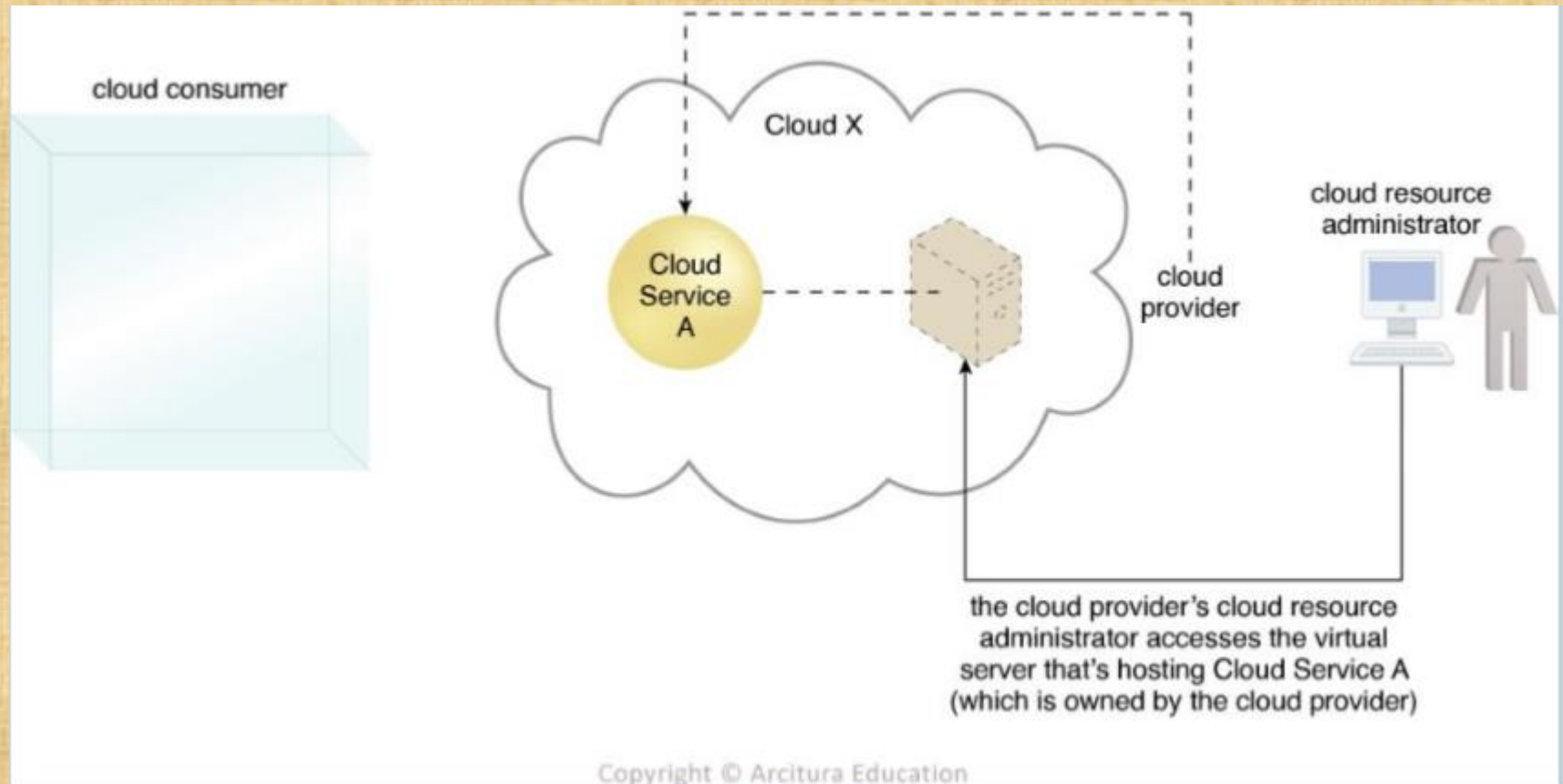


Figure 4.5 - A cloud resource administrator can be with a cloud provider organization for which it can administer IT resources, both internal and externally available, that belong to the cloud provider

Roles and Boundaries (Cont..)

Additional Roles of **cloud service administrator**

- The NIST cloud computing reference architecture defines the following supplementary roles
- **Cloud Auditor** – A third-party (often accredited) that conducts independent assessments of cloud environments assumes the role of the cloud auditor.
- **Cloud Broker** – This role is assumed by a party that assumes the responsibility of managing and negotiating usage of cloud services between cloud consumers and cloud providers.
- **Cloud Carrier** – The party responsible for providing the wire-level connectivity between cloud consumers and cloud providers assumes the role of the cloud carrier.

Roles and Boundaries (Cont..)

Organizational Boundary

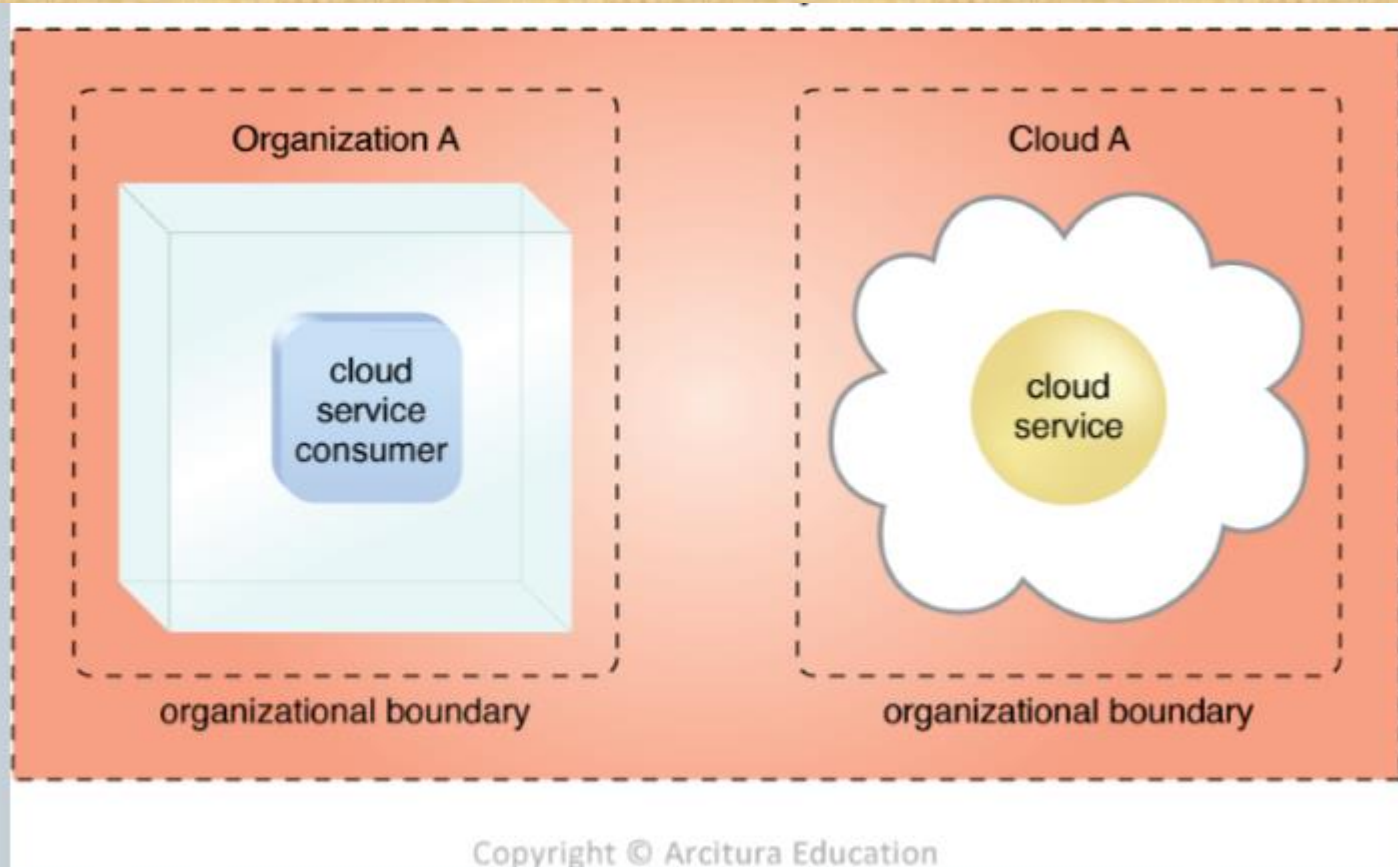
- An organization boundary represents that **physical perimeter that surrounds a set of IT resources** that are owned and governed by an organization.
- The organizational boundary does not represent the boundary of an actual organization, only an organizational set of IT assets and IT resources.

Roles and Boundaries (Cont..)

Trust Boundary

- When a cloud consumer accesses cloud-based IT resources, it needs to **extend its trust beyond the physical boundary** of the organization to include parts of the cloud environment.
- An trust boundary is a **logical perimeter** that typically spans beyond physical boundaries to represents the extent to which IT resources are trusted.
- When analyzing cloud environments, the trust boundary is most frequently associated with the trust issued by the organization acting as the cloud consumer.

Roles and Boundaries (Cont..)



- *Figure 4.7 - An extended trust boundary encompasses the organizational boundaries for the cloud provider and the cloud consumer.*

Cloud Characteristics

- On-demand usage
- Ubiquitous usage
- Multitenancy (and Resource Pooling)
- Elasticity
- Measured Usage
- Resiliency

On-demand usage

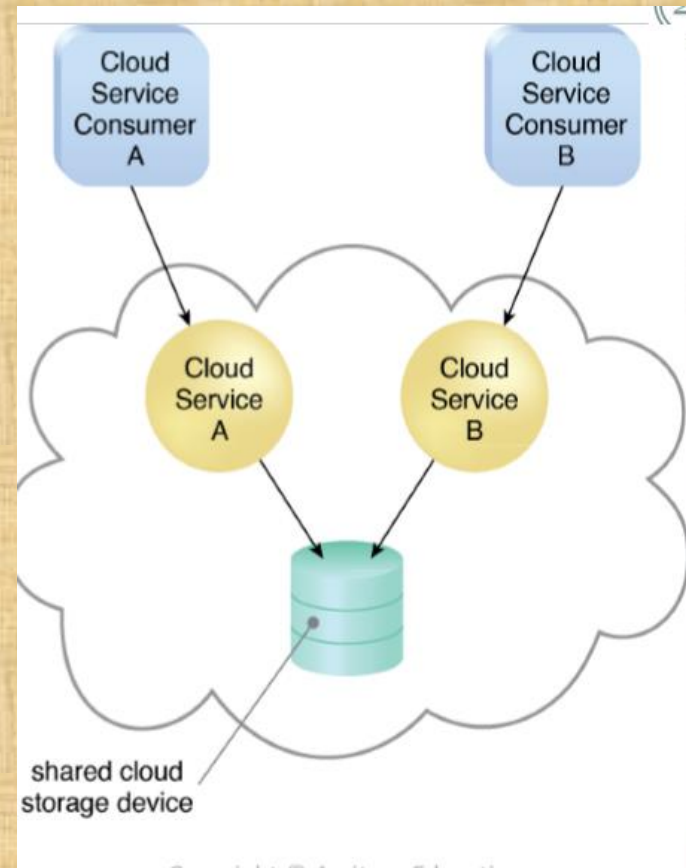
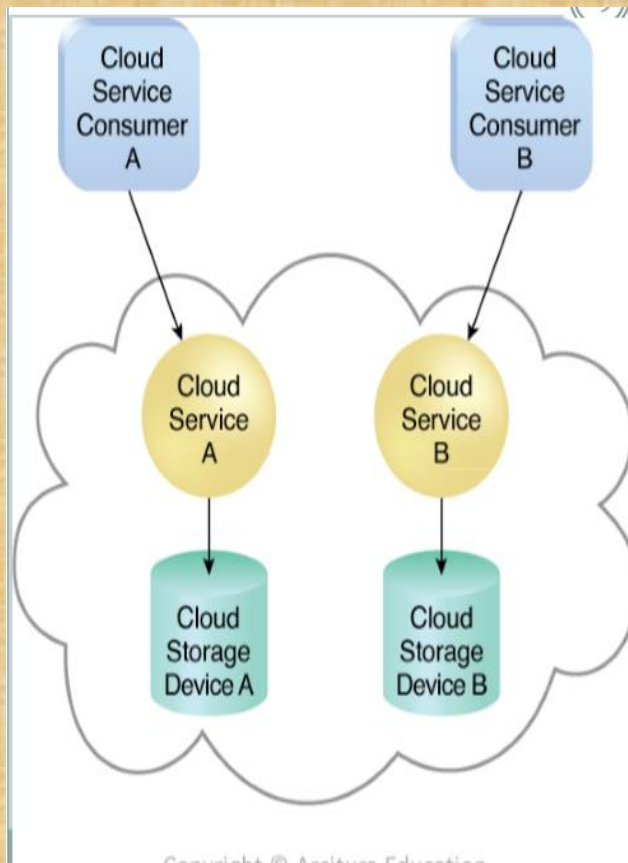
- **On-demand usage** is the ability of a cloud consumer to *self-provision* and use necessary cloud-based services without requiring cloud provider interaction.
- This characteristic is related to measured usage, which represents the ability of a cloud to measure the usage of its IT resources.

Ubiquitous Access

- The ability for a cloud service to be widely accessible.
- Range of device, transport protocols, interfaces, and security technologies.

Multitenancy

- The ability of a single instance of an IT resource to transparently serve multiple cloud consumers simultaneously



Elasticity

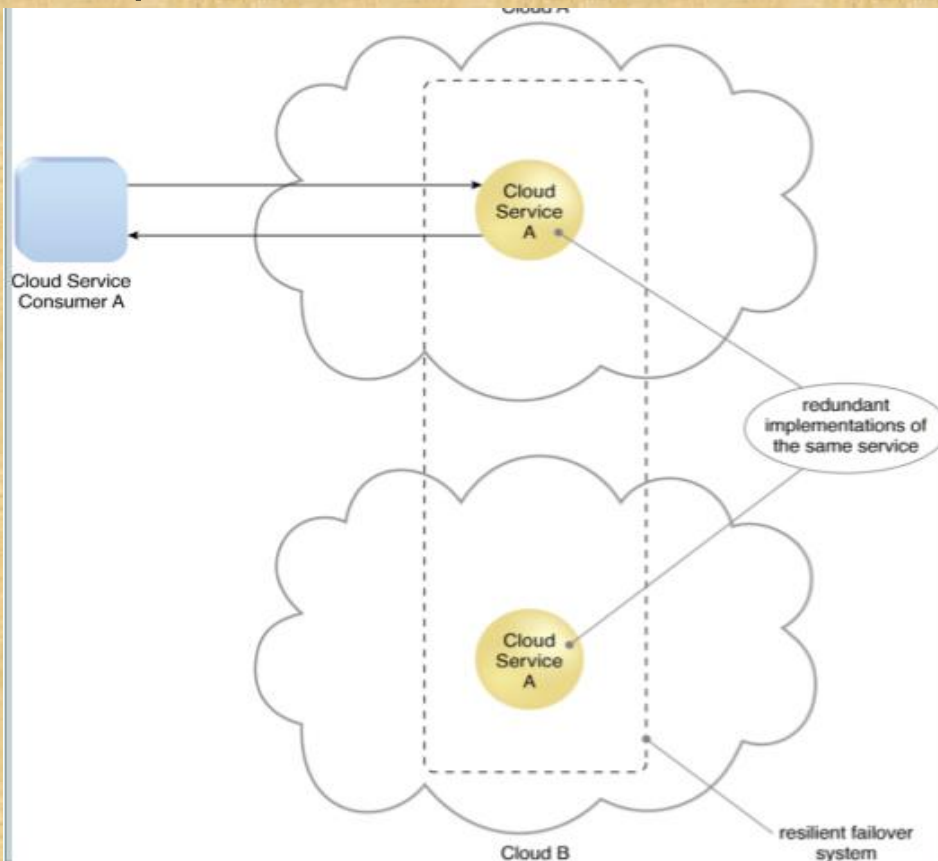
- The elasticity characteristic represents the ability of a cloud to transparently and automatically scale IT resources out or in.
- It is closely associated with the reduced investment and proportional cost benefits.

Measured Usage

- The ability to keep track of the usage of IT resources, primarily by cloud consumers.

Resiliency

- Is a form of failover that distributes redundant implementations of IT resources across physical locations.

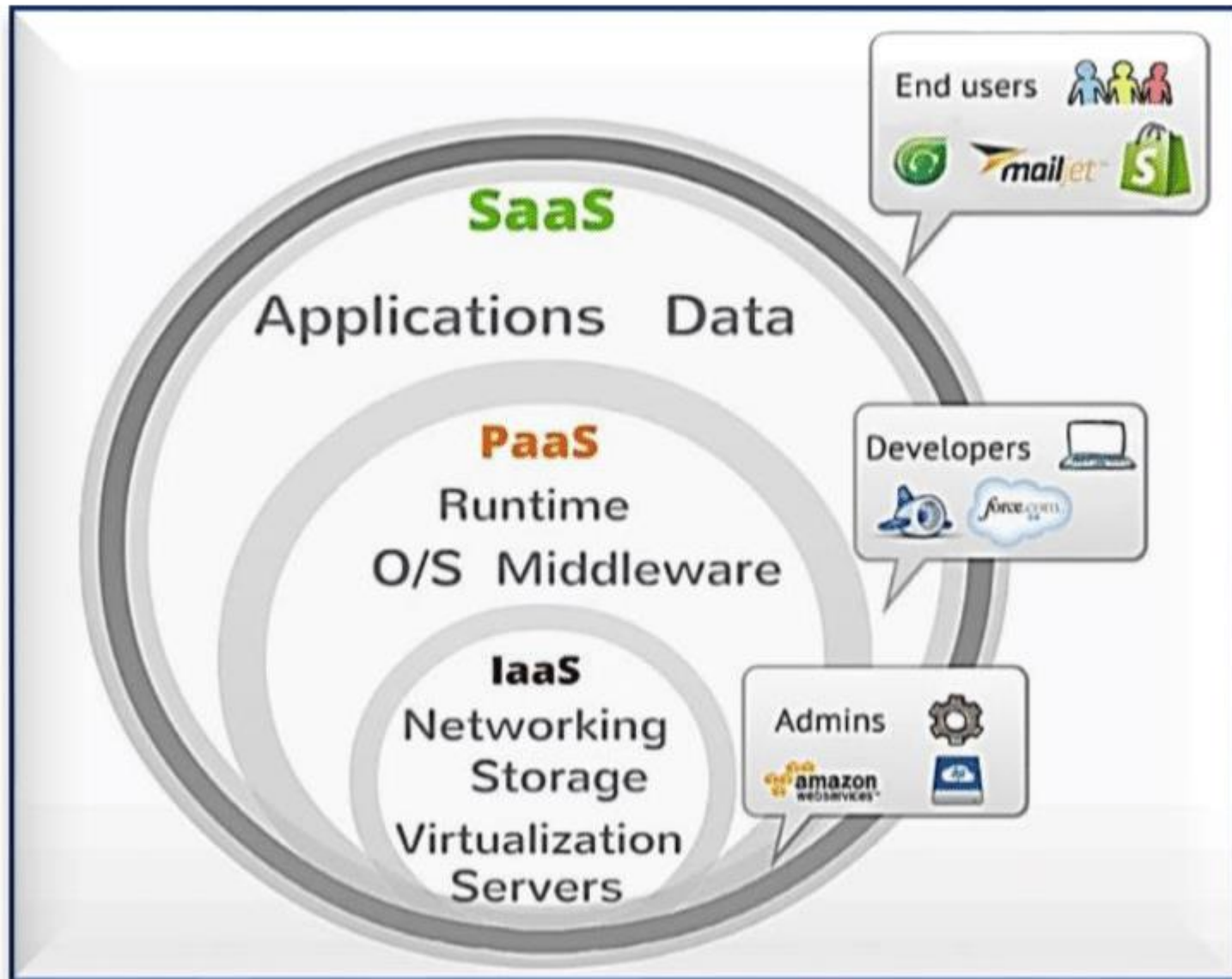


- Figure 4.10 - A resilient system in which Cloud B has a redundant implementation of Service A to provide a failover capacity in case Service A on Cloud A becomes unavailable.*

Cloud Delivery Models

- ❑ Infrastructure-as-a-Service (IaaS)
- ❑ Platform-as-a-Service (PaaS)
- ❑ Software-as-a-Service (SaaS)
- ◆ Variations are emerged by comprised of a distinct combination of IT resources, such as
 - storage-as-a-service
 - database-as-a-service
 - security-as-a-service
 - communication-as-a-service
 - integration-as-a-service

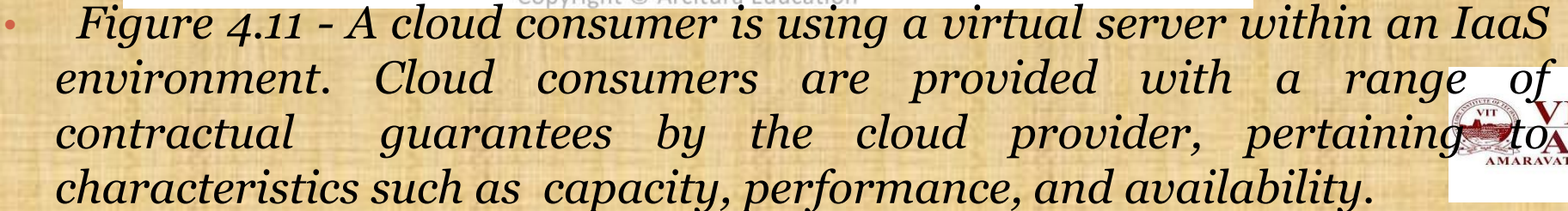
Cloud Delivery Model



IaaS Characteristics:

- IaaS platforms are:
 - Highly flexible and highly scalable.
 - Accessible by multiple users.
 - Cost-effective.

●



Platform-as-a-Service (PaaS)

Platform-as-a-Service (PaaS)

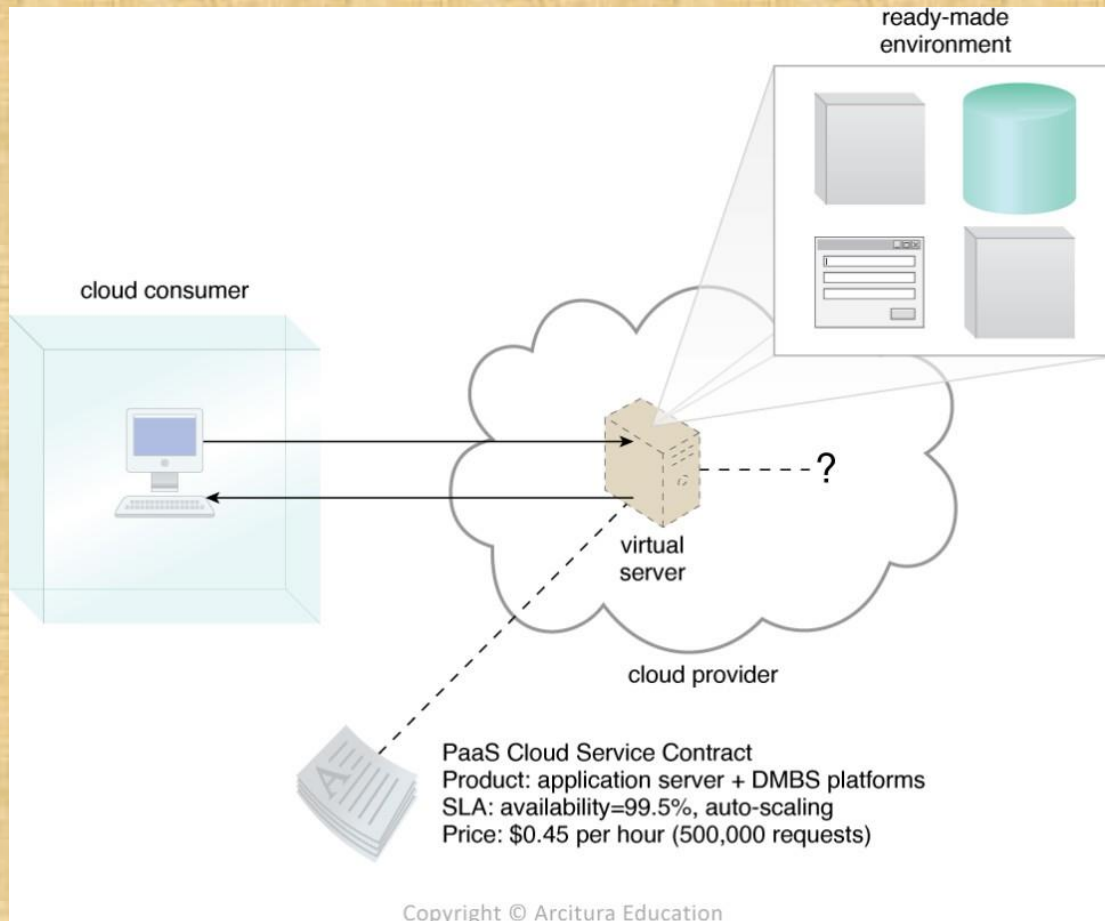
- It represents a pre-defined **ready-to-use** environment typically comprised of already deployed and configured IT resources.
- PaaS relies on the usage of a **ready-made environment** that establishes a set of pre-packaged products and tools used to support the entire delivery lifecycle of custom applications.
- As an example, GAE offers a Java and Python-based environment.

PaaS Characteristics:

PaaS platforms are:

- Accessible by multiple users.
- Scalable – you can choose from various tiers of resources to suit the size of your business.
- Built on virtualization technology.
- Easy to run without extensive system administration knowledge.

PaaS



A cloud consumer is accessing a ready-made PaaS environment. The question mark indicates that the cloud consumer is intentionally shielded from the implementation details of the platform.

Software-as-a-Service (SaaS)

Software-as-a-Service (SaaS)

- A software program positioned as a shared cloud service and made available as a product or generic utility represents the typical profile of a SaaS offerings.
- A cloud consumer is generally granted very limited administrative control over a SaaS implementation.

SaaS Characteristics

- SaaS platforms are:
- Available over the internet.
- Hosted on a remote server by a third-party provider.
- Scalable, with different tiers for small, medium, and enterprise-level businesses.
- Inclusive, offering security, compliance, and maintenance as part of the cost.

SaaS

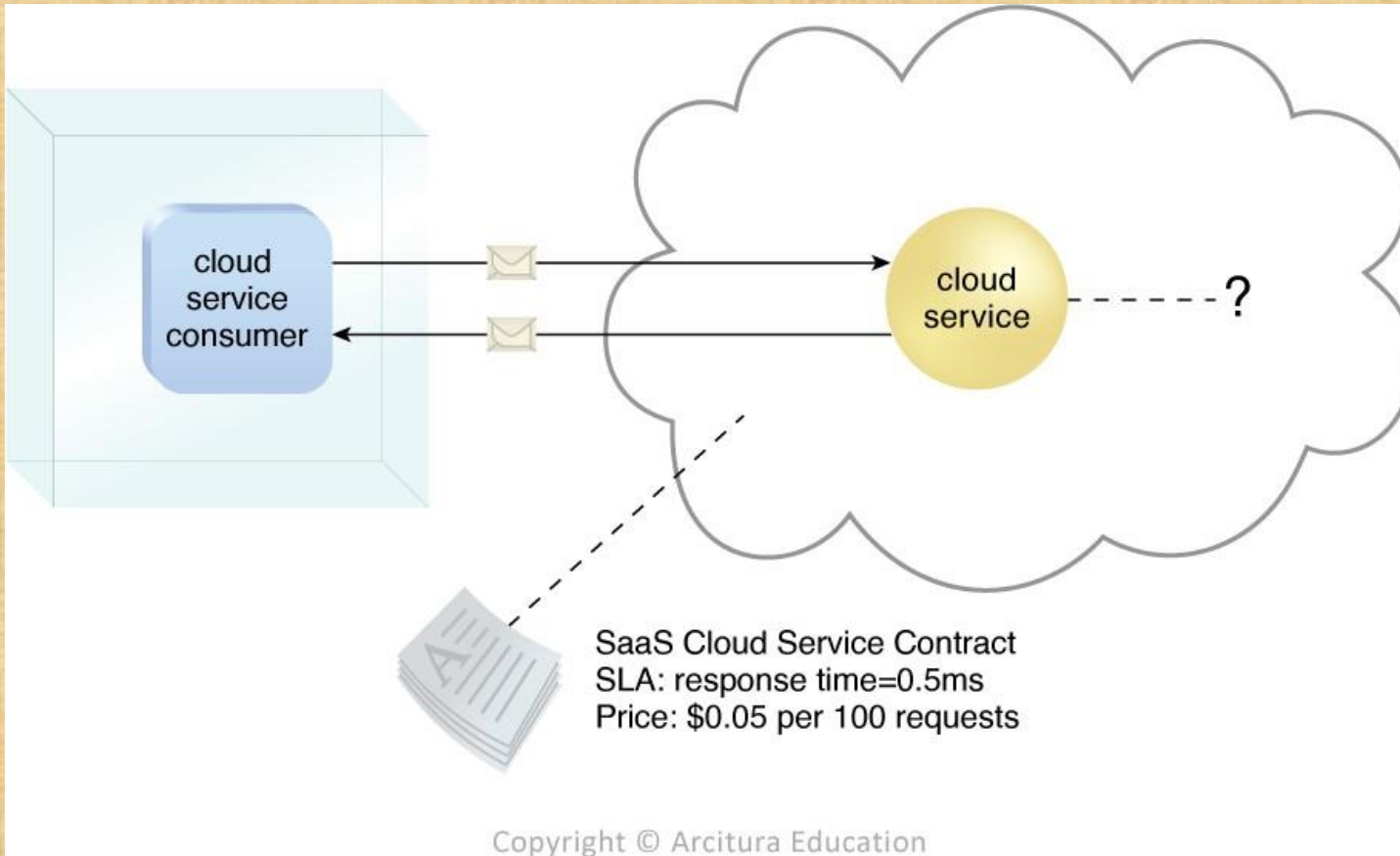
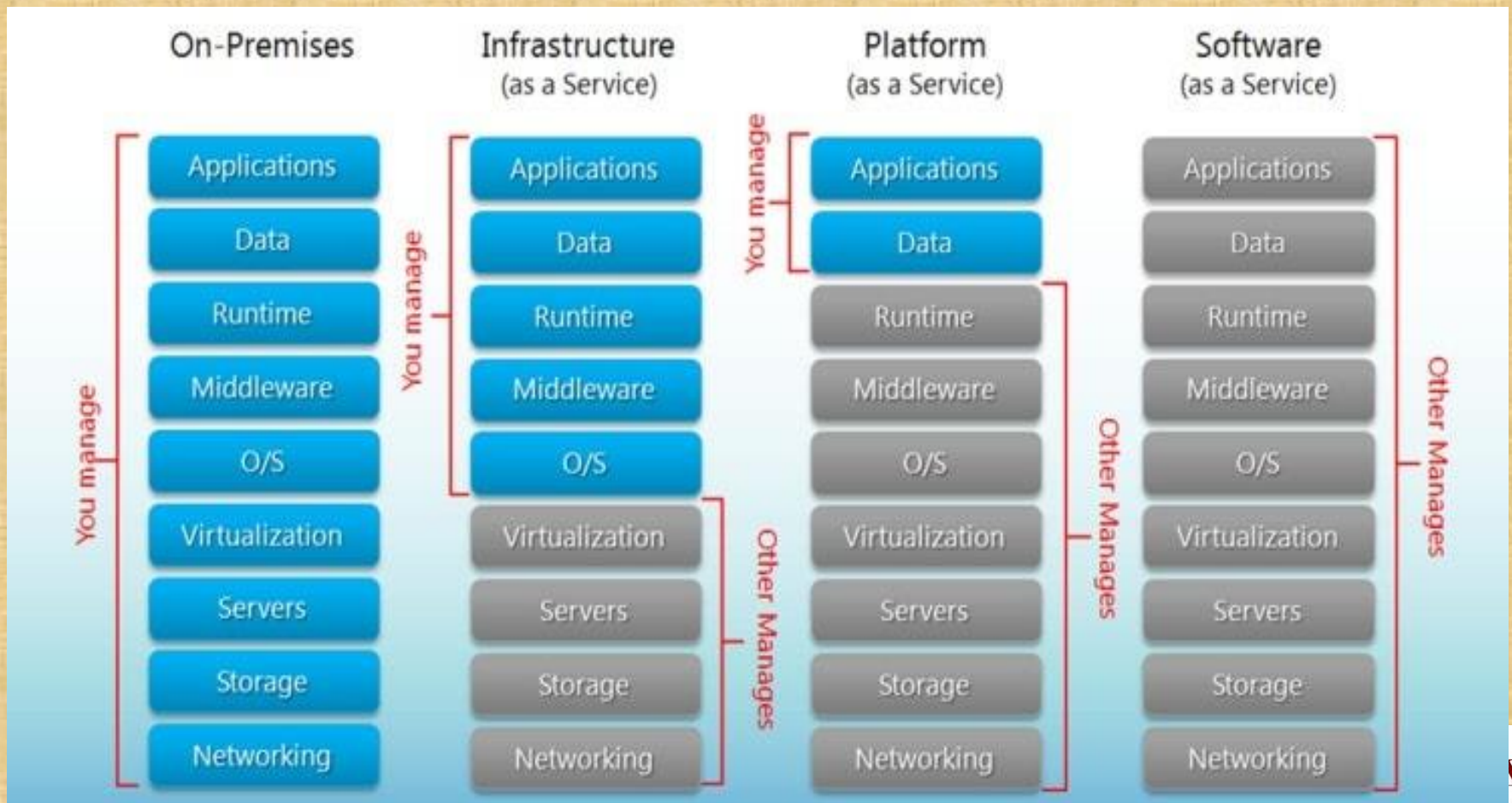


Figure 4.13 - The cloud service consumer is given access the cloud service contract, but not to any underlying IT resources or implementation details.

Differences in service models



Pros and Cons of different service models

Type	Advantages	Disadvantages
SaaS	<ul style="list-style-type: none">• Fast to realise benefits, quick set up and deployment• Lower up-front cost• Scalability and integration• New releases (upgrades)• Accessibility	<ul style="list-style-type: none">• Lack of control• Vendor drives upgrades and new feature timelines• Security and data sovereignty concerns• Limited range of applications• Connectivity requirement• Performance concerns (speed, reliability, support)
PaaS	<ul style="list-style-type: none">• Simple, cost-effective development and deployment of applications• Scalable• Highly available• No need for maintaining software• Significant reduction in the amount of coding required• Automation of business processes/policies	<ul style="list-style-type: none">• Dependency on vendor• Security and data concerns• Compatibility of existing infrastructure• Performance concerns (speed, reliability, support)
IaaS	<ul style="list-style-type: none">• Most flexible cloud computing model• Easy to automate deployment of storage, networking, servers, and processing power• Hardware purchases can be based on consumption• Clients retain complete control of their infrastructure• Resources can be purchased as needed• Highly scalable	<ul style="list-style-type: none">• Security and data concerns• Legacy systems operating in the cloud• Internal resources and training• Multi-tenant security• Control over costs if scalability is unlimited

Examples

- **SaaS providers:** BigCommerce, Google Apps, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot.
- **PaaS providers:** AWS Elastic Beanstalk, Heroku, Windows Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud.
- **IaaS providers:** AWS EC2, Rackspace, Google Compute Engine (GCE), Digital Ocean, Magento 1 Enterprise Edition*.

Cloud Delivery Models - Comparisons

Cloud Delivery Model	Typical Level of Control Granted to Cloud Consumer	Typical Functionality Made Available to Cloud Consumer
SaaS	usage and usage-related configuration	access to front-end user-interface
PaaS	limited administrative	moderate level of administrative control over IT resources relevant to cloud consumer's usage of platform
IaaS	full administrative	full access to virtualized infrastructure-related IT resources and possibly, to underlying physical IT resources

Table 4.2 Typical activities carried out by cloud consumers and cloud providers in relation to the cloud delivery models.

Cloud Delivery Model	Common Cloud Consumer Activities	Common Cloud Provider Activities
SaaS	uses and configures cloud service	implements, manages, and maintains cloud service Monitors usage by cloud consumers
PaaS	develops, tests, deploys, and manages cloud services and cloud-based solutions	pre-configures platform and provisions underlying infrastructure, middleware, and other needed IT resources, as necessary monitors usage by cloud consumers
IaaS	sets up and configures bare infrastructure, and installs, manage, and monitors any needed software	provisions and manages the physical processing, storage, networking, and hosting required monitors usage by cloud consumers

Cloud Delivery Models - Combinations

Combining Cloud Delivery Models

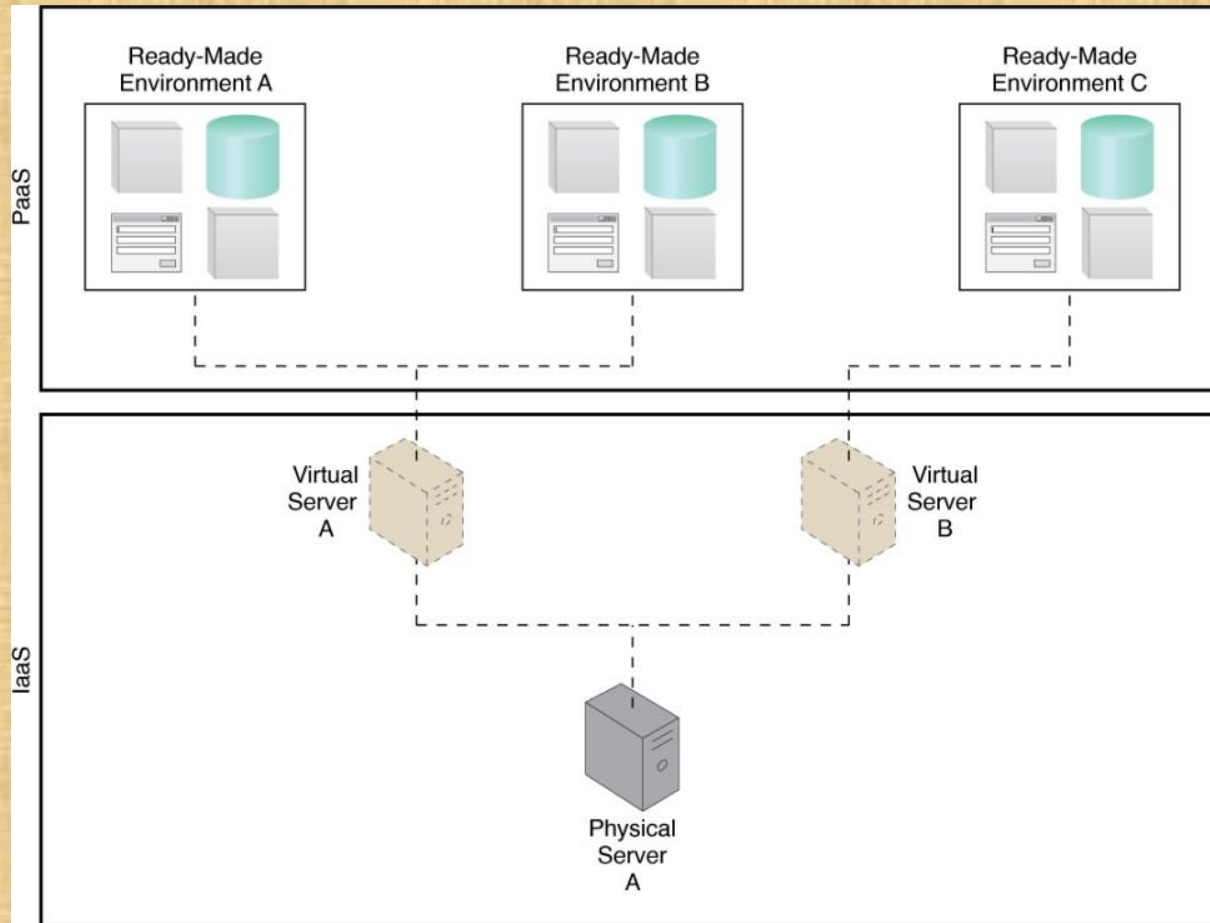
○ IaaS + PaaS

- For instance, the cloud provider offering the PaaS environment chose to lease an IaaS environment from a different cloud provider.

○ IaaS + PaaS + SaaS

- For instance, by adding on to the preceding layered architecture, the ready-made environment provided by the PaaS environment can be used by the cloud consumer organization to develop and deploy its own SaaS cloud services that it can then make available as commercial products.

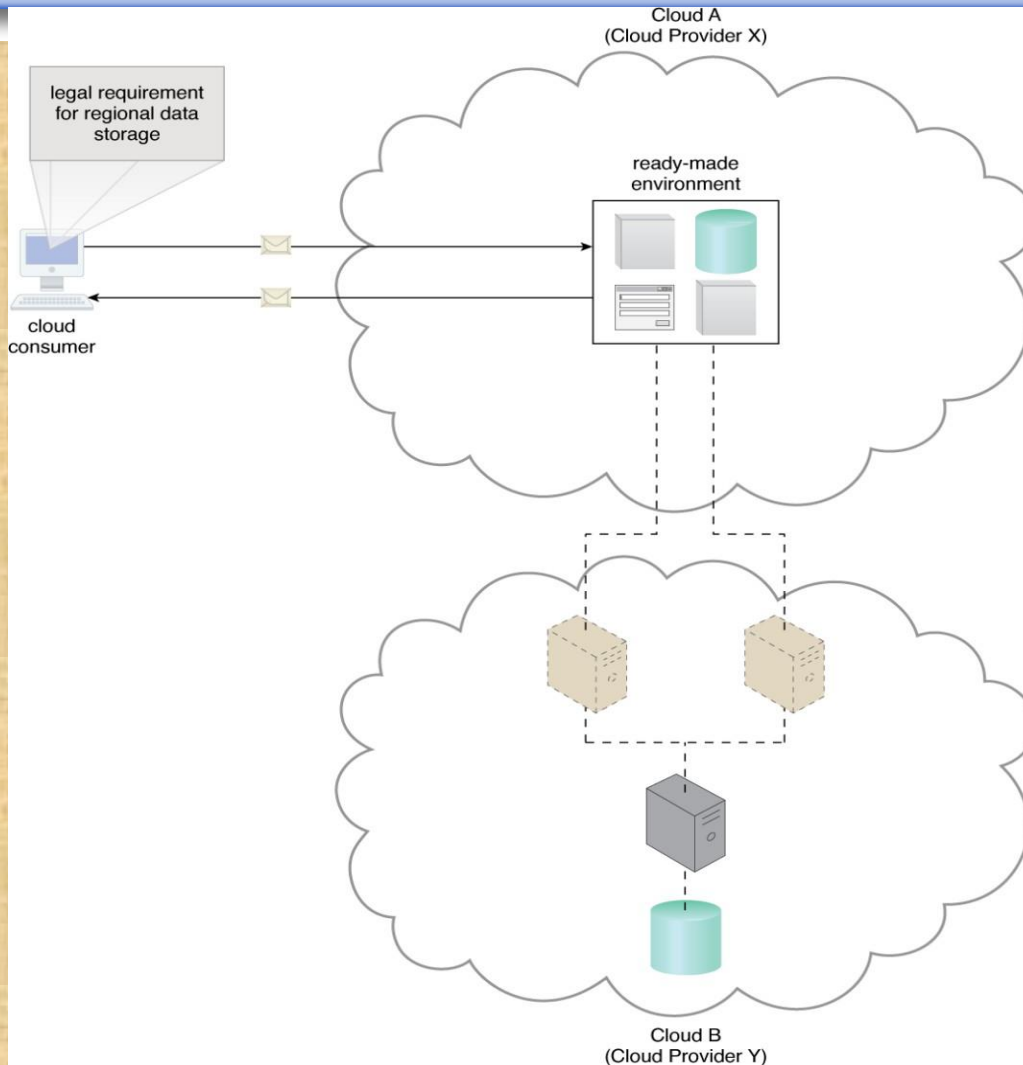
PaaS+IaaS



PaaS environment based on the IT resources provided by an underlying IaaS environment.

A

Different vendors delivery Models



- Figure 4.15 - An example of a contract between Cloud Providers X and Y, in which services offered by Cloud Provider X are physically hosted on virtual servers belonging to Cloud Provider Y. Sensitive data that is legally required to stay in a specific region is physically kept in Cloud B which is physically located in that region.

Multi-Regional Compliance and Legal Issues

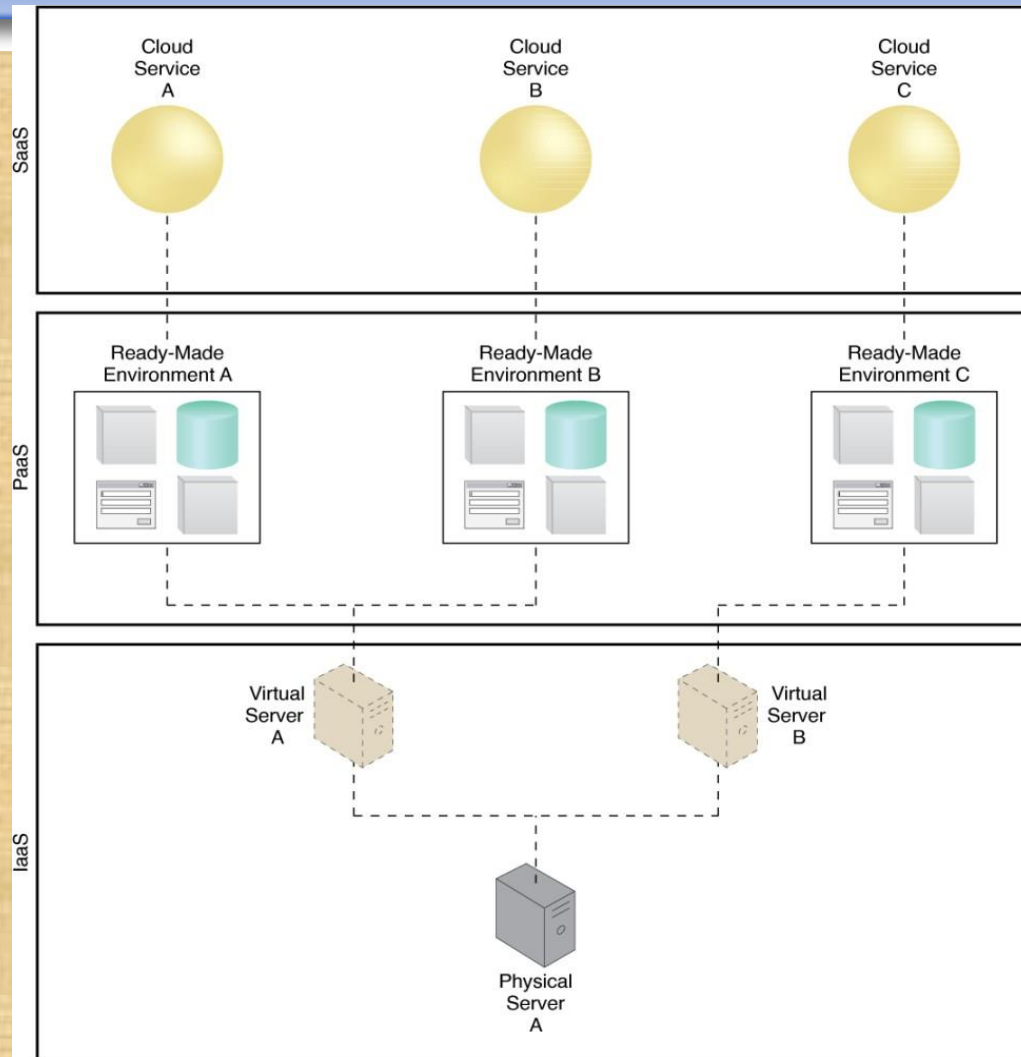


Figure 4.16 - A simple layered view of an architecture comprised of IaaS and PaaS environments hosting three SaaS cloud service implementations.

Summary of Key Points

- The **IaaS delivery model** offers cloud consumers a high level of administrative control over “raw” infrastructure-based IT resources.
- The **PaaS delivery model** enables a cloud provider to offer a preconfigured environment that cloud consumers can use to build and deploy cloud services and solutions, albeit with decreased administrative control.
- **SaaS** is a cloud deliver model for shared cloud services that can be positioned as commercialized products hosted by clouds.
- Different **combinations of IaaS, PaaS, and SaaS** are possible, depending on how cloud consumers and cloud providers choose to leverage the natural hierarchy established by these base cloud delivery models.

Cloud Service Models Forecast for 2020

74%

of the total cloud workloads will be **Software-as-a-Service (SaaS)** workloads, up from 65% in 2015.

8%

of the total cloud workloads will be **Platform-as-a-Service (PaaS)** workloads, down from 9% in 2015

17%

of the total cloud workloads will be **Infrastructure-as-a-Service (IaaS)** workloads, down from 26% in 2015.

92%

of all workloads will be processed in the cloud

Cloud Deployment Models

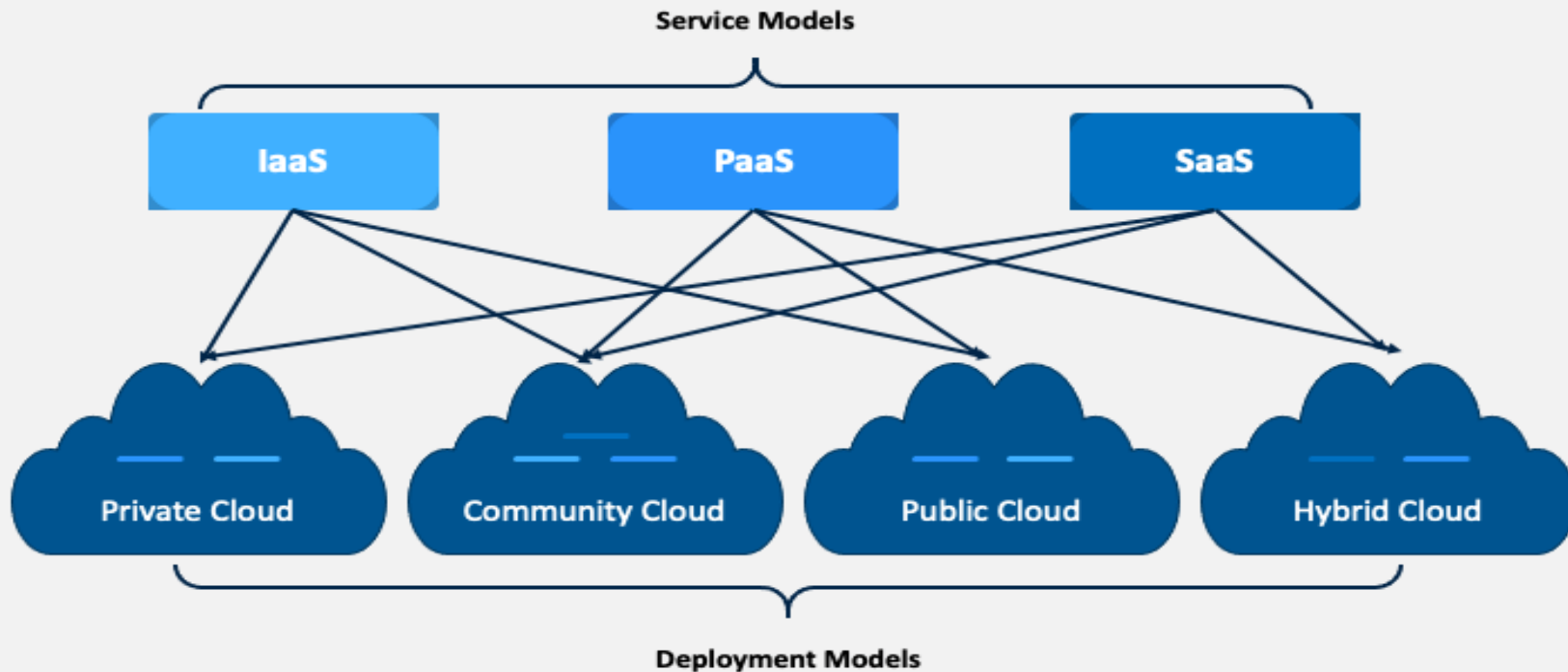
The cloud deployment model represents the exact category of cloud environment based on proprietorship, size, and access and also describes the nature and purpose of the cloud.

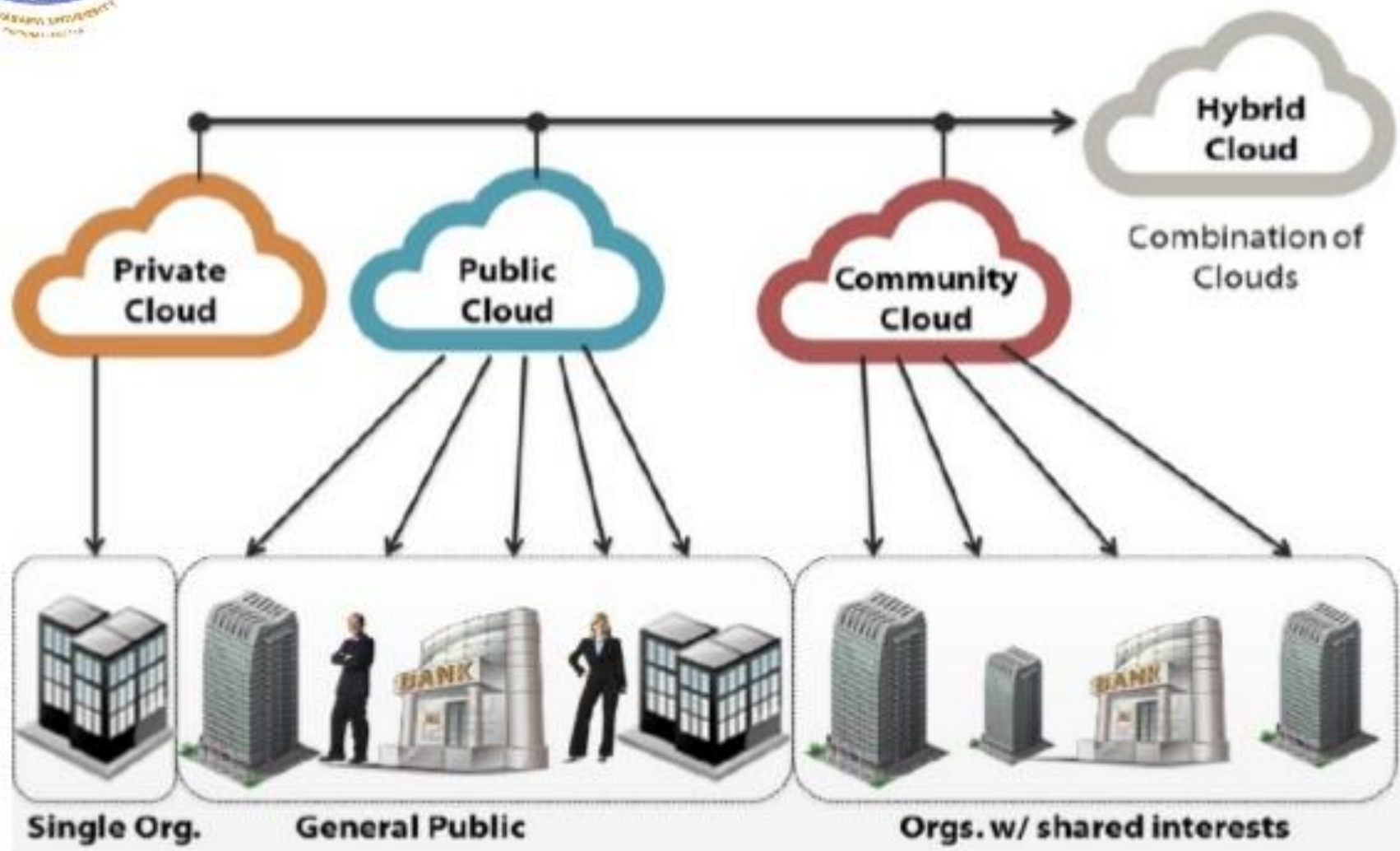
- Public Cloud Model
- Private Cloud Model
- Hybrid Cloud Model
- Community Cloud Model

Cloud Deployment Models

CLOUD DEPLOYMENT MODELS

Enter your sub headline here





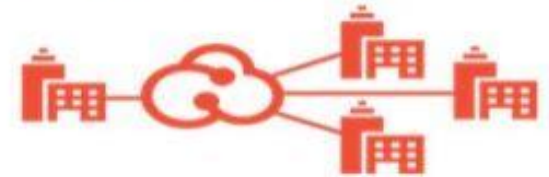
Cloud delivery models

Customers are choosing a variety of cloud models to meet their unique needs and priorities.



Private Cloud

On or off premises cloud infrastructure operated solely for an organization and managed by the organization or a third party



Public Cloud

Available to the general public or a large industry group and owned by an organization selling cloud services



Hybrid Cloud

Traditional IT and clouds (public and private) that remain separate but are bound together by technology that enables data and application portability



Traditional IT

Appliances, pre-integrated systems and standard hardware, software, and networking

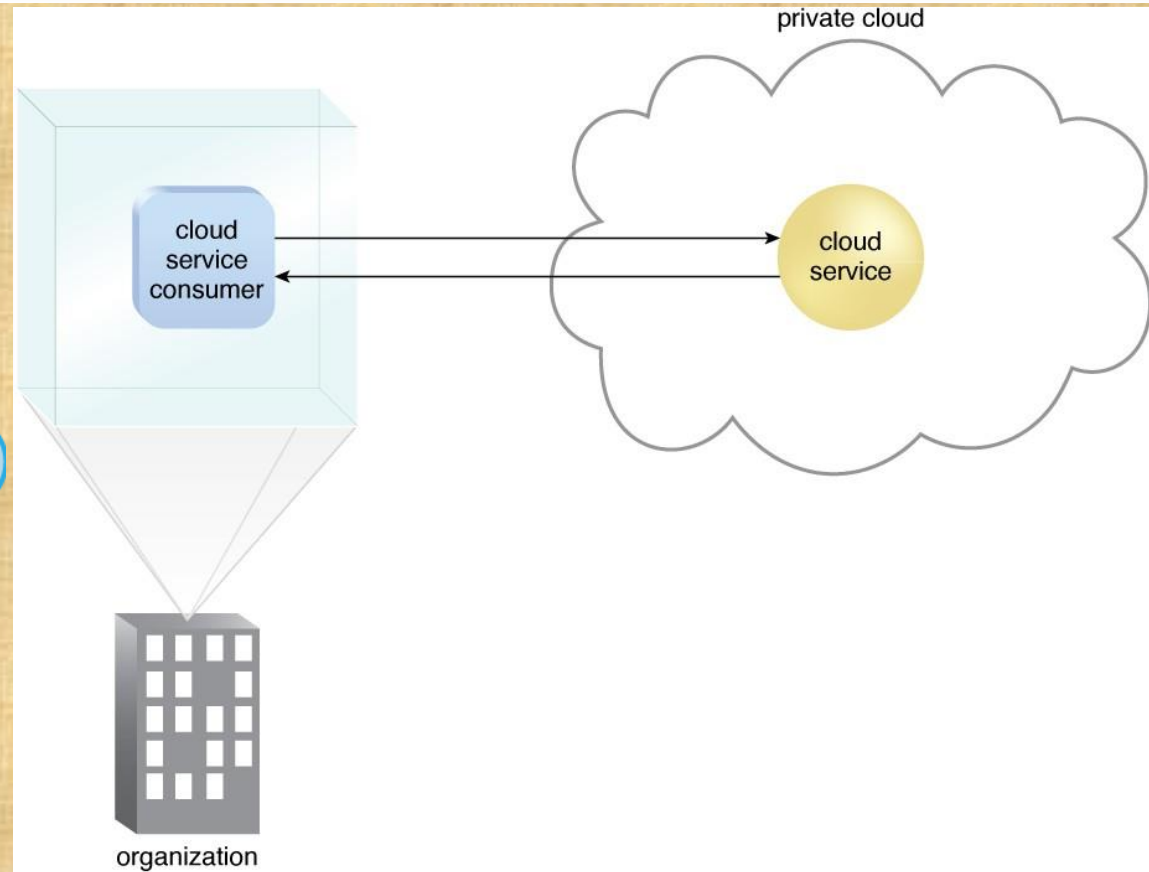
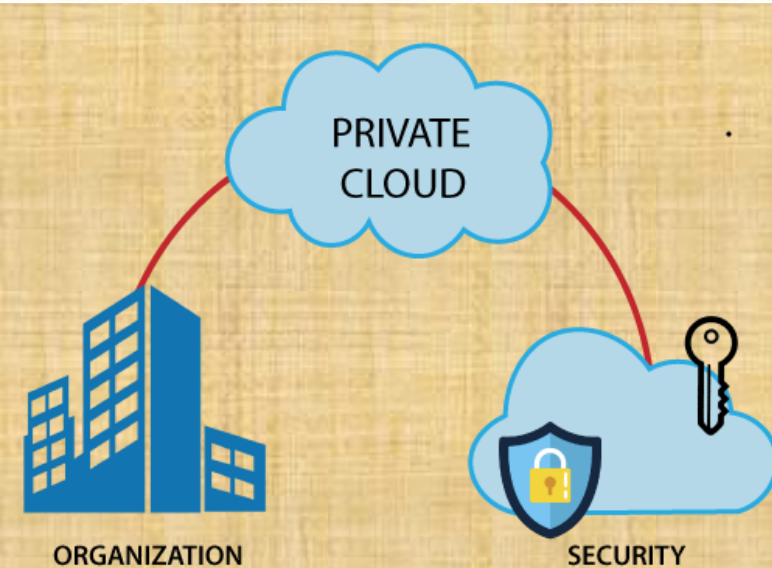
Private Cloud

- A private cloud is owned by a single organization.
- Private clouds enable an organization to use cloud computing technology as a means of centralizing access to IT resources by different parts, locations, or departments of the organization.
- When a private cloud exists as a controlled environment, the problems described in the Risks and Challenges section do not tend to apply.

Private Cloud

- Cloud infrastructure built in house
- Retains control of resources
- More security & privacy
- Can conform to regulatory requirement
- Needs capital investment
- Needs expertise to build and maintain

Private Cloud



Copyright © Arcitura Education

Private Cloud

Benefits

- Better security
- Better control
- Predictable costs
- Legal compliance

Limitations

- Limited scalability
- Huge initial capex
- Limited access

Use Case

- Highly regulated businesses
- Tech companies that require complete control
- Large companies that require custom solutions

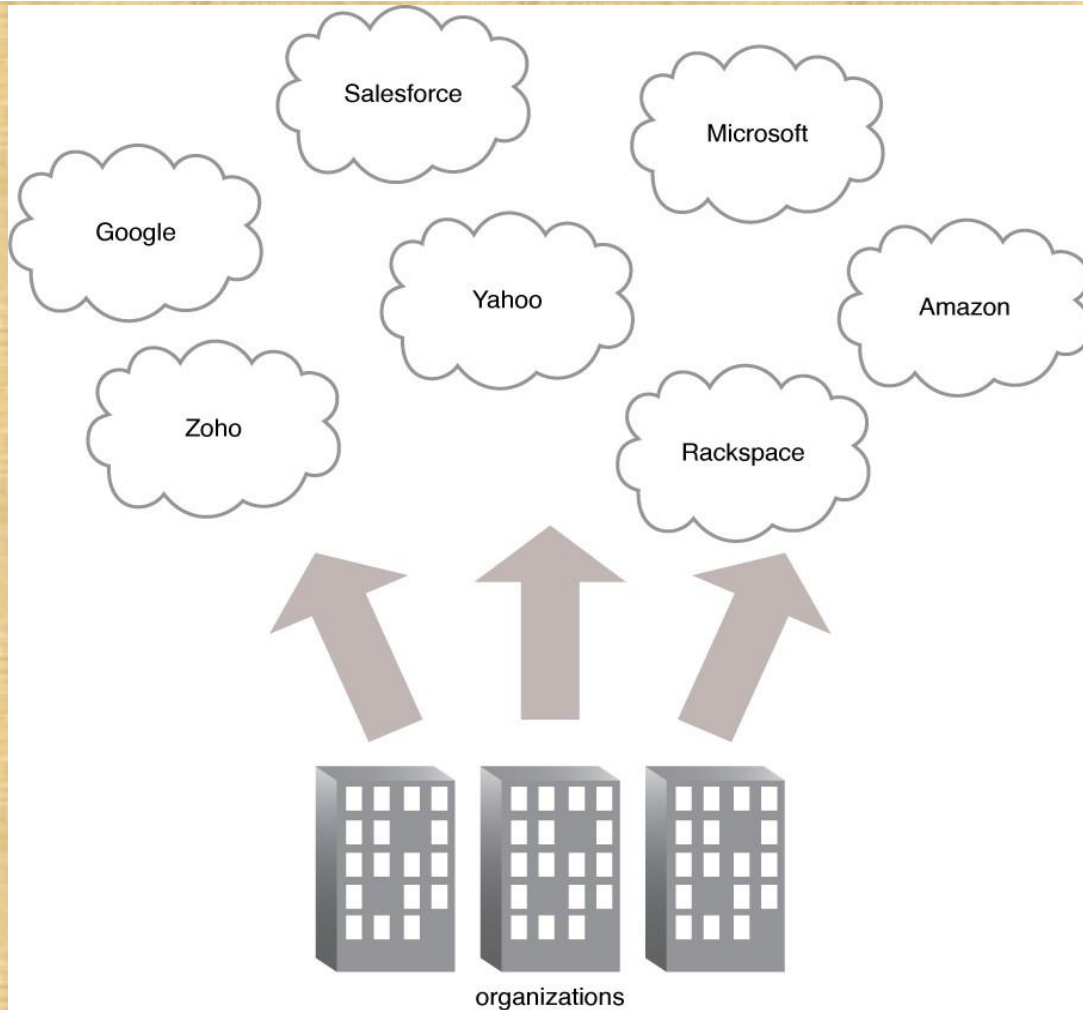
Public Cloud

- A public cloud is a publicly accessible cloud environment owned by a third-party cloud provide.
- The IT resources on public clouds are usually provisioned via cloud delivery models.
- The cloud provider is responsible for the creation and on-going maintenance of the public cloud and its IT resources.

Public Cloud

- Available to everyone.
- Anyone can go and signup for the service.
- Economies of Scale due to Size.
- Some public cloud concerns
 - Ownership
 - Control
 - Regulatory compliance
 - Data/Application security
 - Liability for SLA breaches

Public cloud



- *Organizations act as cloud consumers when accessing cloud services and IT resources made available by different cloud providers.*



Public Clouds

Advantages to Public Cloud Computing

- Minimal capital expenditures
- No upfront risk or commitments
- Highly agile in dynamically sharing resources with multiple customers
- Cost efficient
- Pay-for what is used
- Internet accessible
- Maintenance

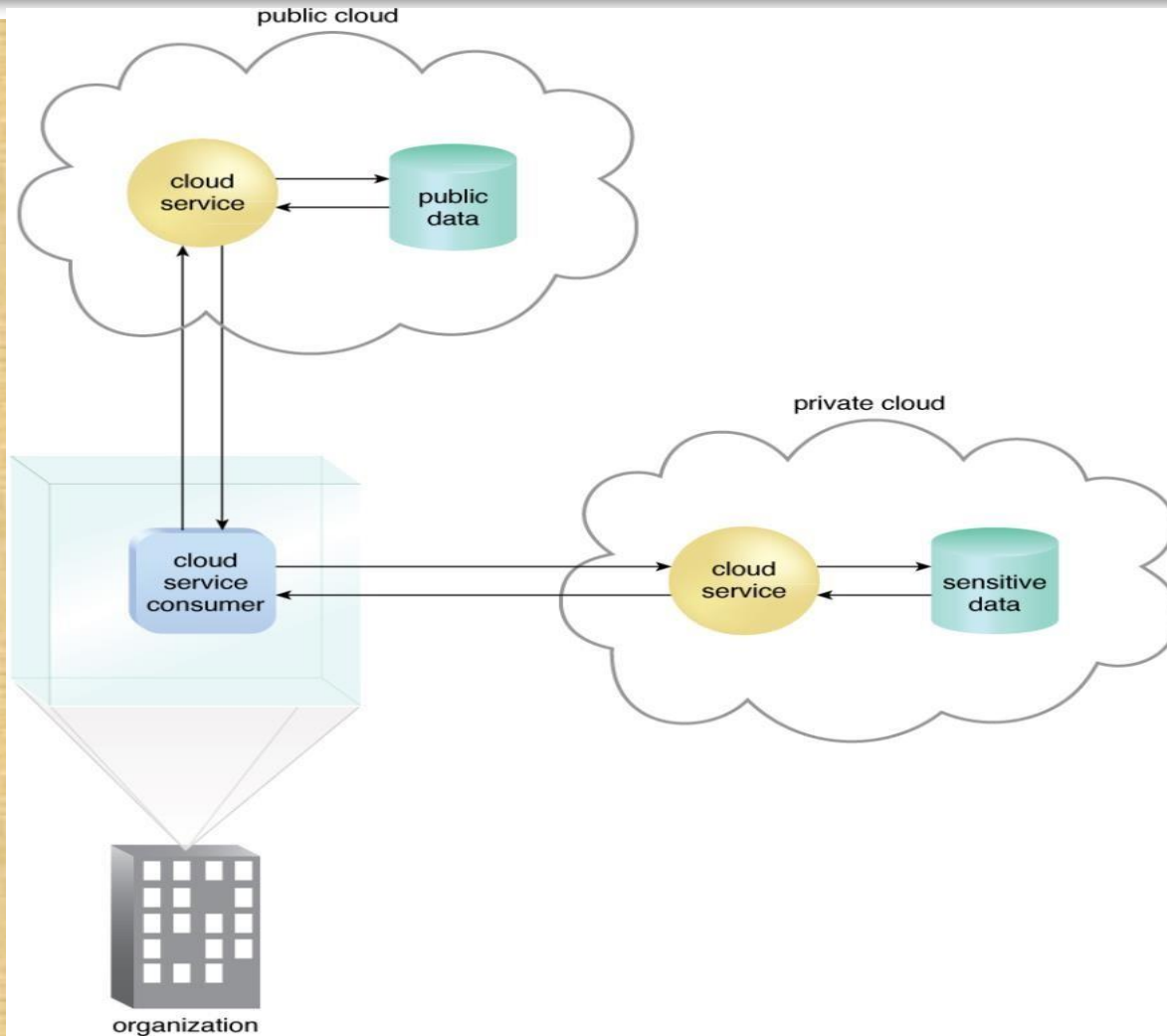
Disadvantages to Public Cloud Computing

- Lack of Control
- Scalability within instances
- Lack of Investment
- Speed and Performance
- Reliability and Security
- Legacy systems

Hybrid Clouds

- A hybrid cloud is a cloud environment comprised of two or more different cloud deployment models.
- Best of Both World.
- Workload is deployed mostly on private cloud.
- Resources can be used from public cloud when there is a surge in peak load (Cloud Burst)

Hybrid Cloud



- *An organization using a hybrid cloud architecture that utilizes both a private and public cloud.*

Hybrid Cloud

Advantages of Hybrid Cloud Model

1) Scalable

- It provides both the features of public and private cloud scalability.

2) Flexible and secure

- It provides secure resources because of private cloud and scalable resources because of public cloud.

3) Cost effective

- It is having less cost as compared to private cloud.

Disadvantages of Hybrid Cloud Model

1) Networking issues

- Networking becomes complex because of private and public cloud.

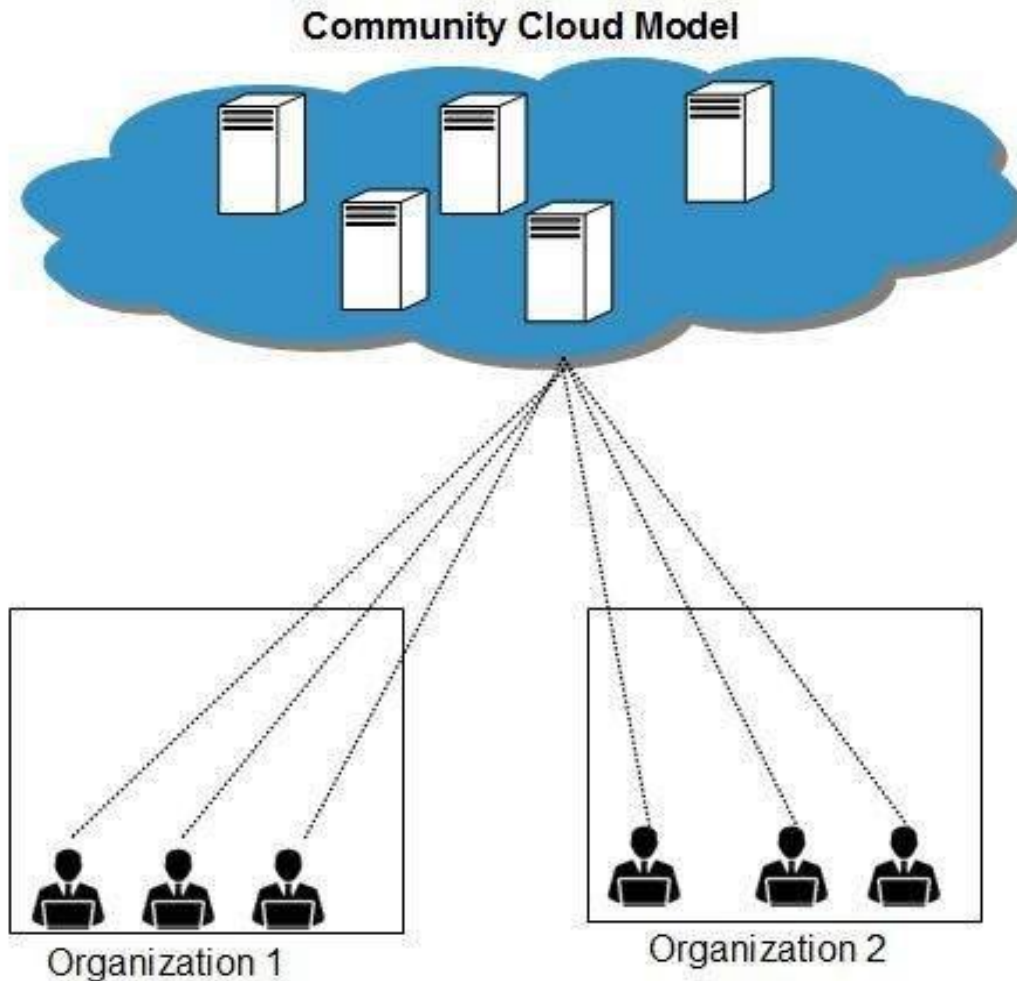
2) Security Compliance

- It is necessary to ensure that cloud services are compliant with the security policies of an organization.

Community Cloud

- The cloud service shares among various organizations and companies which belong to the same community with the common concerns. This can manage either by the third party or internally.
- Organizations having similar computing concern and have shared interest can share it.
- Community cloud diminishes the cost pressure, security concerns, technical complexities, and lack of specific services.

Example of a Community Cloud





Top Cloud Priority for Enterprises

