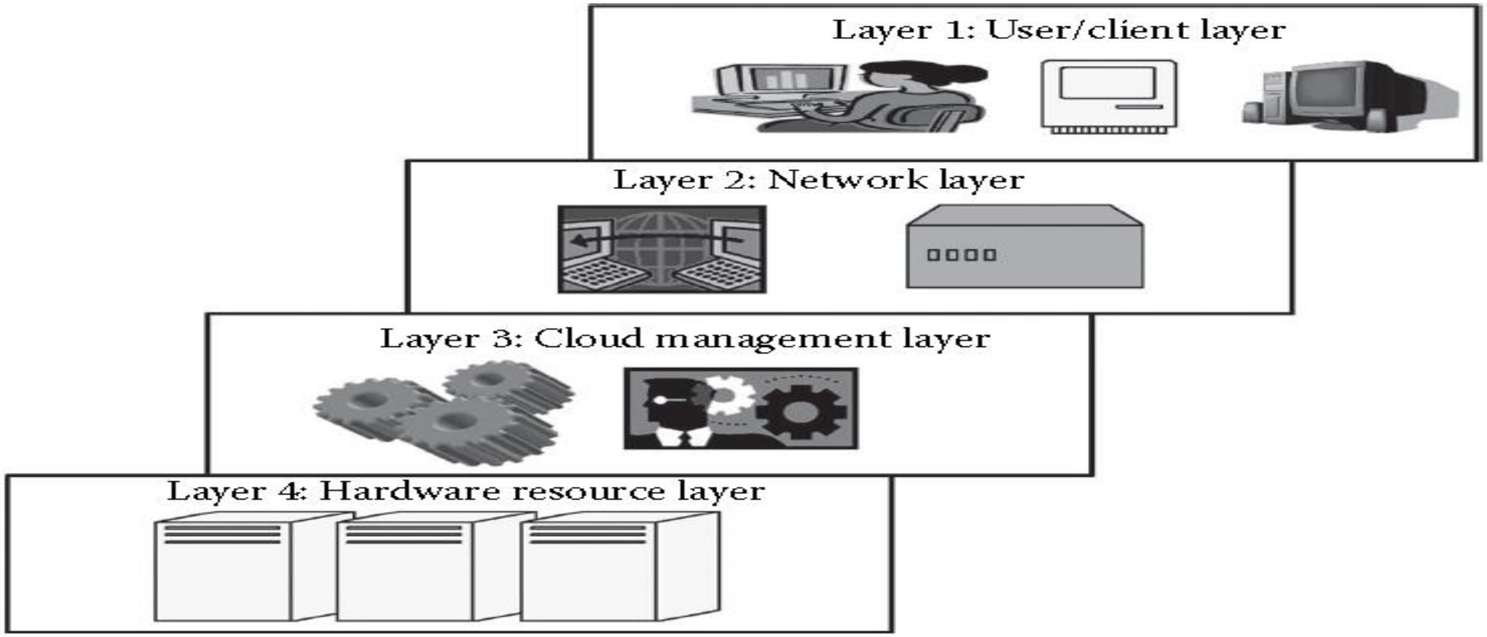
CAP470: Cloud Computing

Unit-2: Cloud Computing Architecture

Dr. Manmohan Sharma
Professor
School of Computer Applications
Lovely Professional University

Cloud Architecture

- The cloud also has an architecture that describes its working mechanism. It includes the dependencies on which it works and the components that work over it. The cloud is a recent technology that is completely dependent on the Internet for its functioning.
- Following figure depicts the 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)

- This layer is the lowest layer in the cloud architecture.
- 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.
- Similarly, 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. But internally, the properties of cloud applications are significantly different. Thus, this layer consists of client devices.

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). Even in this case, the cloud completely depends on the network that is used. Usually, when accessing the public or private cloud, the users require minimum bandwidth, which is sometimes defined by the cloud providers.
- This layer does not come under the purview of service-level agreements (SLAs), that is, SLAs do not take into account the Internet connection between the user and cloud for quality of service (QoS).

Layer 3 (Cloud Management Layer)

- This layer consists of software that are used in managing the cloud. The software 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 software usually allow resource management (scheduling, provisioning, etc.), optimization (server consolidation, storage workload consolidation), and internal cloud governance.
- This layer comes under the purview of SLAs, 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.
- Any delay in processing or any discrepancy in service provisioning may lead to an SLA violation.
- As per rules, any SLA violation would result in a penalty to be given by the service provider.

Layer 4 (Hardware Resource Layer)

- Layer 4 consists of provisions for actual hardware resources. Usually, in the case of a public cloud, a data center is used in the back end.
- Similarly, in a private cloud, it can be a data center, which is a huge collection of hardware resources interconnected to each other that is present in a specific location or a high configuration system.
- This layer comes under the purview of SLAs. This is the most important layer that governs the SLAs. This layer affects the SLAs most in the case of data centers.
- Whenever a user accesses the cloud, it should be available to the users as quickly as possible and should be within the time that is defined by the SLAs.

- If there is any discrepancy in provisioning the resources or application, the service provider has to pay the penalty.
- Hence, 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 for a cloud, and similarly, a number of clouds can share a data center.

Cloud Model Types

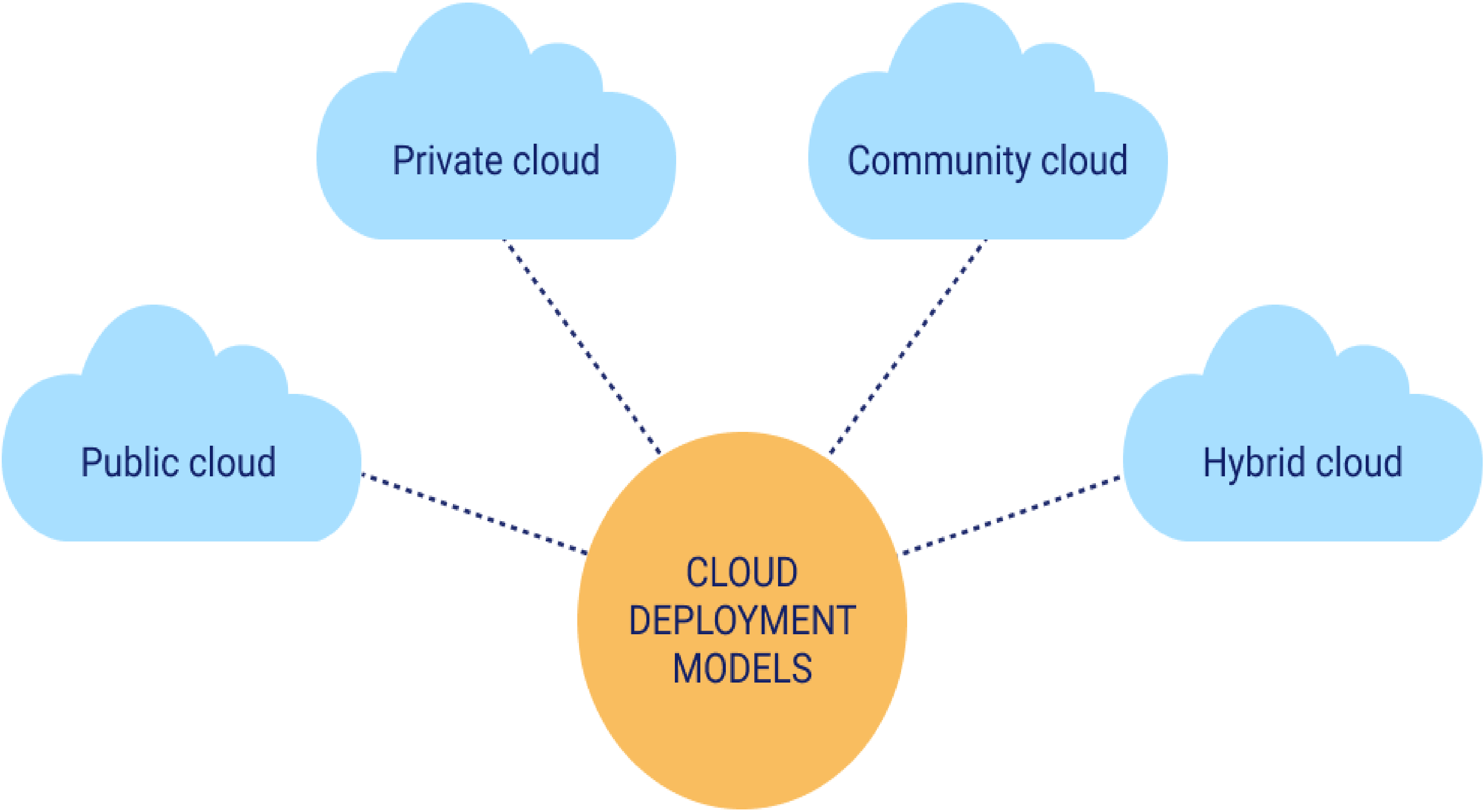
Cloud computing is divided into two distinct sets of models:

- **Deployment models:** This refers to the location and management of the cloud's infrastructure.
  - Public cloud
  - Private cloud
  - Hybrid cloud
  - Community cloud
- **Service models:** This consists of the particular types of services that you can access on a cloud computing platform.
  - Infrastructure as a Service
  - Platform as a Service
  - Software as a Service

Deployment Models

The NIST definition for the four deployment models is as follows:

- **Public cloud:** The public cloud infrastructure is available for public use alternatively for a large industry group and is owned by an organization selling cloud services.
- **Private cloud:** The private cloud infrastructure is operated for the exclusive use of an organization. The cloud may be managed by that organization or a third party. Private clouds may be either on or off premises.
- **Hybrid cloud:** A hybrid cloud combines multiple clouds (private, community of public) where those clouds retain their unique identities, but are bound together as a unit. A hybrid cloud may offer standardized or proprietary access to data and applications, as well as application portability.
- **Community cloud:** A community cloud is one where the cloud has been organized to serve a common function or purpose.



Private cloud

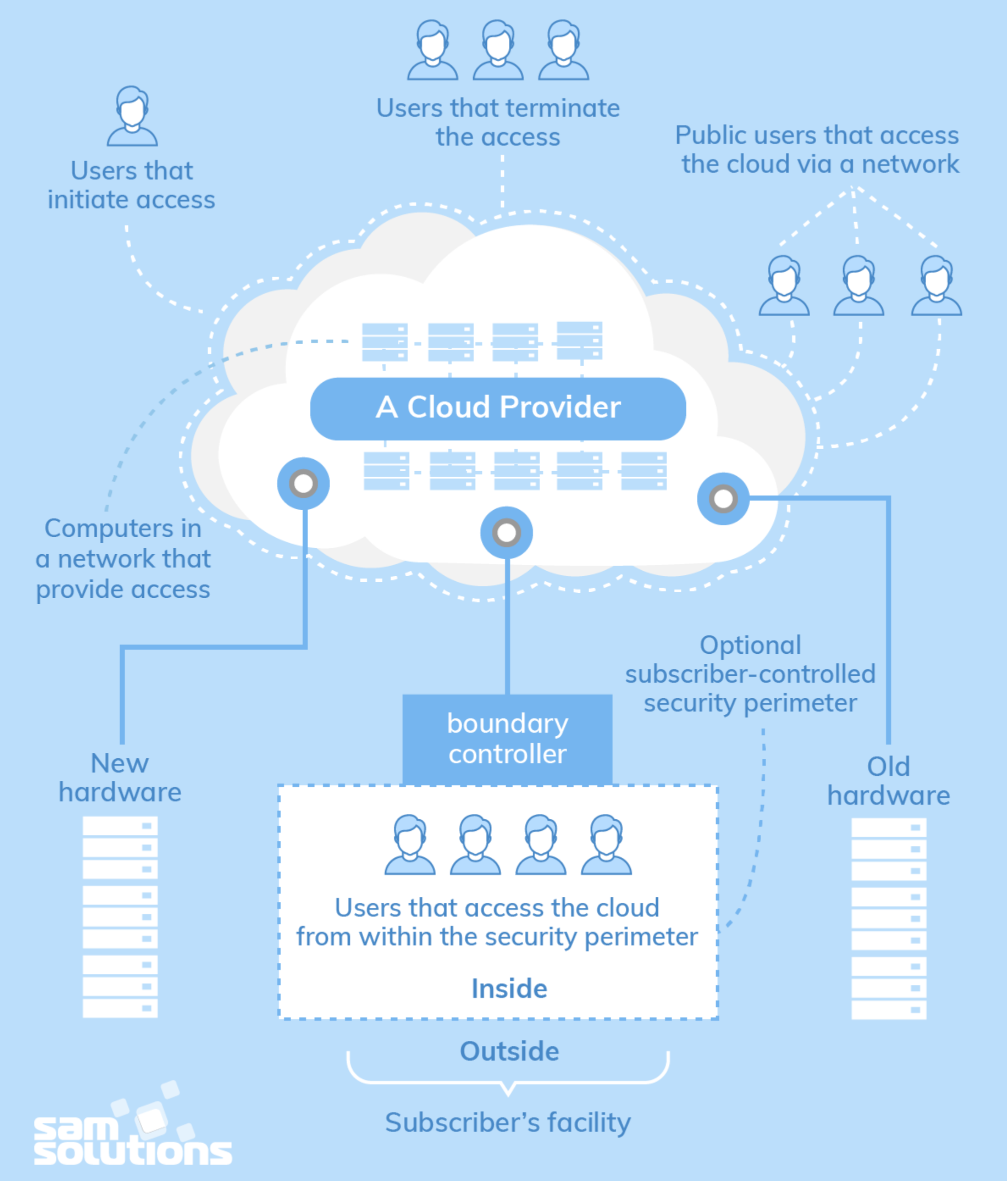
Community cloud

Public cloud

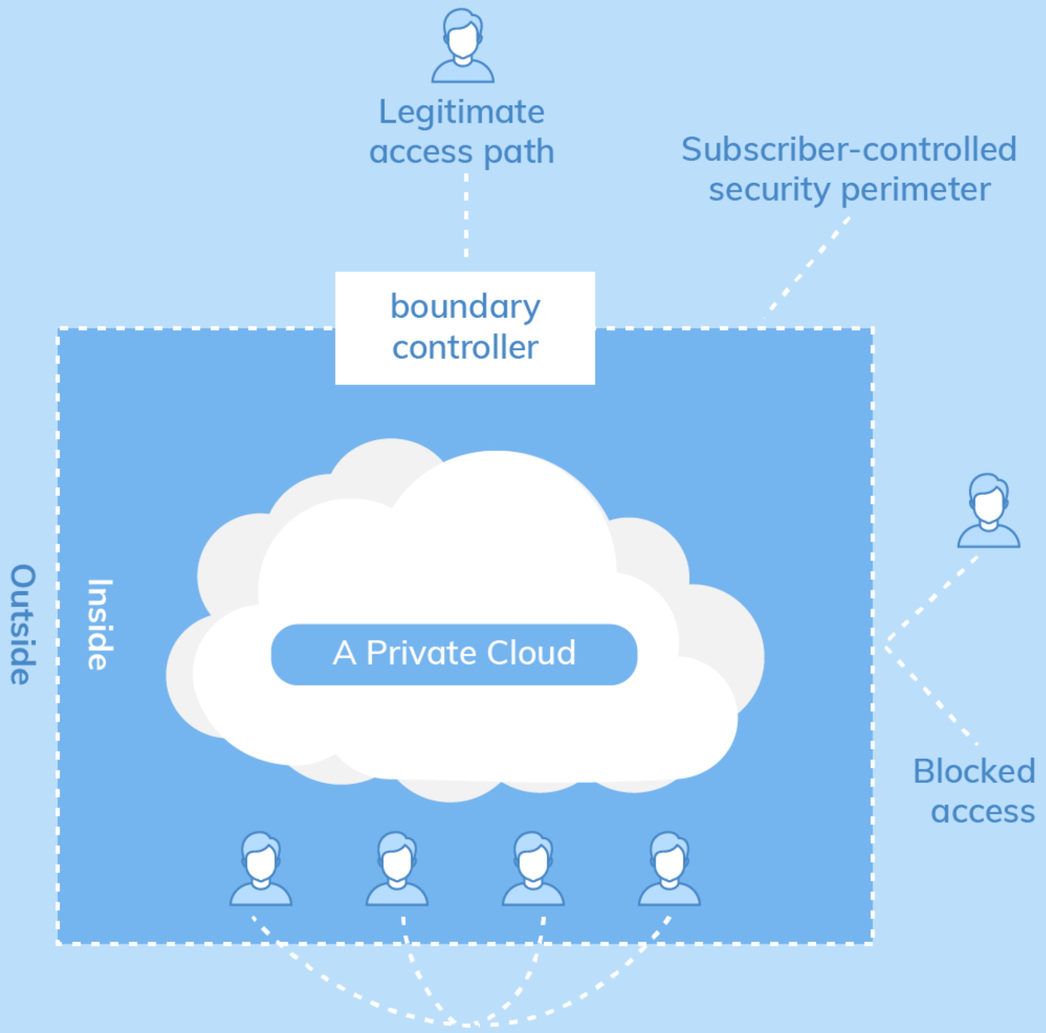
Hybrid cloud

CLOUD DEPLOYMENT MODELS

Public Cloud


Users that terminate the access
Users that initiate access
Public users that access the cloud via a network
A Cloud Provider
Computers in a network that provide access
Optional subscriber-controlled security perimeter
boundary controller
New hardware
Old hardware
Users that access the cloud from within the security perimeter
Inside
Outside
Subscriber's facility

Private Cloud



Legitimate access path

Subscriber-controlled security perimeter

boundary controller

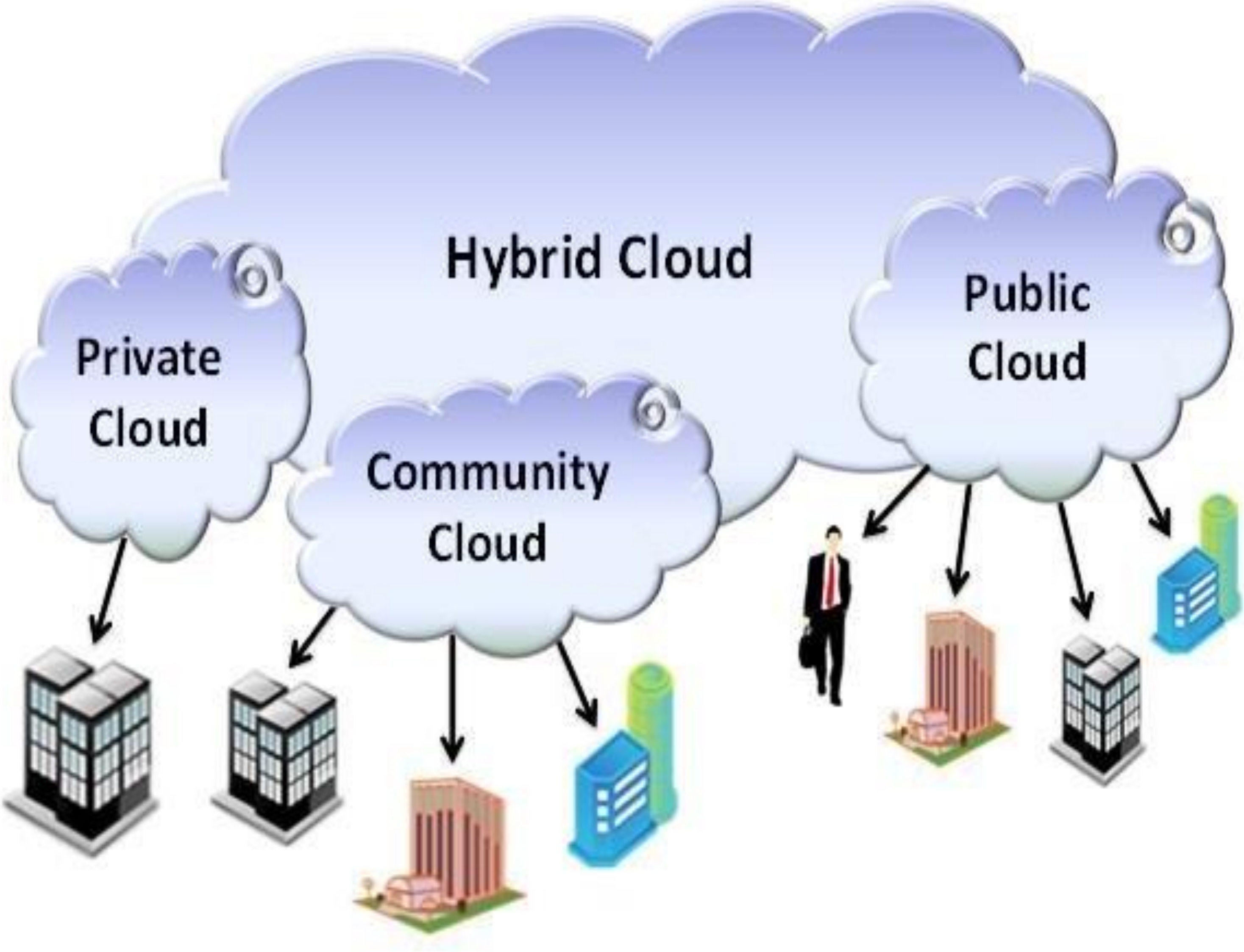
Outside

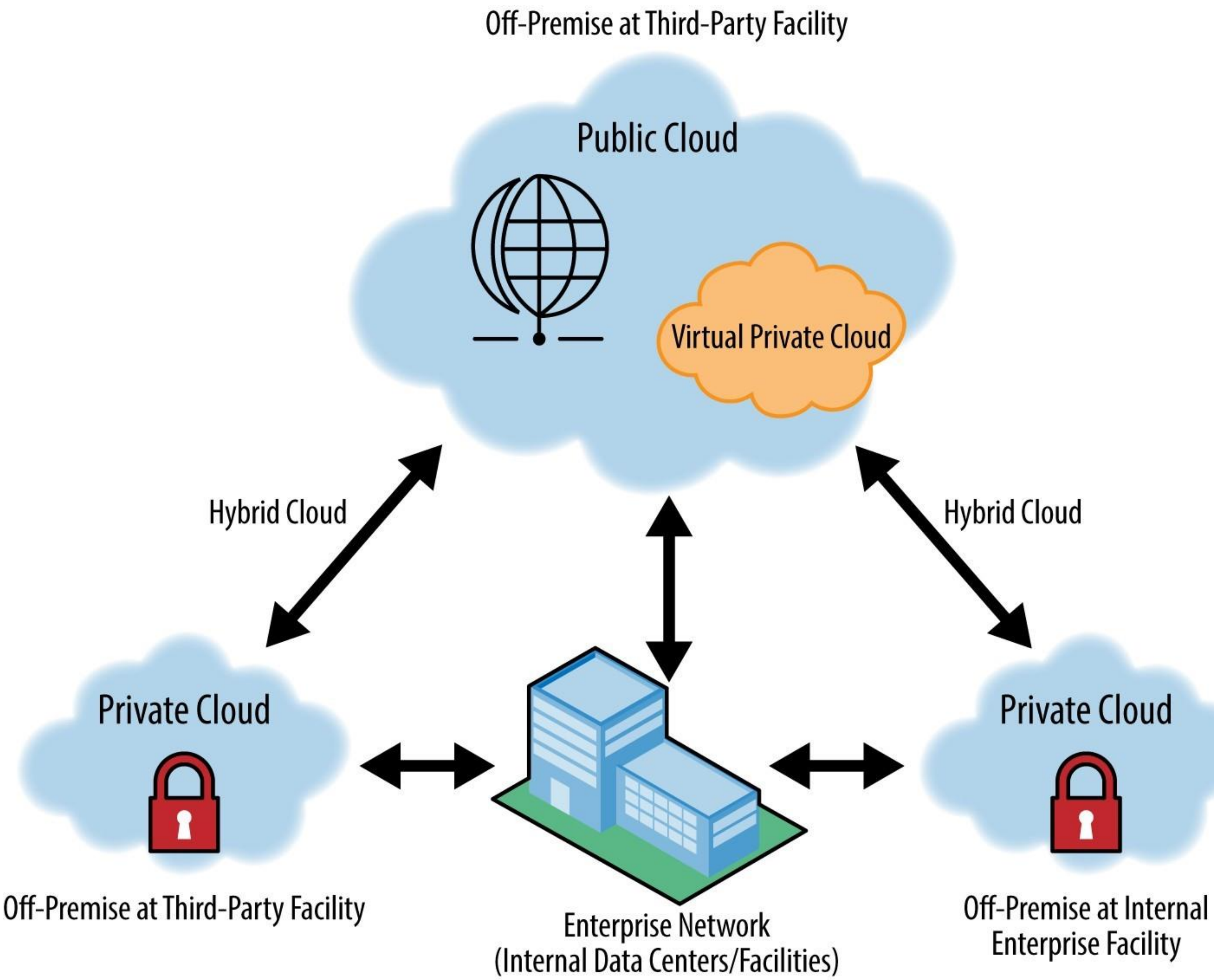
Inside

A Private Cloud

Blocked access

Users that acces the cloud from within the perimeter


Hybrid Cloud
Private Cloud
Community Cloud
Public Cloud

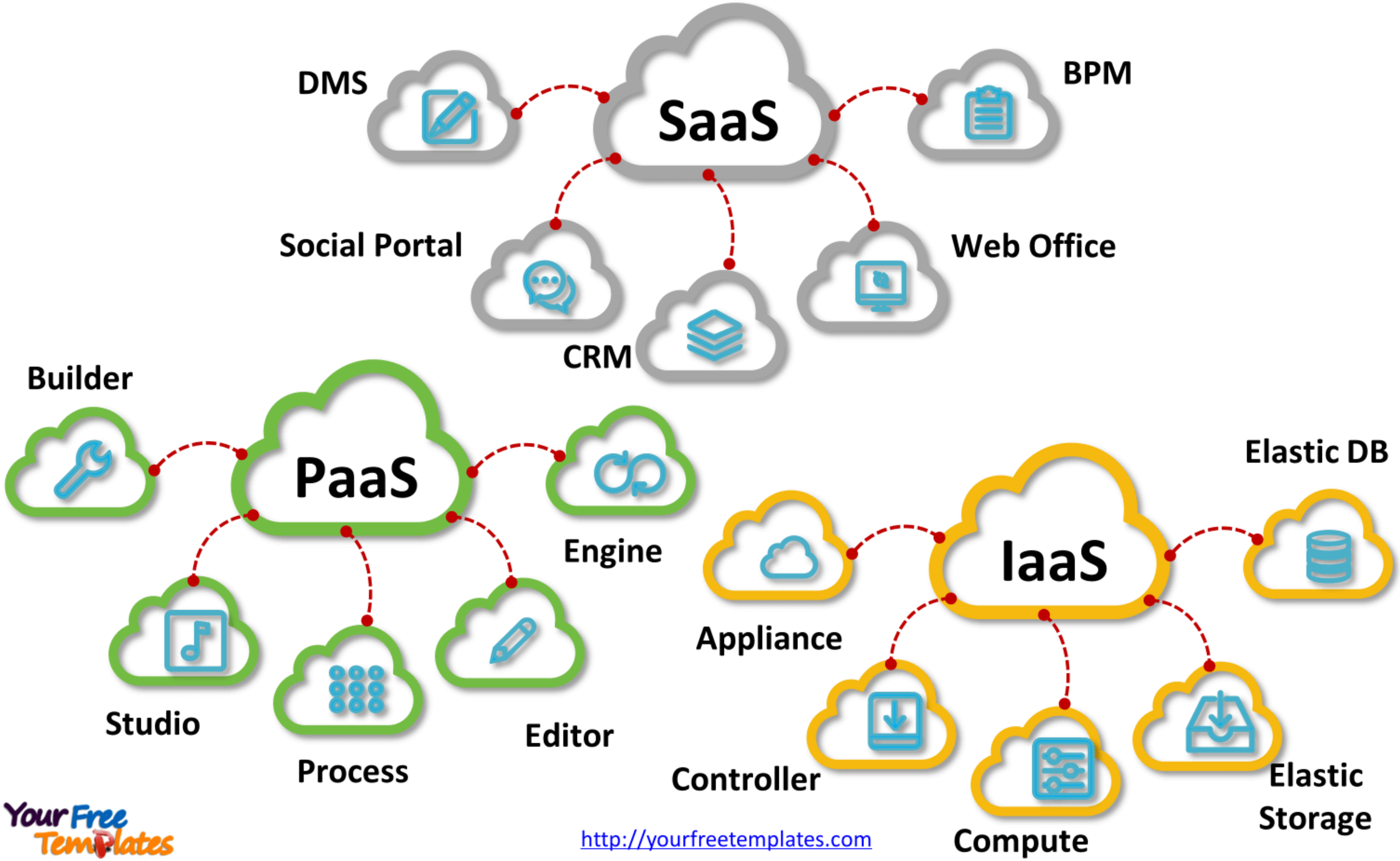

Off-Premise at Third-Party Facility
Public Cloud
Virtual Private Cloud
Hybrid Cloud
Hybrid Cloud
Private Cloud
Private Cloud
Off-Premise at Third-Party Facility
Enterprise Network
(Internal Data Centers/Facilities)
Off-Premise at Internal
Enterprise Facility

Service Models

Three service models have been universally accepted:

- **Infrastructure as a Service:** IaaS provides virtual machines, virtual storage, virtual infrastructure, and other hardware assets as resources that clients can provision.
    - The IaaS service provider manages all the infrastructure, while the client is responsible for all other aspects of the deployment. This can include the operating system, applications, and user interactions with the system.
- **Platform as a Service:** PaaS provides virtual machines, operating systems, applications, services, development frameworks, transactions, and control structures. The client can deploy its applications on the cloud infrastructure or use applications that were programmed using languages and tools that are supported by the PaaS service provider.
    - The service provider manages the cloud infrastructure, the operating systems, and the enabling software. The client is responsible for installing and managing the application that it is deploying.
- **Software as a Service:** SaaS is a complete operating environment with applications, management, and the user interface.

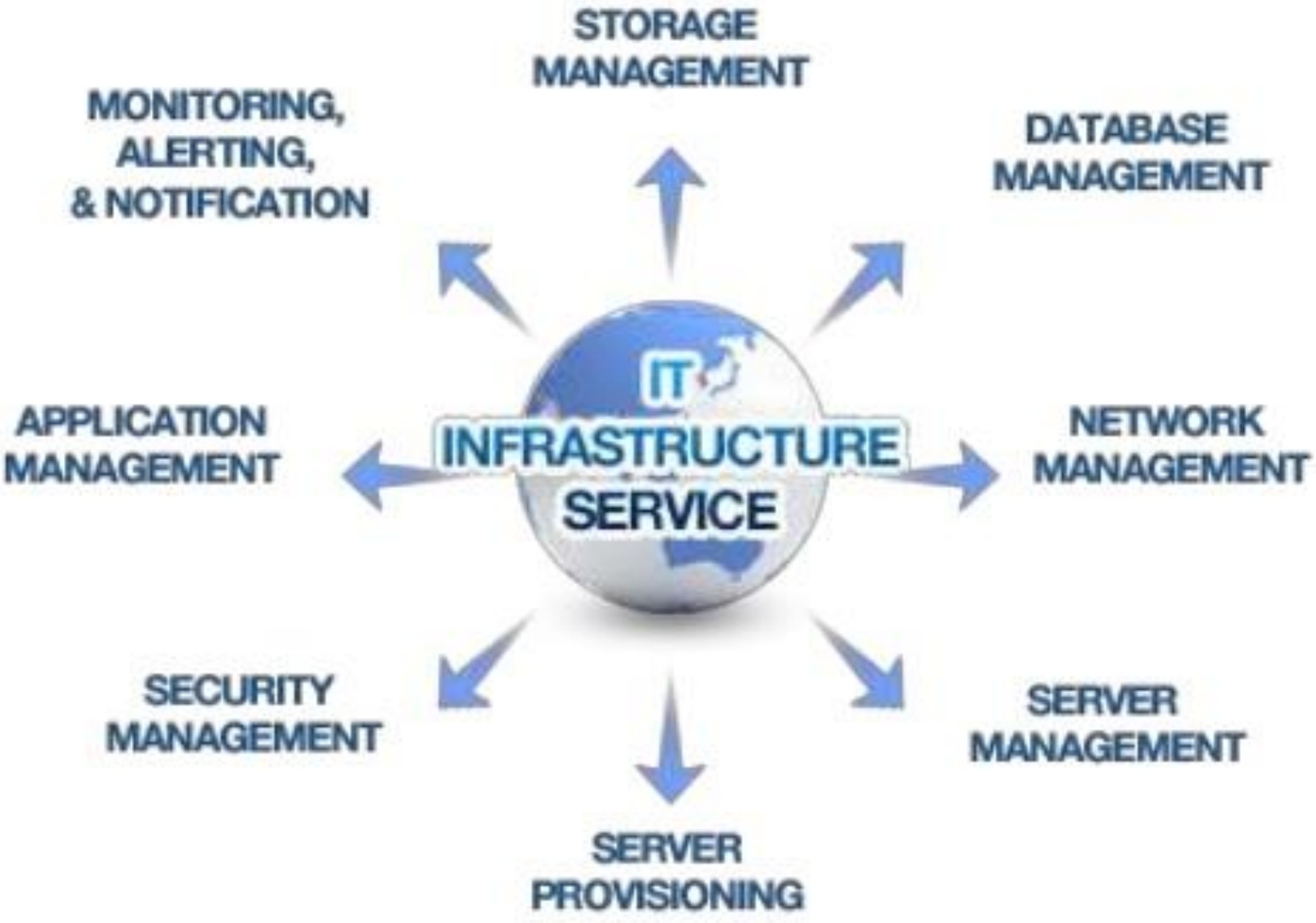
Three service models



Your Free Templates

http://yourfreetemplates.com

IaaS



STORAGE MANAGEMENT

MONITORING, ALERTING, & NOTIFICATION

DATABASE MANAGEMENT

IT INFRASTRUCTURE SERVICE

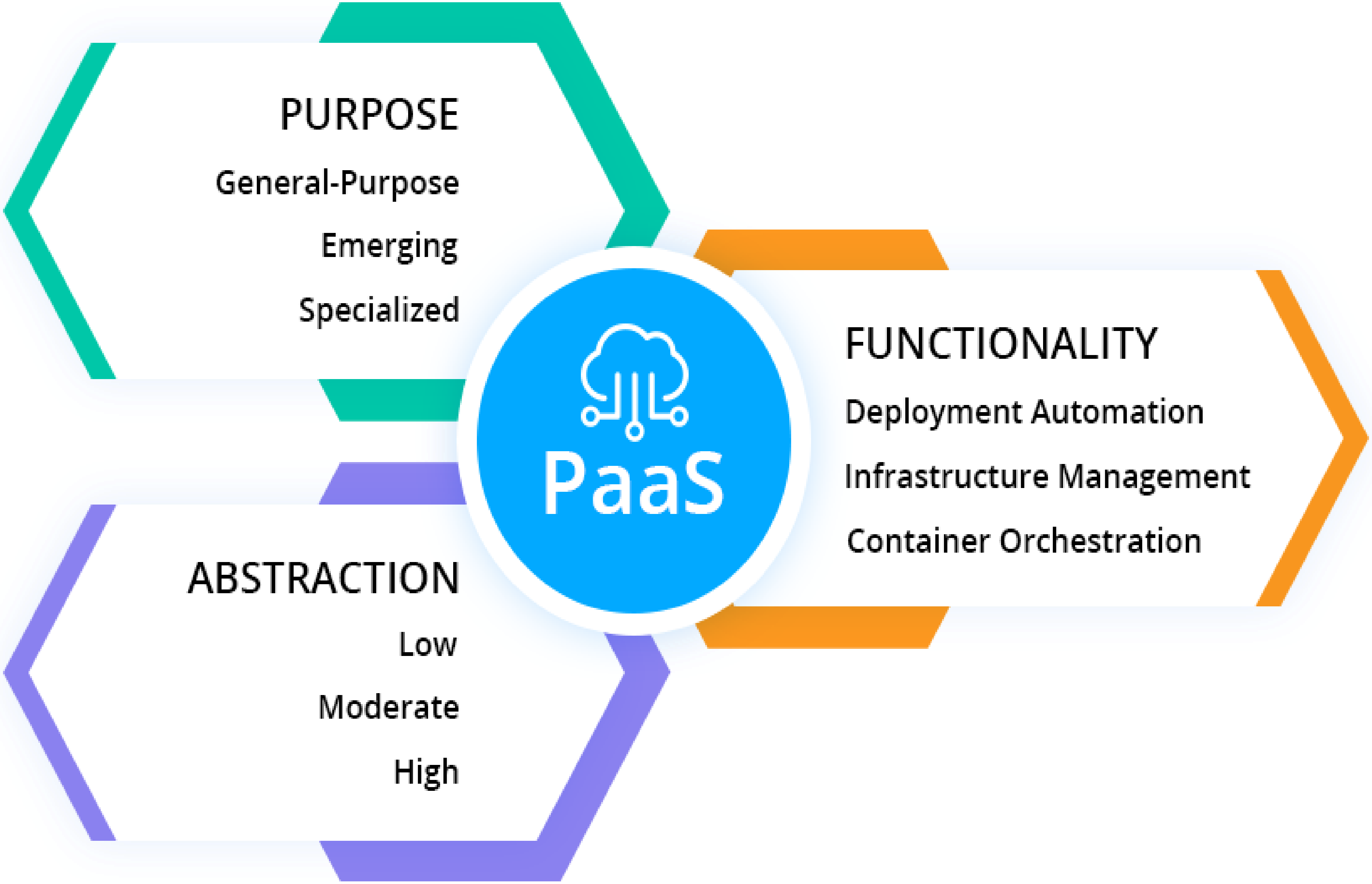
APPLICATION MANAGEMENT

NETWORK MANAGEMENT

SECURITY MANAGEMENT

SERVER MANAGEMENT

SERVER PROVISIONING



PaaS

PURPOSE

General-Purpose

Emerging

Specialized

FUNCTIONALITY

Deployment Automation

Infrastructure Management

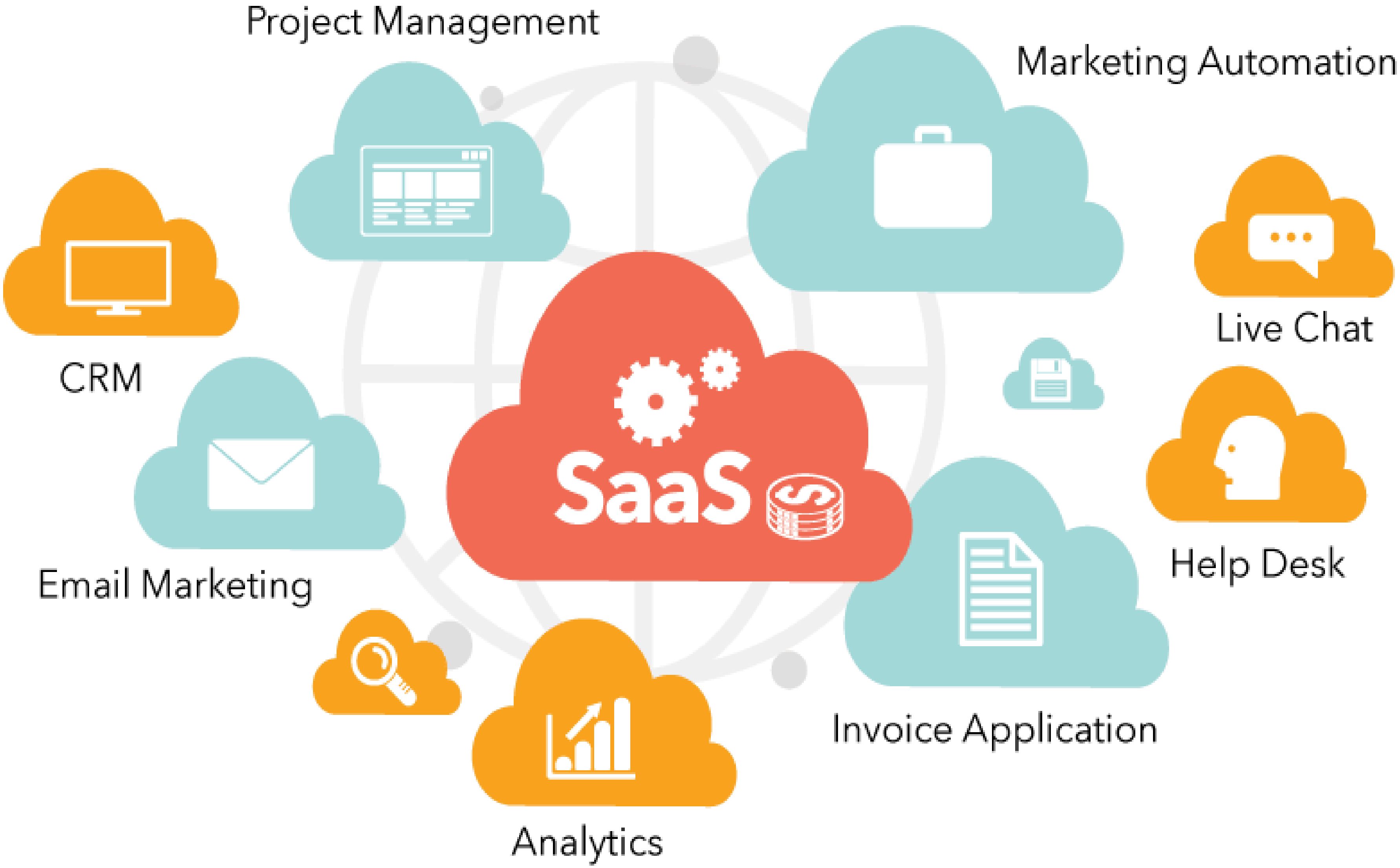
Container Orchestration

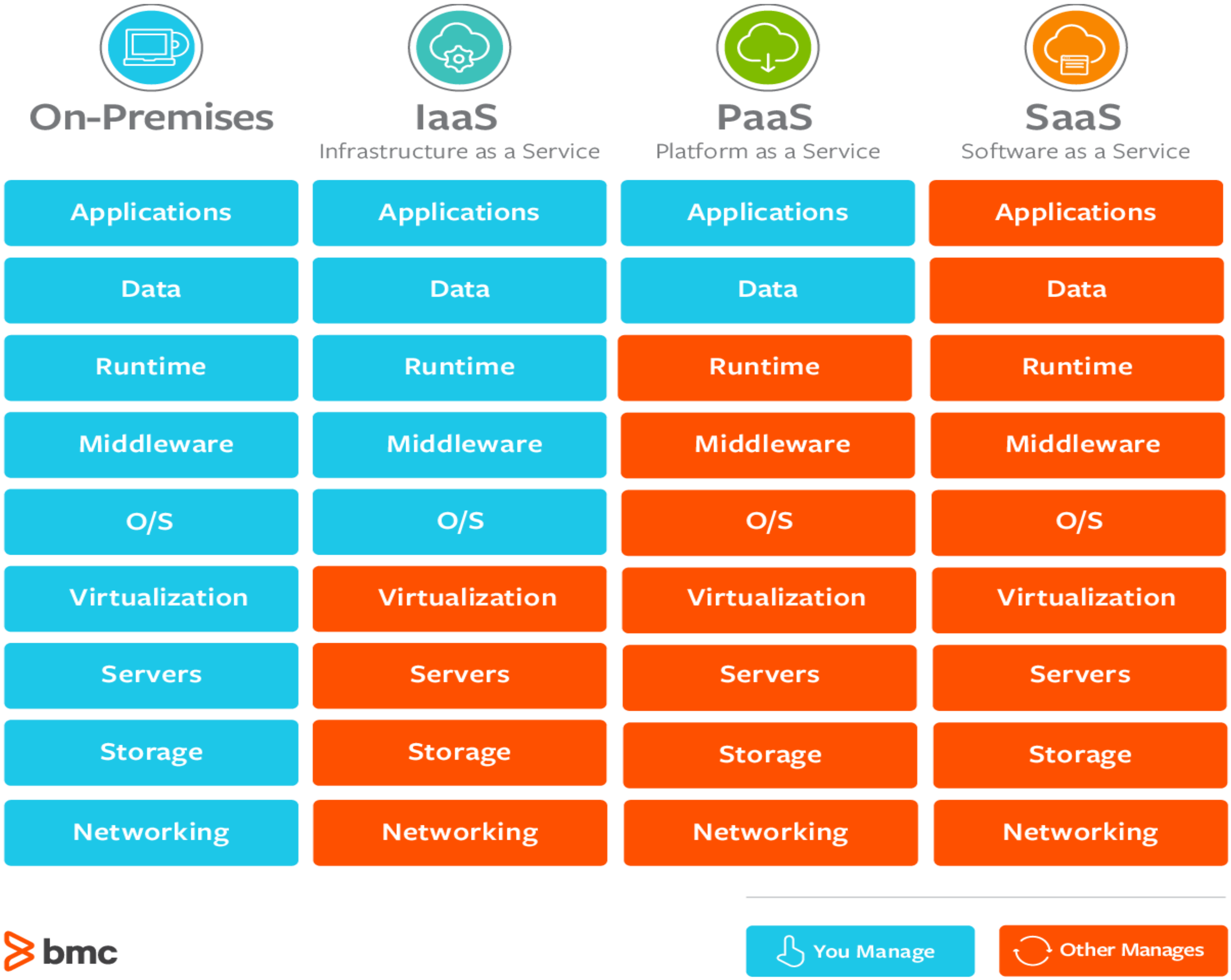
ABSTRACTION

Low

Moderate

High


Project Management
Marketing Automation
CRM
Live Chat
SaaS
Email Marketing
Help Desk
Invoice Application
Analytics



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

🟦 You Manage

🟧 Other Manages

bmc

The three different service models taken together have come to be known as the SPI model of cloud computing.

Many other service models have also been mentioned:

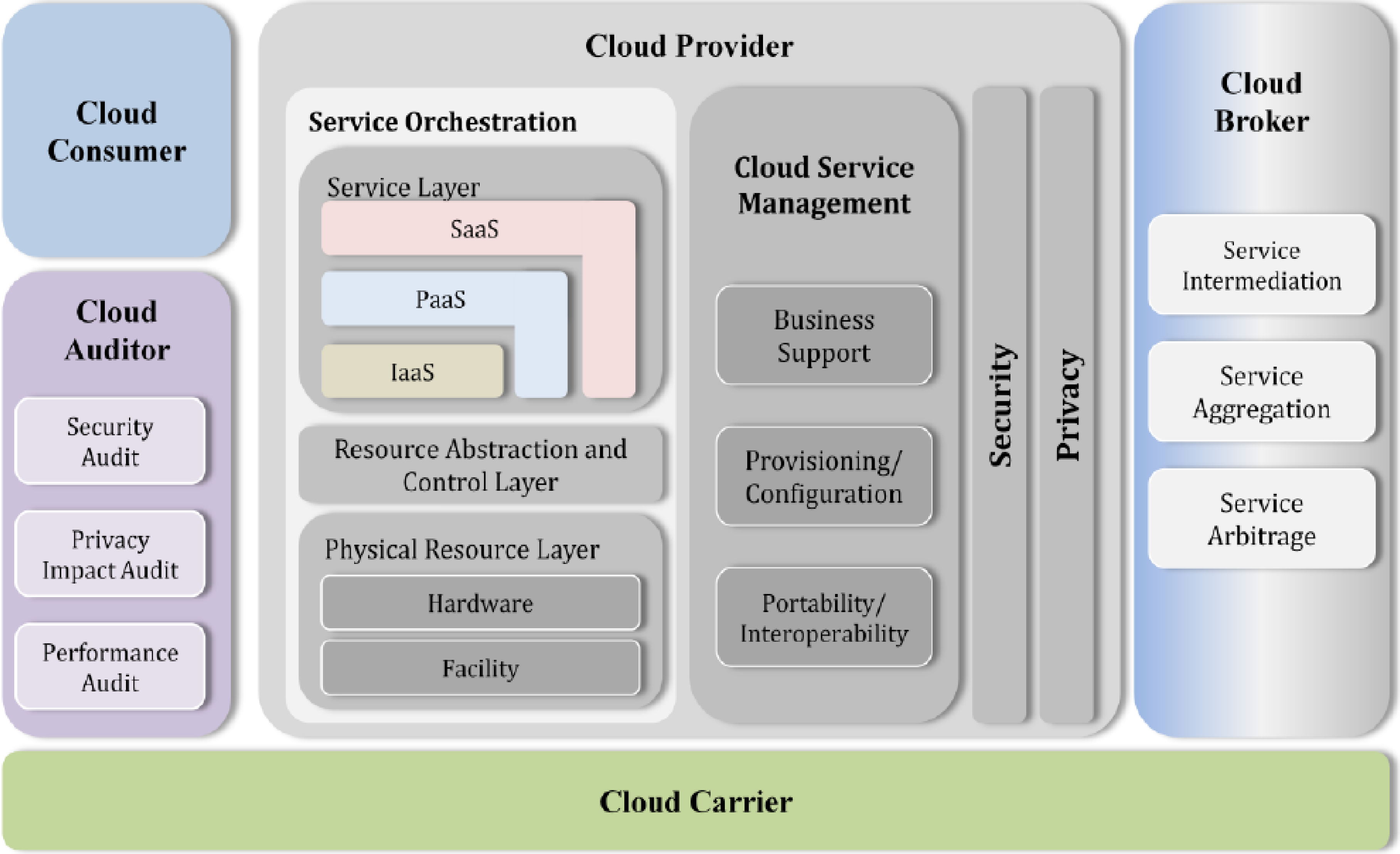
- StaaS - Storage as a Service;
- IdaaS - Identity as a Service;
- CmaaS - Compliance as a Service; and so forth.

However, the SPI services encompass all the other possibilities.

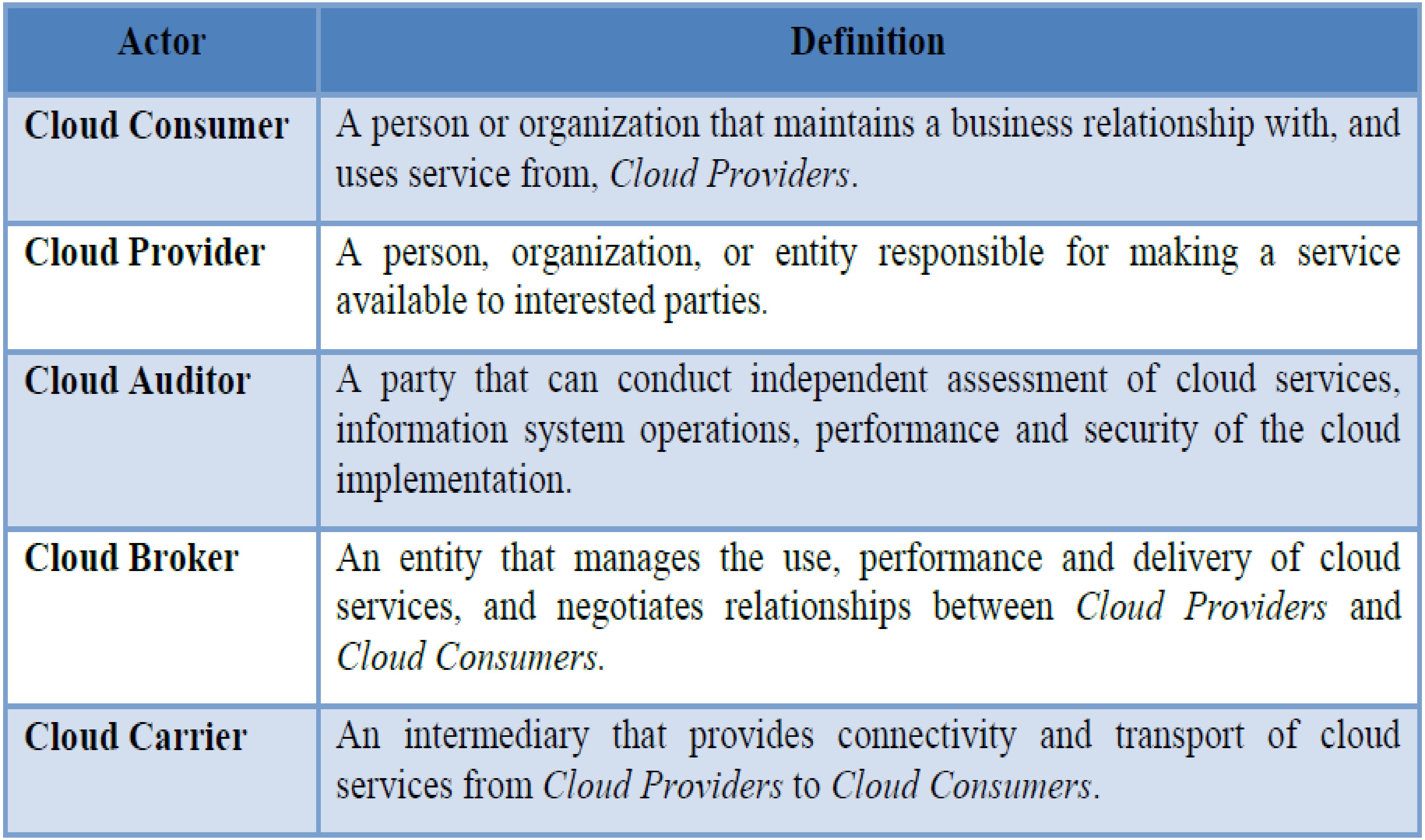
Business Models

- NIST Cloud Computing Reference Model
- Cloud Cube Model

NIST Cloud Computing Reference Model

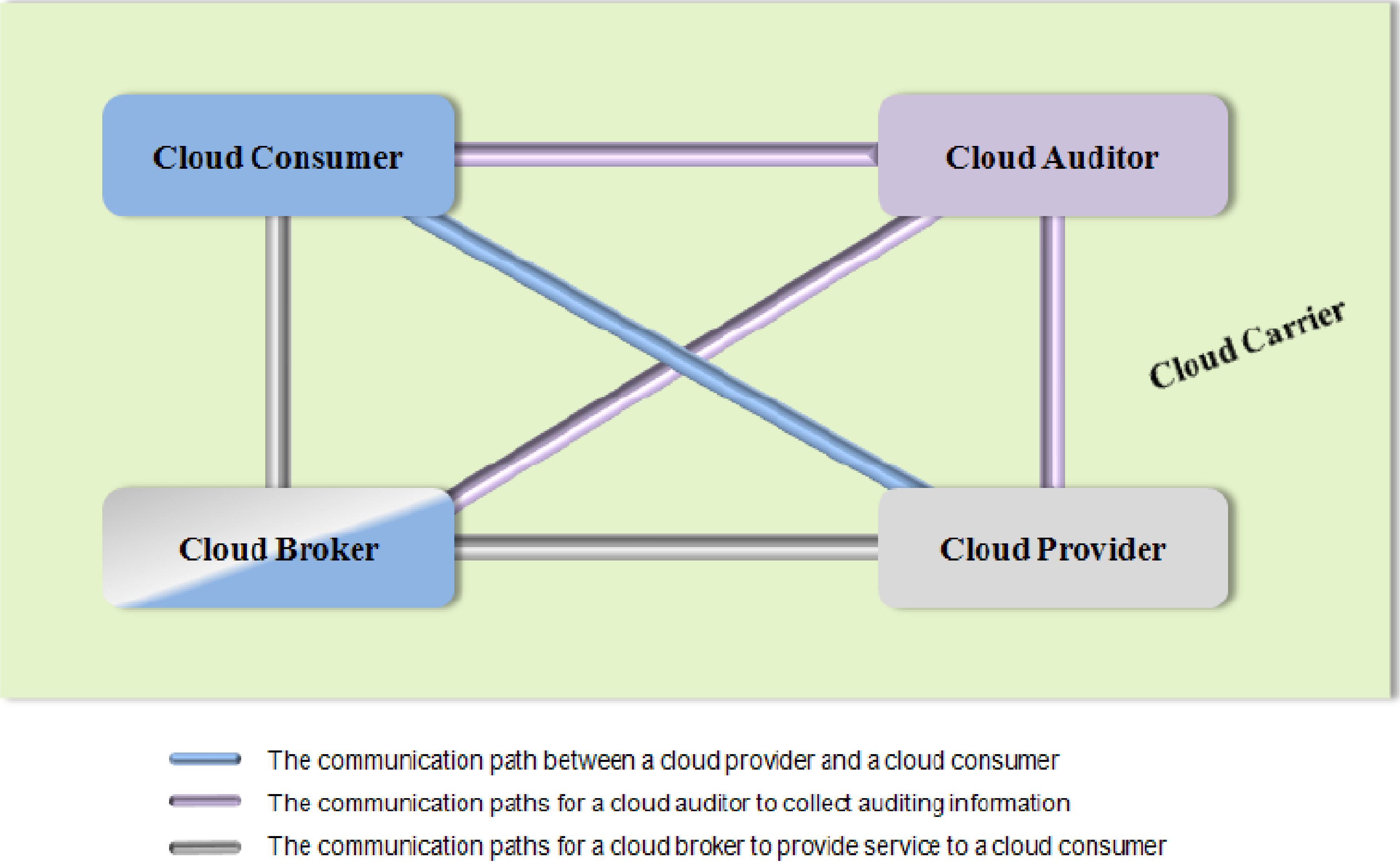


Actors in Cloud Computing



Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

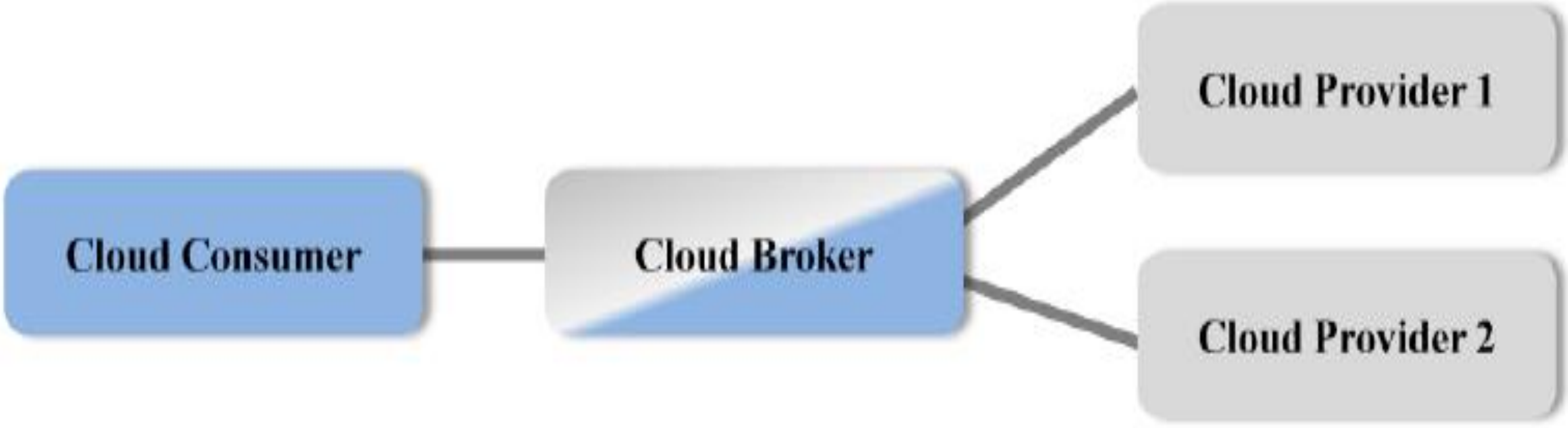
Interactions between the Actors in Cloud Computing



- The communication path between a cloud provider and a cloud consumer
- The communication paths for a cloud auditor to collect auditing information
- The communication paths for a cloud broker to provide service to a cloud consumer

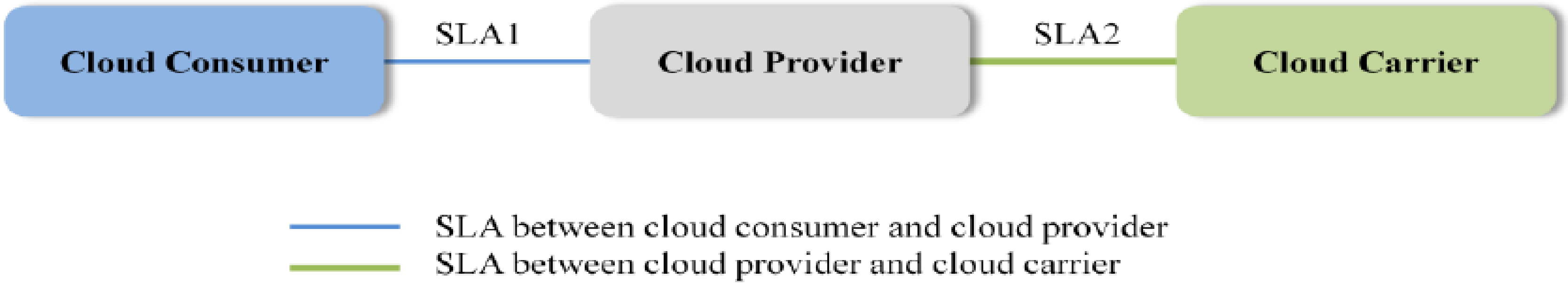
Usage Scenario for Cloud Brokers

A cloud consumer may request service from a cloud broker instead of contacting a cloud provider directly. The cloud broker may create a new service by combining multiple services or by enhancing an existing service. In this example, the actual cloud providers are invisible to the cloud consumer and the cloud consumer interacts directly with the cloud broker.



Usage Scenario for Cloud Carriers

Cloud carriers provide the connectivity and transport of cloud services from cloud providers to cloud consumers. As illustrated in Figure, a cloud provider participates in and arranges for two unique service level agreements (SLAs), one with a cloud carrier (e.g. SLA2) and one with a cloud consumer (e.g. SLA1). A cloud provider arranges service level agreements (SLAs) with a cloud carrier and may request dedicated and encrypted connections to ensure the cloud services are consumed at a consistent level according to the contractual obligations with the cloud consumers. In this case, the provider may specify its requirements on capability, flexibility and functionality in SLA2 in order to provide essential requirements in SLA1.



Cloud Consumer

SLA1

Cloud Provider

SLA2

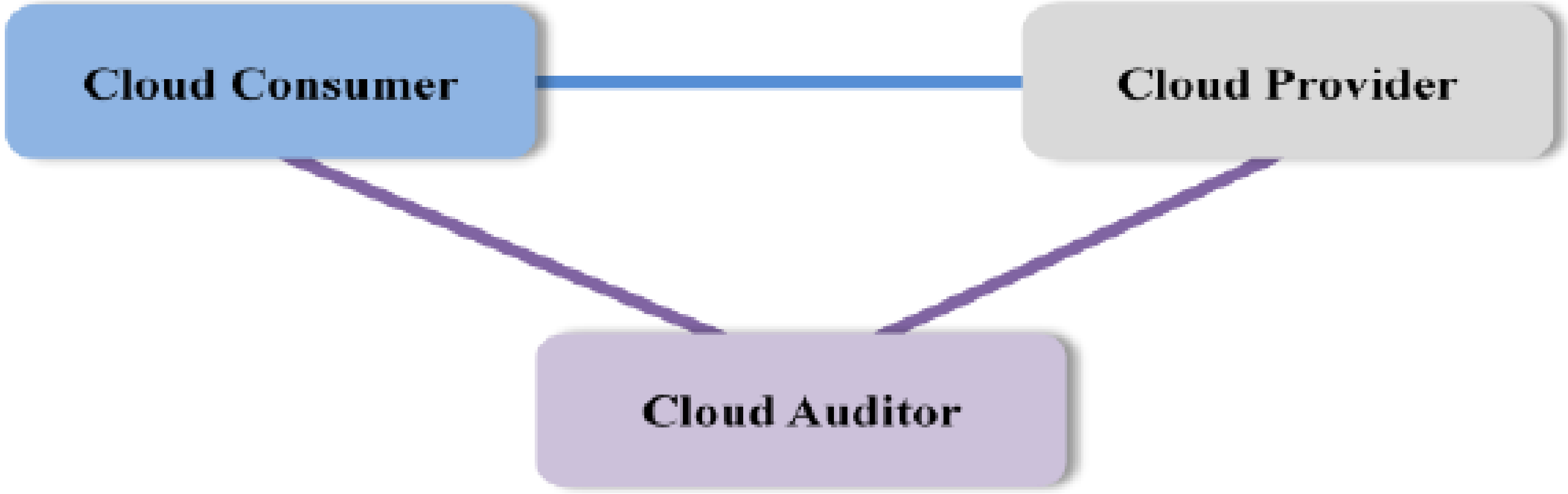
Cloud Carrier

SLA between cloud consumer and cloud provider

SLA between cloud provider and cloud carrier

Usage Scenario for Cloud Auditors

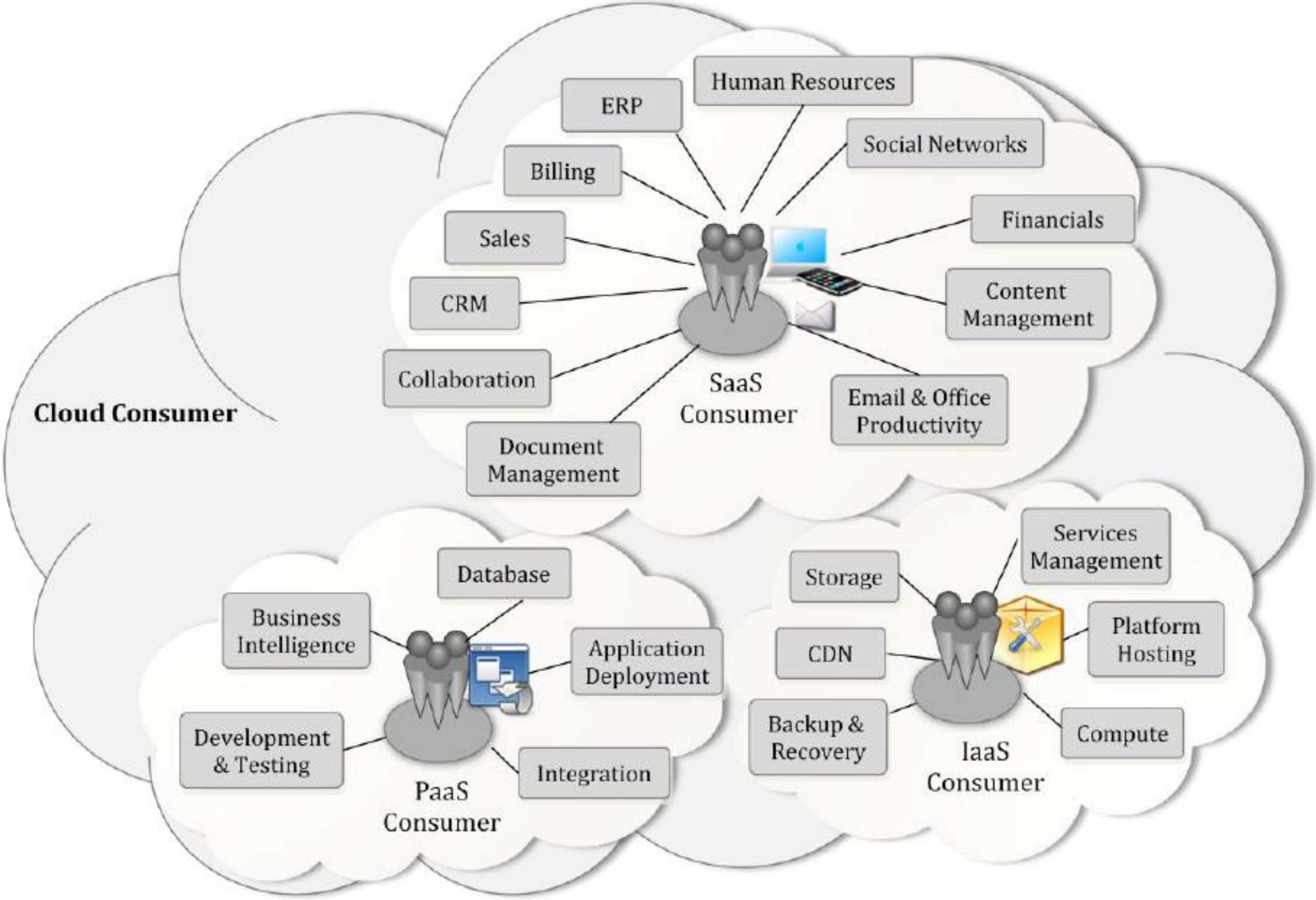
For a cloud service, a cloud auditor conducts independent assessments of the operation and security of the cloud service implementation. The audit may involve interactions with both the Cloud Consumer and the Cloud Provider.



1. Cloud Consumer

The cloud consumer is the principal stakeholder for the cloud computing service.

- A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider.
- A cloud consumer browses the service catalogue from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service.
- The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly.



Example Services Available to a Cloud Consumer

2. Cloud Provider

A cloud provider is a person, an organization; it is the entity responsible for making a service available to interested parties. A Cloud Provider:

- acquires and manages the computing infrastructure required for providing the services,
- runs the cloud software that provides the services, and
- makes arrangement to deliver the cloud services to the Cloud Consumers through network access.

A Cloud Provider's activities can be described in five major areas:

- *service deployment*,
- *service orchestration*,
- *cloud service management*,
- *security*, and
- *privacy*.

3. Cloud Auditor

A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon.

- Audits are performed to verify conformance to standards through review of objective evidence.
- A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.
- The auditor may ensure that fixed content has not been modified and that the legal and business data archival requirements have been satisfied.

4. Cloud Broker

As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage.

- A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly.
- A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.

In general, a cloud broker can provide services in three categories:

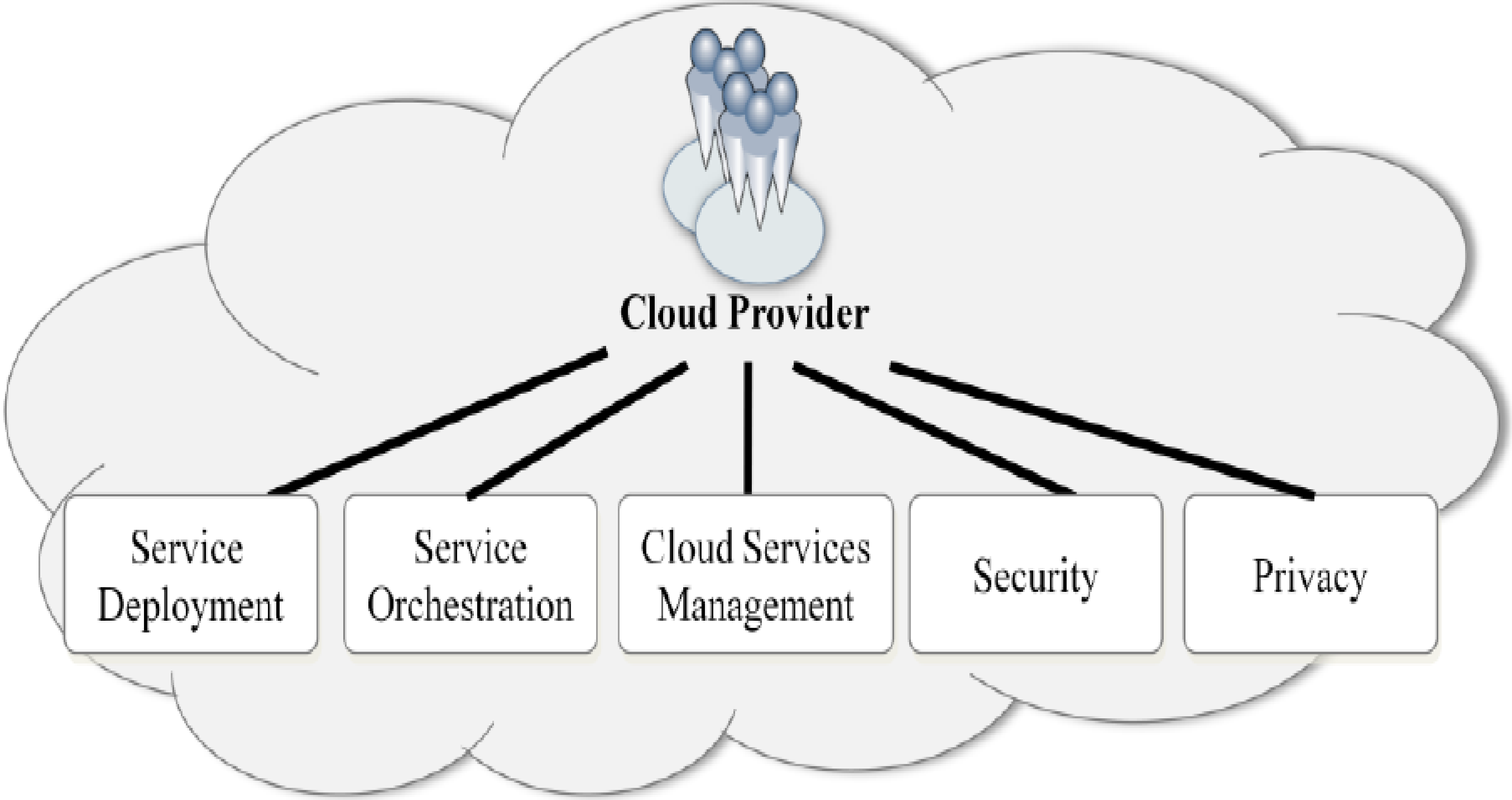
- **Service Intermediation:** A cloud broker enhances a given service by improving some specific capability and providing value-added services to cloud consumers.
  - The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.
- **Service Aggregation:** A cloud broker combines and integrates multiple services into one or more new services.
  - The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.
- **Service Arbitrage:** Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies.
  - The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score.

5. Cloud Carrier

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

- Cloud carriers provide access to consumers through network, telecommunication and other access devices.
  - For example, cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile Internet devices (MIDs), etc.
- The distribution of cloud services is normally provided by network and telecommunication carriers or a transport agent, where a transport agent refers to a business organization that provides physical transport of storage media such as high-capacity hard drives.
  - Note that a cloud provider will set up SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and may require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

Major activities of Cloud Provider



Cloud Provider

Service Deployment

Service Orchestration

Cloud Services Management

Security

Privacy

A. Service Deployment

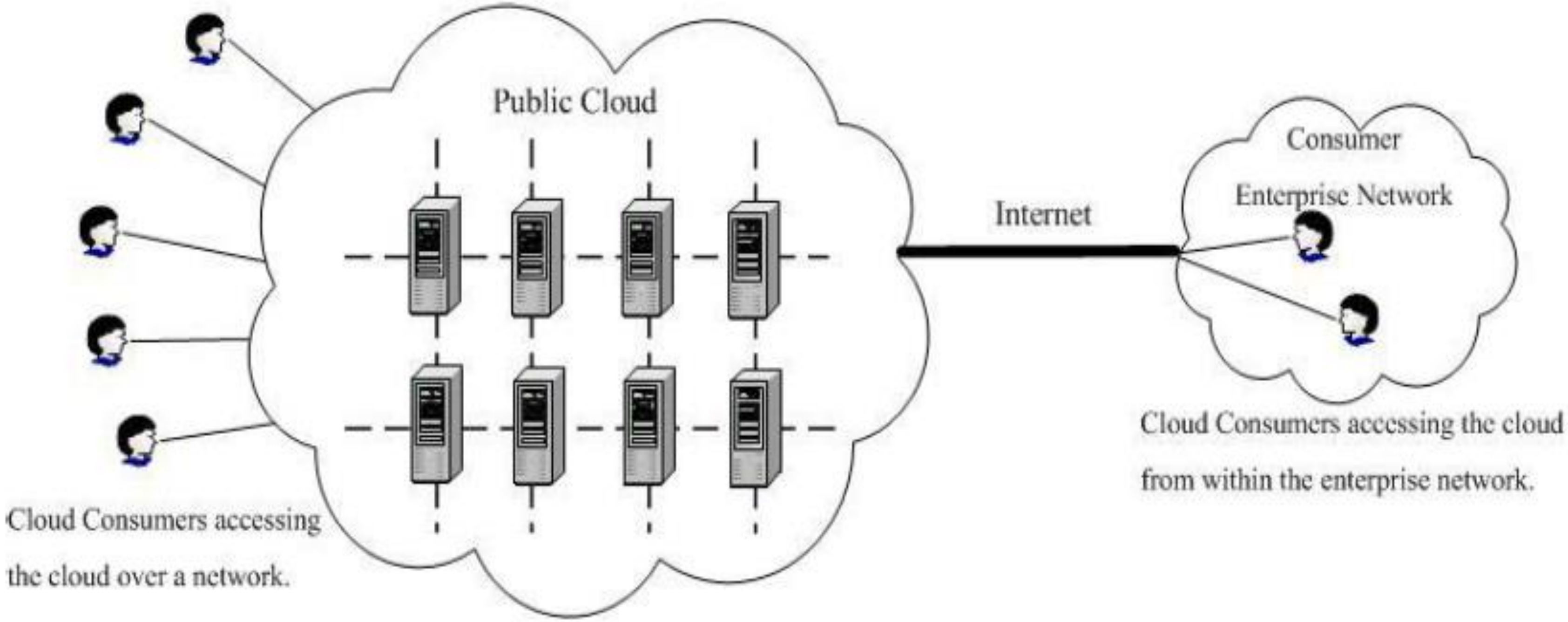
A cloud infrastructure may be operated in one of the following deployment models:

- public cloud,
- private cloud,
- community cloud, or
- hybrid cloud.

The differences are based on how exclusive the computing resources are made to a Cloud Consumer.

Public Cloud

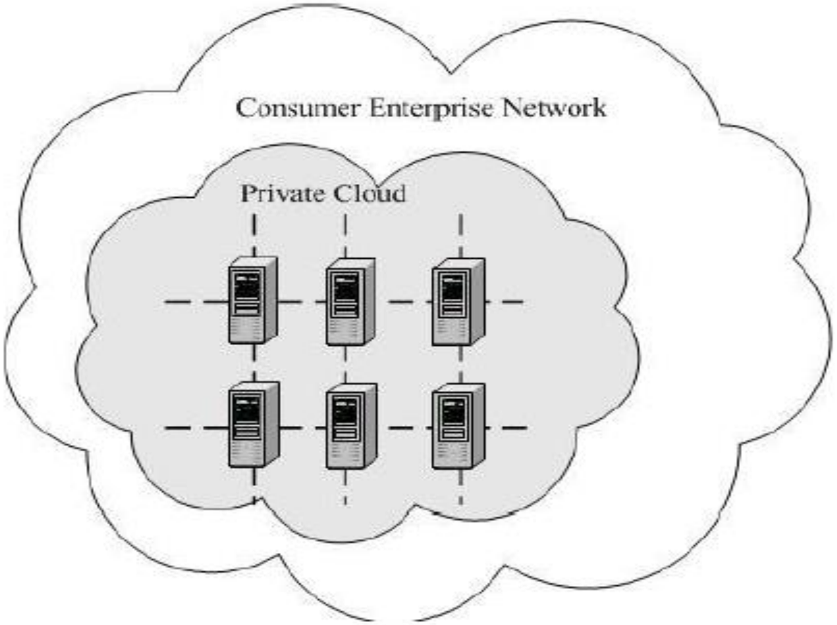
A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network. A public cloud is owned by an organization selling cloud services, and serves a diverse pool of clients.


Public Cloud
Internet
Consumer
Enterprise Network
Cloud Consumers accessing the cloud from within the enterprise network.
Cloud Consumers accessing the cloud over a network.

Private Cloud

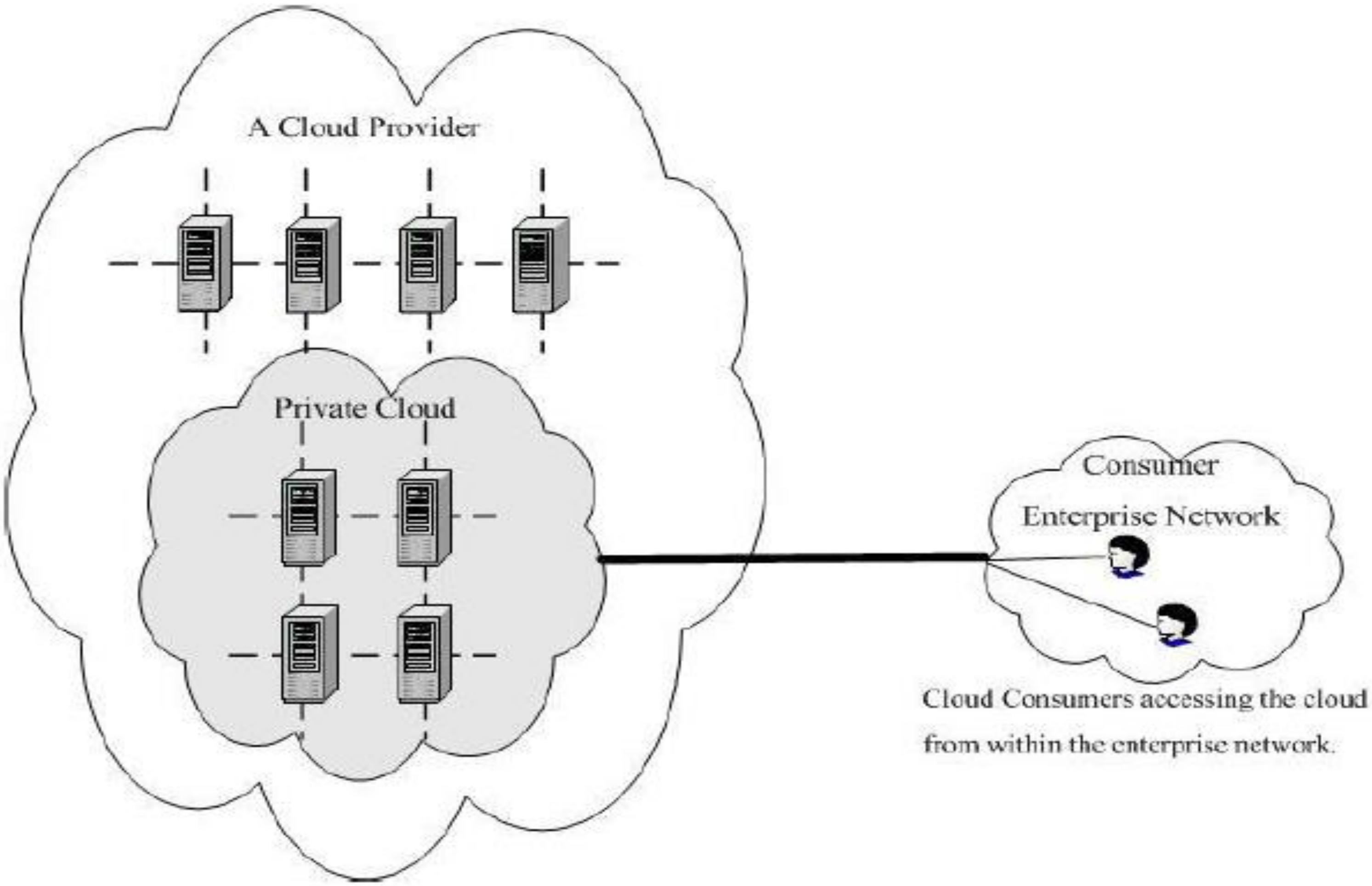
A private cloud gives a single Cloud Consumer's organization the exclusive access to and usage of the infrastructure and computational resources. It may be managed either by:

- The Cloud Consumer organization and may be hosted on the organization's premises (i.e. *on-site private clouds*), or



On-site Private Cloud

- A third party, outsourced to a hosting company (i.e. *outsourced private clouds*).


A Cloud Provider
Private Cloud
Consumer
Enterprise Network
Cloud Consumers accessing the cloud
from within the enterprise network.

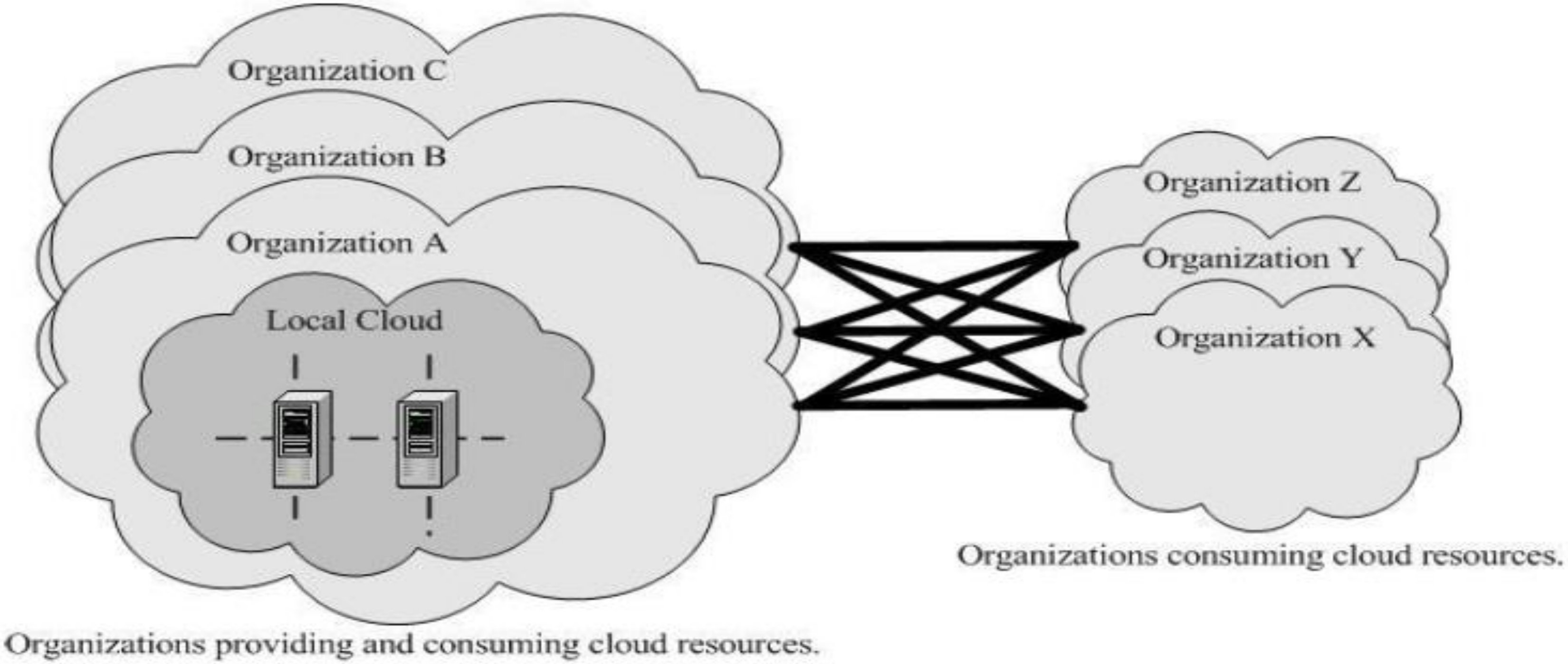
Outsourced Private Cloud

Community Cloud

A community cloud serves a group of Cloud Consumers which have shared concerns such as mission objectives, security, privacy and compliance policy, rather than serving a single organization as does a private cloud. Similar to private clouds, a community cloud may be managed by

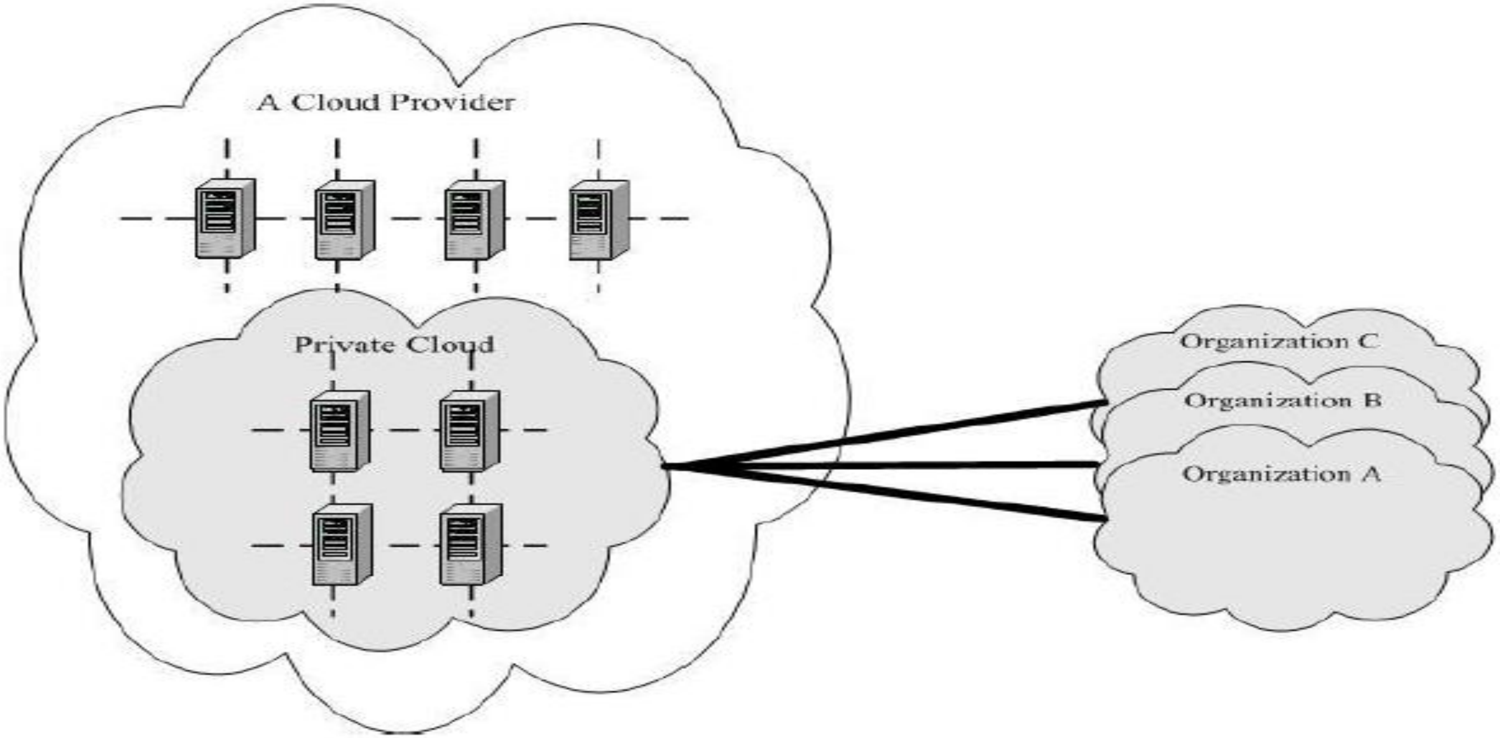
- The organizations and may be implemented on customer premise (i.e. *on-site community cloud*), or
- A third party, outsourced to a hosting company (i.e. *outsourced community cloud*).

Following figure depicts an on-site community cloud comprised of a number of participant organizations. A cloud consumer can access the local cloud resources, and also the resources of other participating organizations through the connections between the associated organizations.



On-site Community Cloud

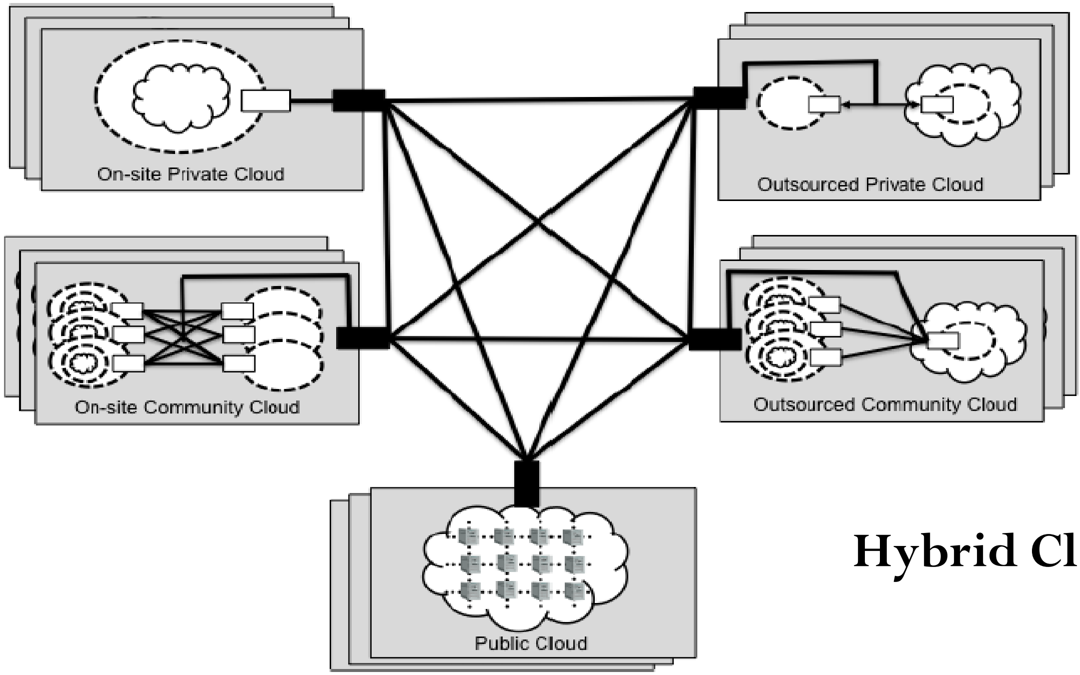
Following figure shows an outsourced community cloud, where the server side is outsourced to a hosting company. In this case, an outsourced community cloud builds its infrastructure off premise, and serves a set of organizations that request and consume cloud services.



Outsourced Community Cloud

Hybrid Cloud

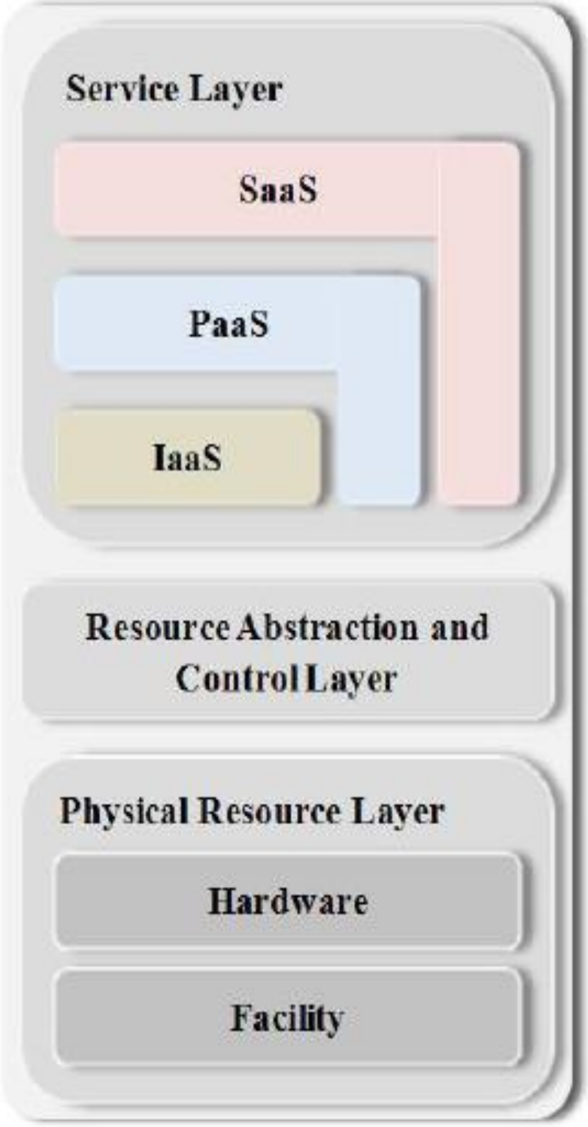
A hybrid cloud is a composition of two or more clouds (on-site private, on-site community, off-site private, off-site community or public) that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability.



Hybrid Cloud

B. Cloud Service Orchestration

Service Orchestration refers to the composition of system components to support the Cloud Providers activities in arrangement, coordination and management of computing resources in order to provide cloud services to Cloud Consumers. Figure shows a generic stack diagram of this composition that underlies the provisioning of cloud services. A three-layered model is used in this representation, representing the grouping of three types of system components Cloud Providers need to compose to deliver their services.



Service layer

This is where Cloud Providers define interfaces for Cloud Consumers to access the computing services.

- Access interfaces of each of the three service models are provided in this layer. It is possible, though not necessary, that SaaS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components.
- The optional dependency relationships among SaaS, PaaS, and IaaS components are represented graphically as components stacking on each other; while the angling of the components represents that each of the service component can stand by itself.

Resource Abstraction and Control Layer

This layer contains the system components that Cloud Providers use to provide and manage access to the physical computing resources through software abstraction.

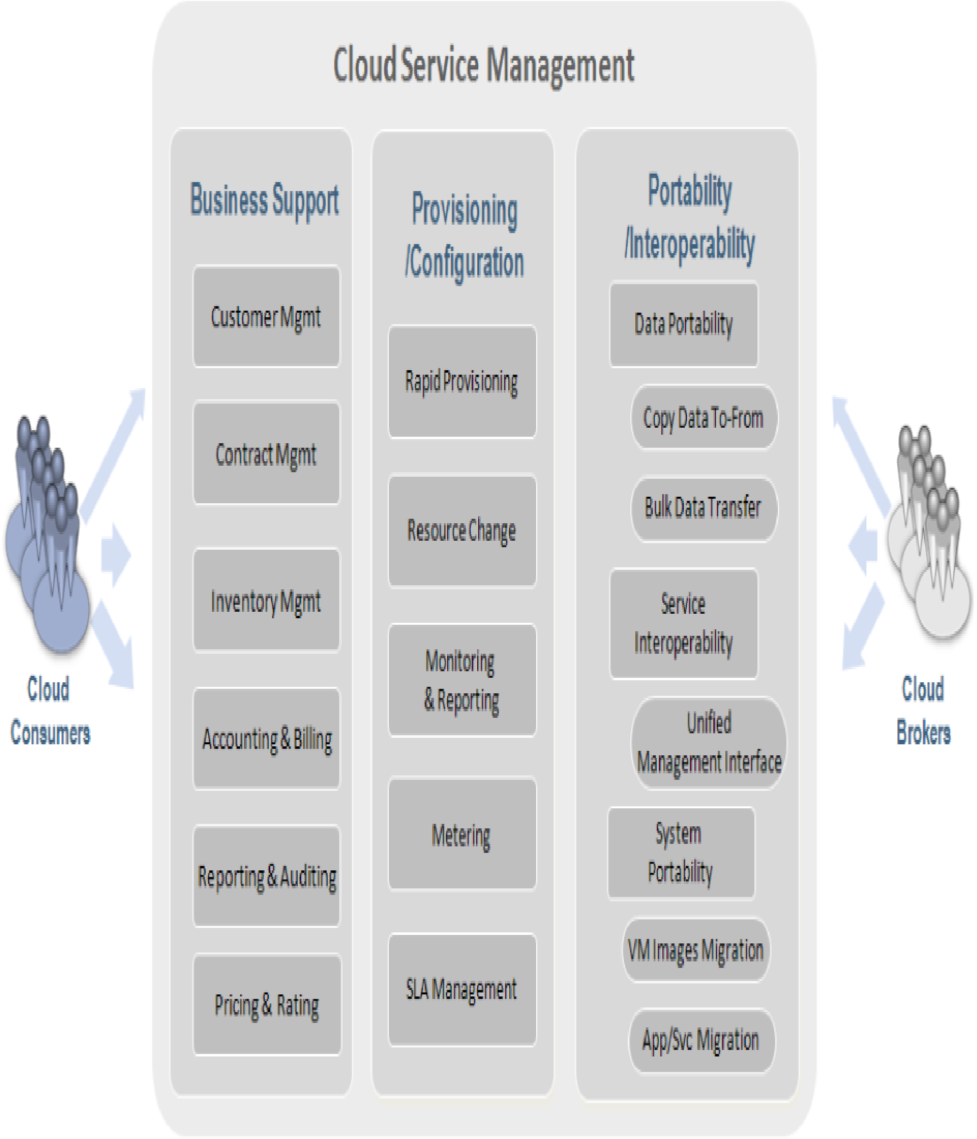
- The **resource abstraction** needs to ensure efficient, secure, and reliable usage of the underlying physical resources. While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are also possible.
  - Examples of resource abstraction components include software elements such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions.
- The **control** aspect of this layer refers to the software components that are responsible for resource allocation, access control, and usage monitoring.
  - This is the software fabric that ties together the numerous underlying physical resources and their software abstractions to enable resource pooling, dynamic allocation, and measured service.
  - Various open source and proprietary cloud software are examples of this type of middleware.

Physical Resource Layer

- This layer includes **hardware resources**, such as computers (CPU and memory), networks (routers, firewalls, switches, network links and interfaces), storage components (hard disks) and other physical computing infrastructure elements.
- It also includes **facility resources**, such as heating, ventilation and air conditioning (HVAC), power, communications, and other aspects of the physical plant.

C. Cloud Service Management

Cloud Service Management includes all of the service-related functions that are necessary for the management and operation of those services required by or proposed to cloud consumers. As illustrated in Figure, cloud service management can be described from the perspective of *business support, provisioning and configuration*, and from the perspective of *portability and interoperability* requirements.



Business Support

- *Business Support* entails the set of business-related services dealing with clients and supporting processes. It includes the components used to run business operations that are client-facing.
- *Customer management*: Manage customer accounts, open/close/terminate accounts, manage user profiles, manage customer relationships by providing points-of-contact and resolving customer issues and problems, etc.
- *Contract management:* Manage service contracts, setup/negotiate/close/ terminate contract, etc.
- *Inventory Management:* Set up and manage service catalogues, etc.
- *Accounting and Billing:* Manage customer billing information, send billing statements, process received payments, track invoices, etc.
- *Reporting and Auditing:* Monitor user operations, generate reports, etc.
- *Pricing and Rating:* Evaluate cloud services and determine prices, handle promotions and pricing rules based on a user's profile, etc.

Provisioning and Configuration

- *Rapid provisioning:* Automatically deploying cloud systems based on the requested service/resources/capabilities.
- *Resource changing:* Adjusting configuration/resource assignment for repairs, upgrades and joining new nodes into the cloud.
- *Monitoring and Reporting:* Discovering and monitoring virtual resources, monitoring cloud operations and events and generating performance reports.
- *Metering:* Providing a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).
- *SLA management:* Encompassing the SLA contract definition (basic schema with the QoS parameters), SLA monitoring and SLA enforcement according to defined policies.

Portability and Interoperability

The proliferation of cloud computing promises cost savings in technology infrastructure and faster software upgrades. The US government, along with other potential cloud computing customers, has a strong interest in moving to the cloud. However, the adoption of cloud computing depends greatly on how the cloud can address users concerns on security, portability and interoperability.

- For portability, prospective customers are interested to know whether they can move their data or applications across multiple cloud environments at low cost and minimal disruption.
- From an interoperability perspective, users are concerned about the capability to communicate between or among multiple clouds.

Cloud providers should provide mechanisms to support *data portability*, *service interoperability*, and *system portability*.

- **Data portability** is the ability of cloud consumers to copy data objects into or out of a cloud or to use a disk for bulk data transfer.
- **Service interoperability** is the ability of cloud consumers to use their data and services across multiple cloud providers with a unified management interface.
- **System portability** allows the migration of a fully-stopped virtual machine instance or a machine image from one provider to another provider, or migrate applications and services and their contents from one service provider to another.

It should be noted that various cloud service models may have different requirements in related with portability and interoperability.

For example,

- IaaS requires the ability to migrate the data and run the applications on a new cloud. Thus, it is necessary to capture virtual machine images and migrate to new cloud providers which may use different virtualization technologies. Any provider-specific extensions to the VM images need to be removed or recorded upon being ported.
- While for SaaS, the focus is on data portability, and thus it is essential to perform data extractions and backups in a standard format.

D. Security

- It is critical to recognize that security is a cross-cutting aspect of the architecture that spans across all layers of the reference model, ranging from physical security to application security.
- Therefore, security in cloud computing architecture concerns is not solely under the purview of the Cloud Providers, but also Cloud Consumers and other relevant actors.
- Cloud-based systems still need to address security requirements such as authentication, authorization, availability, confidentiality, identity management, integrity, audit, security monitoring, incident response, and security policy management.

While these security requirements are not new, we discuss cloud specific perspectives to help discuss, analyse and implement security in a cloud system.

- **Cloud Service Model Perspectives**
- **Implications of Cloud Deployment Models**
- **Shared Security Responsibilities**

E. Privacy

Cloud providers should protect the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) and personally identifiable information (PII) in the cloud.

- PII is the information that can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.
- Though cloud computing provides a flexible solution for shared resources, software and information, it also poses additional privacy challenges to consumers using the clouds.

Cloud Cube Model

- According to cloud cube model, there are several “cloud formations” - or forms of cloud computing. Each offers
  - different characteristics,
  - varying degrees of flexibility,
  - different collaborative opportunities, and
  - different risks.
- One of the key challenges that businesses face when considering cloud computing as an option is to determine how to choose the cloud formation best suited to their various types of business operations.
- The Jericho Forum’s developed Cloud Cube Model with objectives related to cloud computing to distinctive enabling secure collaboration in the appropriate cloud formations best suited to the business needs.

The Jericho Forum

The Jericho Forum is actively encouraging solution providers and vendors to develop the missing capabilities and services to ensure customers are protected from the stormier implications of clouds.

In Feb 2009, they delivered a practical framework geared to showing how to create the right **Collaboration Oriented Architecture (COA)** to assure secure business collaboration in de-perimeterised environments. For the Jericho Forum, the natural evolution from this is to address how to follow a well-structured path towards enabling secure business collaboration without becoming vulnerable to issues which may put at risk your data, or your ability to work with your chosen business parties, or your regulatory compliance.

Recommendation

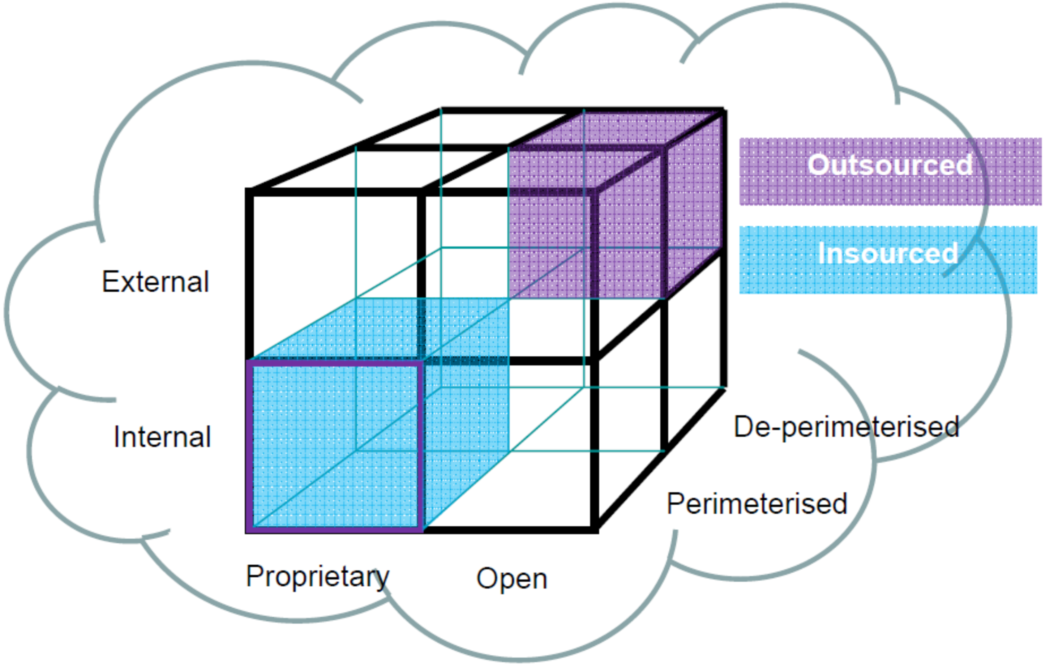
- First you need to classify your data so as to know what rules must apply to protecting it:
  - it's sensitivity
  - what regulatory/compliance restrictions apply on it.
- We can only meet this requirement if we have universally adopted standards for:
  - a data classification model
  - an associated standard for managing trust levels
  - standardised metadata that signals to "cloud security" what security needs be applied to each item of data.

With an understanding on what security you need to apply to your data, you’re in a position to decide:

- What data and processes to move to the Clouds
- At what level you want to operate in the Clouds? Cloud models separate layers of business service from each other, for example, Infrastructure / Platform / Software / Process.
- Which Cloud Formations are best suited to your needs.

The Cloud Cube Model

The Jericho Forum has identified 4 criteria to differentiate cloud formations from each other and the manner of their provision. These dimensions are as follows:



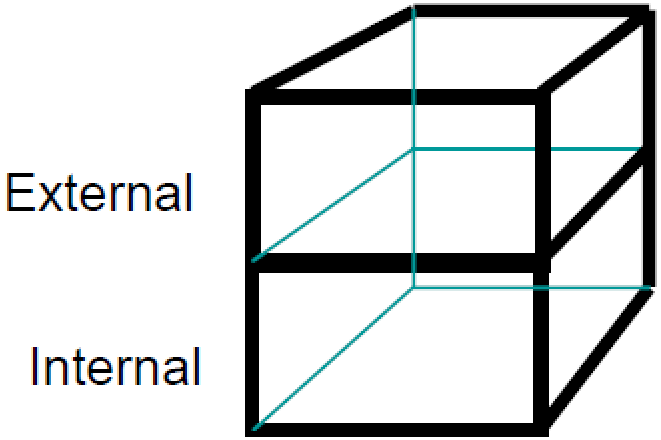
- **Internal (I) / External (E)**
- **Proprietary (P) / Open (O)**
- **Perimeterised (Per) / De-perimeterised (D-p) Architectures**
- **Insourced / Outsourced**

1. Dimension: Internal (I) / External (E)

This is the dimension that defines the physical location of the data: where does the cloud form you want to use exist inside or outside your organization’s boundaries.

- If it is within your own physical boundary then it is Internal.
- If it is not within your own physical boundary then it is External.

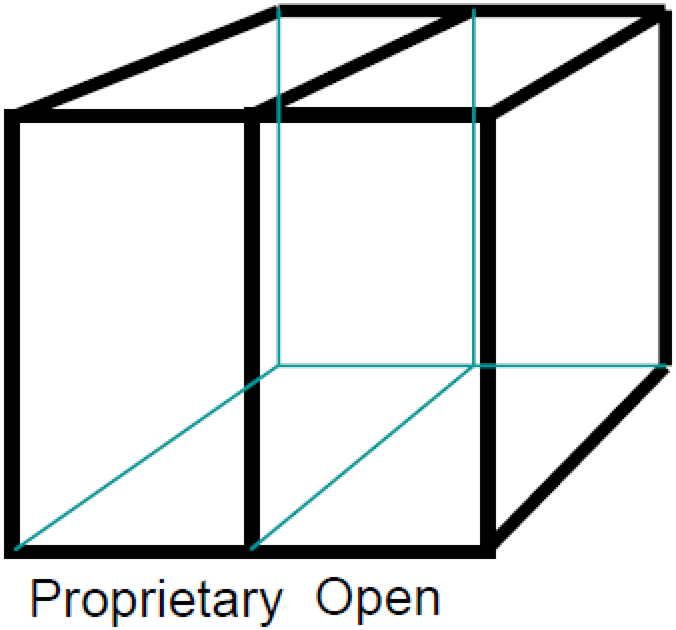
For example, virtualised hard disks in an organisation’s data centre would be internal, while Amazon SC33 would be external at some location “off-site”.



2. Dimension: Proprietary (P) / Open (O)

This is the dimension that defines the state of ownership of the cloud technology, services, interfaces, etc.

- It indicates the degree of interoperability, as well as enabling "data/application transportability" between your own systems and other cloud forms.
- It indicates the ability to withdraw your data from a cloud form or to move it to another without constraint.
- It also indicates any constraints on being able to share applications.



Proprietary means that the organisation providing the service is keeping the means of provision under their ownership.

- As a result, when operating in clouds that are proprietary, you may not be able to move to another cloud supplier without significant effort or investment.
- Often the more innovative technology advances occur in the proprietary domain. As such the proprietor may choose to enforce restrictions through patents and by keeping the technology involved a trade secret.

Clouds that are **Open** are using technology that is not proprietary, meaning that there are likely to be more suppliers, and you are not as constrained in being able to share your data and collaborate with selected parties using the same open technology.

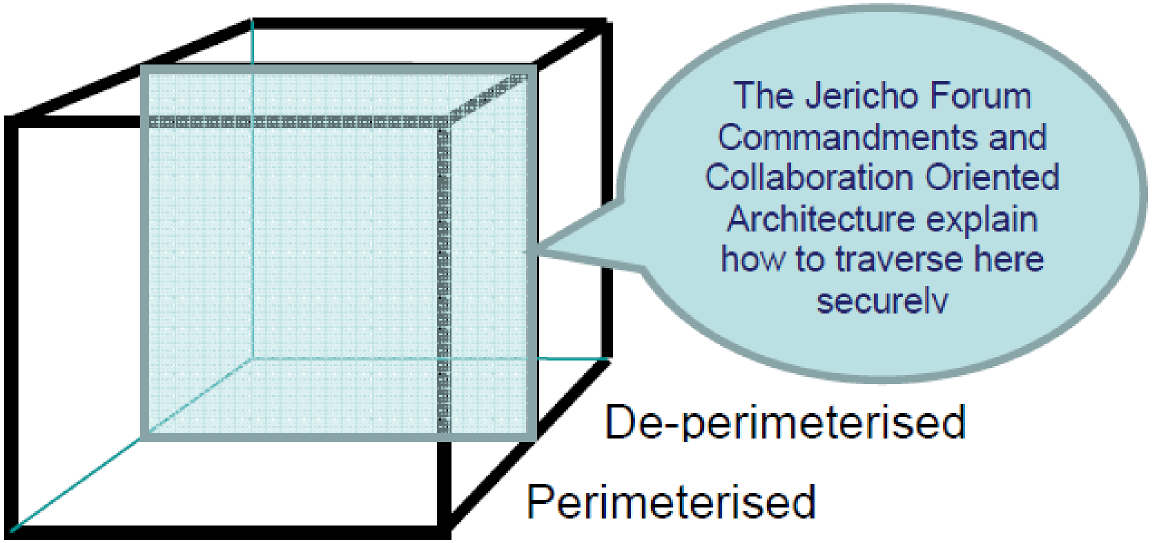
- Open services tend to be those that are widespread and consumerised, and most likely a published open standard, for example email (SMTP).
- An as yet unproven premise is that the clouds that most effectively enhance collaboration between multiple organisations will be Open.

3. Dimension: Perimeterised (Per) / De-perimeterised (D-p) Architectures

The third dimension represents the "architectural mindset" :

Are you operating inside your traditional IT perimeter or outside it?

De-perimeterisation has always related to the gradual failure / removal /shrinking / collapse of the traditional silo-based IT perimeter.


The Jericho Forum Commandments and Collaboration Oriented Architecture explain how to traverse here securelv
De-perimeterised
Perimeterised

Perimeterised implies continuing to operate within the traditional IT perimeter, often signalled by "network firewalls".

- When operating in the perimeterised areas, you may simply extend your own organisation's perimeter into the external cloud computing domain using a VPN and operating the virtual server in your own IP domain, making use of your own directory services to control access.
- Then, when the computing task is completed you can withdraw your perimeter back to its original traditional position. We consider this type of system perimeter to be a traditional, though virtual, perimeter.

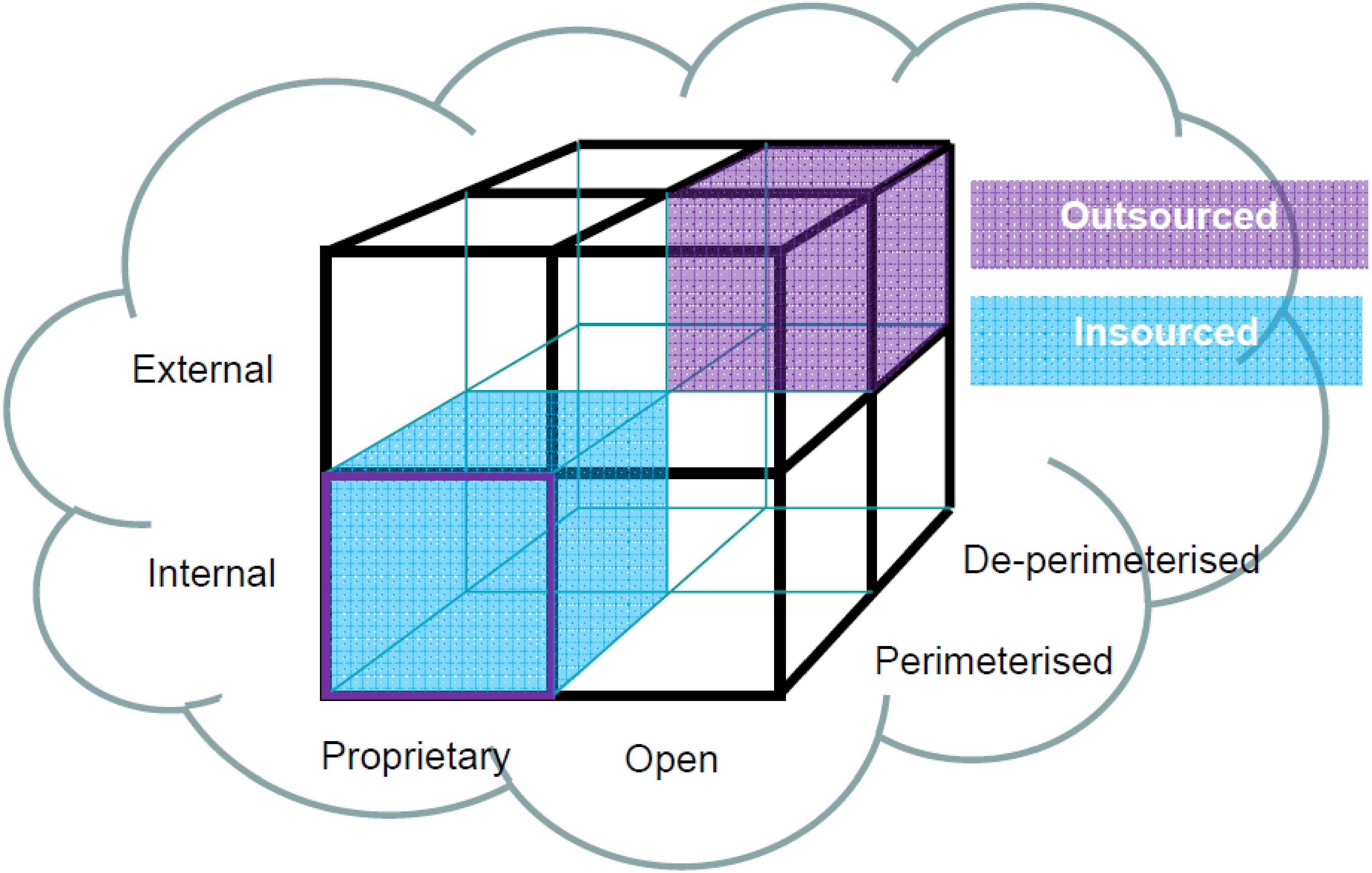
De-perimeterised, assumes that the system perimeter is architected following the principles outlined in the Jericho Forum's Commandments and Collaboration Oriented Architectures Framework.

- In a de-perimeterised environment an organisation can collaborate securely with selected parties (business partner, customer, supplier, outworker) globally over any COA capable network.
- The terms **Micro-Perimeterisation** and **Macro- Perimeterisation** will likely be in active use here - for example in a de-perimeterised frame the data would be encapsulated with meta-data and mechanisms that would protect the data from inappropriate usage. COA-enabled systems allow secure collaboration.

The de-perimeterised areas in our Cloud Cube Model use both internal and external domains but the collaboration or sharing of data should not be seen as internal or external. Rather, it is controlled by and limited to the parties that the using organisations select.

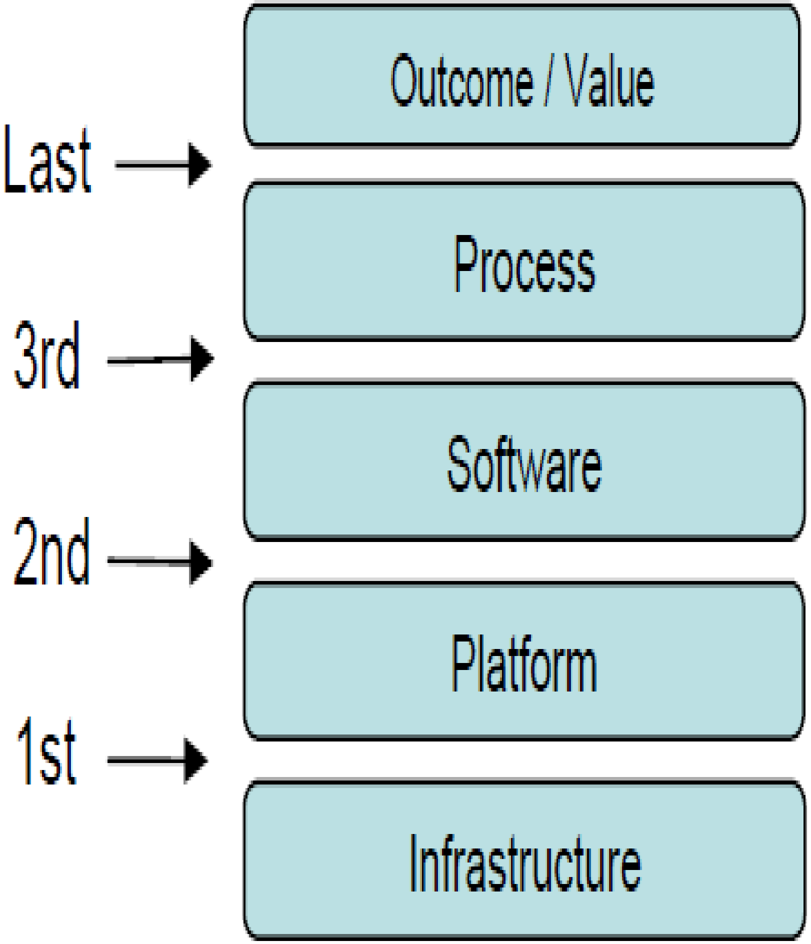
So, Some of the Facts are

- You can operate in any of the four cloud formations so far described (I/P,I/O,E/P,E/O) with either of two architectural mindsets- Perimeterised or De-perimeterised.
- The top-right E/O/D-p cloud formation is likely to be the "sweet spot" where optimum flexibility and collaboration can be achieved.
- A Proprietary cloud provider will likely want to keep you in the left side of the cube, achieved by either continuous innovation that adds value, or by limiting the means of migrating from the proprietary domain.
- The ability to move from that top-left cloud form to the "sweet-spot" top-right cloud form will require a rare interface because facilitating you making this move is going to be rarely in the cloud supplier's best business interests.


Outsourced
Insourced
External
Internal
De-perimeterised
Perimeterised
Proprietary
Open

While the underlying intent remains the same, an added distinction in describing Deperimeterised cloud usage arises in that the detailed description changes based on the level of abstraction at which you choose to operate.

At the heart of all cloud forms is the concept of abstraction. Cloud models separate one layer of business from another, e.g. process from software, platform from infrastructure, etc. We show an example model here with four levels of abstraction; we can expect other models identifying different layers and abstraction levels to emerge to suit different business needs. Most cloud computing activities today are occurring at the lower layers of the stack, so today we have more maturity at the lower level.



4. Dimension: Insourced / Outsourced

A 4th dimension that has 2 states in each of the 8 cloud forms: Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO), that responds to the question

"Who do you want running your Clouds?"

- **Outsourced**: the service is provided by a 3rd party
- **Insourced**: the service is provided by your own staff under your control

These 2 states describe who is managing delivery of the cloud service(s) that you use. This is primarily a policy issue (i.e. a business decision, not a technical or architectural decision) which must be embodied in a contract with the cloud provider.

In the Cloud Cube Model diagram this 4th dimension is shown by 2 colors; any of the 8 cloud forms can take either color.

Key questions customers need to ask their Cloud Computing suppliers

1. Where in our cloud cube model is my cloud supplier operating when providing each of their services?
2. How will my cloud supplier assure that when using their services I am operating in a cloud form that has and will maintain the features I expect?
3. How can I ensure that my data and the cloud services will continue to be available, in the event of the provider's bankruptcy or change in business direction.