CLOUD COMPUTING ARCHITECTURE

By

Utpal Chandra De

School of Computer Applications

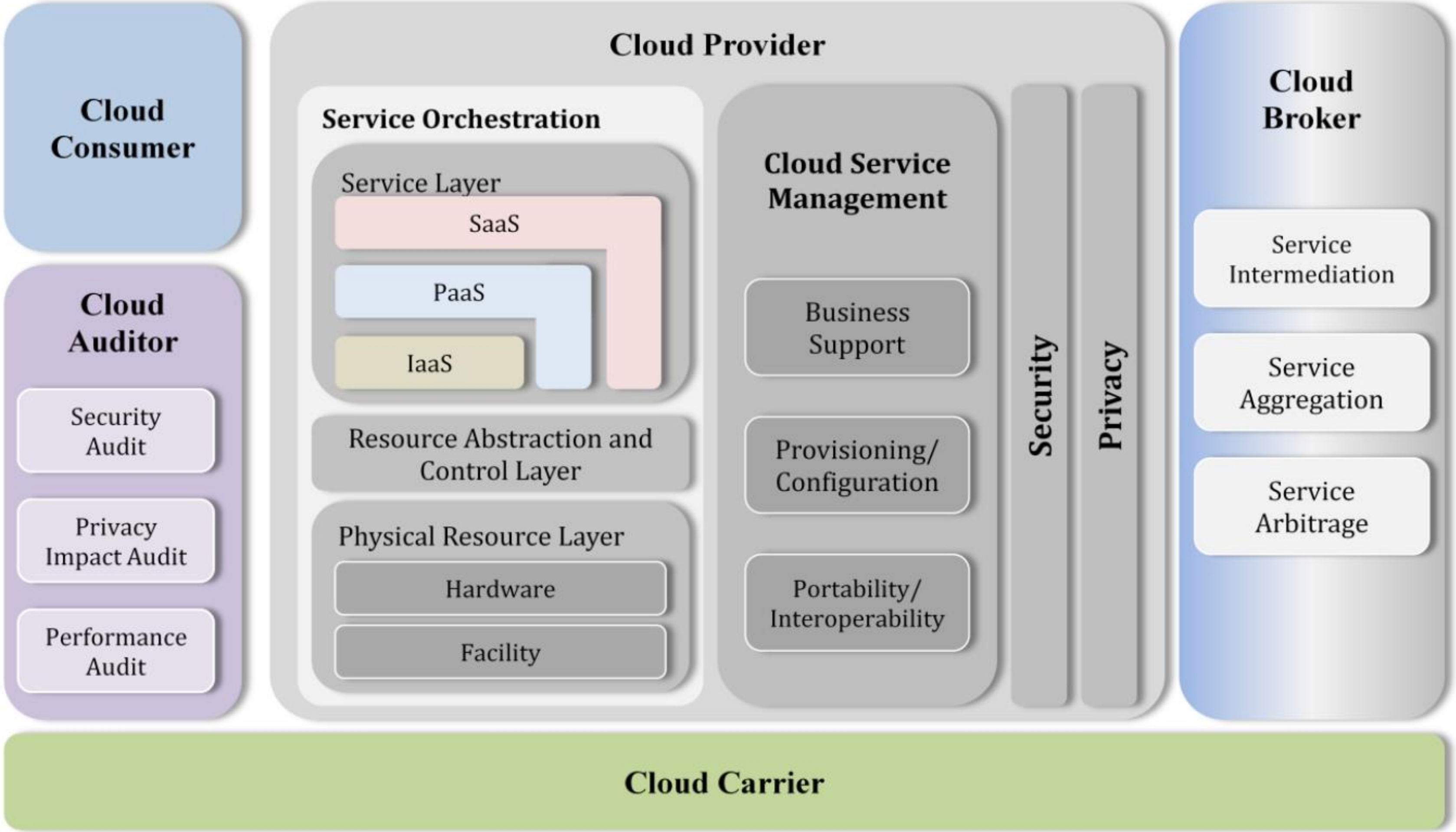
KIIT [Deemed to be University]

Objectives:

- to illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model,
- to provide a technical reference to different agencies and other consumers to understand, discuss, categorize and compare cloud services,
- to facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations.

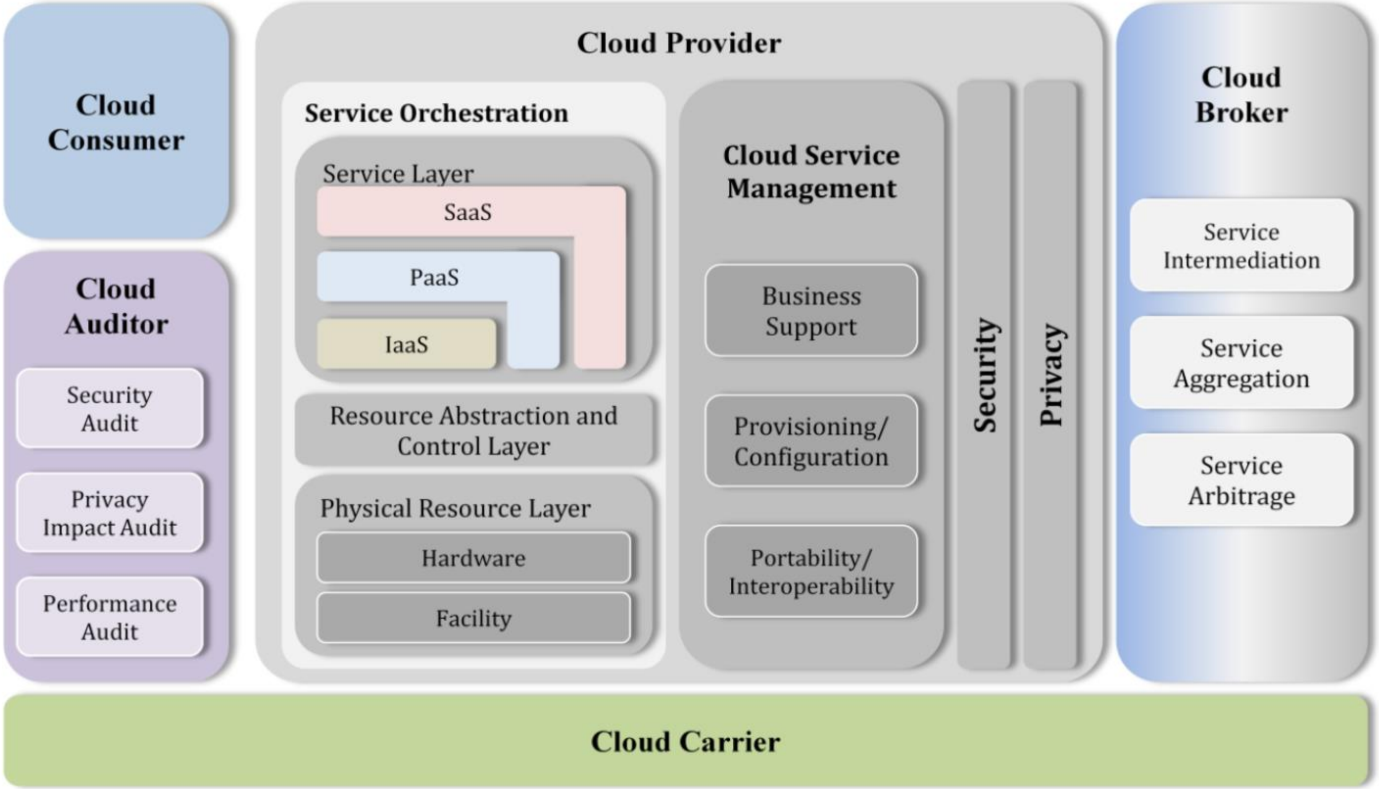
Cloud Computing Reference Architecture: An Overview

- The Conceptual Reference Model:
  - The diagram depicts a generic high-level architecture and is intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud computing.



The Conceptual Reference Model:

- the NIST cloud computing reference architecture defines five major actors:
- cloud consumer,
- cloud provider,
- cloud carrier,
- cloud auditor and
- cloud broker

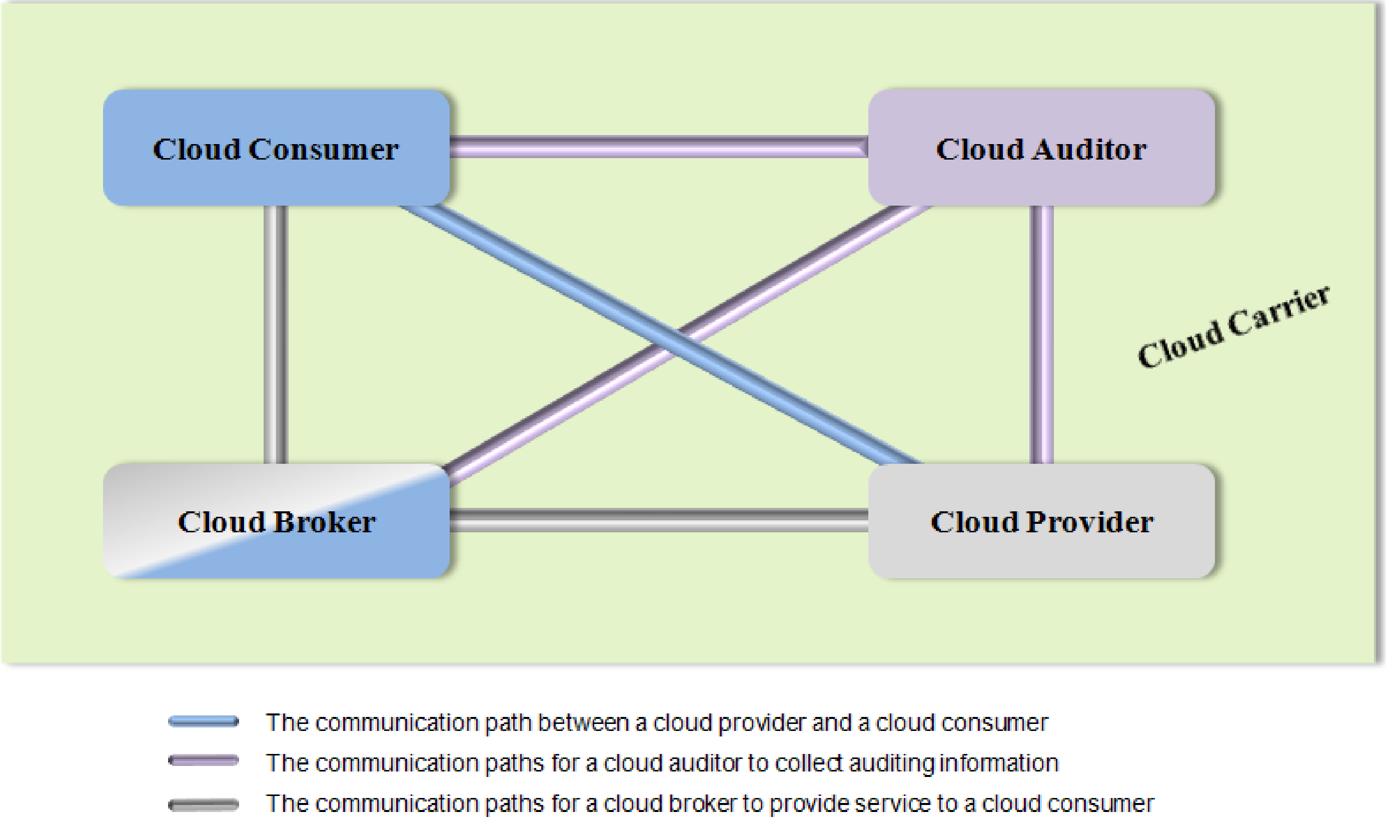


The actors defined briefly in this lists

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.

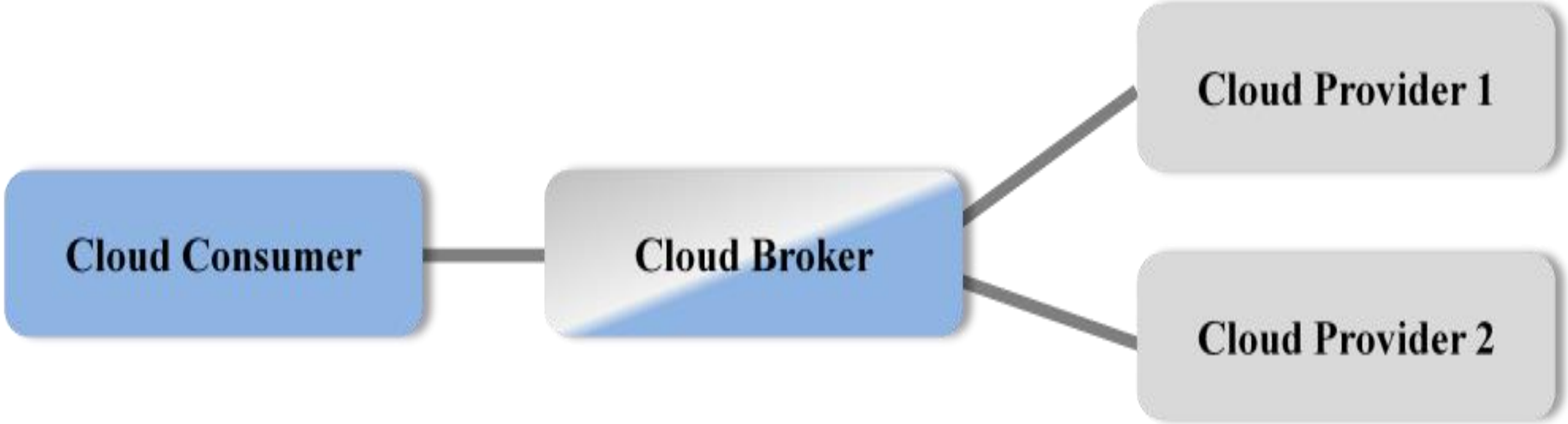
The interactions among the actors

- A cloud consumer may request cloud services from a cloud provider directly or via a cloud broker.
- A cloud auditor conducts independent audits and may contact the others to collect necessary information.


Cloud Consumer
Cloud Auditor
Cloud Carrier
Cloud Broker
Cloud Provider
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

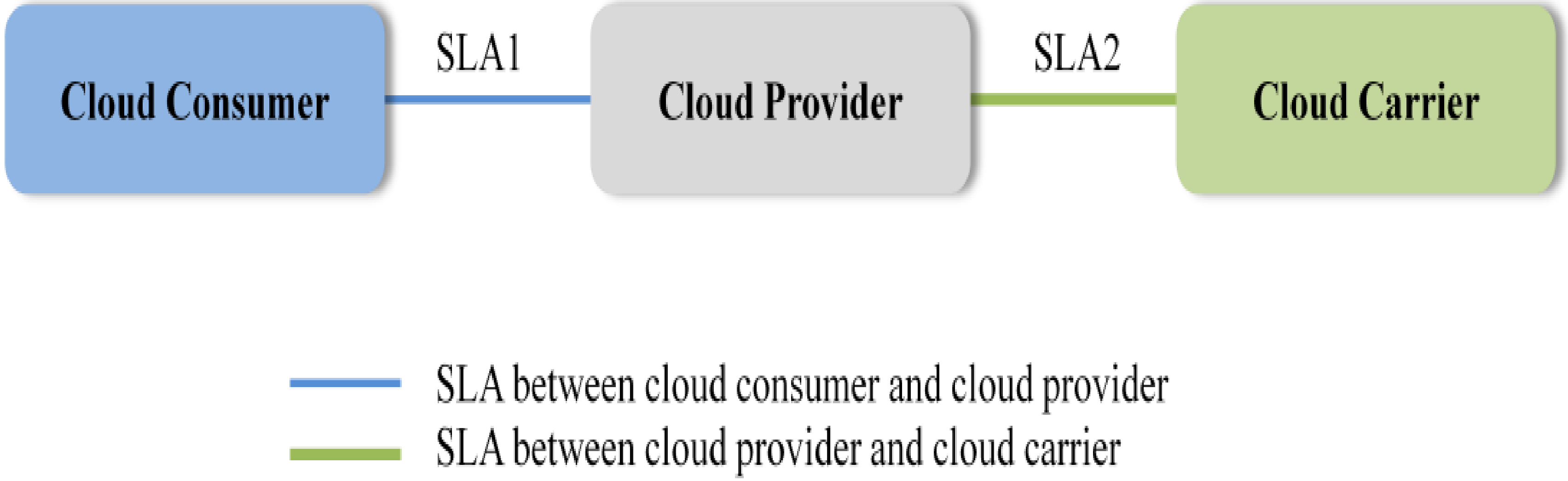
Example Usage Scenario 1: [Cloud Brokers]

- 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.



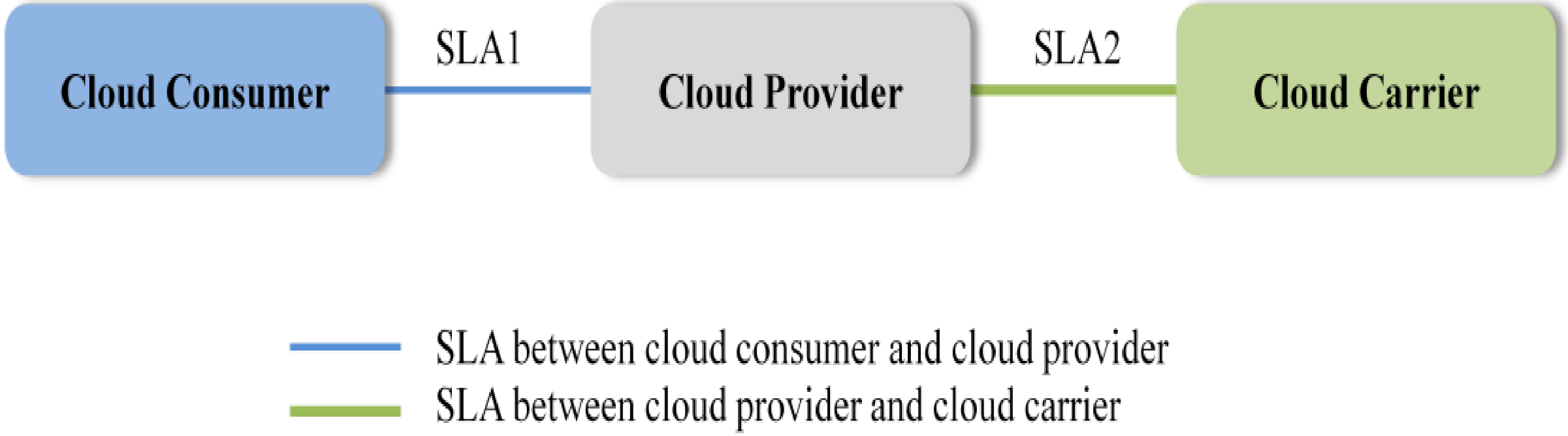
Example Usage Scenario 2: [Cloud carriers]

- Cloud carriers provide the connectivity and transport of cloud services from cloud providers to cloud consumers.
- As illustrated in the 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).


Cloud Consumer
SLA1
Cloud Provider
SLA2
Cloud Carrier
SLA between cloud consumer and cloud provider
SLA between cloud provider and cloud carrier

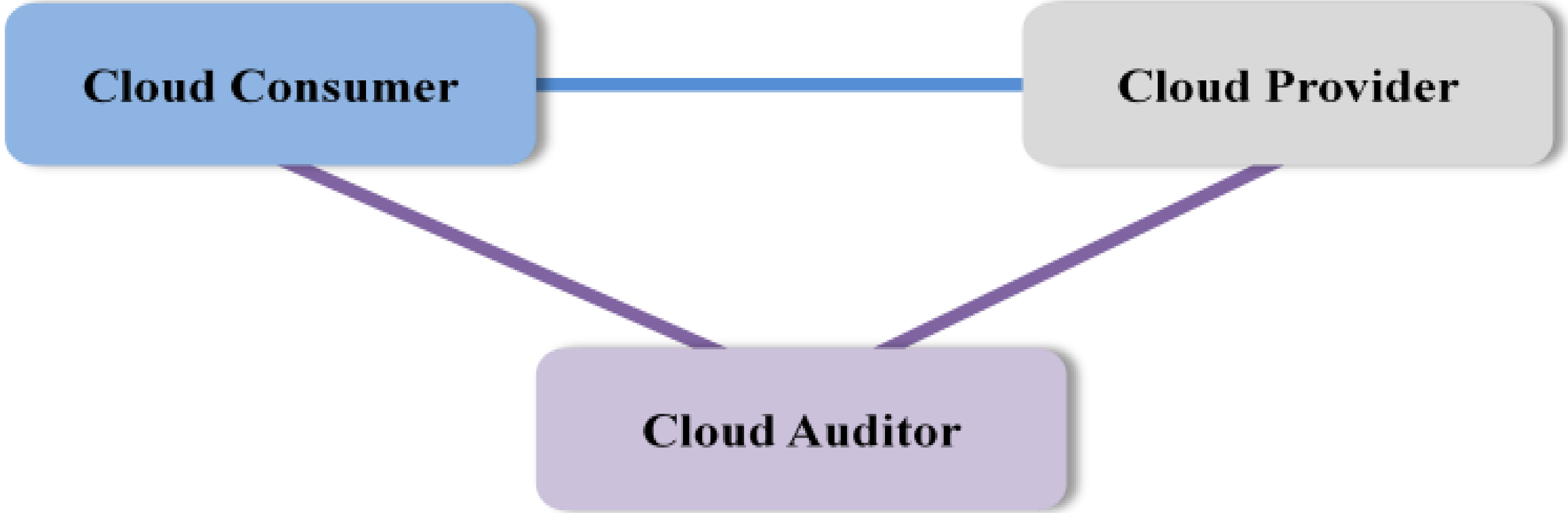
Example Usage Scenario 2: [Cloud carriers]

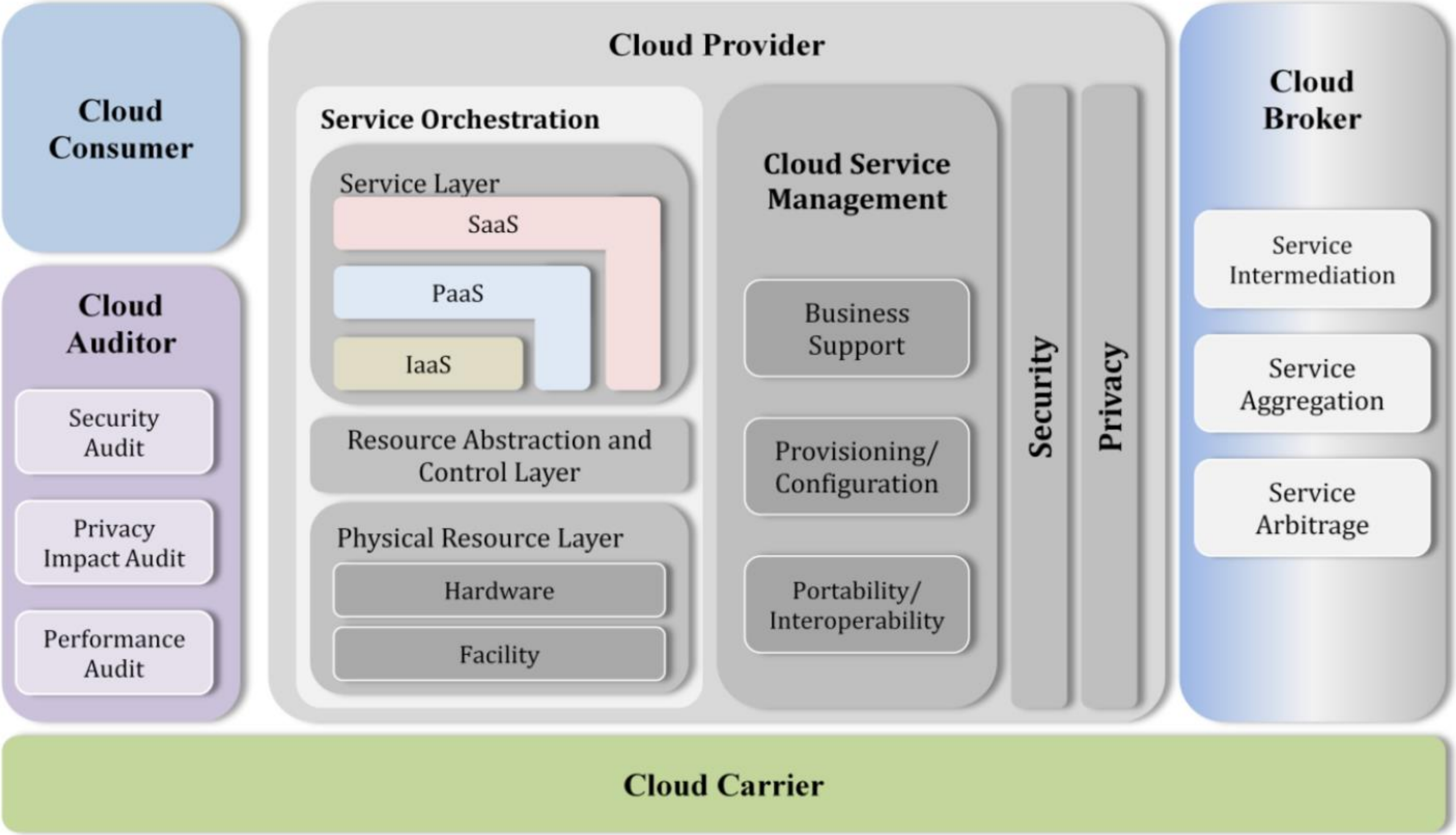
- A cloud provider arranges service level agreements (SLAs) with a cloud carrier and may request dedicated and encrypted connections to ensure the cloud services are consumed at a consistent level according to the contractual obligations with the cloud consumers.
- In this case, the provider may specify 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

Example Usage Scenario 3:[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.




Cloud Consumer
Cloud Auditor
Security Audit
Privacy Impact Audit
Performance Audit
Cloud Provider
Service Orchestration
Service Layer
SaaS
PaaS
IaaS
Resource Abstraction and Control Layer
Physical Resource Layer
Hardware
Facility
Cloud Service Management
Business Support
Provisioning/ Configuration
Portability/ Interoperability
Security
Privacy
Cloud Broker
Service Intermediation
Service Aggregation
Service Arbitrage
Cloud Carrier

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 catalog 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.

Cloud Consumer (cont.)

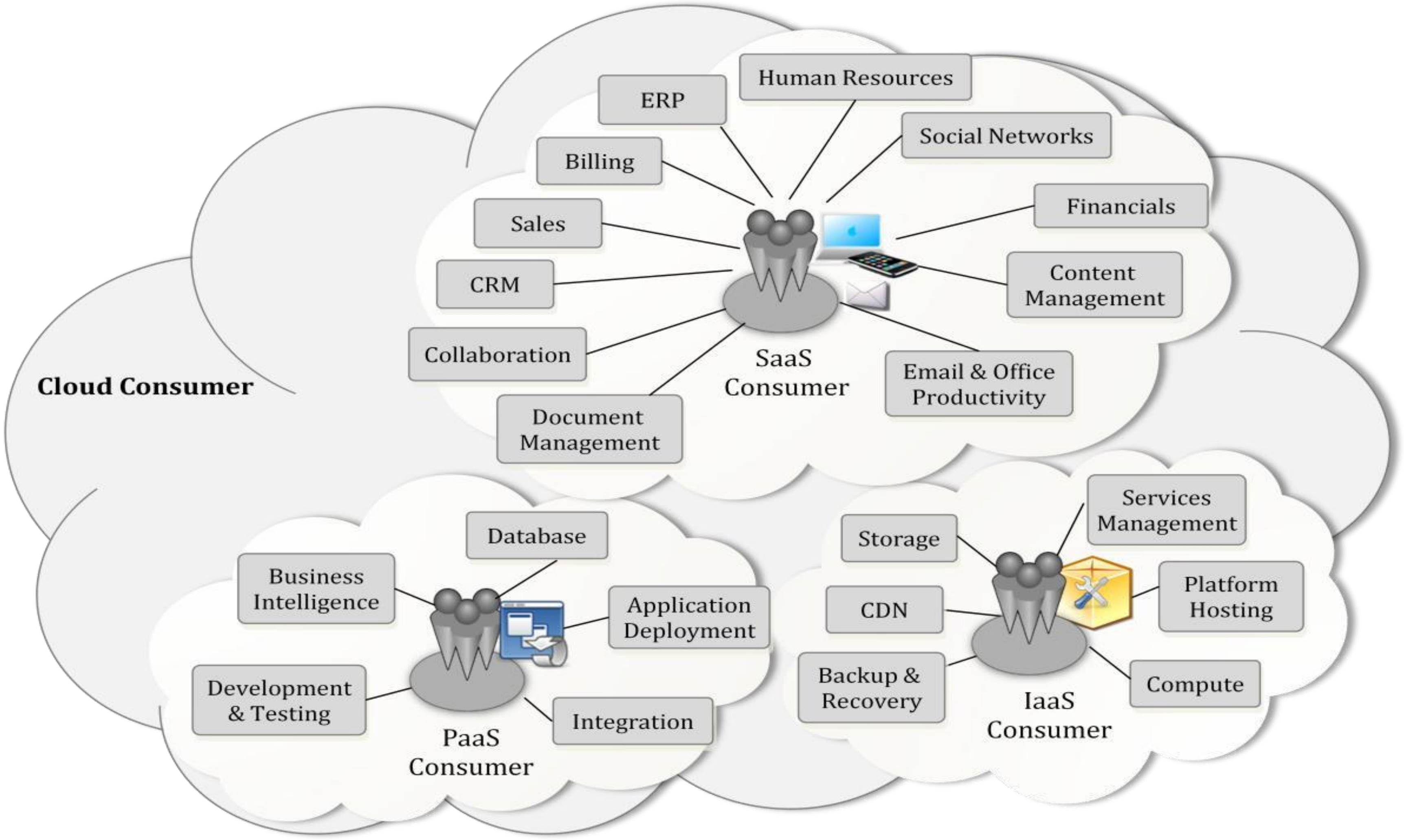
- A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service.
- The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly.

Cloud Consumer (cont.)

- Cloud consumers need SLAs to specify the technical performance requirements fulfilled by a cloud provider.
- SLAs can cover terms regarding the quality of service, security, remedies for performance failures.
- A cloud consumer can freely choose a cloud provider with better pricing and more favorable terms.
- Depending on the services requested, the activities and usage scenarios can be different among cloud consumers

Cloud Consumer (cont.)

- Some Services Available to a Cloud Consumer:



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.

Cloud Provider (cont.)

- For ***Software as a Service***, the cloud provider deploys, configures, maintains and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers.
- The provider of ***SaaS*** assumes most of the responsibilities in managing and controlling the applications and the infrastructure, while the cloud consumers have limited administrative control of the applications.

Cloud Provider (cont.)

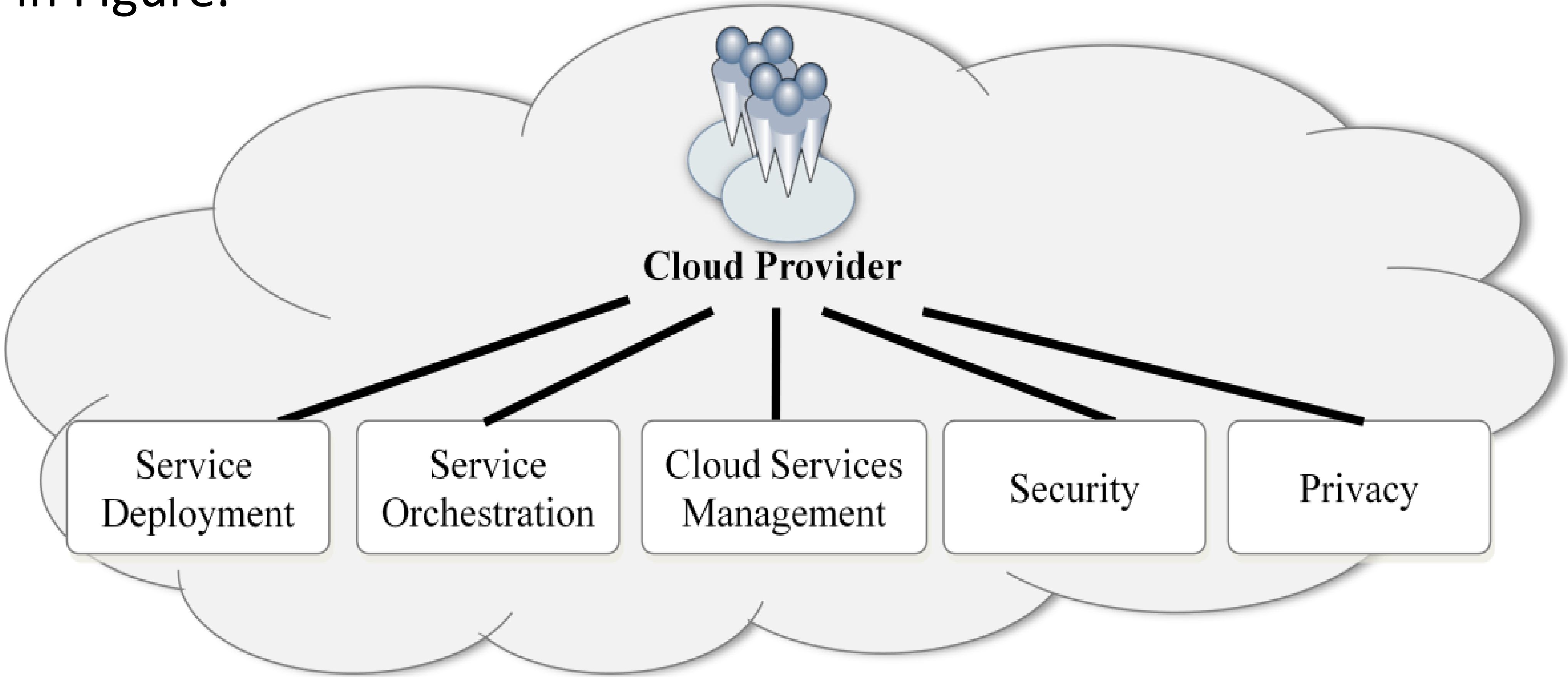
- For ***PaaS***, the Cloud Provider manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as runtime software execution stack, databases, and other middleware components.
- The ***PaaS Cloud Provider*** typically also supports the development, deployment and management process of the ***PaaS Cloud Consumer*** by providing tools such as integrated development environments (IDEs), development version of cloud software, software development kits (SDKs), deployment and management tools.
- The ***PaaS Cloud Consumer*** has control over the applications and possibly some of the hosting environment settings, but has no or limited access to the infrastructure underlying the platform such as network, servers, operating systems (OS), or storage.

Cloud Provider (cont.)

- For ***IaaS***, the Cloud Provider acquires the physical computing resources underlying the service, including the servers, networks, storage and hosting infrastructure.
- The Cloud Provider runs the cloud software necessary to makes computing resources available to the IaaS Cloud Consumer through a set of service interfaces and computing resource abstractions, such as virtual machines and virtual network interfaces.
- The IaaS Cloud Consumer in turn uses these computing resources, such as a virtual computer, for their fundamental computing needs Compared to SaaS and PaaS Cloud Consumers, an IaaS Cloud Consumer has access to more fundamental forms of computing resources and thus has more control over the more software components in an application stack, including the OS and network.
- The IaaS Cloud Provider, on the other hand, has control over the physical hardware and cloud software that makes the provisioning of these infrastructure services possible, for example, the physical servers, network equipment, storage devices, host OS and hypervisors for virtualization

Cloud Provider - Major Activities

- A Cloud Provider's activities can be described in five major areas, as shown in Figure.



Why is Cloud Orchestration important?

- The rapid adoption of containerized, micro-services based applications that communicate via APIs has created the demand for automation of deploying and managing applications across the cloud.
- This increasing complexity has created the demand for cloud orchestration software that can manage the myriad (a large number of) dependencies across multiple clouds, with policy-driven security and management capabilities.

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.
- An audit of a cloud environment is similar to an IT audit.
- Both examine a variety of operational, administrative, security and performance controls.

7 key steps for a cloud audit

1 Gather evidence, including data, reports and screenshots.

2 Interview relevant professionals at cloud service provider.

3 Analyze data and information collected.

4 Compile results into work papers.

5 Prepare final report and recommendations.

6 Submit report to management, and conduct an audit briefing.

7 Assign response team, and set dates for recommended actions.

Resource	Description	Link
Cloud Controls Matrix (CCM) v4	Cybersecurity control framework for cloud computing aligned to CSA best practices	CCM and Consensus Assessment Initiative Questionnaire (CAIQ) v4 (downloadable document)
Security, Trust, Assurance and Risk (STAR) security questionnaire	Checklist tool to ask cloud vendors about security controls	STAR Level 1 Security Questionnaire (downloadable document)
STAR Registry	List of cloud vendors' security and regulatory compliance postures	STAR Registry listing
CSA best practices	Guidance on cloud security, performance and auditing	CSA Security Guidance (downloadable document)
Mapping to other standards	Mapping CCM v4 to other industry standards, such as the International Organization for Standardization 27000 series and Payment Card Industry Data Security Standard	Included in CCM and CAIQ v4
Controls Applicability Matrix	Help for auditors to decide the most appropriate controls to use for a specific vendor	Included in CCM and CAIQ v4
CCM Metrics	Compendium of security metrics for clouds to support governance, risk and compliance activities	Included in CCM and CAIQ v4
CCM v4 Implementation Guidelines	Guidelines for using the CCM v4 audit standards	Included in CCM and CAIQ
Continuous Audit Metrics Catalog	Guidance to plan and implement continuous cloud audit activities	Continuous Audit Metrics (downloadable document)
CCM v4 Auditing Guidelines	Guidance for planning, organizing and conducting a cloud audit engagement using CCM v4	Available Q4 2021

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.

Cloud Broker (cont.)

- 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.

Cloud Broker (cont.)

- 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.

Cloud Broker (cont.)

- 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.

Cloud Carrier

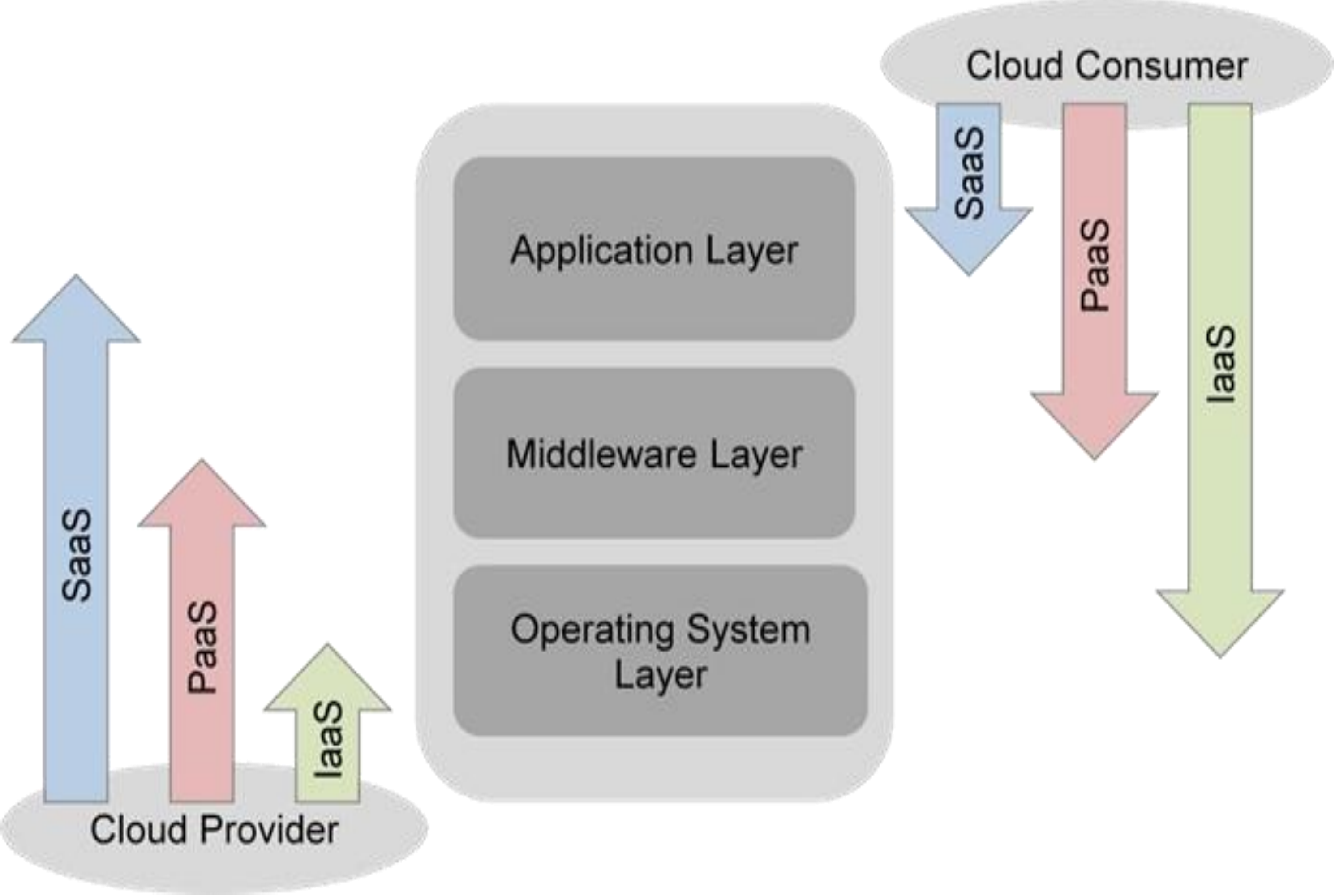
- A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.
- Cloud carriers provide access to consumers through network, telecommunication and other access devices.
- For example, cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile Internet devices (MIDs), etc.

Cloud Carrier (cont.)

- 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.

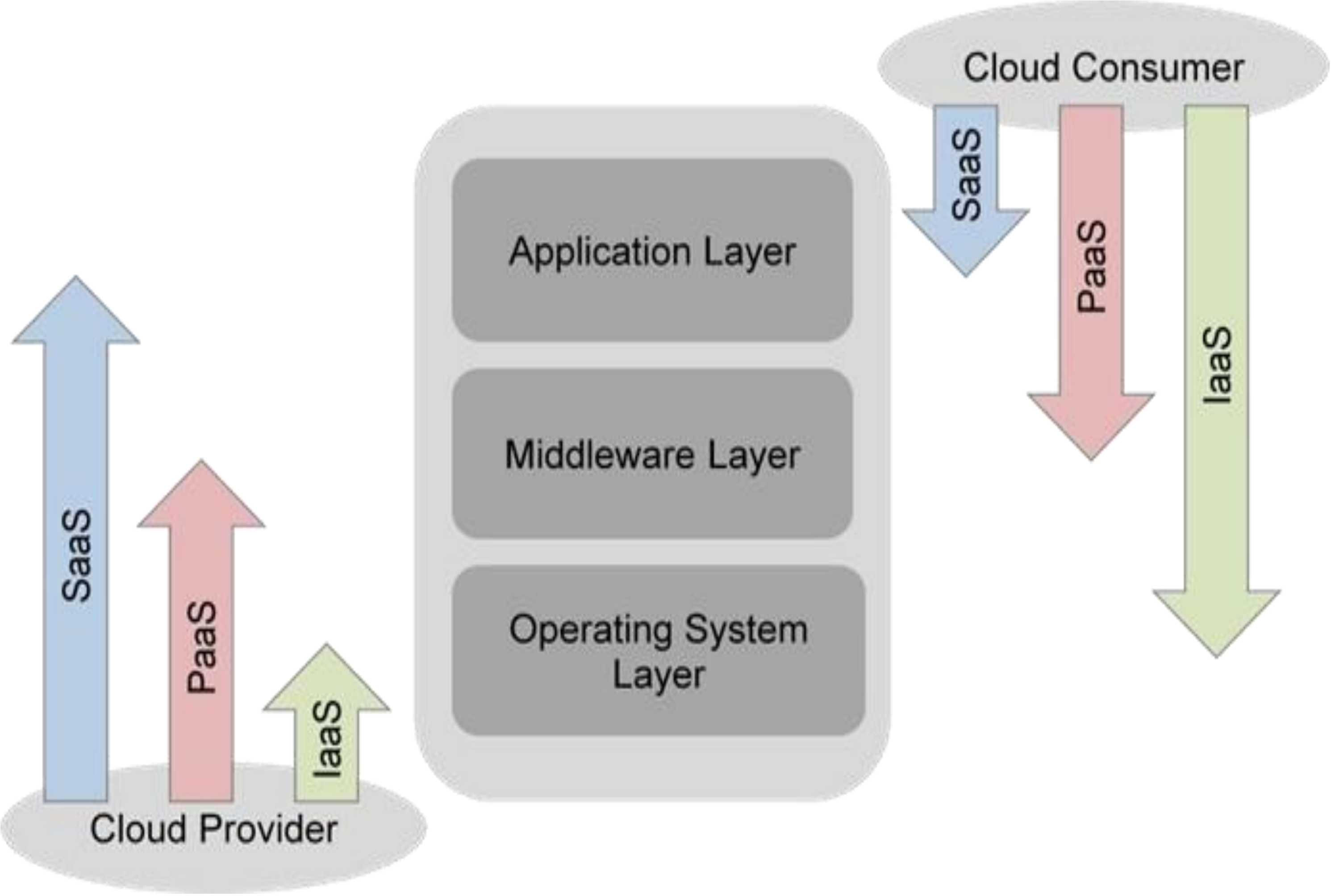
Scope of Control between Provider and Consumer

- The Cloud Provider and Cloud Consumer share the control of resources in a cloud system.
- As illustrated in Figure, different service models affect an organization's control over the computational resources and thus what can be done in a cloud system.
- The figure shows these differences using a classic software stack notation comprised of the application, middleware, and OS layers.
- This analysis of delineation of controls over the application stack helps understand the responsibilities of parties involved in managing the cloud application.



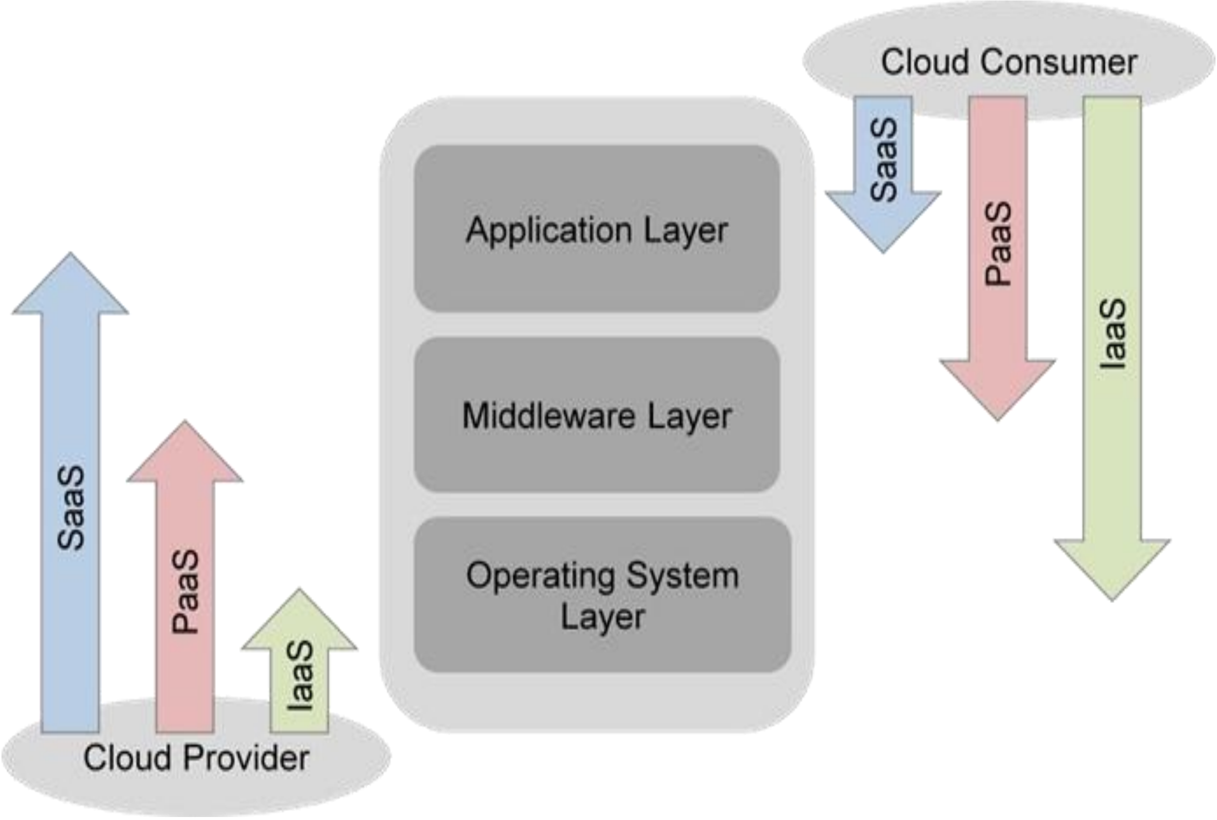
Scope of Control between Provider and Consumer (cont.)

- The application layer includes software applications targeted at end users or programs.
- The applications are used by SaaS consumers, or installed/managed/ maintained by PaaS consumers, IaaS consumers, and SaaS providers.
- The middleware layer provides software building blocks (e.g., libraries, database, and Java virtual machine) for developing application software in the cloud.
- The middleware is used by PaaS consumers, installed/managed/maintained by IaaS consumers or PaaS providers, and hidden from SaaS consumers.



Scope of Control between Provider and Consumer (cont.)

- The OS layer includes operating system and drivers, and is hidden from SaaS consumers and PaaS consumers.
- An IaaS cloud allows one or multiple guest OS‟s to run virtualized on a single physical host.
- Generally, consumers have broad freedom to choose which OS to be hosted among all the OS's that could be supported by the cloud provider.
- The IaaS consumers should assume full responsibility for the guest OS‟s, while the IaaS provider controls the host OS.

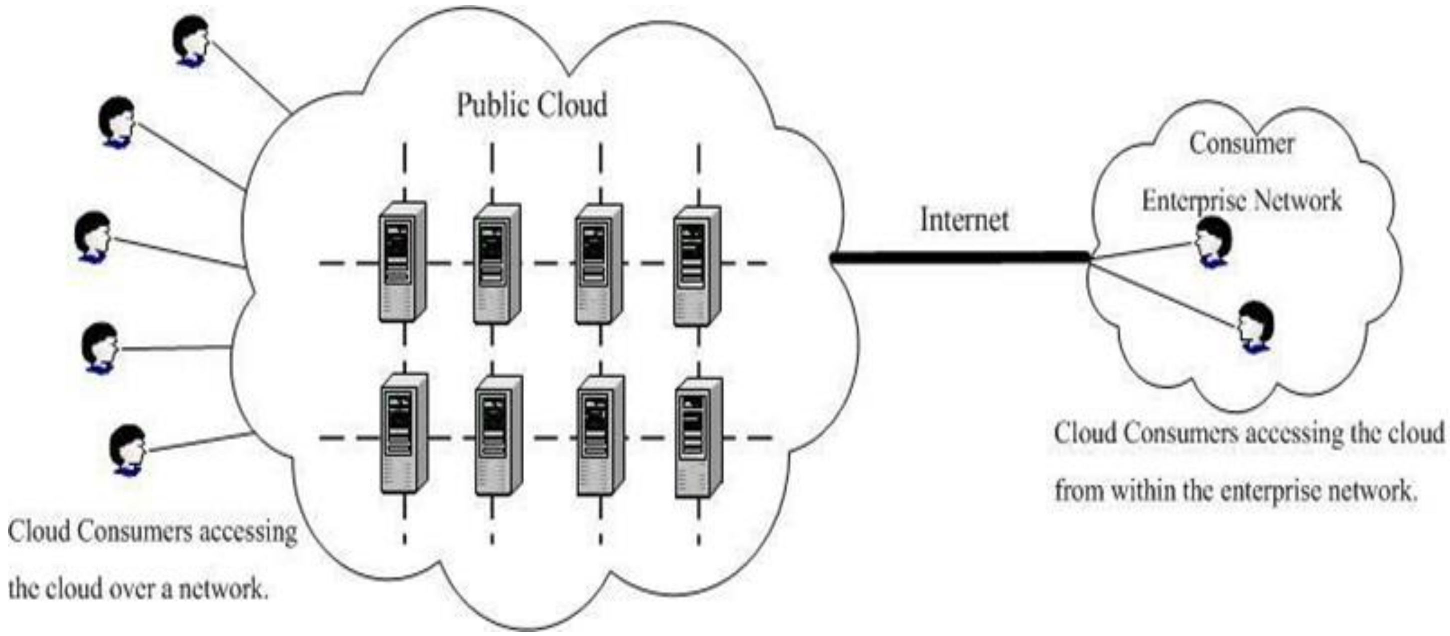


Cloud Computing Reference Architecture: Architectural Components

- Service Deployment: As identified in the NIST cloud computing definition, a cloud infrastructure may be operated in one of the following deployment models:
  - public cloud,
  - private cloud,
  - community cloud,
  - hybrid cloud.
- The differences are based on how exclusive the computing resources are made to a Cloud Consumer.

Public cloud

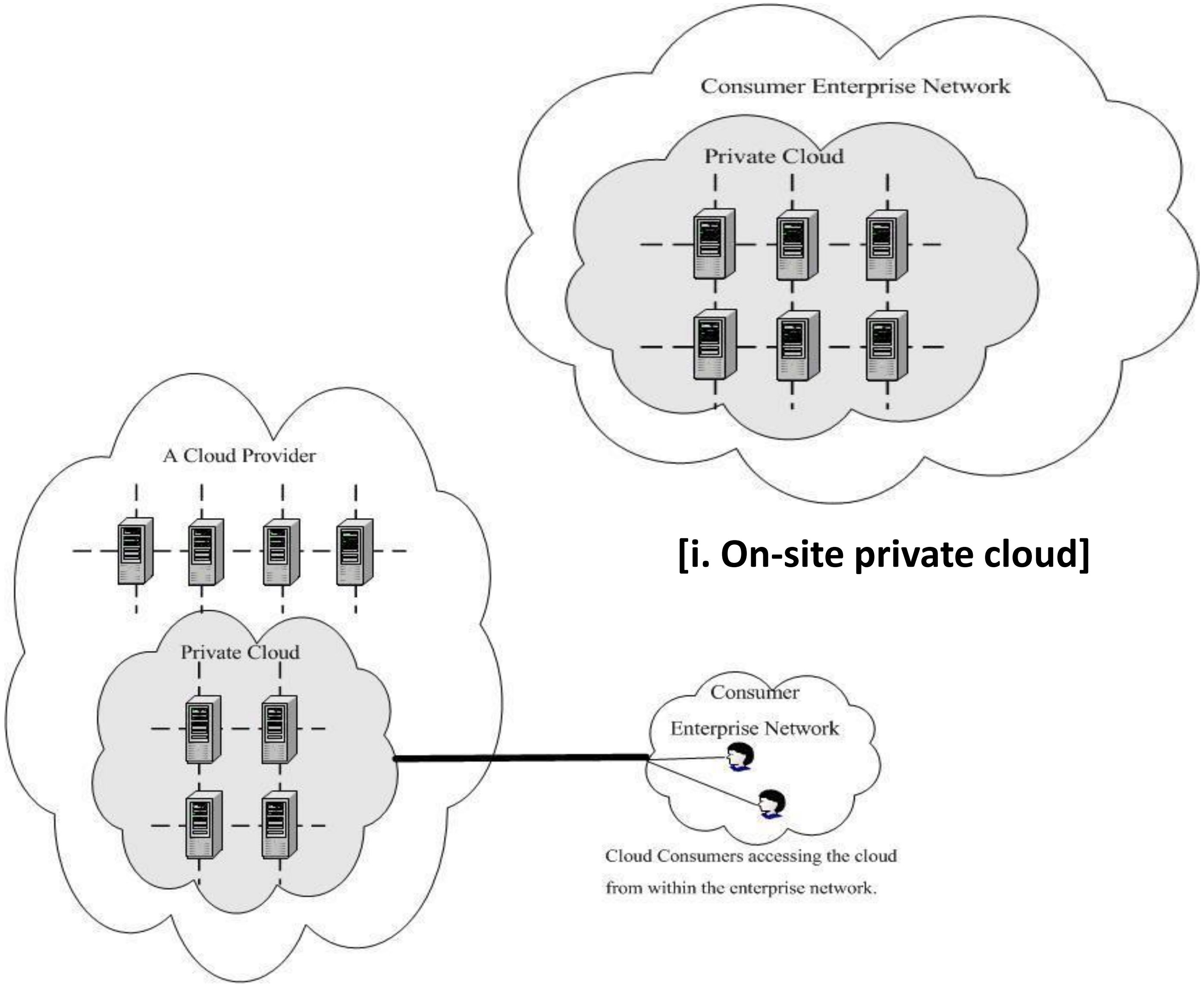
- A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network.
- A public cloud is owned by an organization selling cloud services, and serves a diverse pool of clients.
- Figure presents a simple view of a public cloud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


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

[public cloud]

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 or by a third party, and may be hosted on the organization’s premises (i.e. on-site private clouds) or outsourced to a hosting company (i.e. outsourced private clouds).
- Figure-i and Figure-ii present an on-site private cloud and an outsourced private cloud, respectively.


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

[i. On-site private cloud]

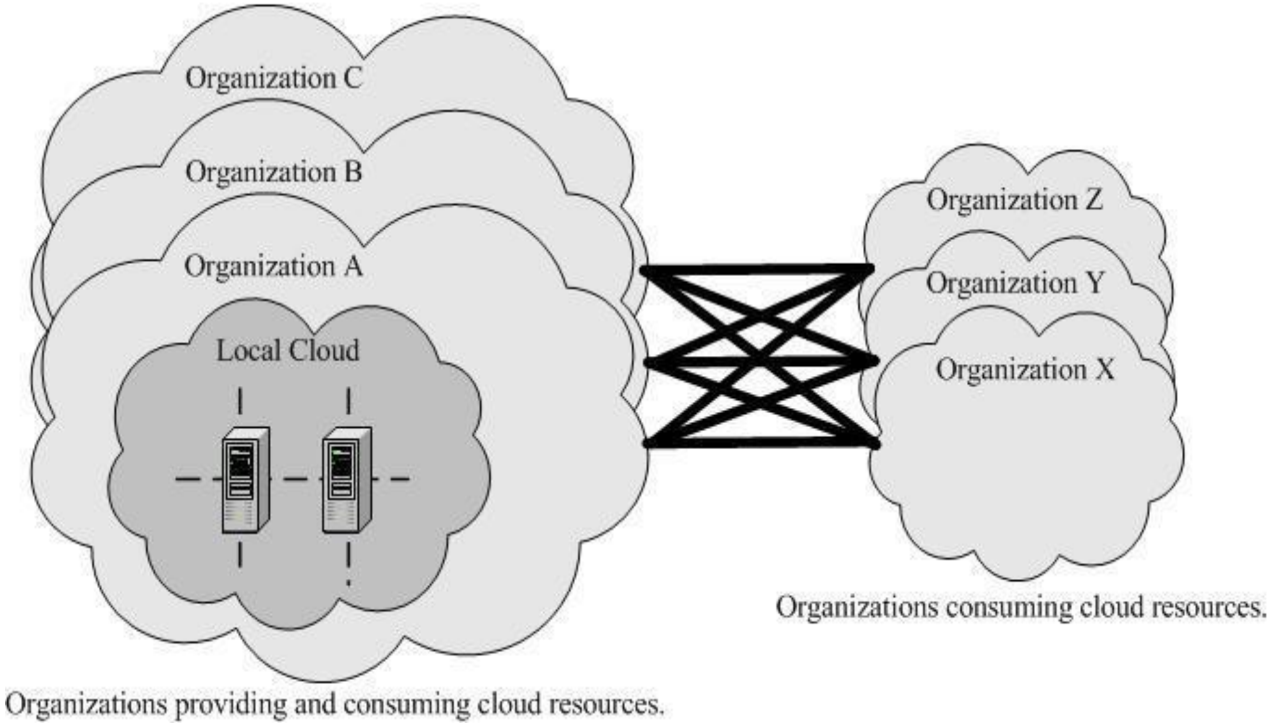
[ii. Out-sourced Private Cloud]

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

Community cloud

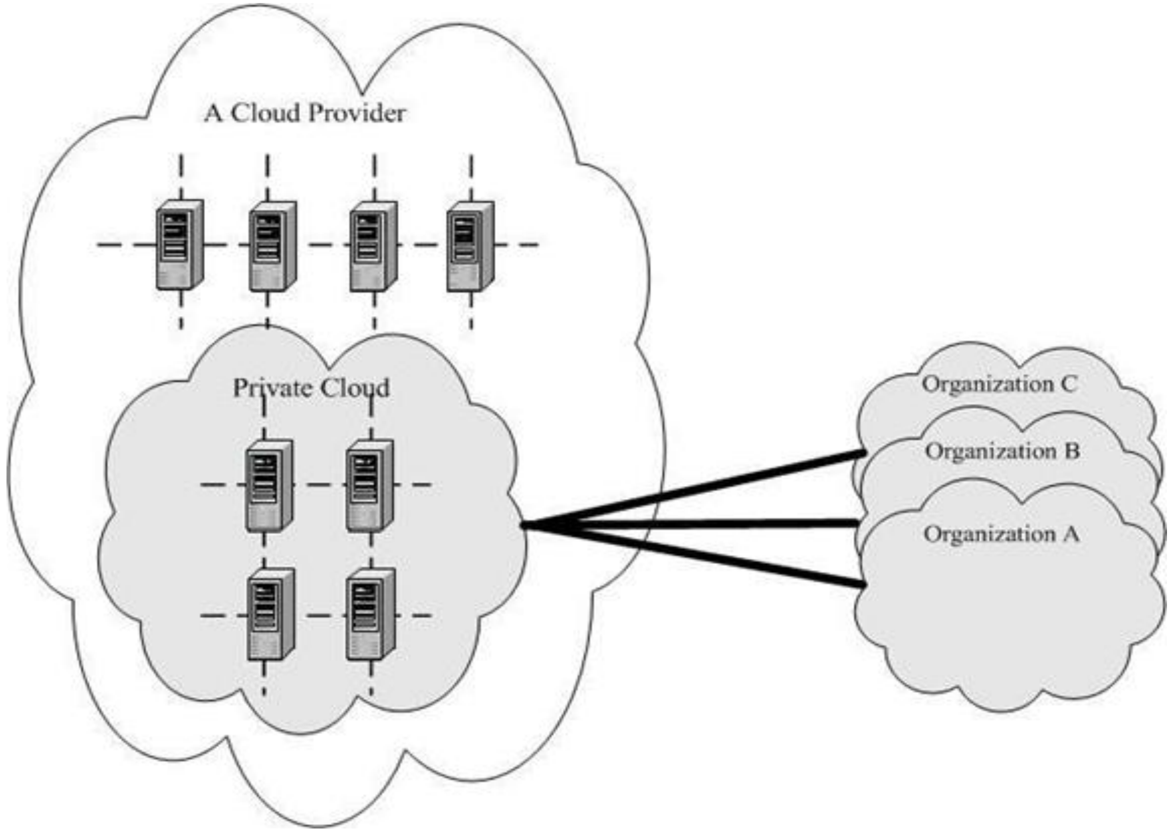
- This figure depicts an on-site community cloud comprised of a number of participant organizations.
- A cloud consumer can access the local cloud resources, and also the resources of other participating organizations through the connections between the associated organizations.



[On-site community cloud]

Community cloud

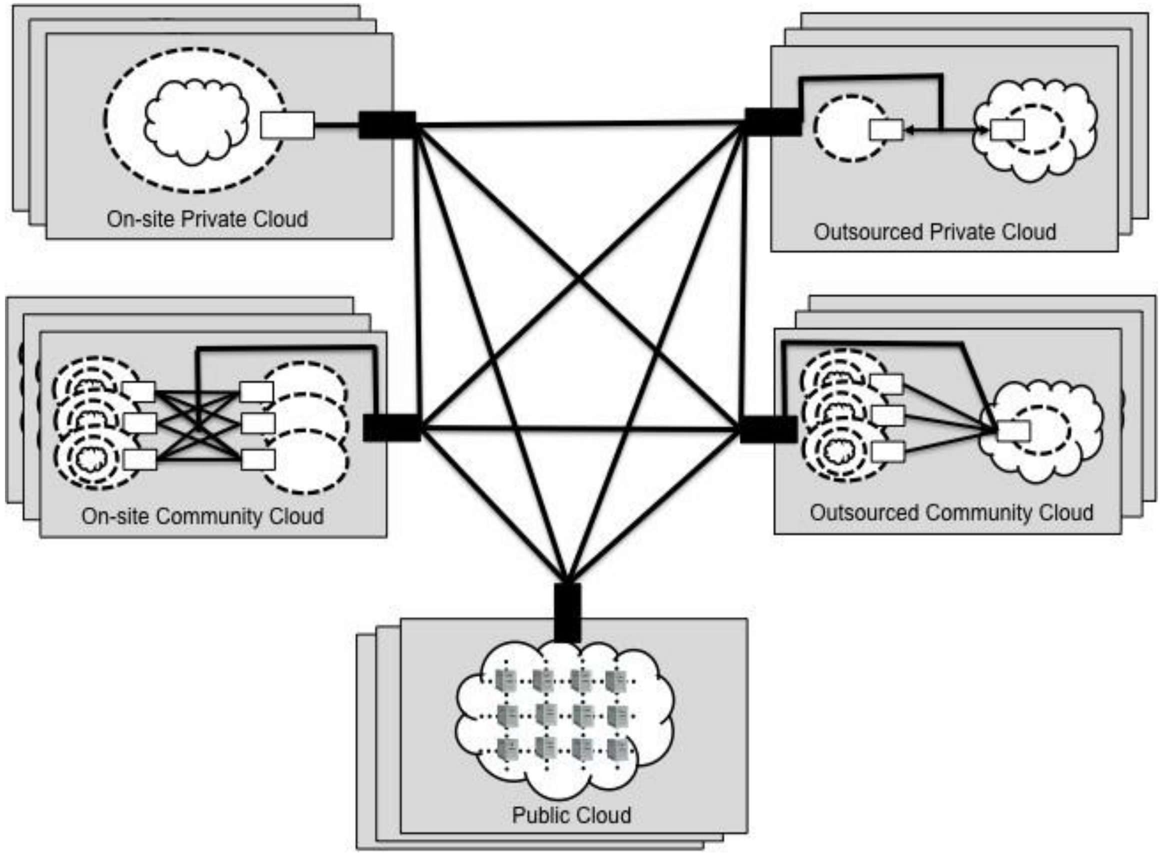
- This figure shows an outsourced community cloud, where the server side is outsourced to a hosting company.
- In this case, an outsourced community cloud builds its infrastructure off premise, and serves a set of organizations that request and consume cloud services.



[Outsourced Community Cloud]

Hybrid cloud

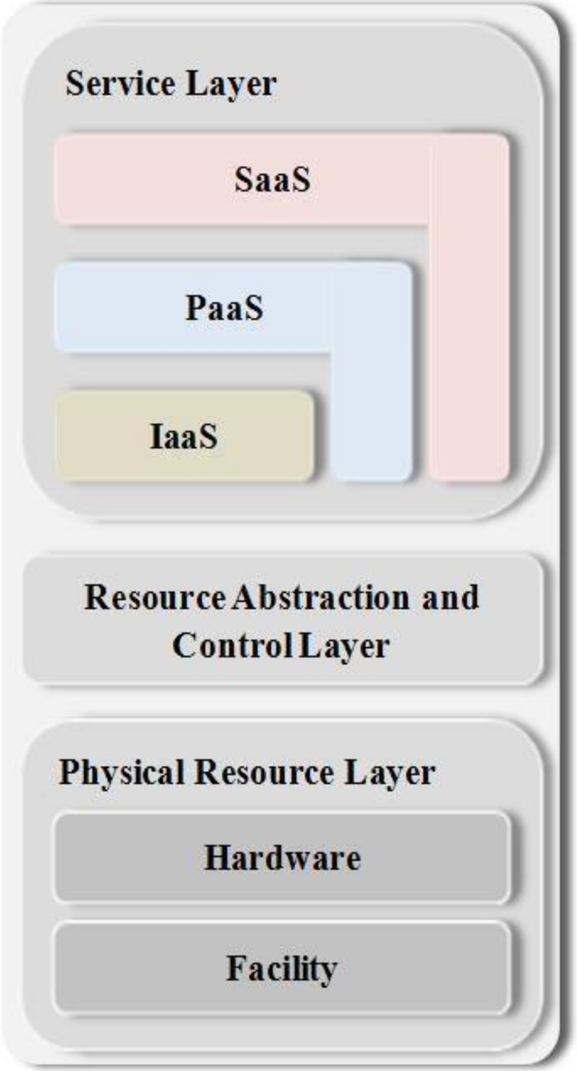
- A hybrid cloud is a composition of two or more clouds (on-site private, on-site community, off-site private, off-site community or public) that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability.
- This figure presents a simple view of a hybrid cloud that could be built with a set of clouds in the five deployment model variants.



[Hybrid Cloud]

Service Orchestration

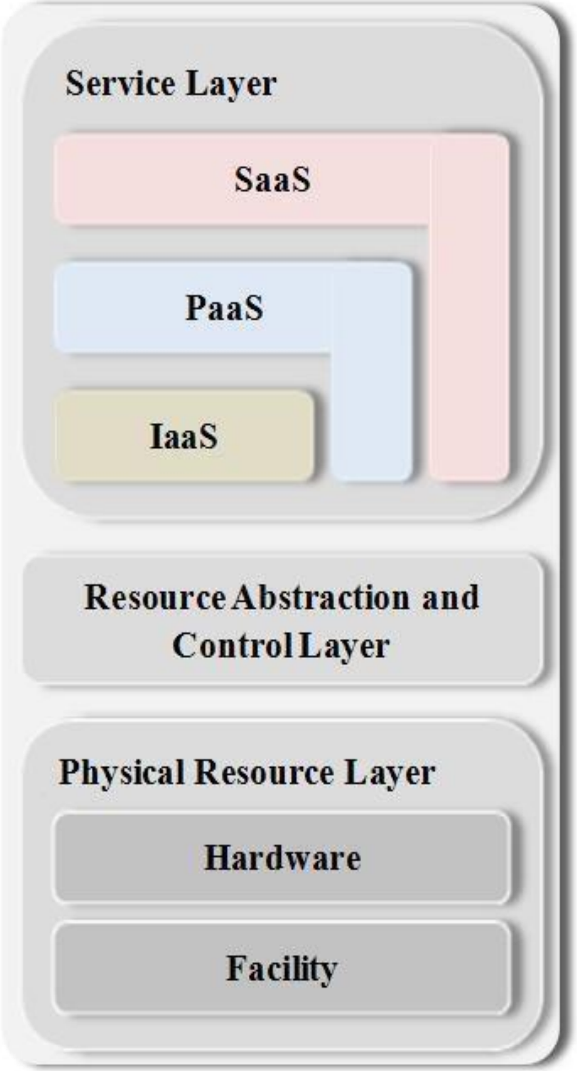
- *Service Orchestration* refers to the composition of system components to support the Cloud Providers activities in arrangement, coordination and management of computing resources in order to provide cloud services to Cloud Consumers.
- This figure shows a generic stack diagram of this composition that underlies the provisioning of cloud services.



[Cloud Provider - Service Orchestration]

Service Orchestration (cont.)

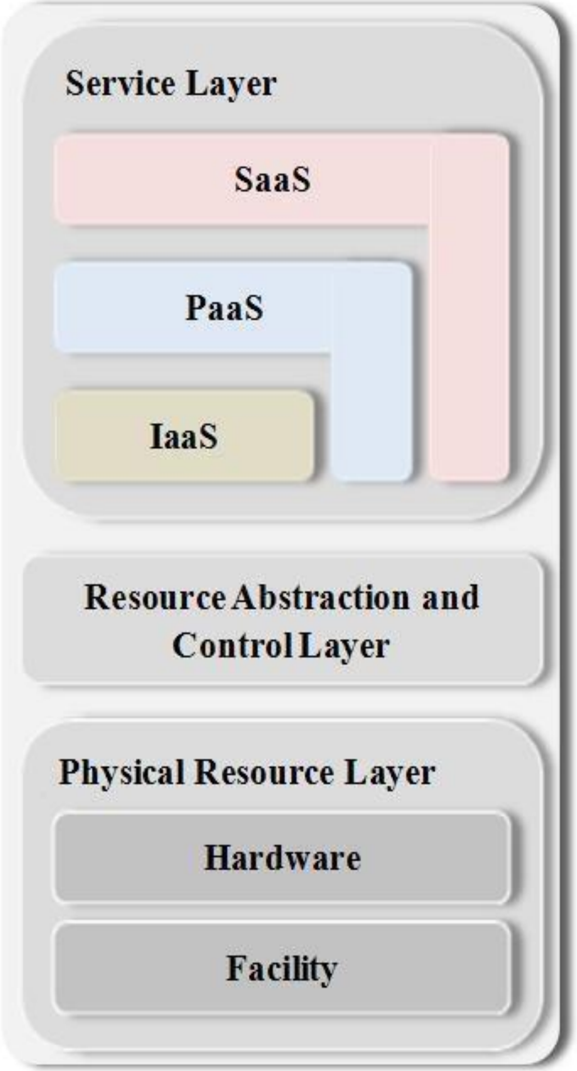
- A three-layered model is used in this representation, representing the grouping of three types of system components Cloud Providers need to compose to deliver their services.
- In the model shown in the figure, the top is the service layer, this is where Cloud Providers define interfaces for Cloud Consumers to access the computing services.



[Cloud Provider - Service Orchestration]

Service Orchestration (cont.)

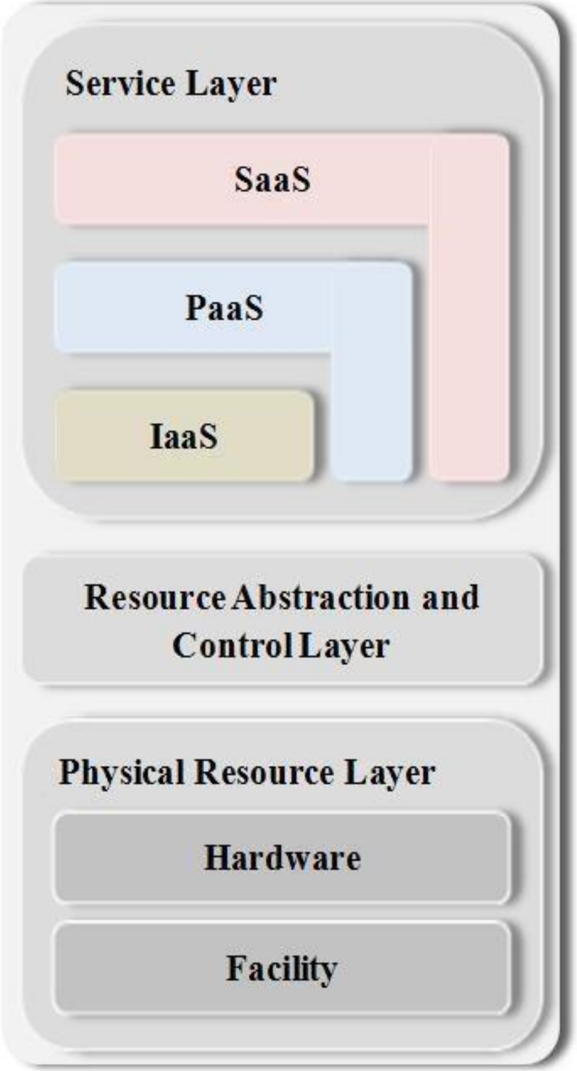
- Access interfaces of each of the three service models are provided in this layer.
- It is possible, though not necessary, that *SaaS* applications can be built on top of *PaaS* components and *PaaS* components can be built on top of *IaaS* components.
- The optional dependency relationships among SaaS, 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.
- For example, a SaaS application can be implemented and hosted on virtual machines from an IaaS cloud or it can be implemented directly on top of cloud resources without using IaaS virtual machines.



[Cloud Provider - Service Orchestration]

Service Orchestration (cont.)

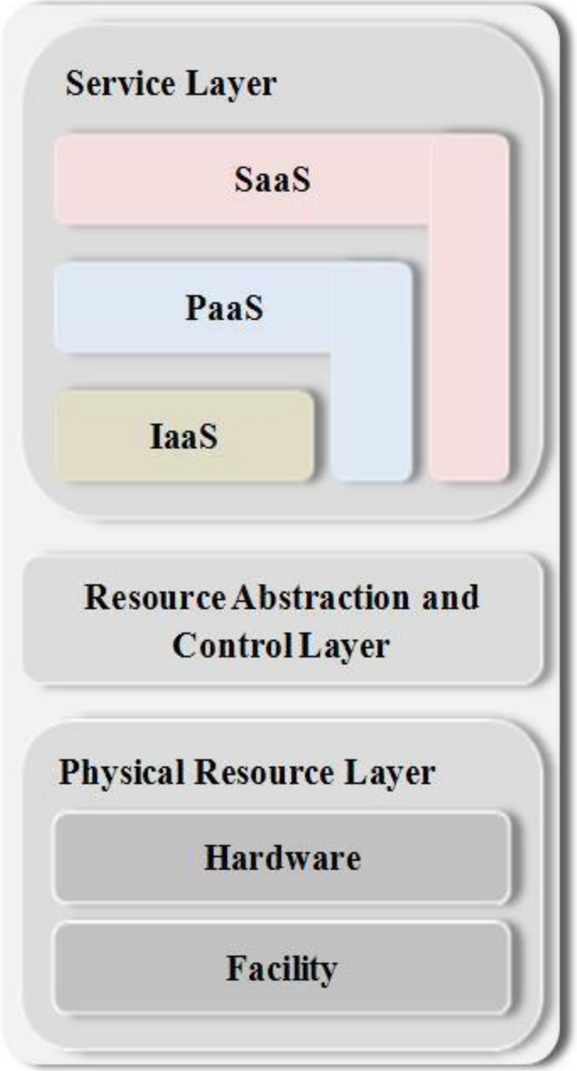
- The middle layer in the model is the resource abstraction and control layer.
- layer contains the system components that Cloud Providers use to provide and manage access to the physical computing resources through software abstraction.
- Examples of resource abstraction components include software elements such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions.



[Cloud Provider - Service Orchestration]

Service Orchestration (cont.)

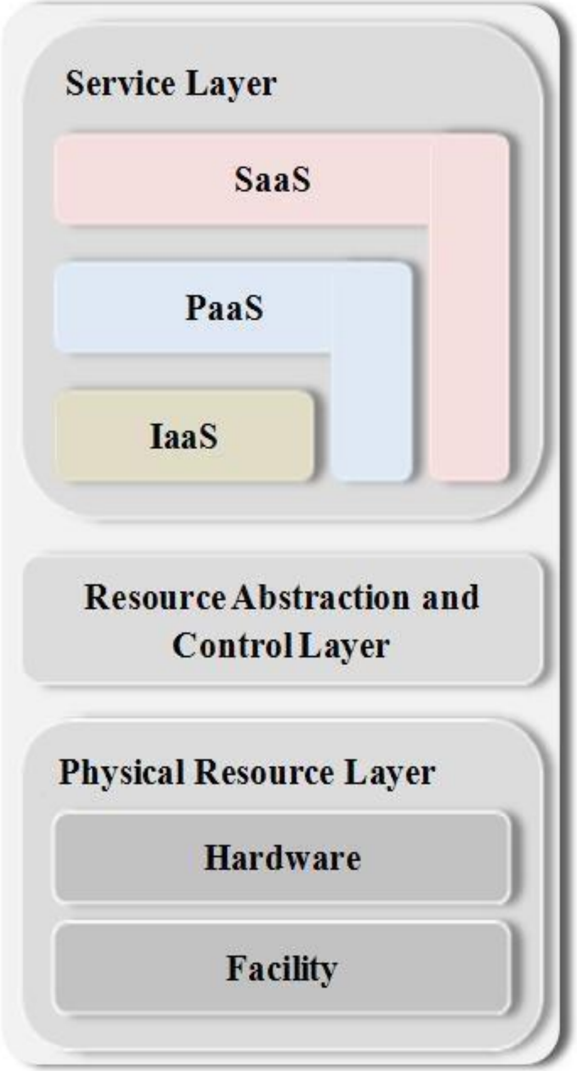
- The resource abstraction needs to ensure efficient, secure, and reliable usage of the underlying physical resources.
- While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are also possible.
- The control aspect of this layer 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.



[Cloud Provider - Service Orchestration]

Service Orchestration (cont.)

- The lowest layer in the stack is the physical resource layer, which includes all the physical computing resources.
- 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.

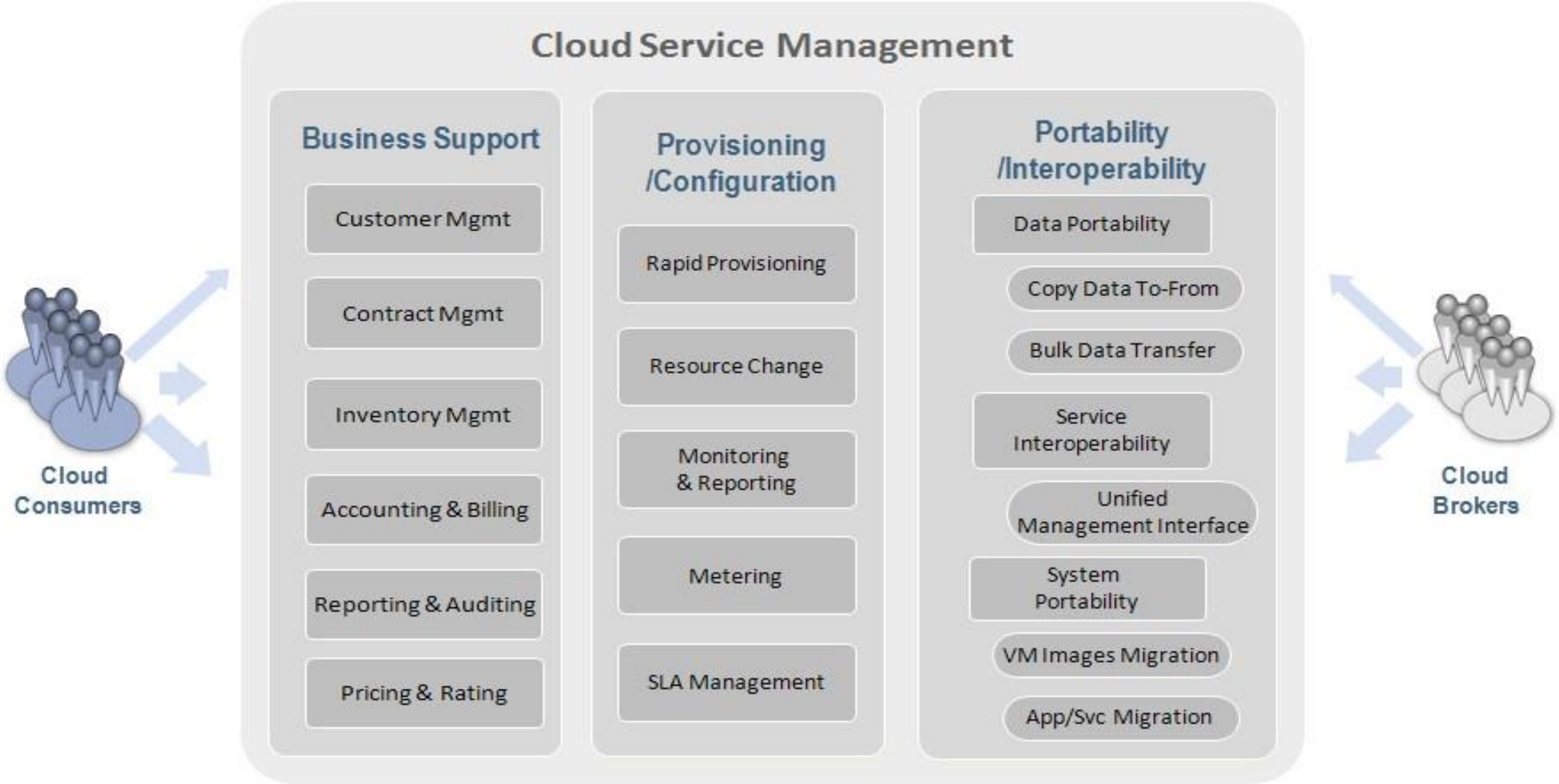


[Cloud Provider - Service Orchestration]

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 the following 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.

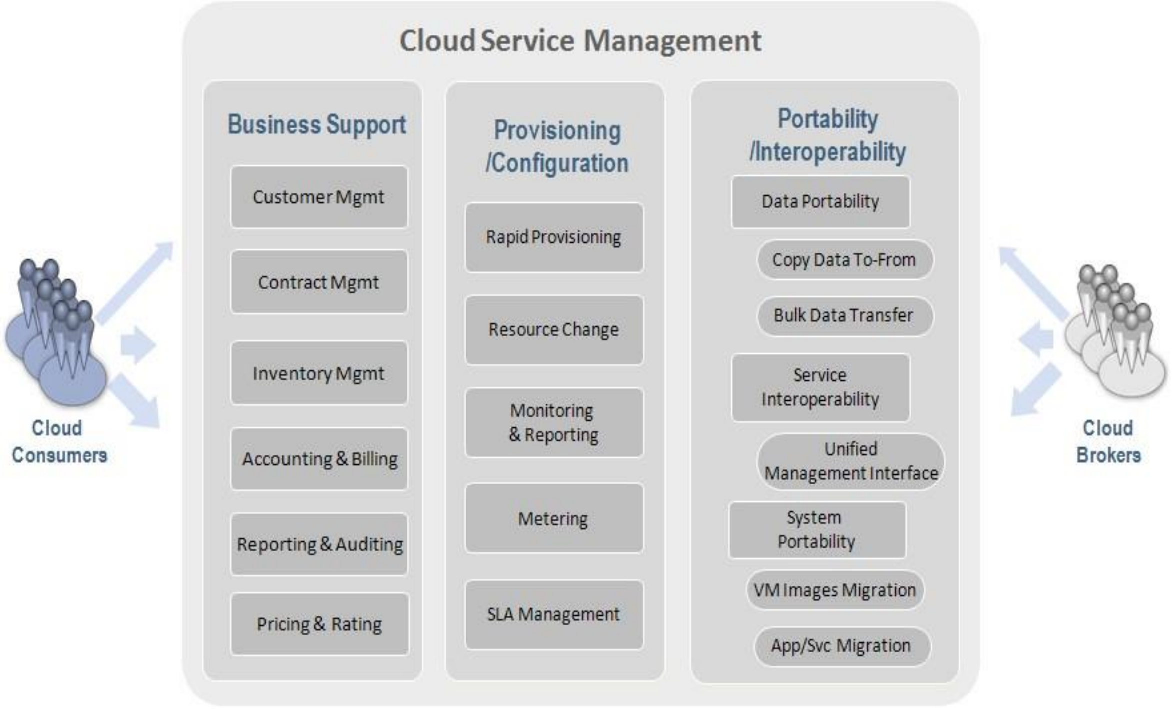
Cloud Service Management (cont.)



[Cloud Provider - Cloud Service Management]

Cloud Service Management : *Business Support*

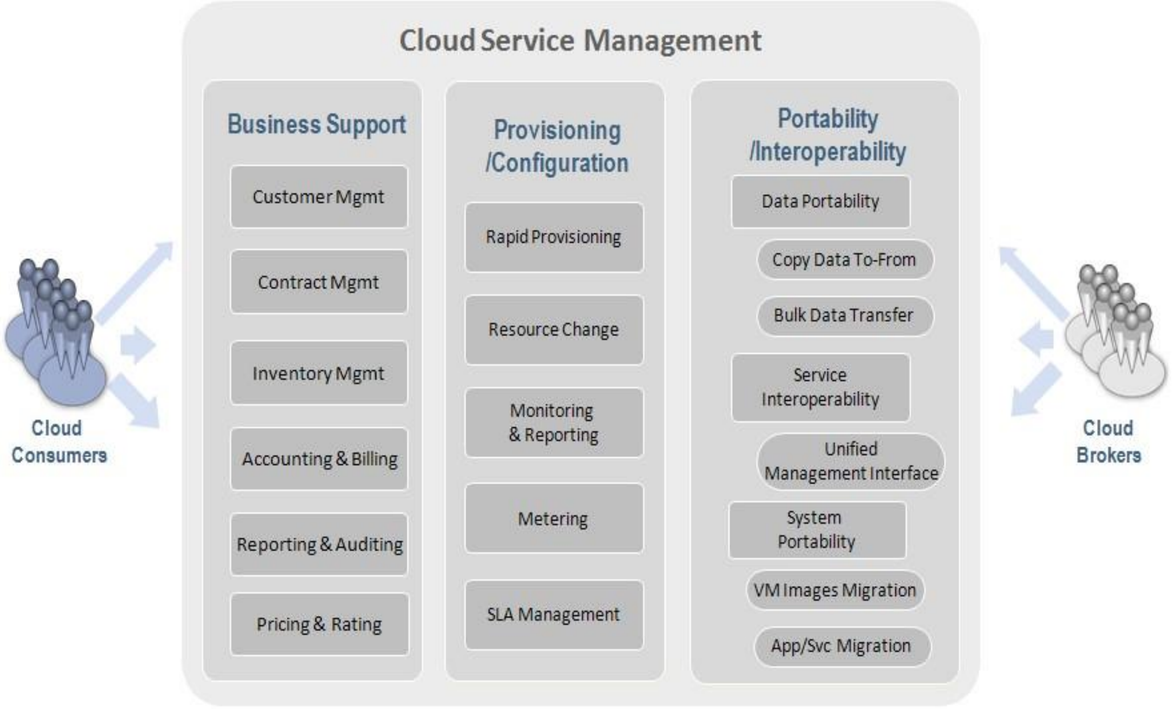
- Business Support entails the set of business-related services dealing with clients and supporting processes.
- It includes the components used to run business operations that are client-facing.



[Cloud Provider - Cloud Service Management]

Cloud Service Management : *Business Support*

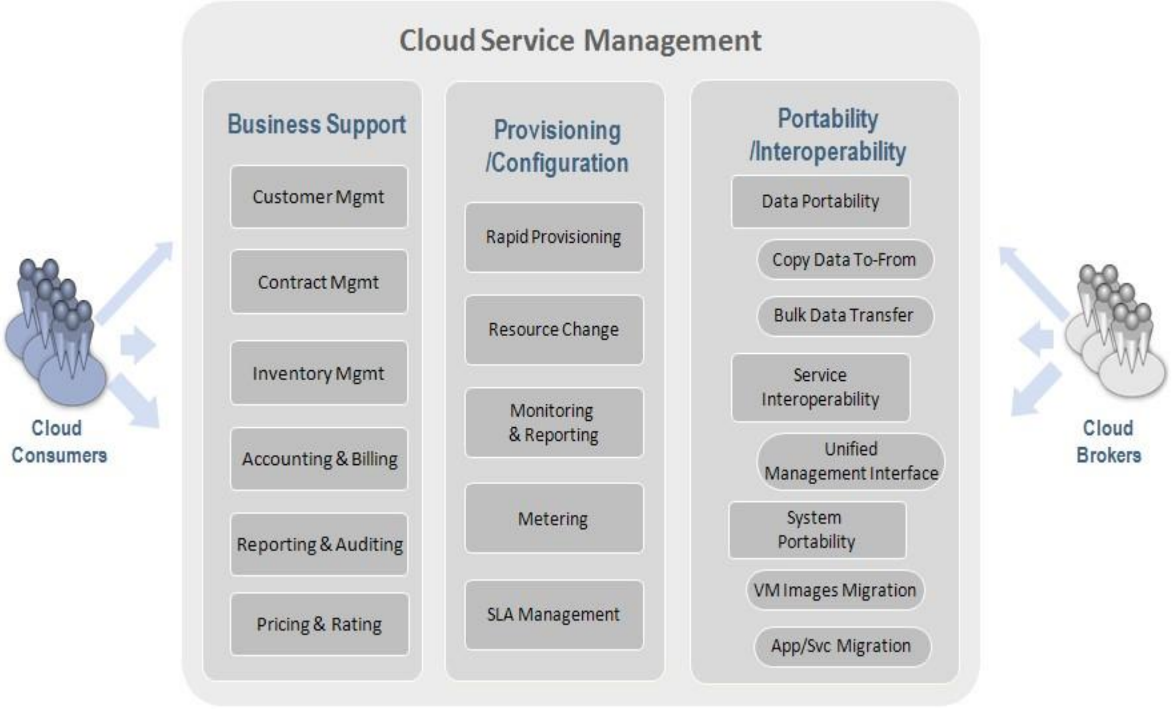
- Customer management:
  - Manage customer accounts,
  - open/close/terminate accounts,
  - manage user profiles,
  - manage customer relationships by providing points-of-contact and resolving customer issues and problems, etc.
- Contract management:
  - Manage service contracts,
  - setup/negotiate/close/terminate contract, etc.



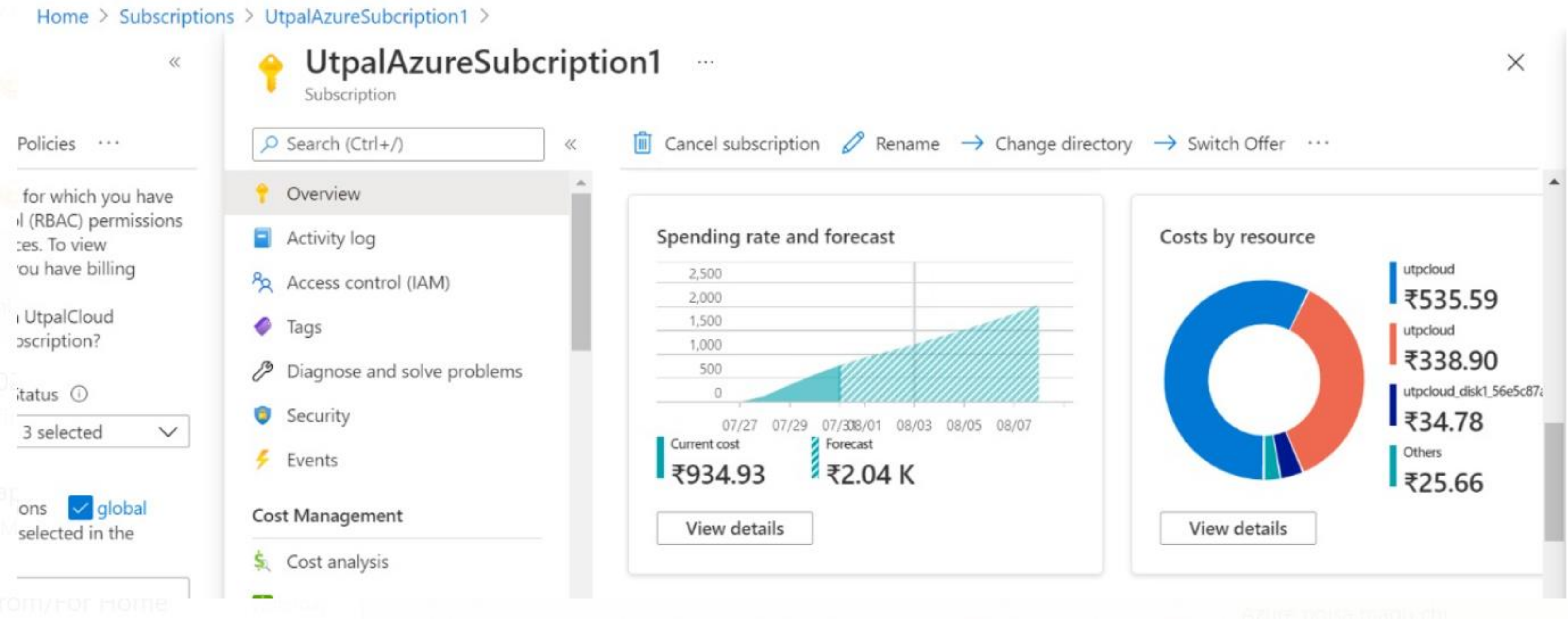
[Cloud Provider - Cloud Service Management]

Cloud Service Management : *Business Support*

- Inventory Management:
  - Set up and manage service catalogs, 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.



[Cloud Provider - Cloud Service Management]



UtpalAzureSubcription1

Subscription

for which you have
l (RBAC) permissions
ces. To view
ou have billing

UtpalCloud
oscription?

itatus

3 selected

ons ☑ global
selected in the

Spending rate and forecast

Current cost ₹934.93

Forecast ₹2.04 K

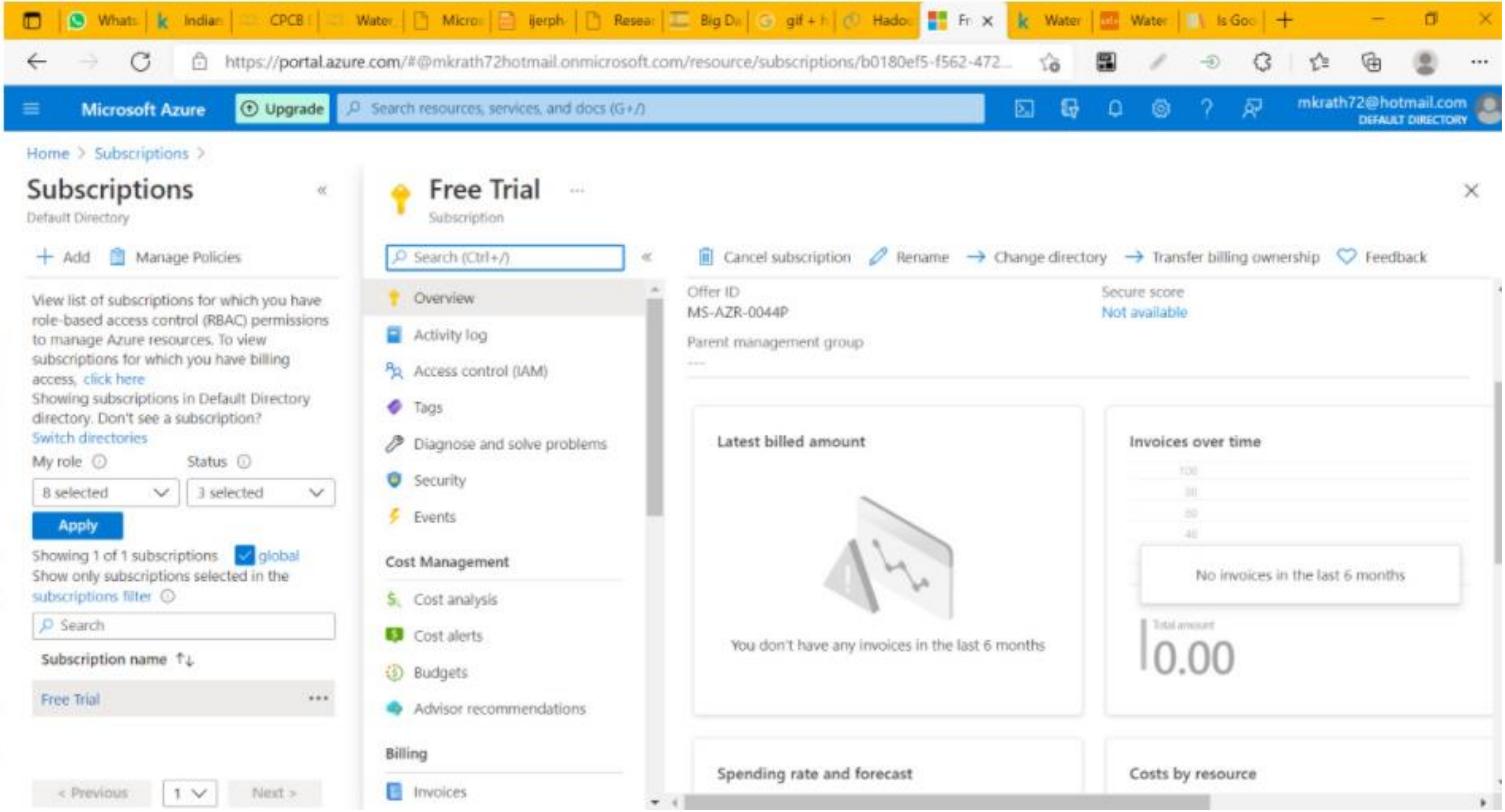
Costs by resource

utpcloud ₹535.59

utpcloud ₹338.90

utpcloud_disk1_56e5c87a ₹34.78

Others ₹25.66



View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here

Showing subscriptions in Default Directory directory. Don't see a subscription? Switch directories

Showing 1 of 1 subscriptions

Show only subscriptions selected in the subscriptions filter

Offer ID: MS-AZR-0044P

Secure score: Not available

Parent management group: ---

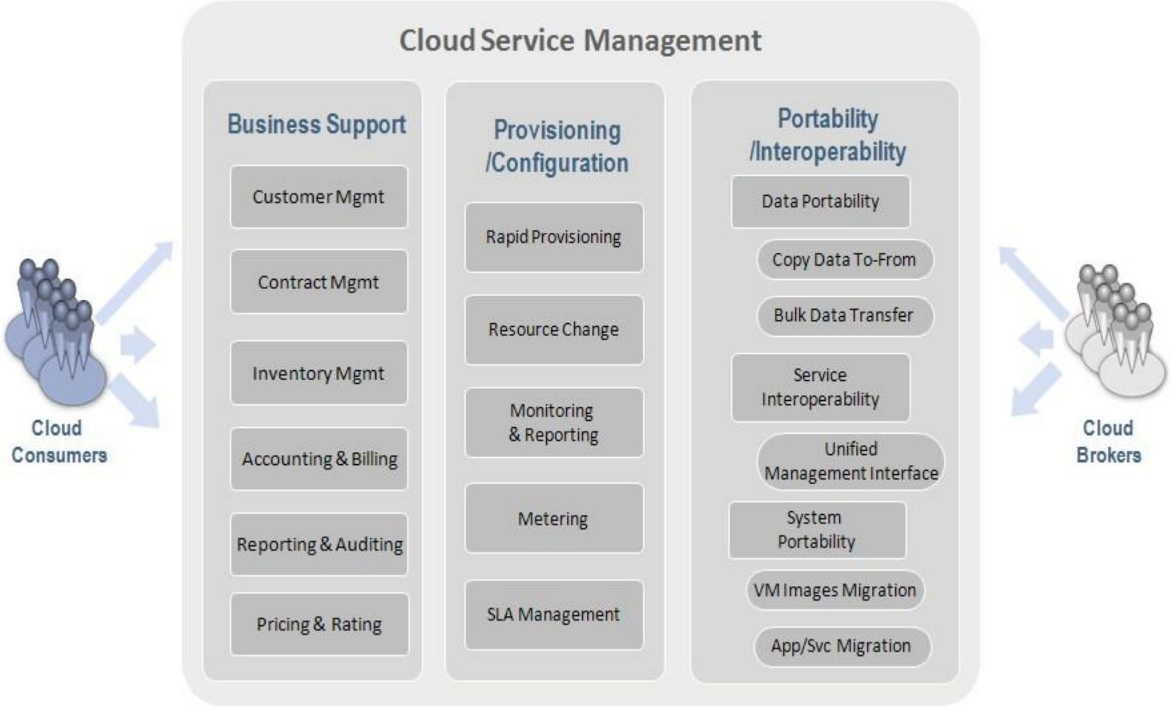
You don't have any invoices in the last 6 months

No invoices in the last 6 months

0.00

Cloud Service Management : *Provisioning and Configuration*

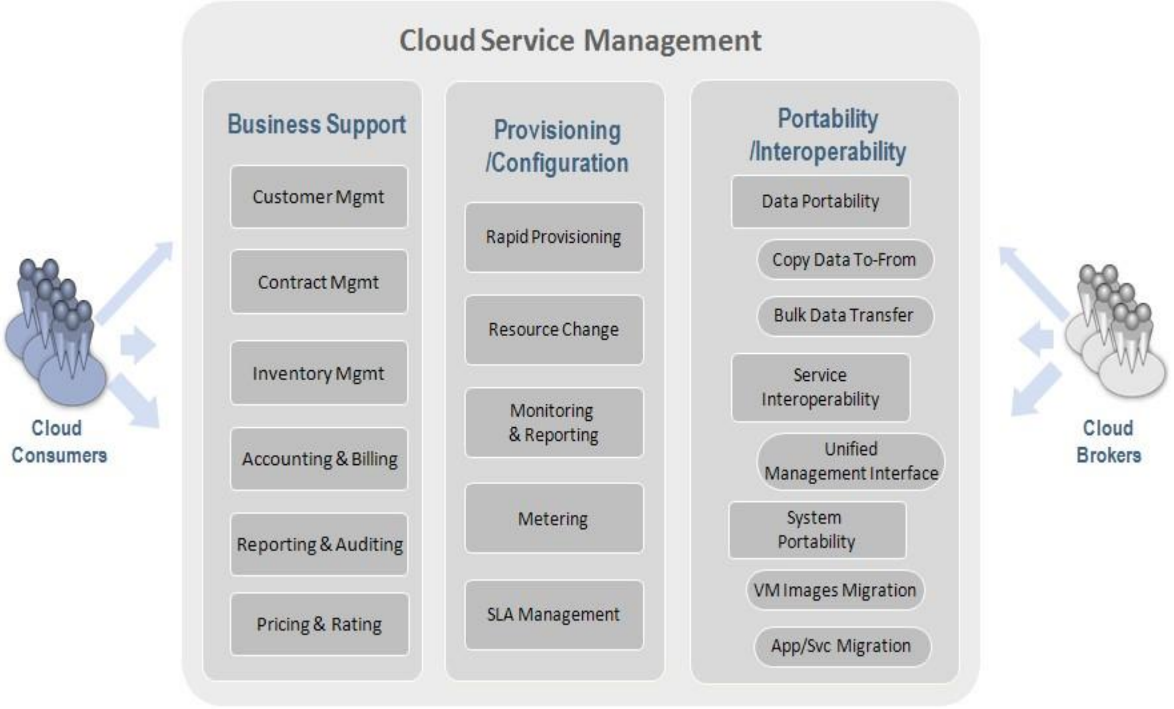
- Rapid provisioning:
  - Automatically deploying cloud systems based on the requested service/resources/capabilities.
- Resource changing:
  - Adjusting configuration/resource assignment for repairs, upgrades and joining new nodes into the cloud.
- Monitoring and Reporting:
  - Discovering and monitoring virtual resources, monitoring cloud operations and events and generating performance reports.



[Cloud Provider - Cloud Service Management]

Cloud Service Management : *Provisioning and Configuration*

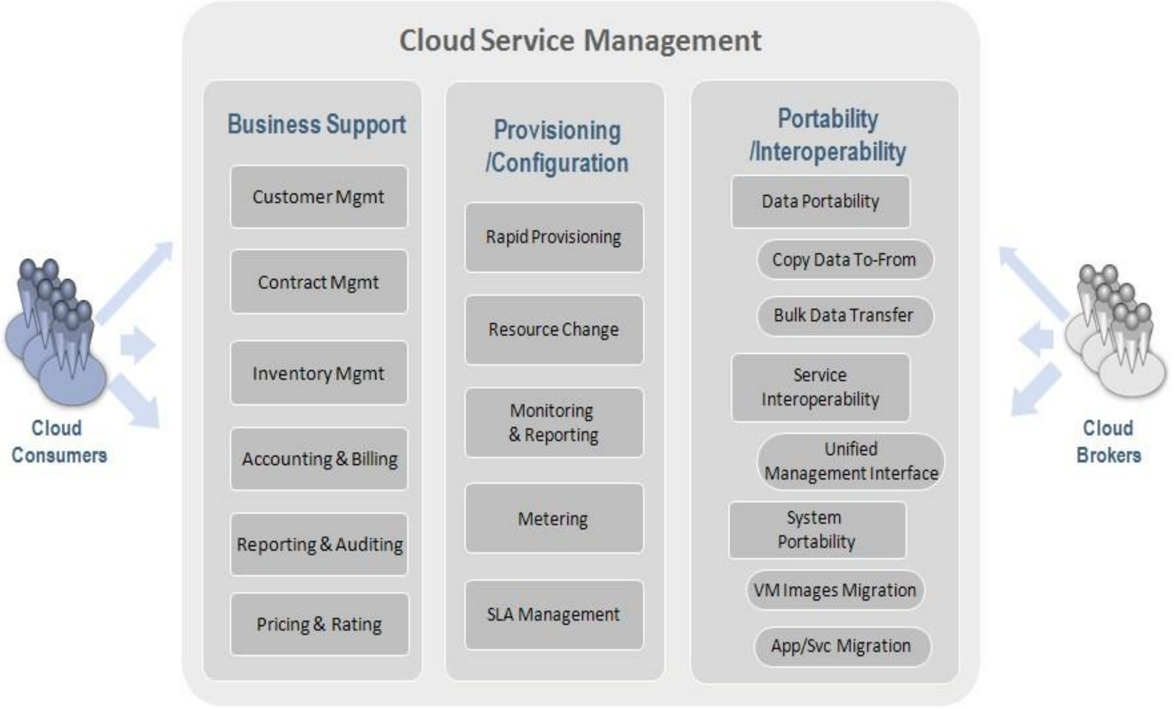
- Metering:
  - Providing a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).
- SLA management:
  - Encompassing the SLA contract definition (basic schema with the QoS parameters),
  - SLA monitoring and SLA enforcement according to defined policies.



[Cloud Provider - Cloud Service Management]

Cloud Service Management : *Portability and Interoperability*

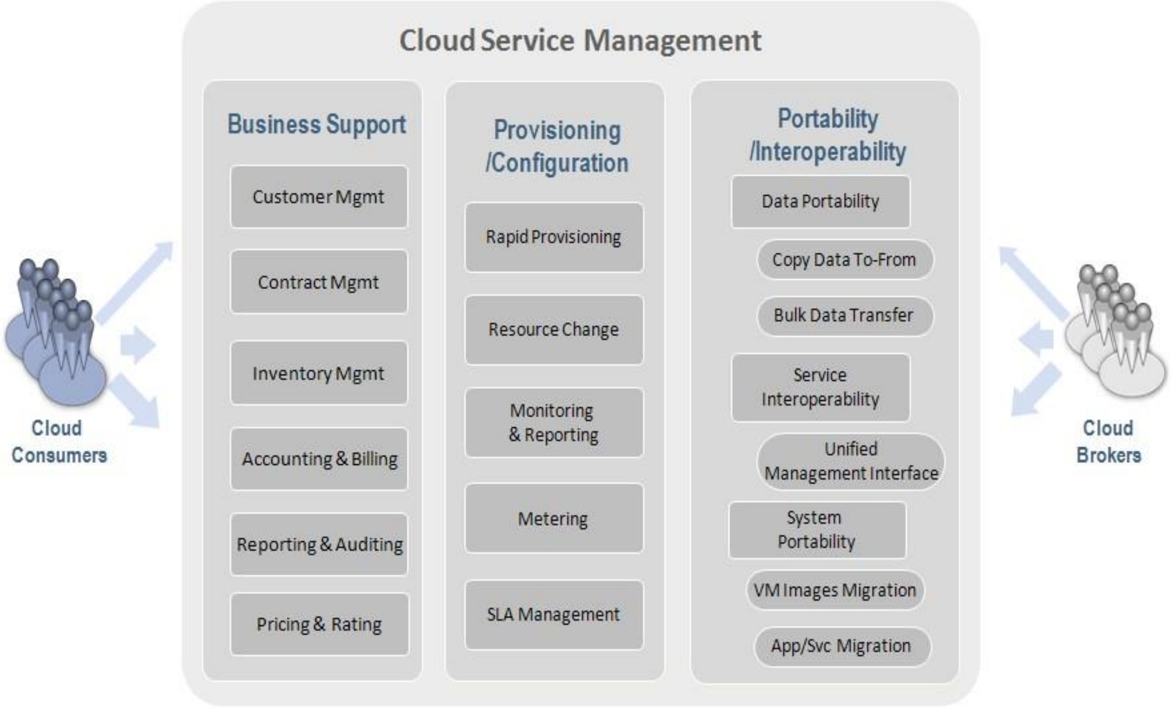
- For portability,
  - prospective customers are interested to know whether they can move their data or applications across multiple cloud environments at low cost and minimal disruption.
- From an interoperability perspective,
  - users are concerned about the capability to communicate between or among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



[Cloud Provider - Cloud Service Management]

Cloud Service Management : *Portability and Interoperability*

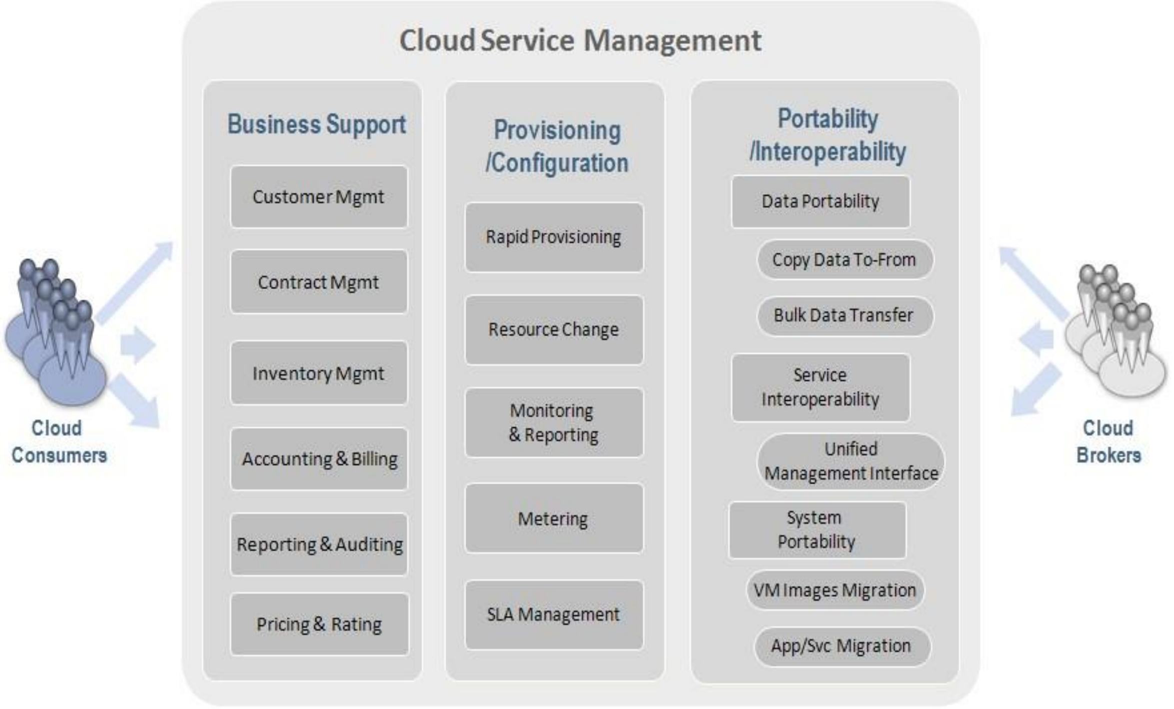
- Cloud providers should provide mechanisms to support
  - data portability,
  - service interoperability,
  - and system portability .
- Data portability is the ability of cloud consumers to copy data objects into or out of a cloud or to use a disk for bulk data transfer.
- Service interoperability is the ability of cloud consumers to use their data and services across multiple cloud providers with a unified management interface.



[Cloud Provider - Cloud Service Management]

Cloud Service Management : *Portability and Interoperability*

- 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..



[Cloud Provider - Cloud Service Management]

Security

- 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

Security : Cloud Service Model Perspectives

- The three service models, i.e. SaaS, PaaS, and IaaS,
  - present consumers with different types of service management operations
  - and expose different entry points into cloud systems,
  - which in turn also create different attacking surfaces for adversaries.
- For Example:
  - SaaS provides users with accessibility of cloud offerings using a network connection, normally over the Internet and through a Web browser. There has been an emphasis on Web browser security in SaaS cloud system security considerations .
  - Cloud Consumers of IaaS are provided with virtual machines (VMs) that are executed on hypervisors on the hosts, therefore, hypervisor security for achieving VM isolation has been studied extensively for IaaS Cloud Providers that use virtualization technologies.

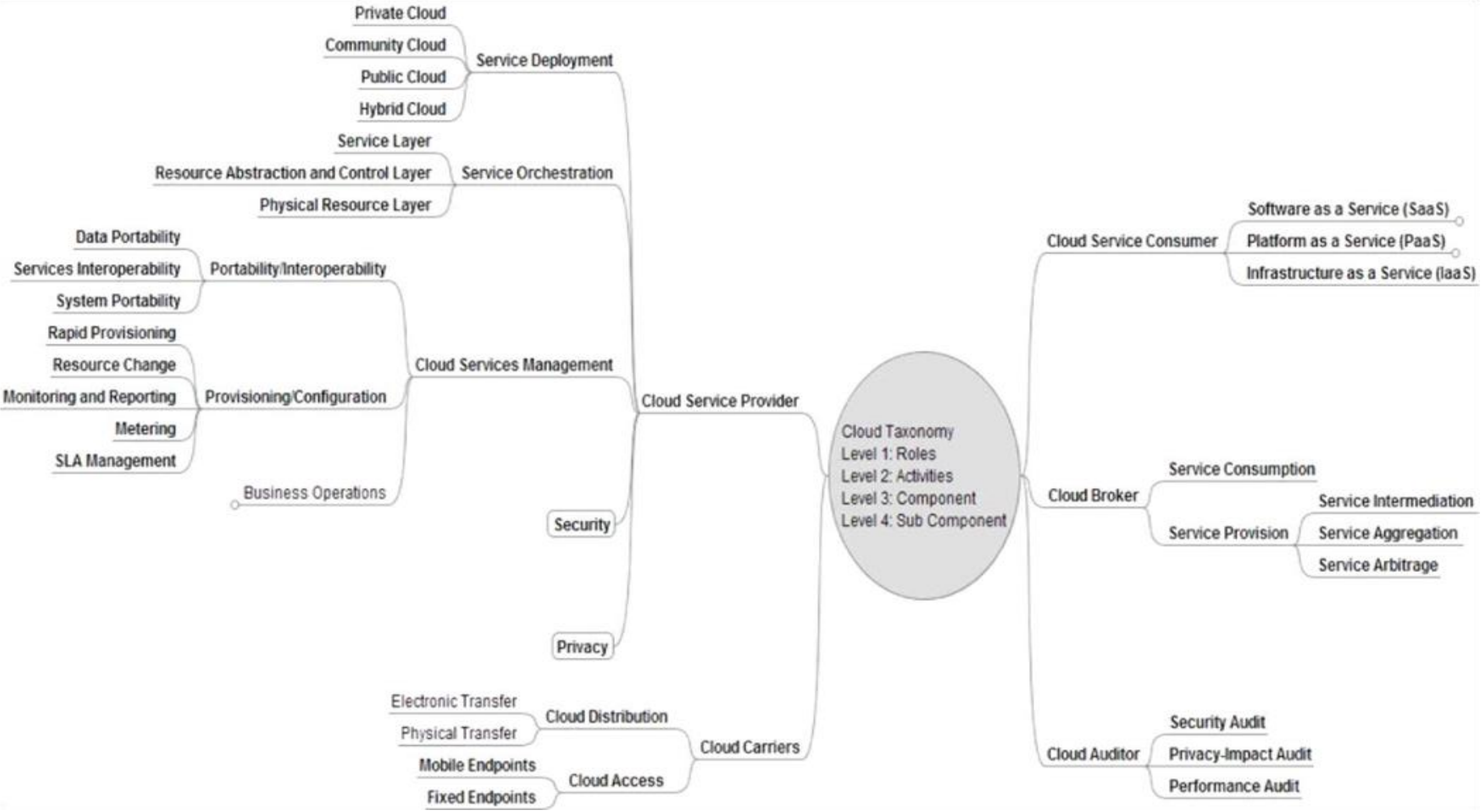
Security : Implications of Cloud Deployment Models

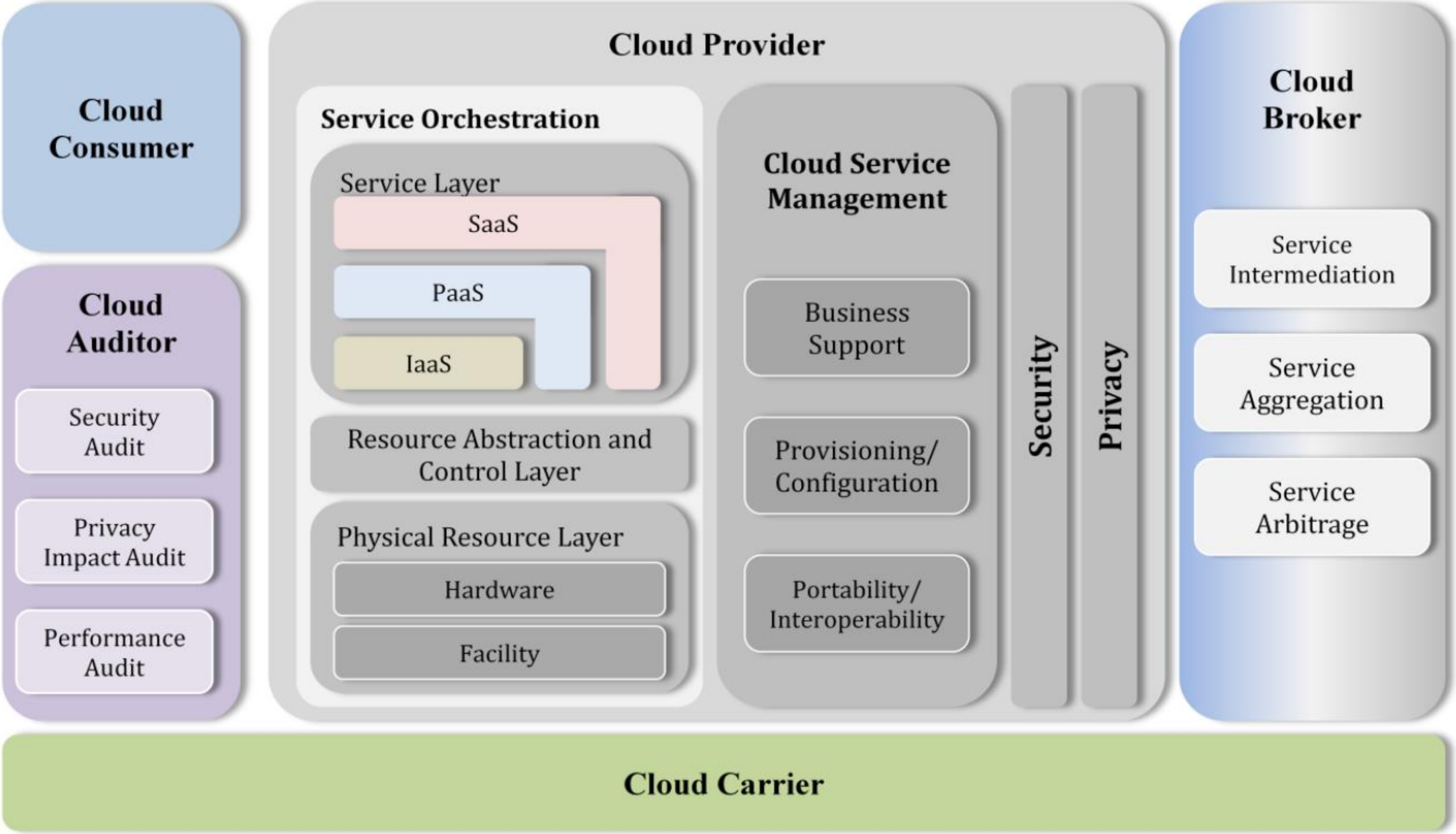
- A private cloud is dedicated to one consumer organization, where as a public cloud could have unpredictable tenants co-existing with each other, therefore, workload isolation is less of a security concern in a private cloud than in a public cloud.

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.

Cloud Taxonomy :




Cloud Consumer
Cloud Auditor
Security Audit
Privacy Impact Audit
Performance Audit
Cloud Provider
Service Orchestration
Service Layer
SaaS
PaaS
IaaS
Resource Abstraction and Control Layer
Physical Resource Layer
Hardware
Facility
Cloud Service Management
Business Support
Provisioning/ Configuration
Portability/ Interoperability
Security
Privacy
Cloud Broker
Service Intermediation
Service Aggregation
Service Arbitrage
Cloud Carrier