Unit 4:
Cloud Computing Reference Architectures

National Institute of Standards and Technology (NIST)

- The National Institute of Standards and Technology (NIST) is a **physical sciences laboratory** of the United States Department of Commerce.

- Its primary purpose is to **develop and promote standards, and technology to enhance productivity, and facilitate trade** by conducting research and development in areas such as cybersecurity, information technology, manufacturing, biotechnology, and nanotechnology.

- NIST also **provides technical services** to industry, government, academia, and other stakeholders to help them comply with regulations, meet their quality and performance objectives, and improve their products and services.

NIST Cloud Computing Program

- The NIST cloud computing program **includes a set of guidelines, standards, and reference architectures** that organizations can use to evaluate cloud computing providers, select appropriate cloud deployment models, and ensure compliance with regulatory requirements.

Objectives of NIST Cloud Computing Program

- Some of the specific objectives of the NIST cloud computing program include:
  - Developing a **common understanding of cloud computing concepts and terminology.**
  - Identifying the **key characteristics, deployment models, and service models** of cloud computing.
  - Providing guidance on **how to assess the security and privacy risks** of cloud computing.
  - Developing **technical standards and reference architectures** for cloud computing.
  - Promoting **interoperability, portability, and data exchange** between cloud services.
  - Ensuring **compliance with regulatory requirements** and best practices for cloud computing.

Key Components of NIST Cloud Computing Program

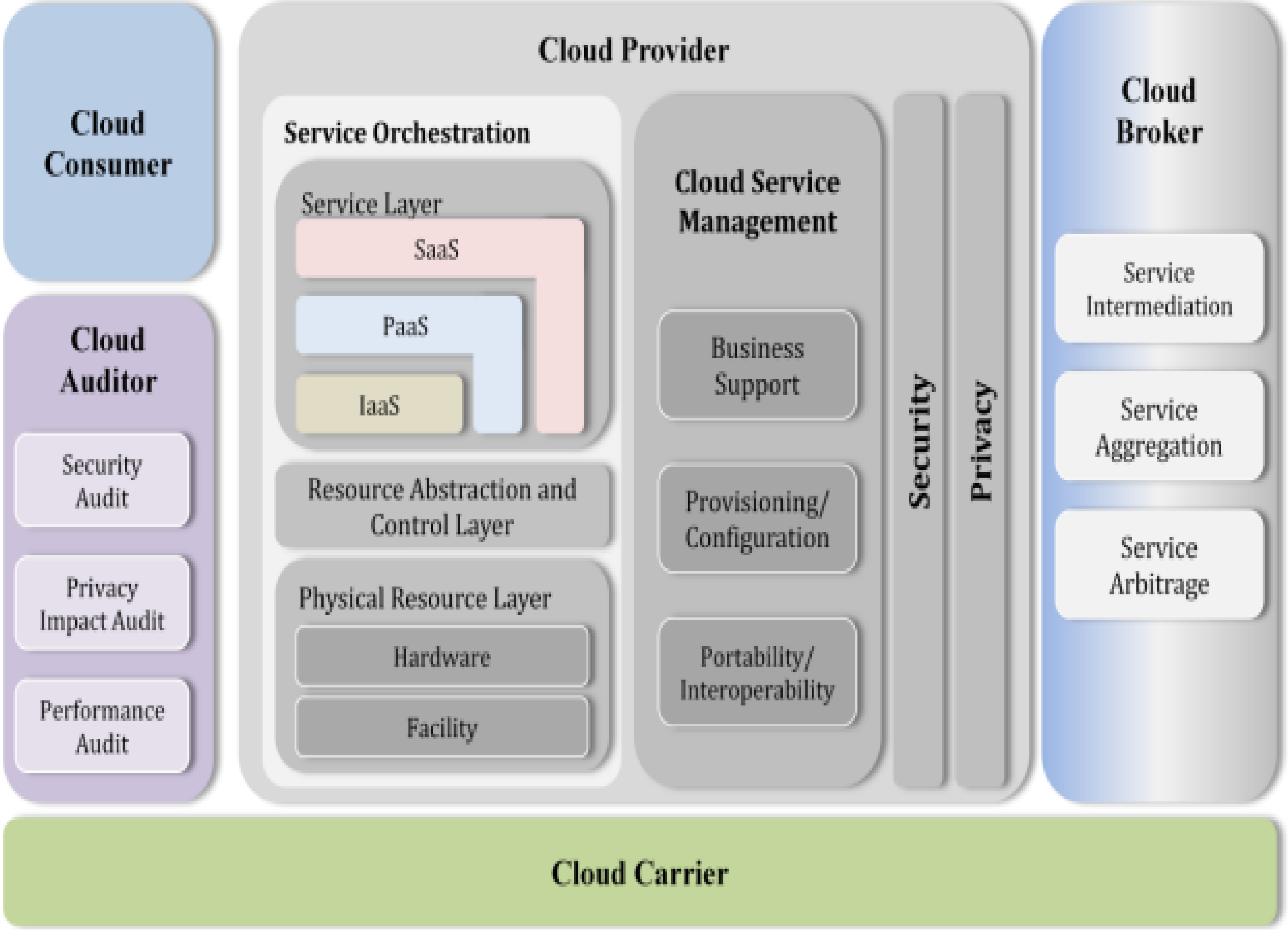
- **Cloud Computing Reference Architecture**: A conceptual model that defines the major components, their activities, and interactions among them.
- **Cloud Computing Taxonomy**: A classification system that defines different types of cloud services, deployment models, and delivery models.
- **Cloud Computing Standards**: A set of technical standards that define the interfaces, protocols, and formats used in cloud computing environments.
- **Cloud Computing Security**: A set of guidelines and best practices for securing cloud computing services and data.

NIST Cloud Computing Reference Architecture

- The NIST Cloud Computing Reference Architecture is a conceptual model **that provides a framework for understanding the major components, their activities, interaction between them** and functions of a cloud computing environment.
- It is designed to help organizations **evaluate, design, and implement cloud computing solutions** that meet their specific business needs and requirements.
- The reference architecture defines **five main components** of a cloud computing environment

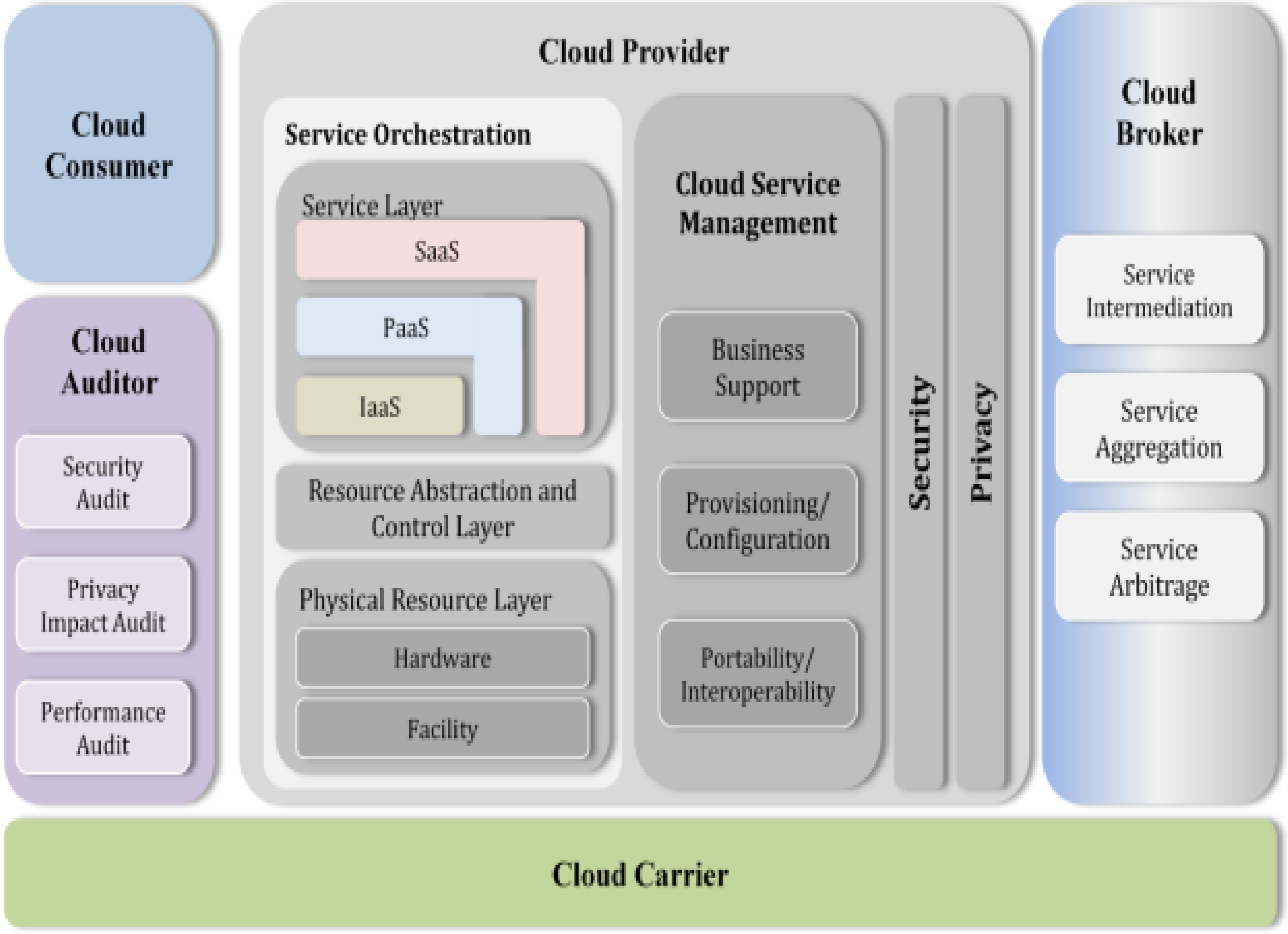
NIST Cloud Computing Reference Architecture

- Cloud Service Provider (CSP)
- Cloud Service Consumer (CSC)
- Cloud Carrier
- Cloud Broker
- Cloud Auditor



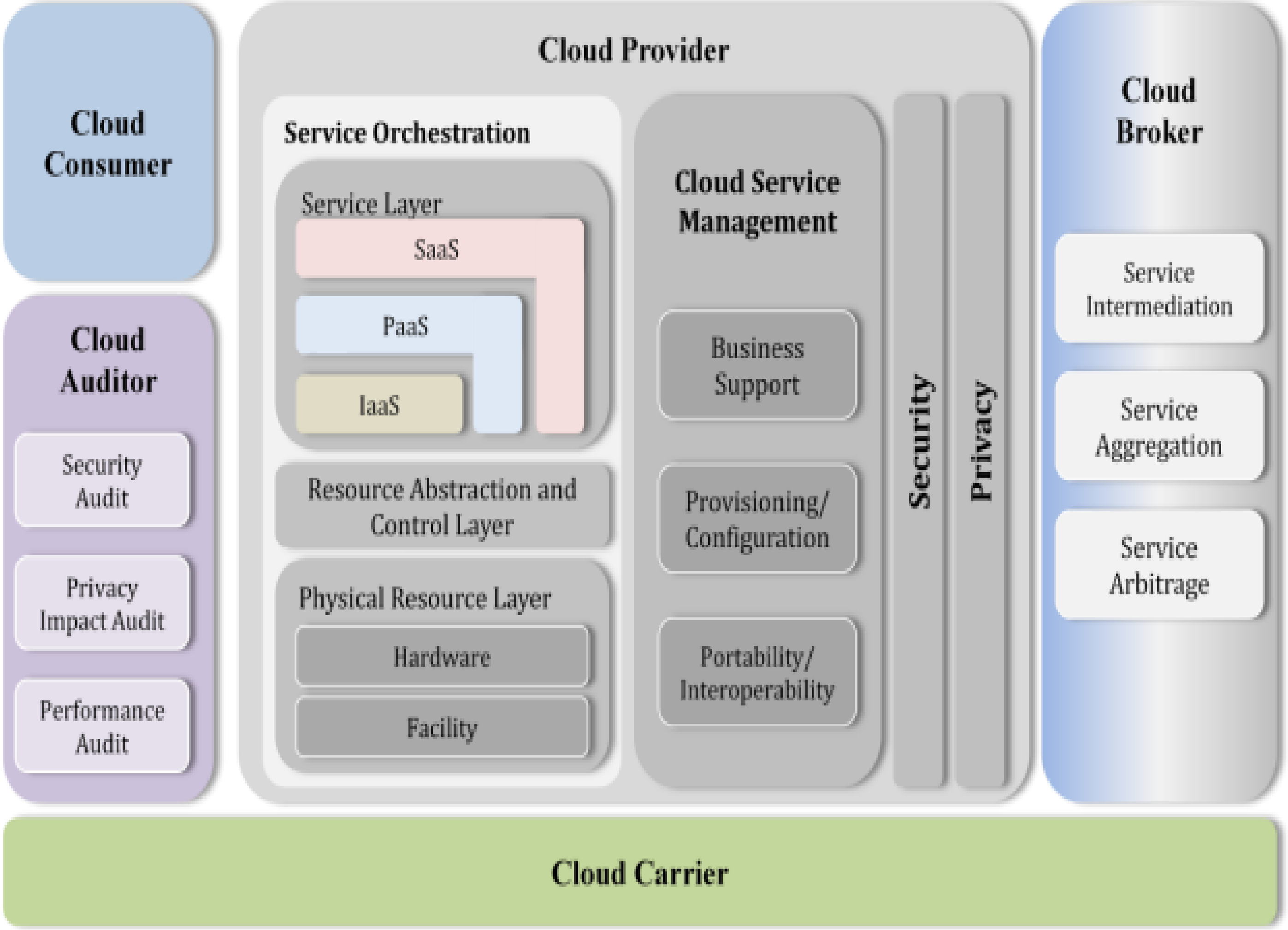
NIST Cloud Computing Reference Architecture

- Cloud Service Provider (CSP): The organization that provides cloud computing services to customers.
- This can include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) providers.



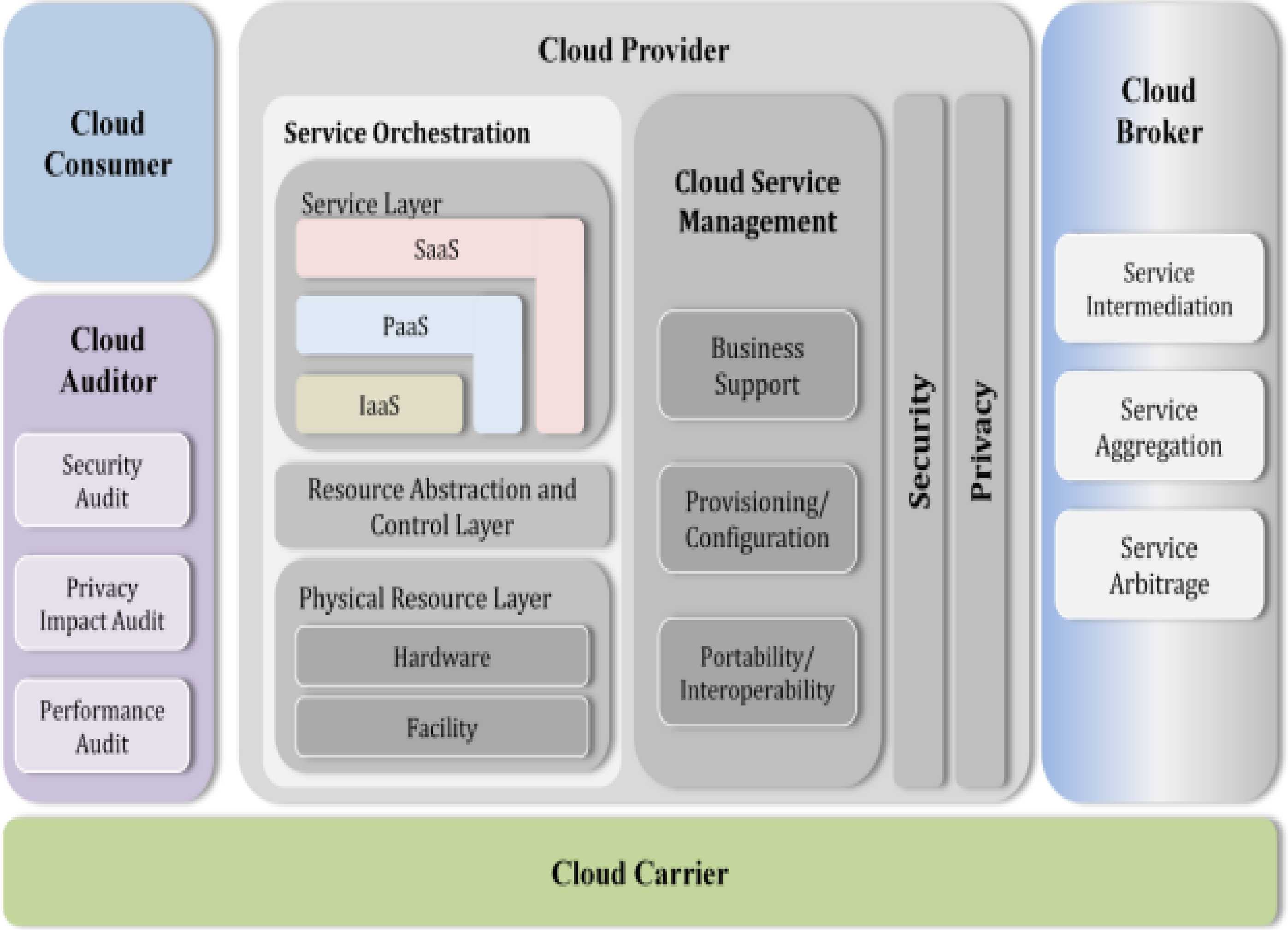
NIST Cloud Computing Reference Architecture

- Cloud Service Consumer (CSC): The organization or individual that consumes cloud computing services from a CSP.



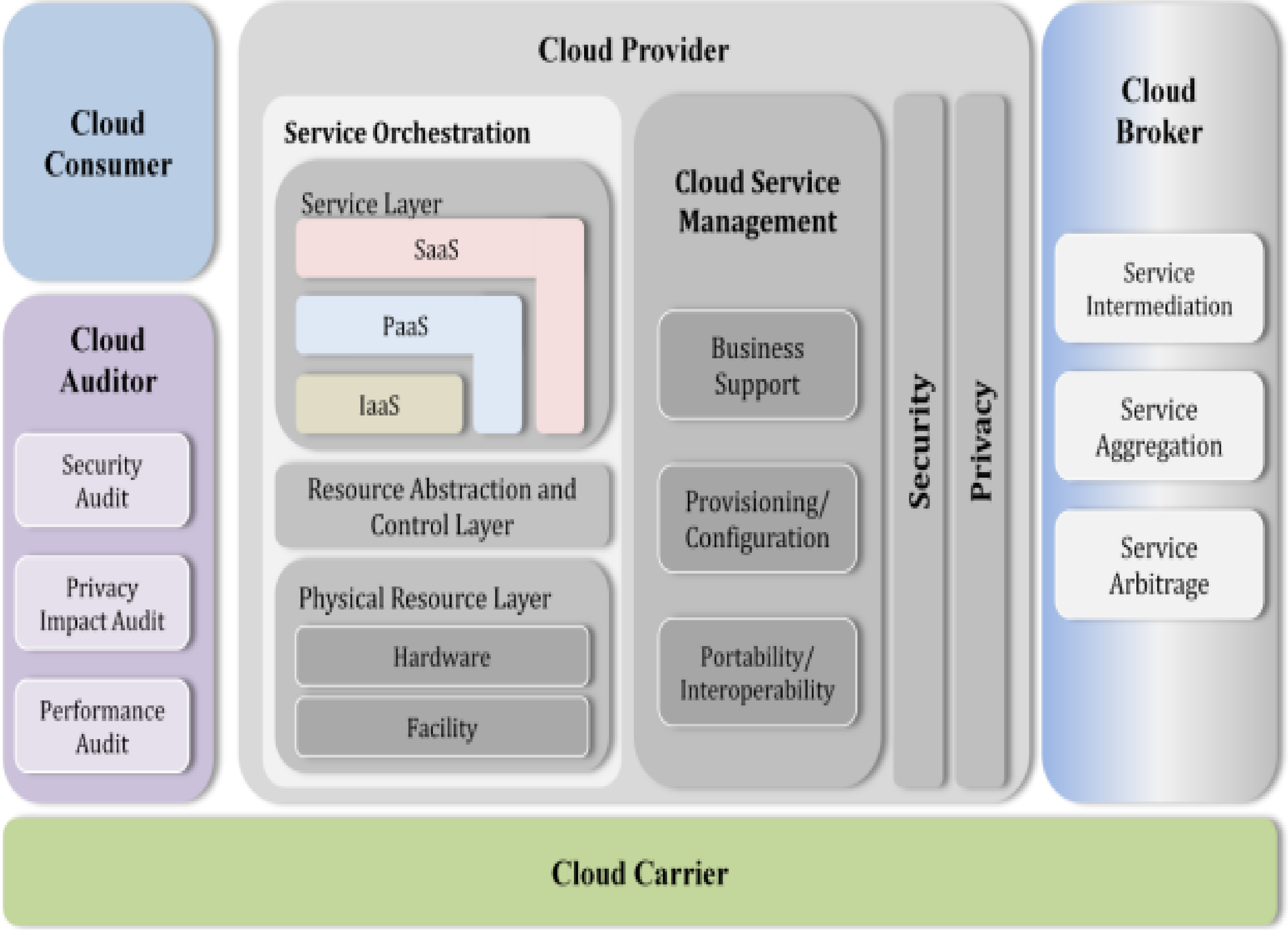
NIST Cloud Computing Reference Architecture

- Cloud Carrier: The intermediary that provides connectivity and transport of cloud services between the CSP and the CSC.



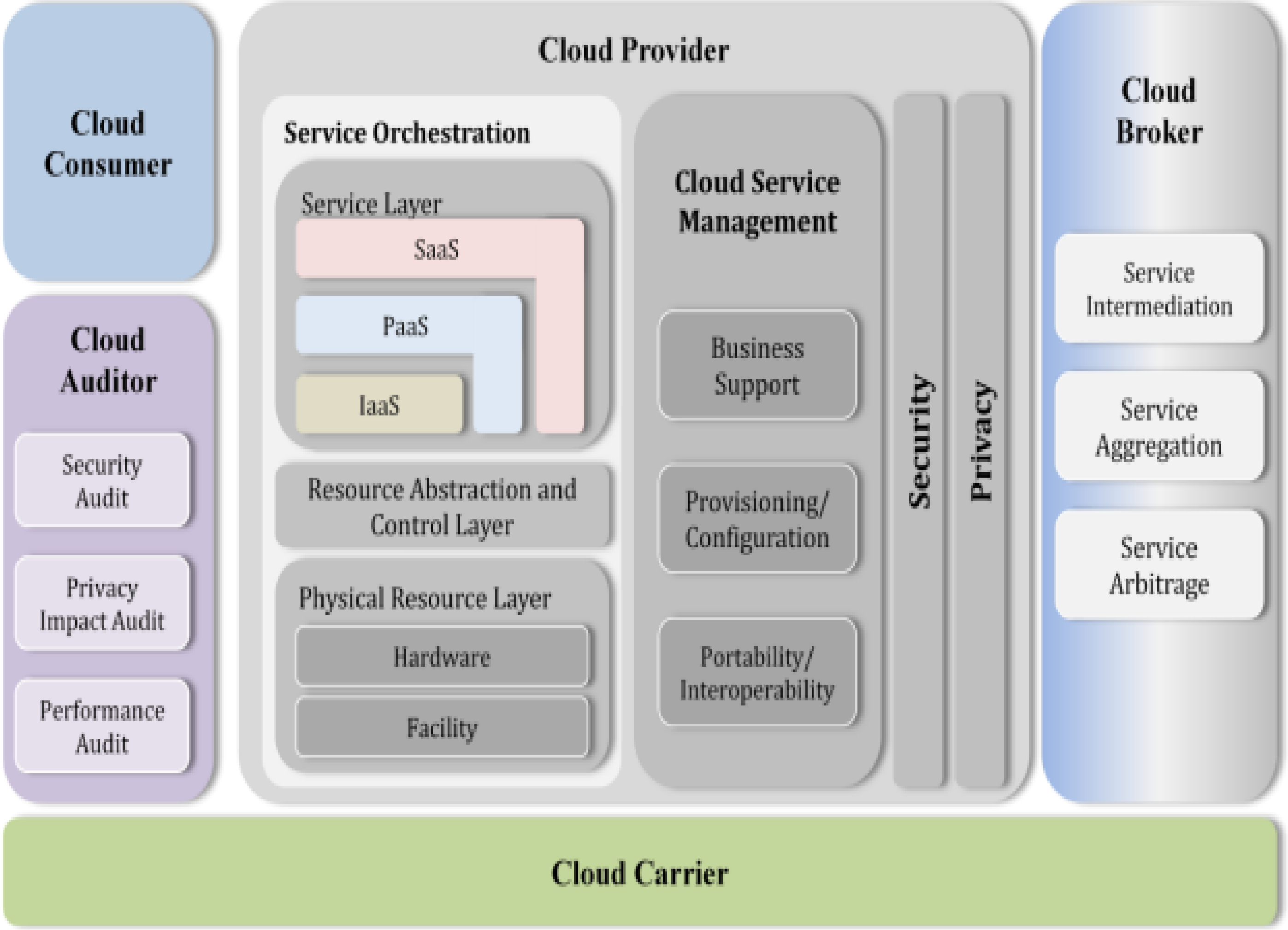
NIST Cloud Computing Reference Architecture

- Cloud Broker: The intermediary that facilitates the negotiation and management of cloud services between the CSP and the CSC.



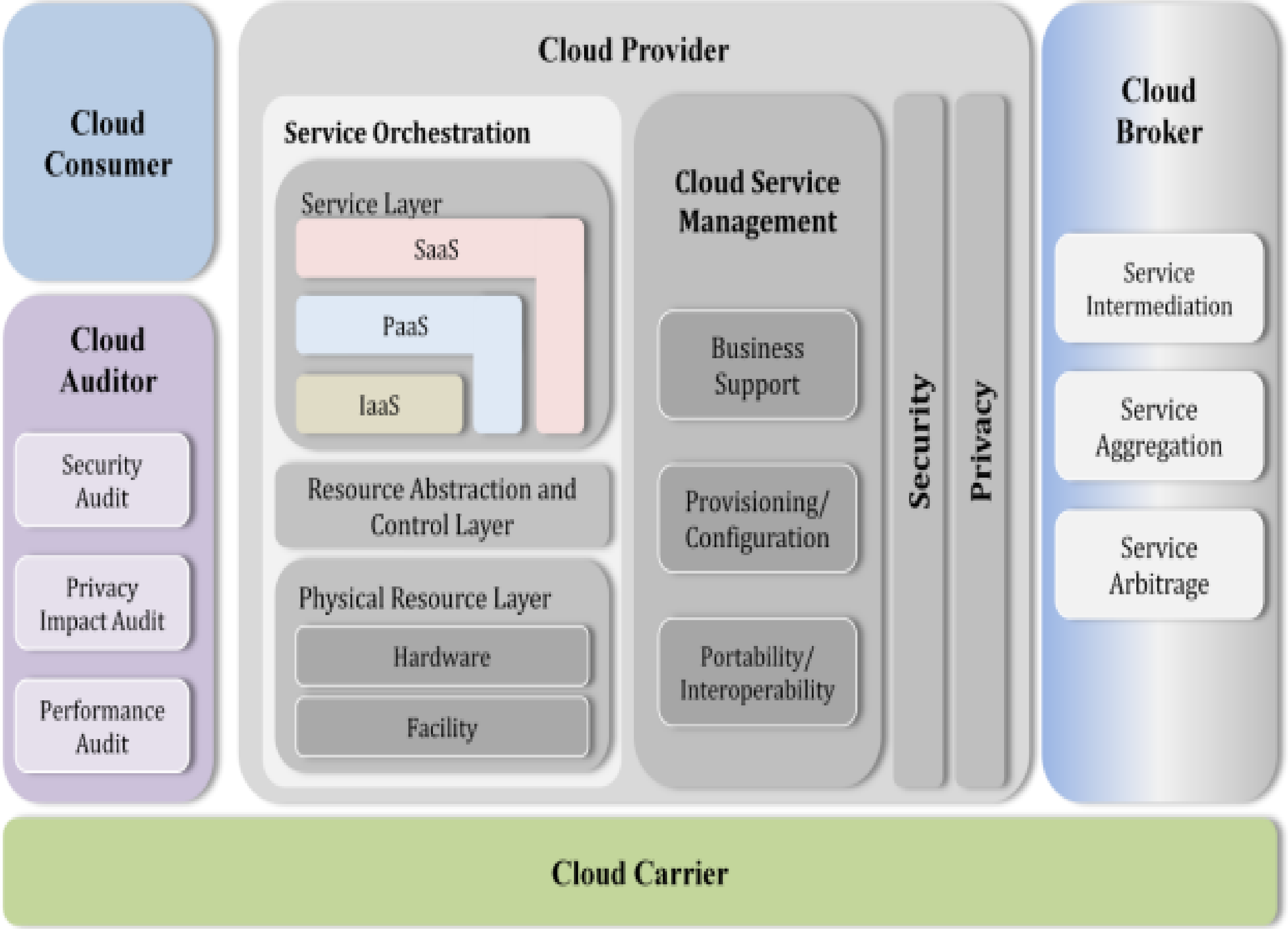
NIST Cloud Computing Reference Architecture

- Cloud Auditor: The entity that performs independent assessments of cloud services to ensure compliance with regulatory requirements and best practices.

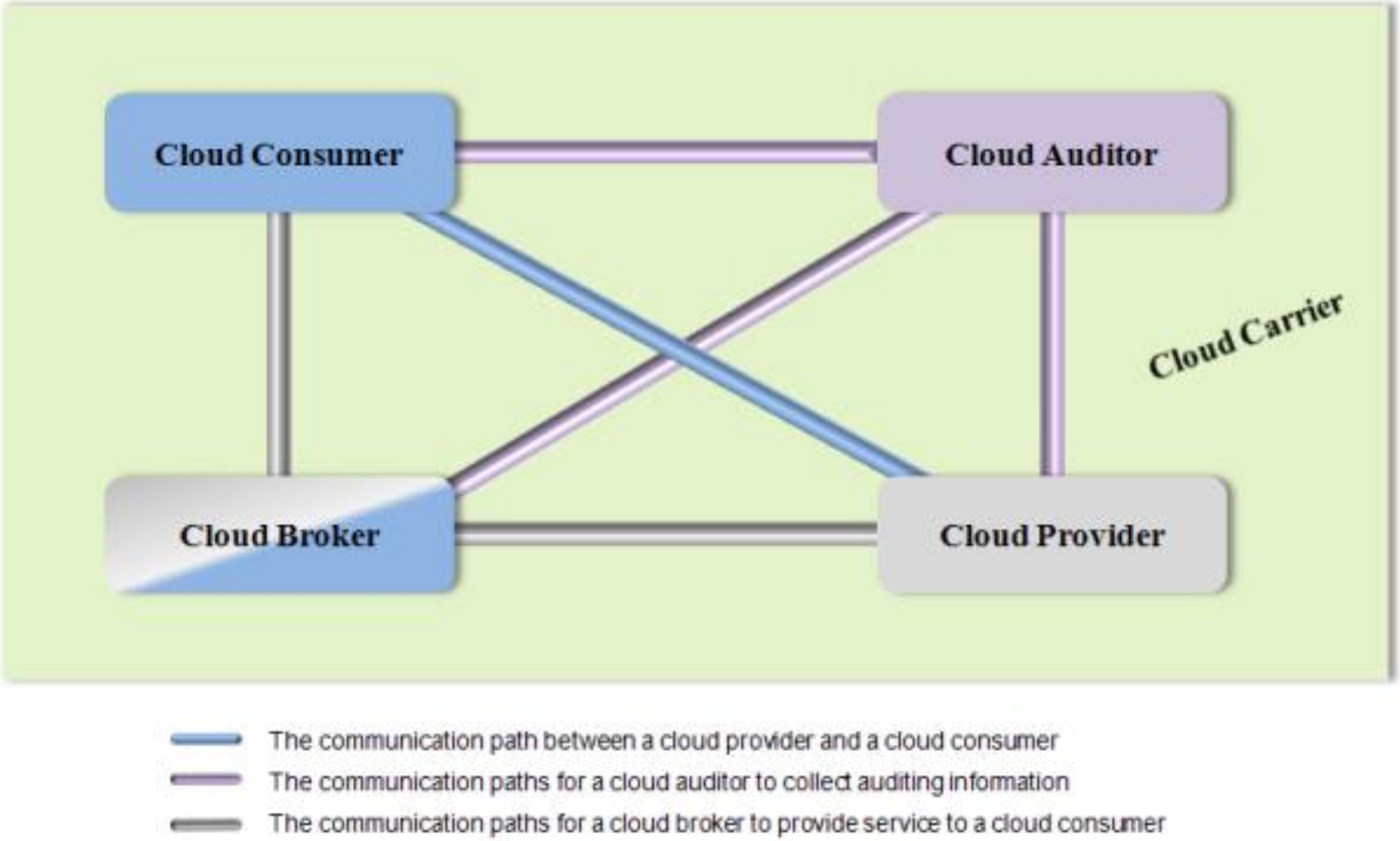


NIST Cloud Computing Reference Architecture

Overall, the NIST Cloud Computing Reference Architecture provides **a comprehensive framework for understanding the major components and functions of a cloud computing environment**, and can help organizations evaluate, design, and implement cloud computing solutions that meet their specific needs and requirements.



Interactions Between the Actors in Cloud Computing



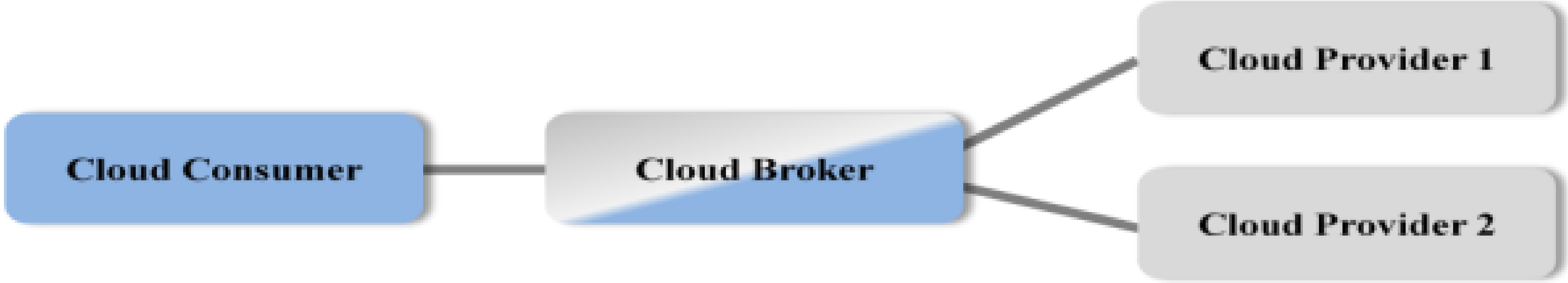
The communication path between a cloud provider and a cloud consumer

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

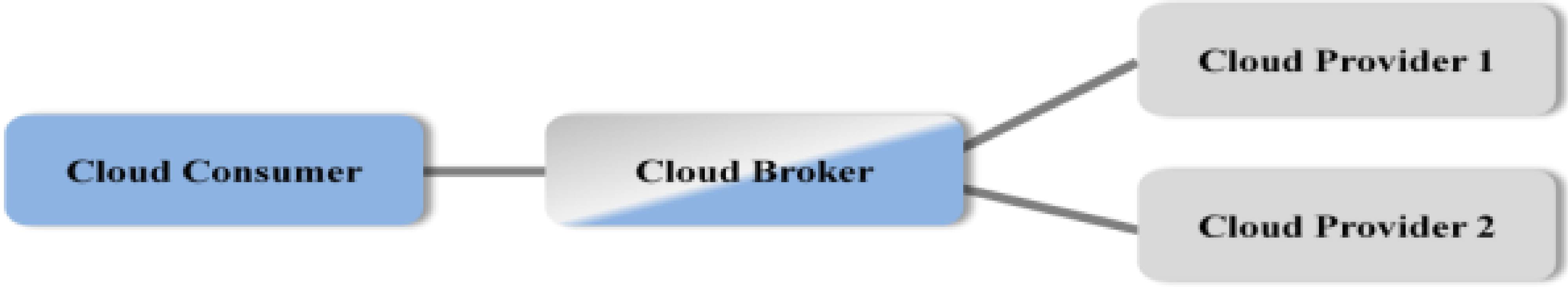
Interactions between the Actors in Cloud Computing

Interactions Between the Actors in Cloud Computing



Usage Scenario for Cloud Brokers

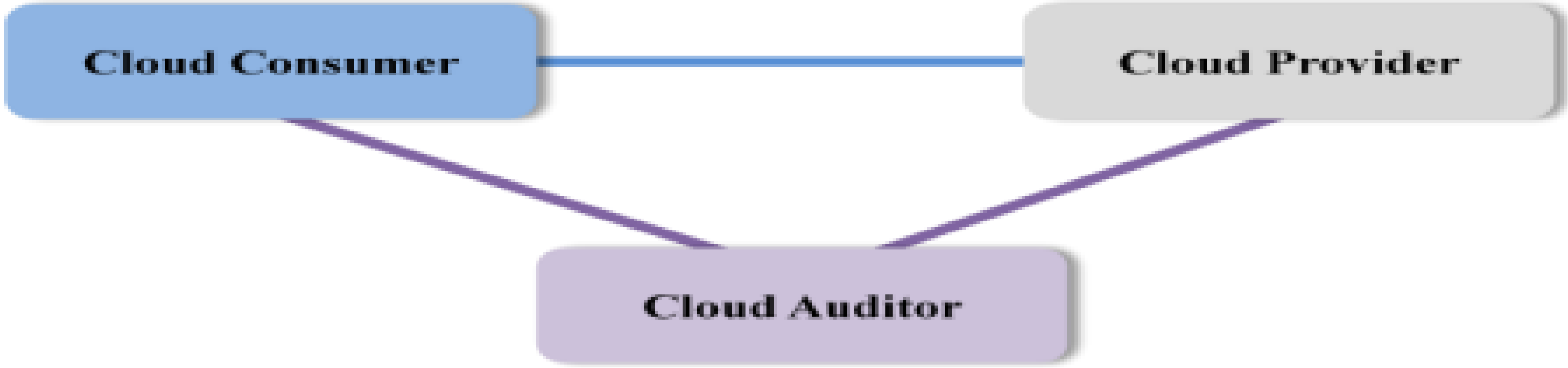
Interactions Between the Actors in Cloud Computing



Usage Scenario for Cloud Brokers

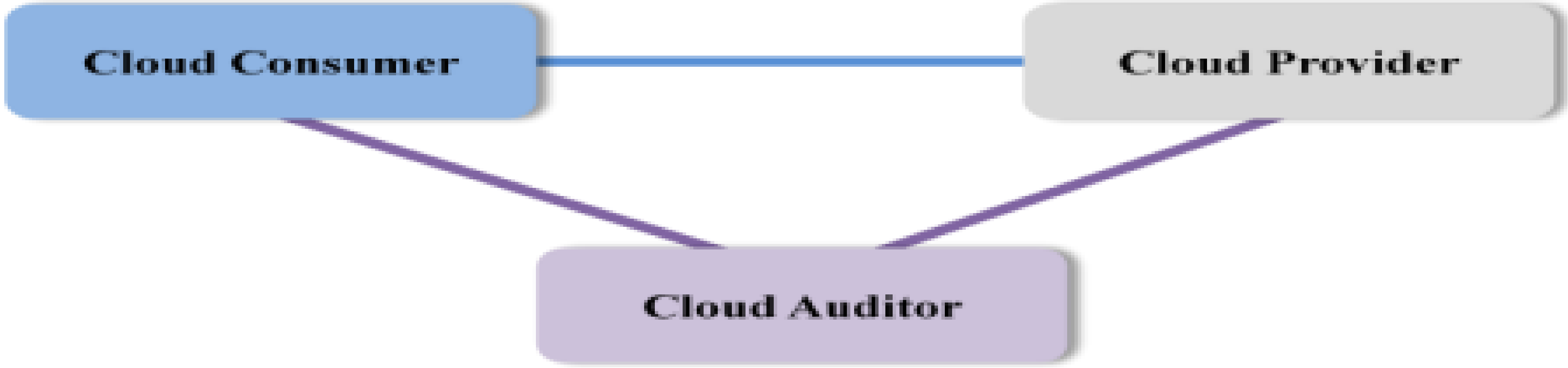
Example Usage Scenario 1: A cloud consumer may request service from a cloud broker instead of contacting a cloud provider directly. The cloud broker may create a new service by combining multiple services or by enhancing an existing service. In this example, the actual cloud providers are invisible to the cloud consumer and the cloud consumer interacts directly with the cloud broker.

Interactions Between the Actors in Cloud Computing



Usage Scenario for Cloud Auditors

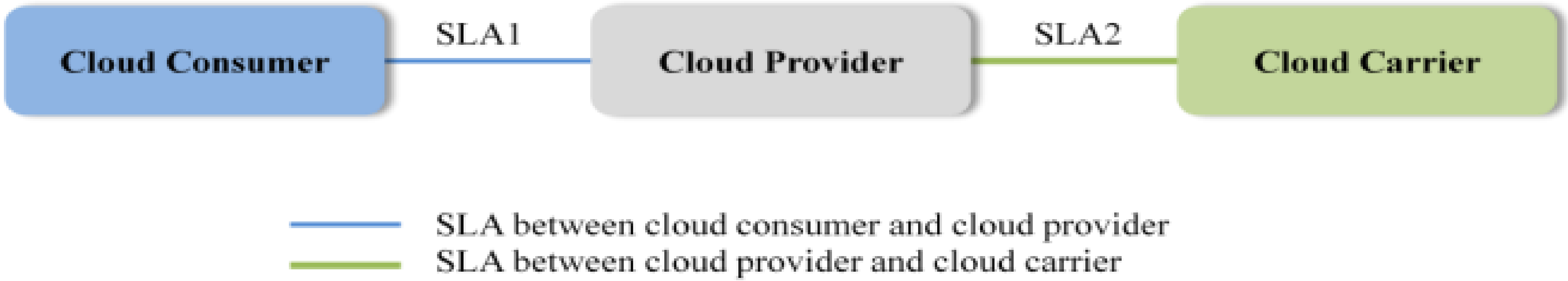
Interactions Between the Actors in Cloud Computing



Usage Scenario for Cloud Auditors

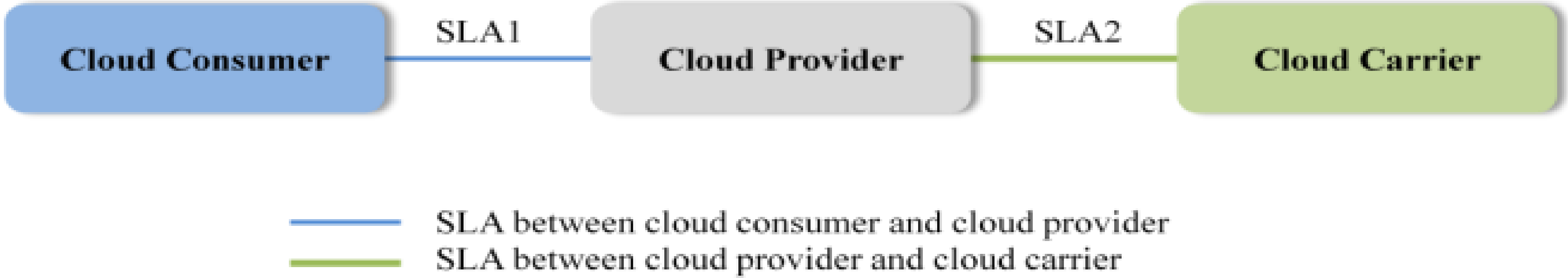
Example Usage Scenario 2: For a cloud service, a cloud auditor conducts independent assessments of the operation and security of the cloud service implementation. The audit may involve interactions with both the Cloud Consumer and the Cloud Provider

Interactions Between the Actors in Cloud Computing


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 Carriers

Interactions Between the Actors in Cloud Computing


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 Carriers

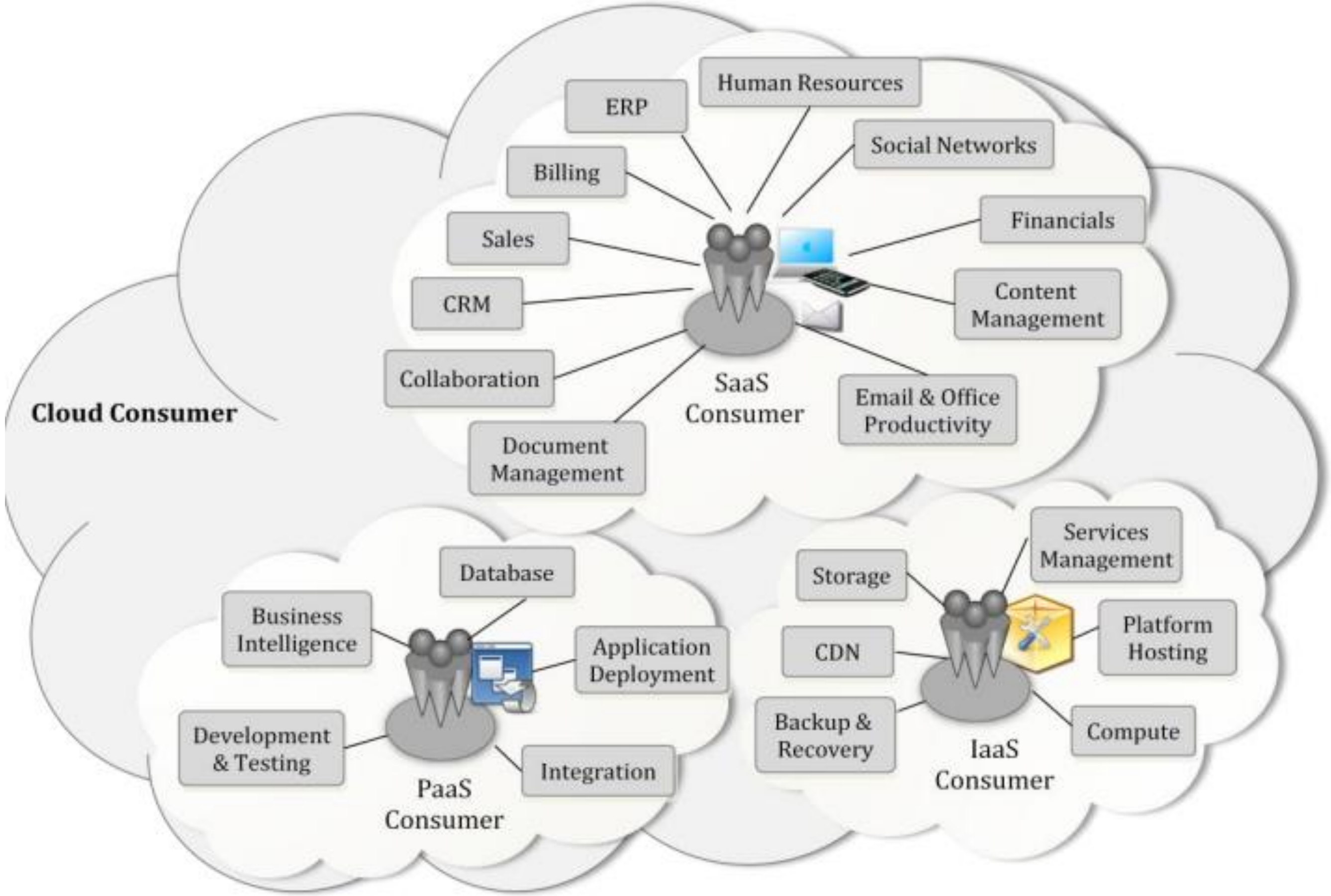
Example Usage Scenario 3: Cloud carriers provide the connectivity and transport of cloud services from cloud providers to cloud consumers. As illustrated in Figure, a cloud provider participates in and arranges for two unique service level agreements (SLAs), one with a cloud carrier (e.g., SLA2) and 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

- Principal stakeholder of cloud services
- Person/Organization
- Steps to avail cloud services are as follows:
  - Browses the service catalog
  - Requests the appropriate service
  - Sets up service contracts with the cloud provider
  - Uses the service.
  - Pay for the service as per rates.
- SLA is used to specify the technical requirements. It includes the following:
  - Quality of service
  - Security
  - Remedies for performance failures
  - Limitations, and obligations that cloud consumers must accept

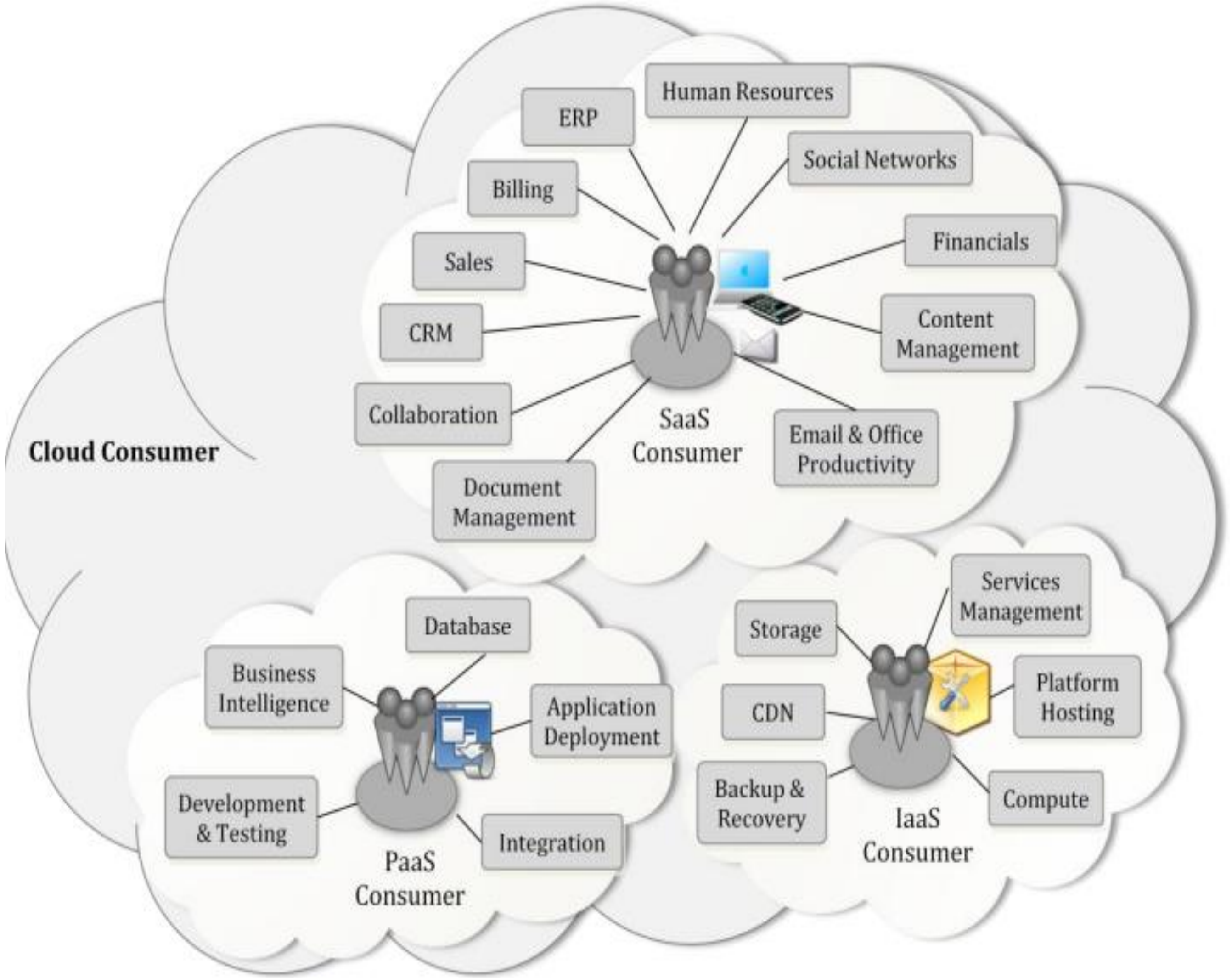
Cloud Consumer

- some example cloud services available to a cloud consumer.



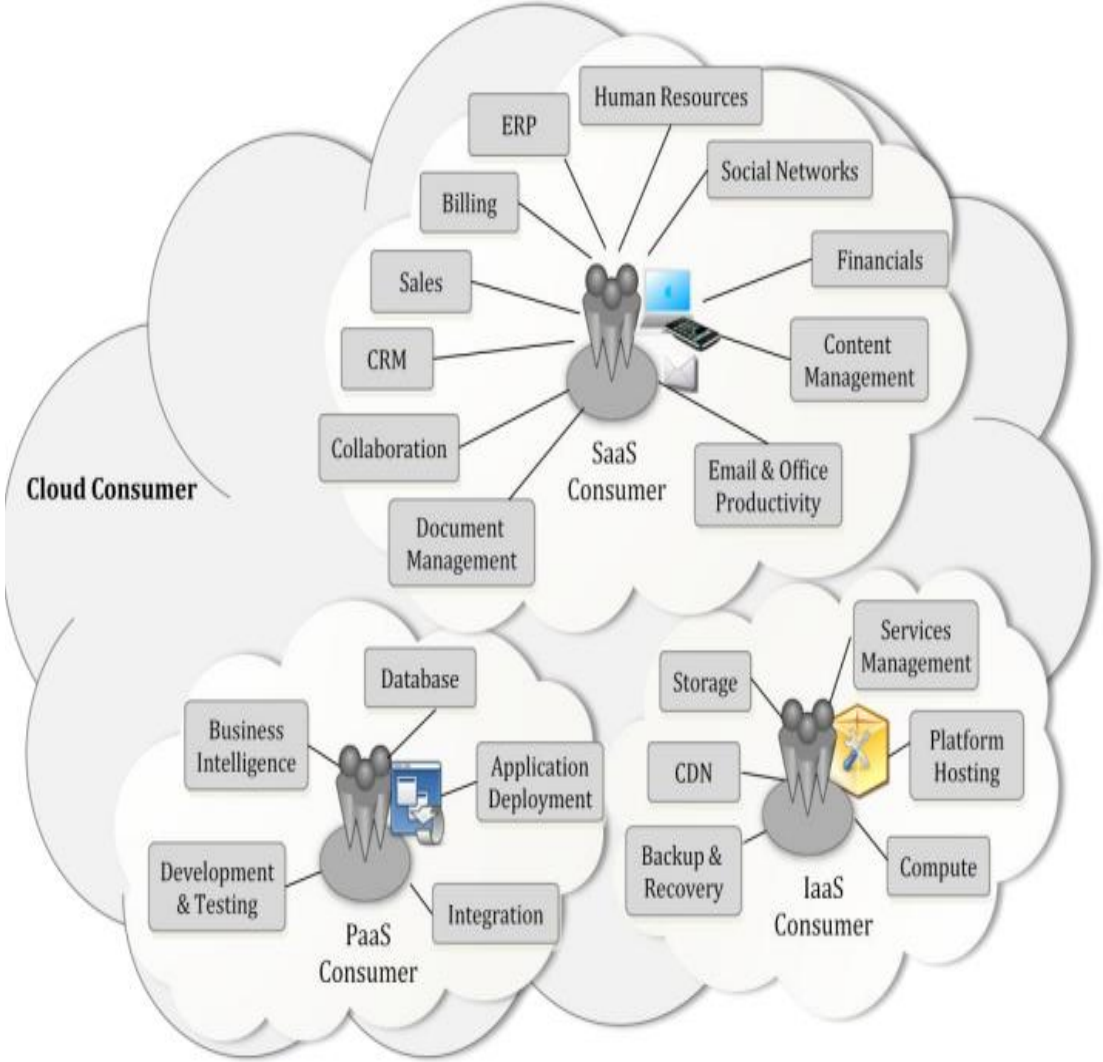
Cloud Consumer

- SaaS applications in the cloud and made accessible via a network to the SaaS consumers. The consumers of SaaS can be
  - Organizations that provide their members with access to software applications
  - End users who directly use software applications.
  - Software application administrators who configure applications for end users.
- SaaS consumers can be billed based on the number of end users, the time of use etc.



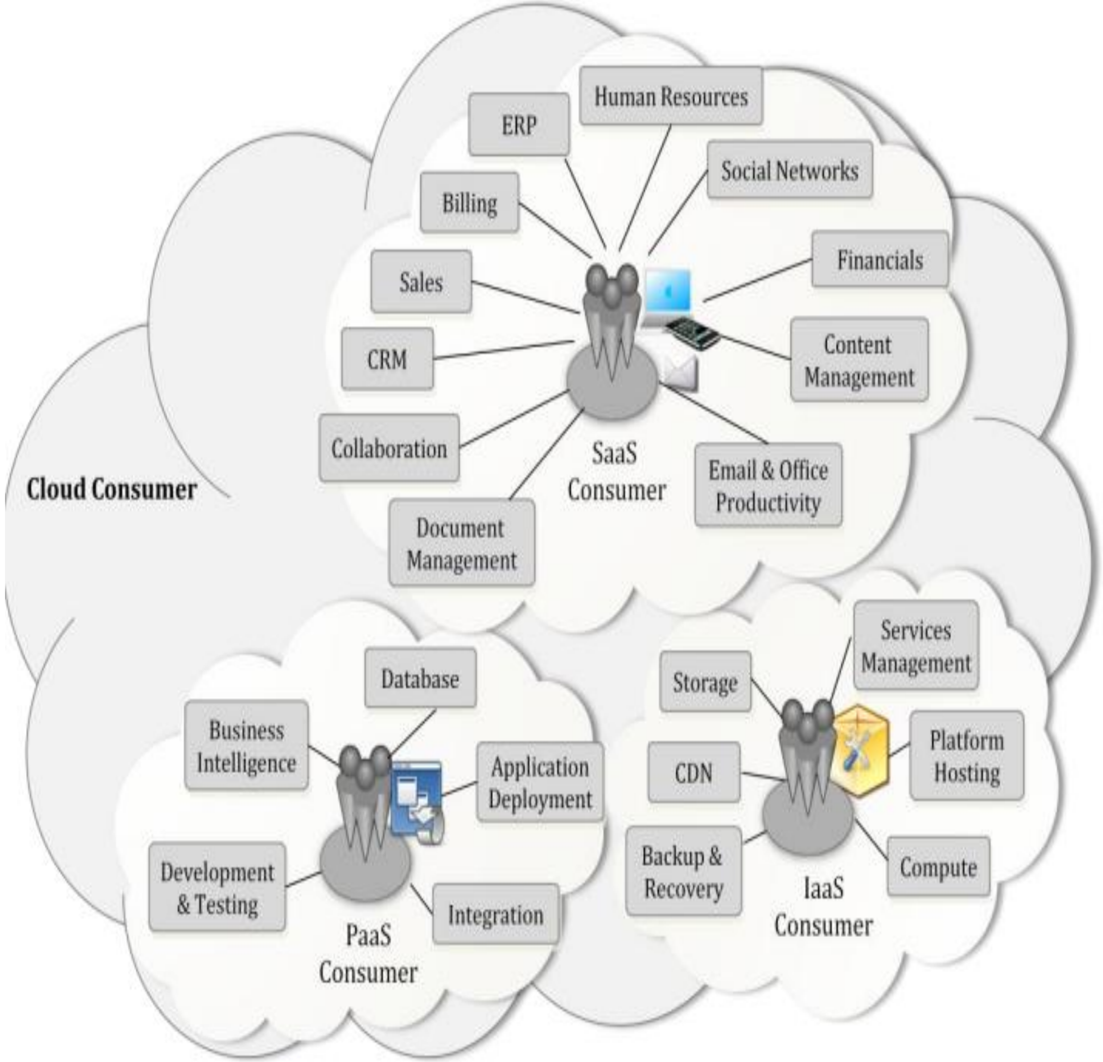
Cloud Consumer

- Cloud consumers of PaaS can employ the tools and execution resources provided by cloud providers to develop, test, deploy and manage the applications hosted in a cloud environment. PaaS consumers can be
  - Application developers who design and implement application software,
  - Application testers who run and test applications in cloud-based environments
  - Application deployers who publish applications into the cloud
  - Application administrators who configure and monitor application performance on a platform.
- PaaS consumers can be billed according to, processing, database storage and network resources consumed by the PaaS application, and the duration of the platform usage.



Cloud Consumer

- Consumers of IaaS have access to virtual computers, network-accessible storage, network infrastructure components, and other fundamental computing resources on which they can deploy and run arbitrary software. The consumers of IaaS can be
  - System developers, system administrators and IT managers who are interested in creating, installing, managing and monitoring services for IT infrastructure operations.
- IaaS consumers are provisioned with the capabilities to access these computing resources and are billed according to the amount or duration of the resources consumed, such as CPU hours used by virtual computers, volume and duration of data stored, network bandwidth consumed, number of IP addresses used for certain intervals.



Cloud Broker

- A cloud broker is a third-party that acts as an intermediary between cloud service providers and cloud consumers. The role of a cloud broker is to provide services that help cloud consumers make informed decisions about which cloud services to use based on their needs and requirements. A cloud broker may provide a range of services, such as:
  - 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 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.
  - 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 Auditor

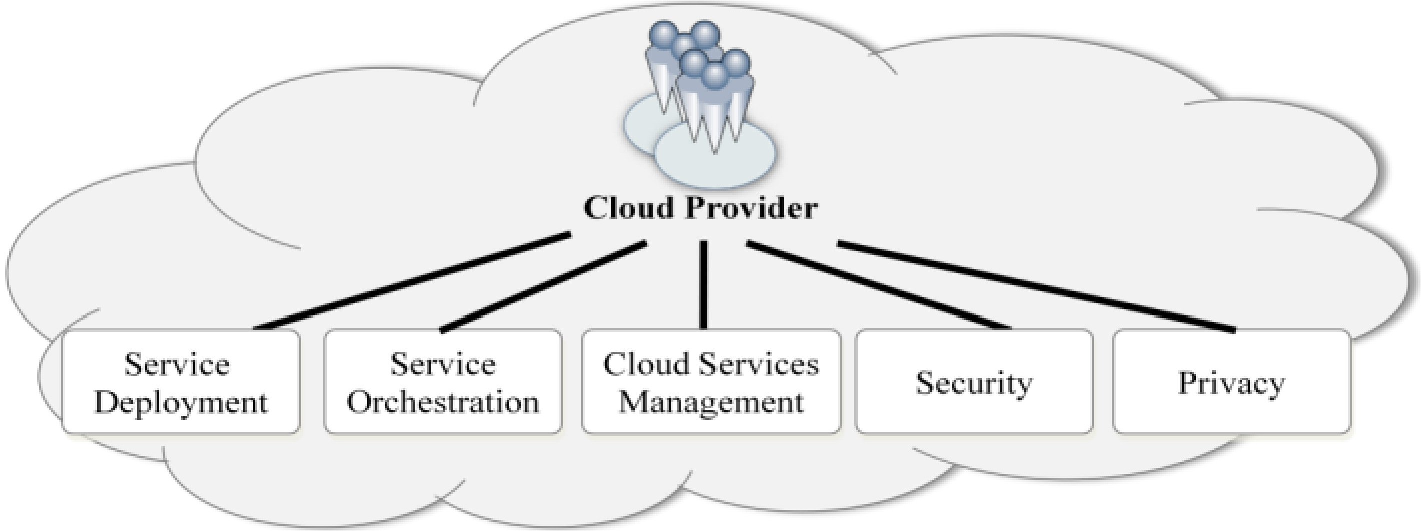
- A cloud auditor is a professional who is responsible for assessing and evaluating the security, compliance, and performance of cloud computing systems used by an organization.
- Cloud auditors typically work with cloud service providers to ensure that their services meet the requirements of the organization's security and compliance policies.
- They may also review the organization's internal processes and procedures to ensure that they are compliant with industry regulations and standards.
- Some of the key responsibilities of a cloud auditor include:
  - Assessing the security of cloud computing systems, including data encryption, access control, and network security.
  - Evaluating the performance and availability of cloud computing systems to ensure they meet the organization's requirements.
  - Reviewing compliance with industry standards.
  - Recommending improvements to cloud computing systems to enhance their security, compliance, and performance.
  - Developing and implementing auditing policies and procedures for cloud computing systems.

Cloud Carrier

- A cloud carrier refers to a network or telecommunications infrastructure that provides connectivity and transport services for accessing cloud-based services.
- A cloud carrier can be thought of as a middleman or intermediary between cloud service providers and cloud service customers which provides the underlying network infrastructure that connects cloud services to end-users, enabling them to access and use cloud-based resources over the internet.
- 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.

Cloud Service Provider

- Person, an organization who is responsible for making a service available to interested parties through cloud carrier.
- A cloud provider conducts its activities in the areas of service deployment, service orchestration, cloud service management, security, and privacy



Cloud Provider - Major Activities

Cloud Service Provider

- 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 Service Provider

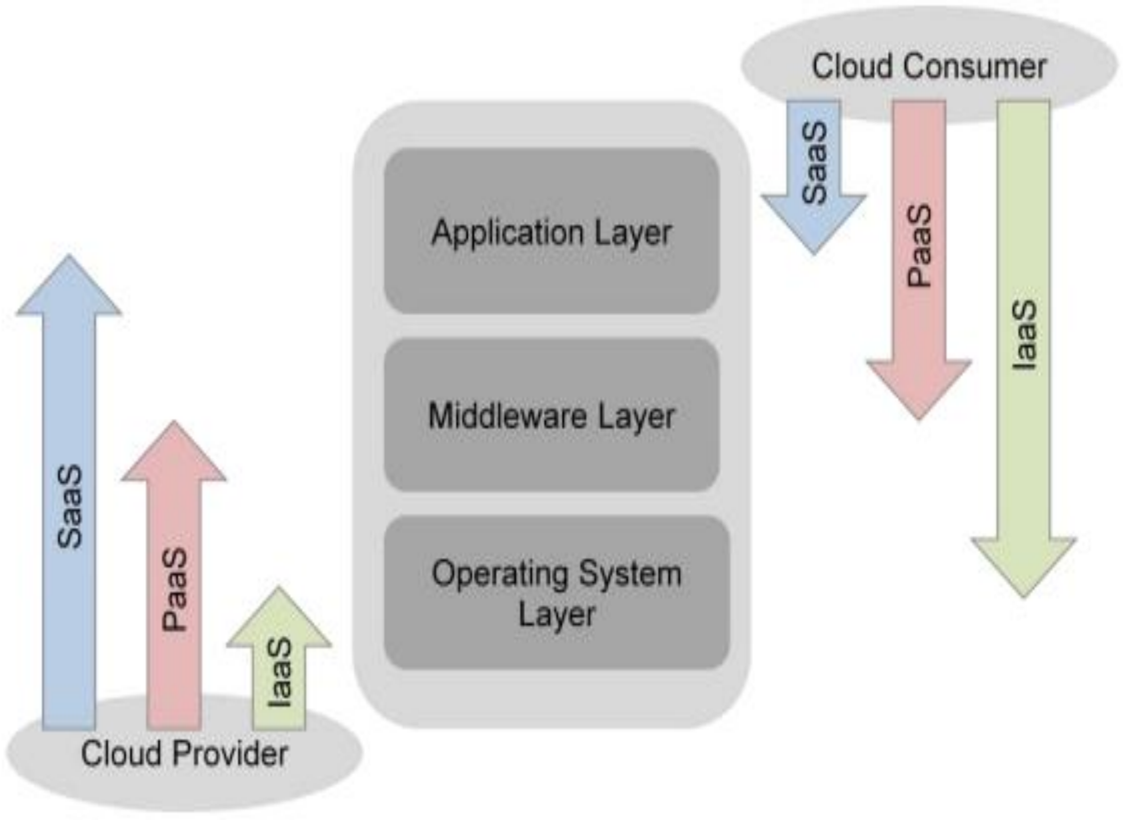
- For PaaS, the Cloud Provider manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as runtime software execution stack, databases, and other middleware components.
- The PaaS Cloud Provider typically also supports the development, 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 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 Service Provider

- 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's, storage devices, host OS and hypervisors for virtualization.

Scope of Control between Provider and Consumer

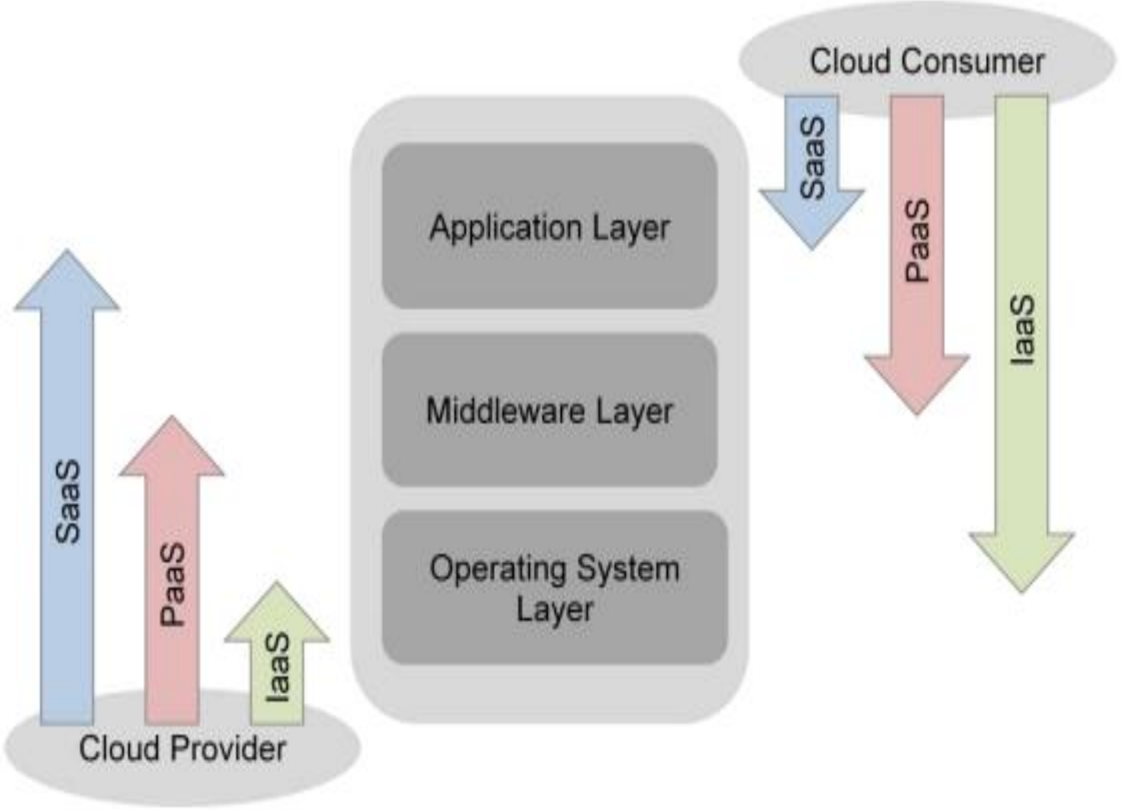
- The application layer includes software applications targeted at end users or programs.
- The applications are used by SaaS consumers, or installed/managed/ maintained by PaaS consumers, IaaS consumers, and SaaS providers.



Scope of Controls between Provider and Consumer

Scope of Control between Provider and Consumer

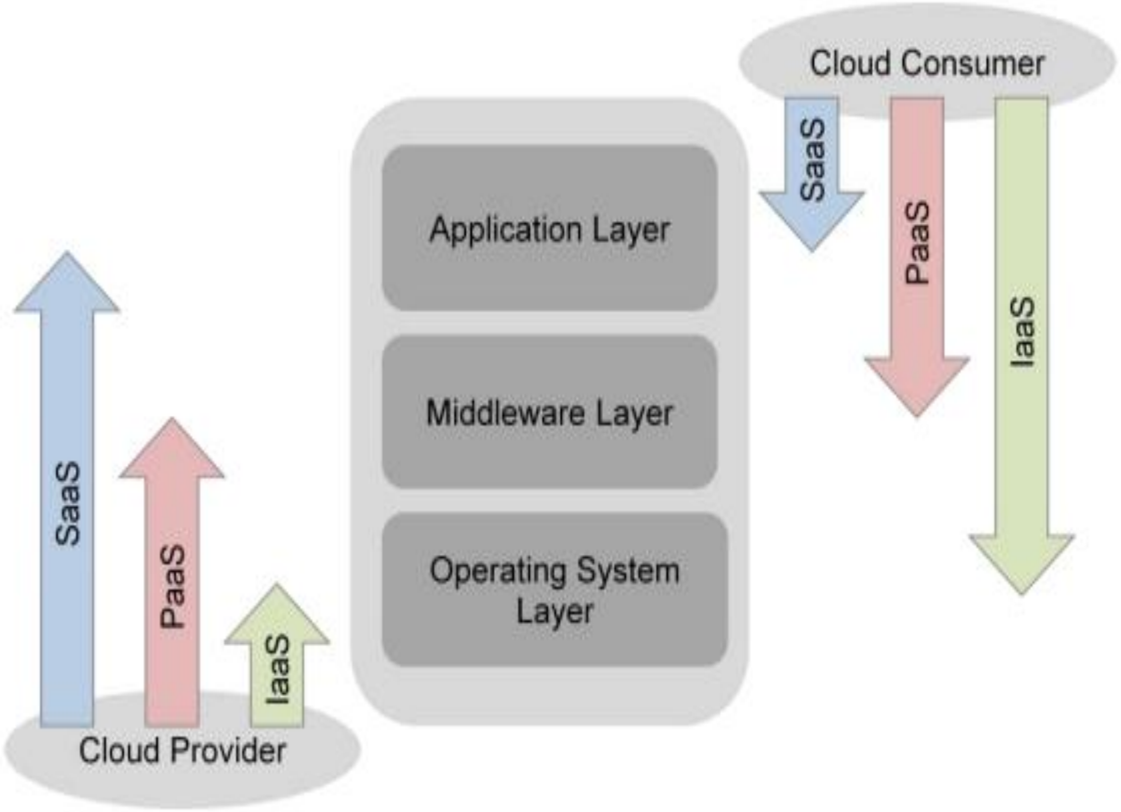
- The middleware layer provides software building blocks (e.g., libraries, database, and Java virtual machine) for developing application software in the cloud.
- The middleware is used by PaaS consumers, installed/managed/maintained by IaaS consumers or PaaS providers, and hidden from SaaS consumers.



Scope of Controls between Provider and Consumer

Scope of Control between Provider and Consumer

- 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 OSs to run virtualized on a single physical host.
- Generally, consumers have broad freedom to choose which OS to be hosted among all the OSs that could be supported by the cloud provider.
- The IaaS consumers should assume full responsibility for the guest OSs, while the IaaS provider controls the host OS.



Scope of Controls between Provider and Consumer

NIST Cloud Computing Reference Architectural Component: Service Deployment

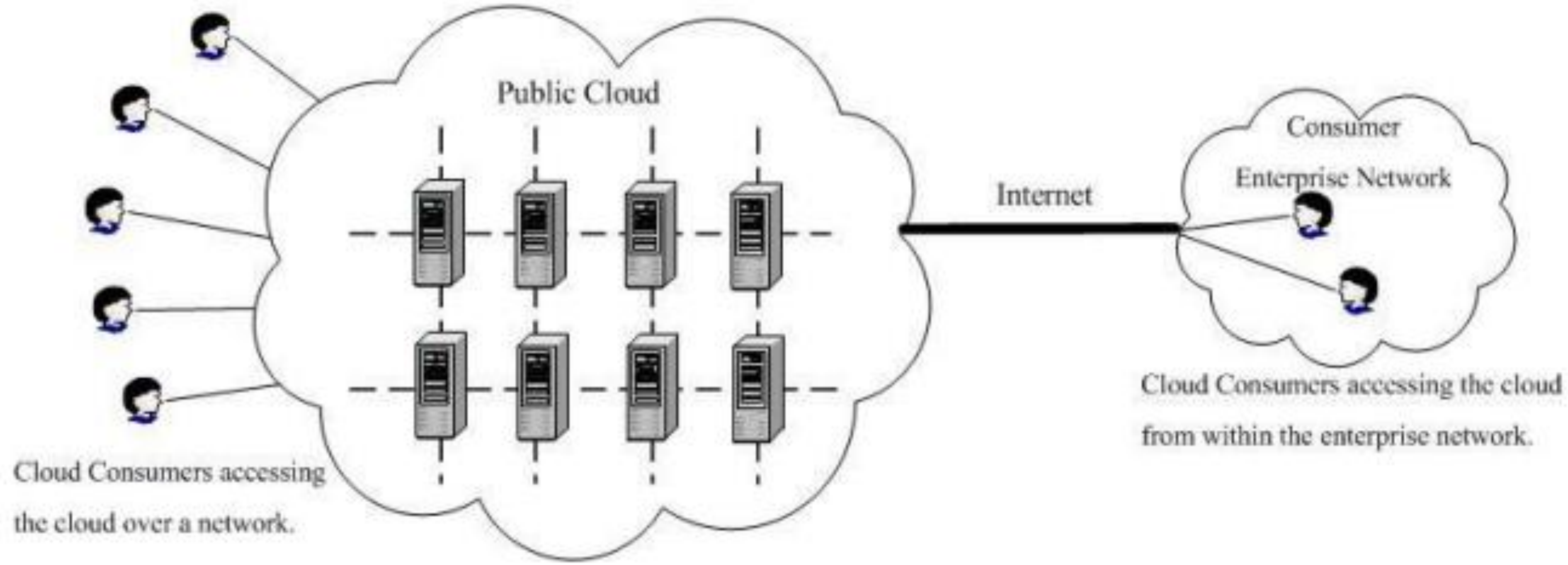
As identified in the NIST cloud computing definition, a cloud infrastructure may be operated in one of the following deployment models:

- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud

The differences are based on how exclusive computing resources are made to a cloud consumer.

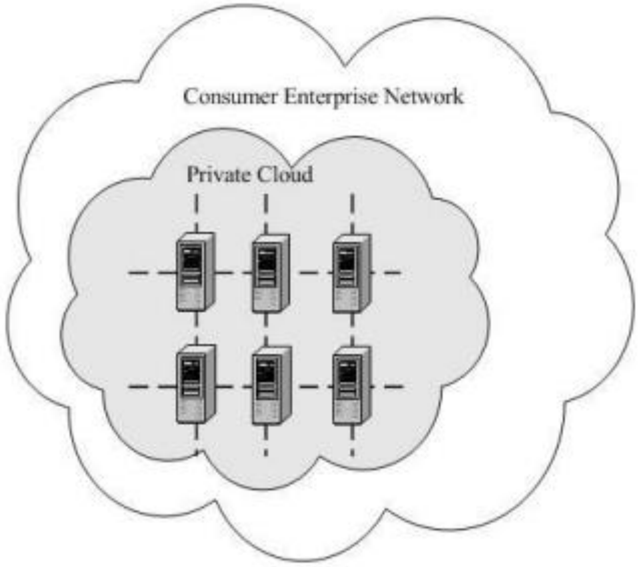
NIST Cloud Computing Reference Architectural Component: Service Deployment

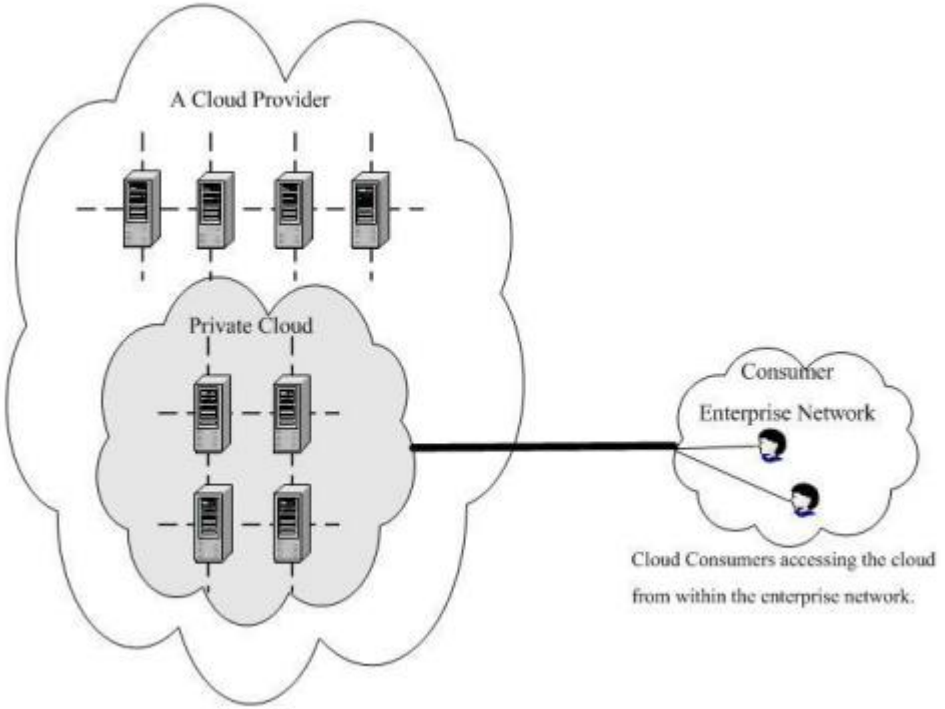
A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network. A public cloud is owned by an organization selling cloud services and serves a diverse pool of clients.


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

NIST Cloud Computing Reference Architectural Component: Service Deployment

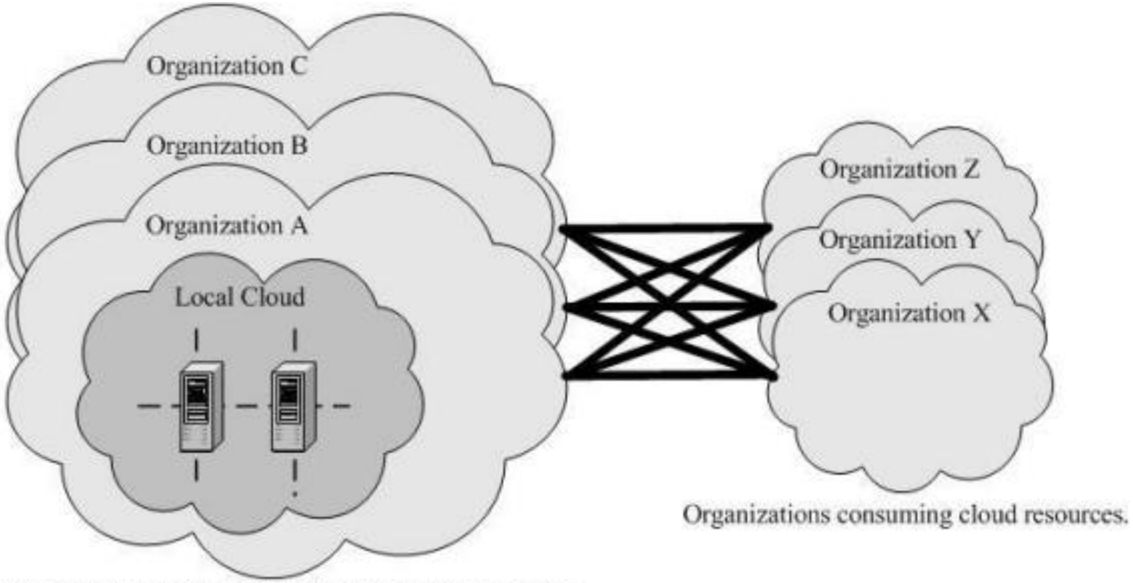
A private cloud gives a single Cloud Consumer's organization the exclusive access to and usage of the infrastructure and computational resources. It may be managed either by the Cloud Consumer organization or by a third party and may be hosted on the organization's premises (i.e., on-site private clouds) or outsourced to a hosting company (i.e., outsourced private clouds).




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

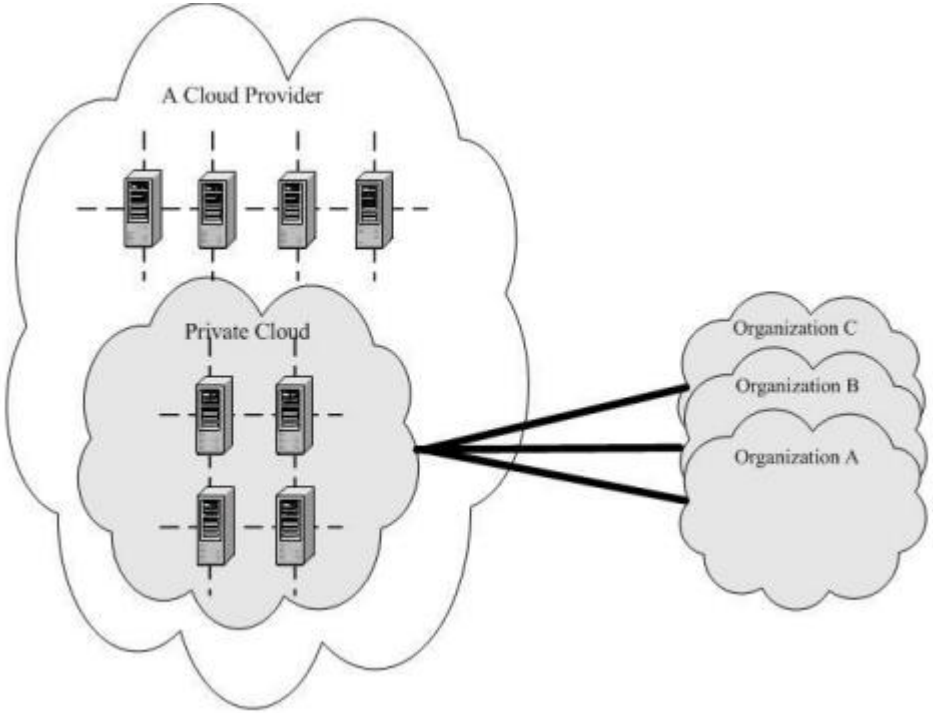
NIST Cloud Computing Reference Architectural Component: Service Deployment

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. Like 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).



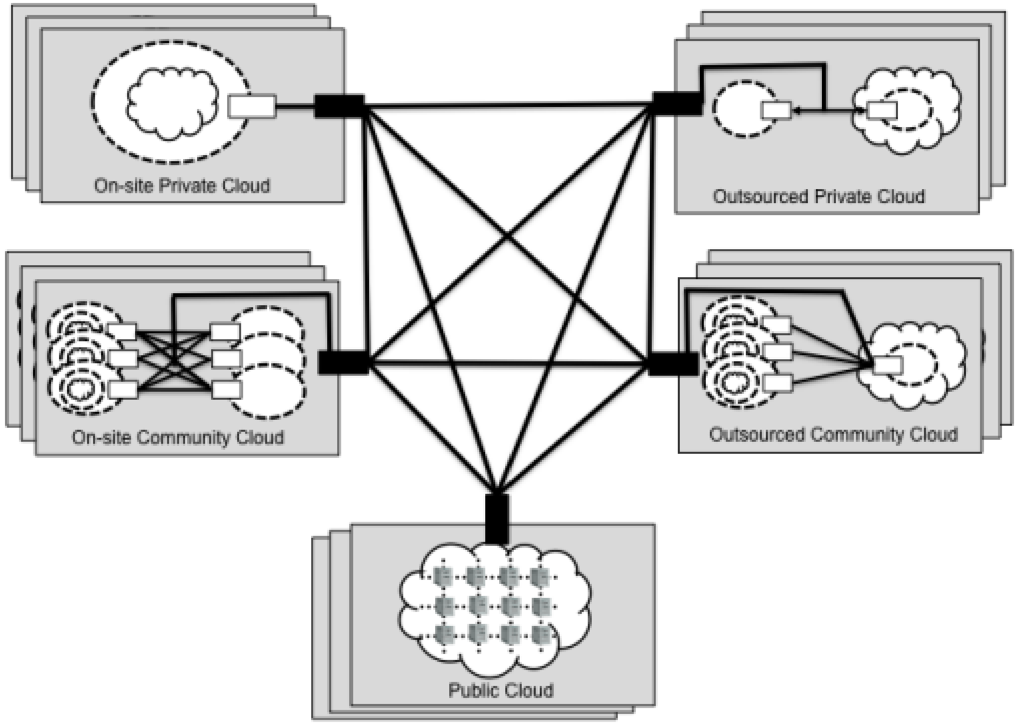
Organizations consuming cloud resources.

Organizations providing and consuming cloud resources.



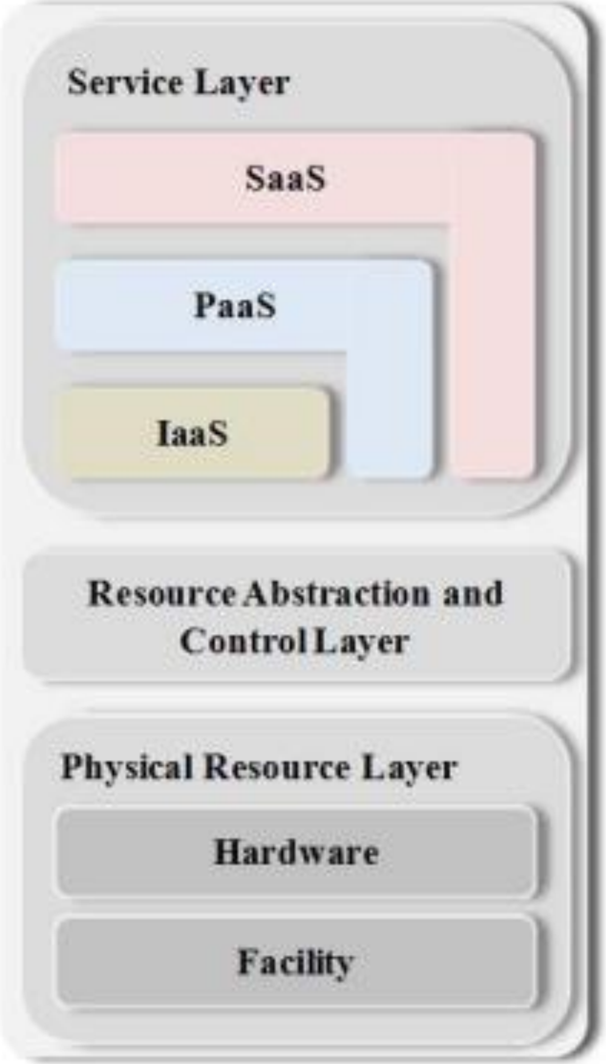
NIST Cloud Computing Reference Architectural Component: Service Deployment

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.



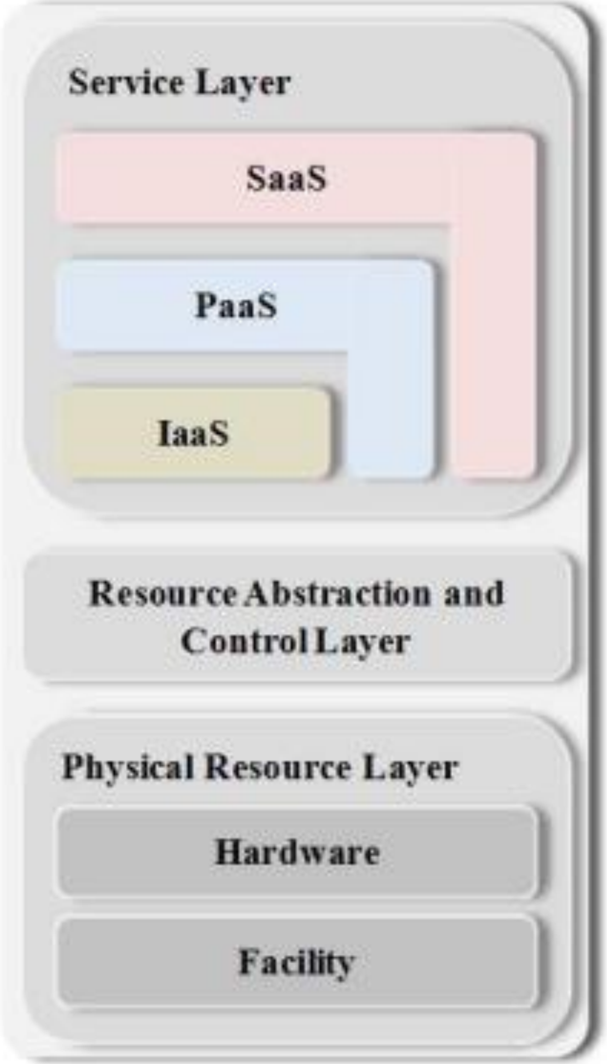
NIST Cloud Computing Reference Architectural Component: Service Orchestration

- 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.
- 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.



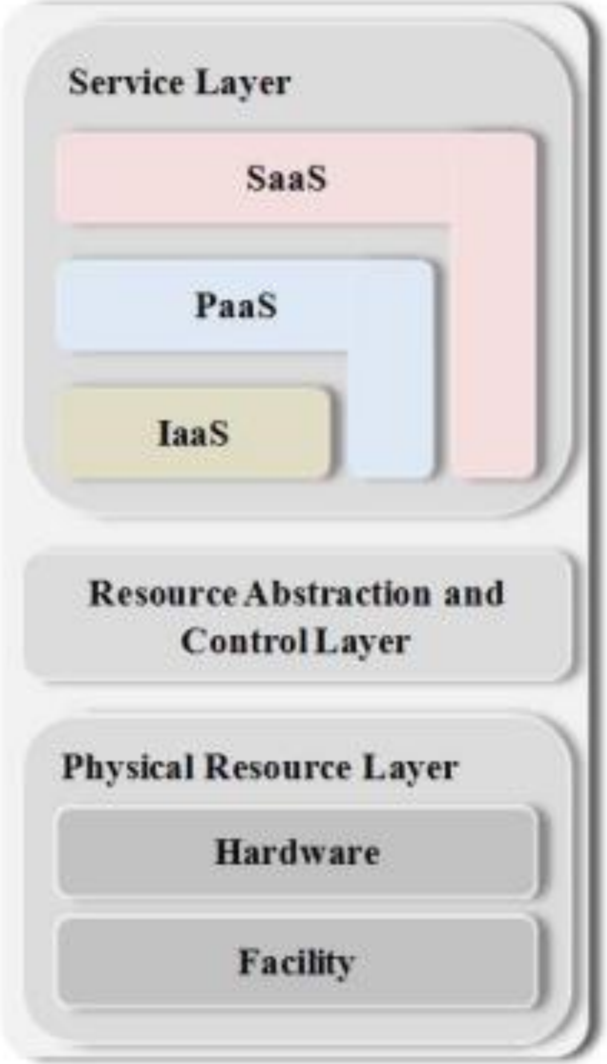
NIST Cloud Computing Reference Architectural Component: Service Orchestration

- Top layer is the service layer, where Cloud Providers define access interfaces for each of the service models for Cloud Consumers to access the different services.
- SaaS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components or 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.



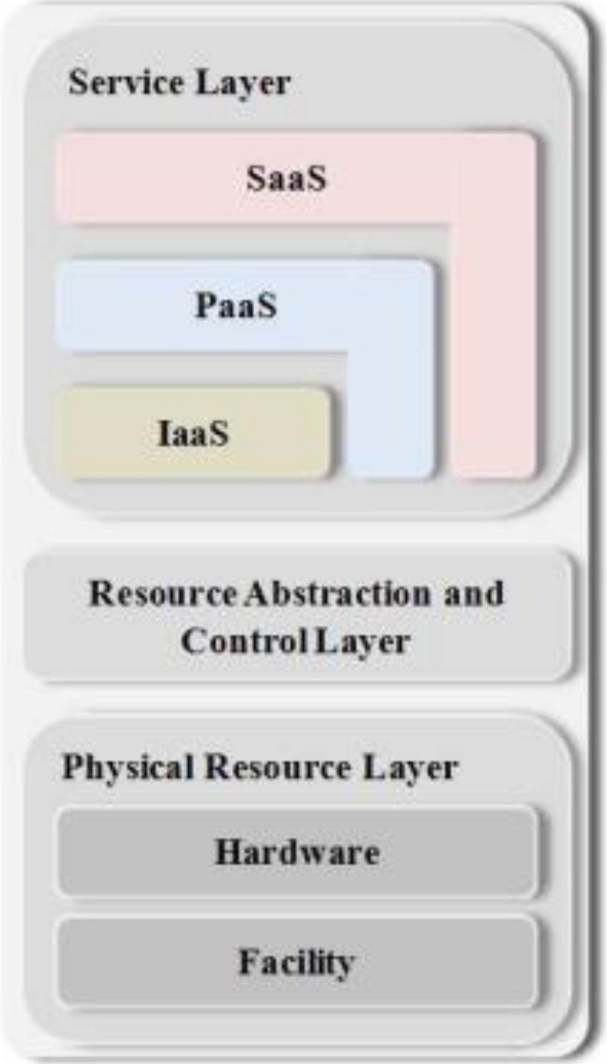
NIST Cloud Computing Reference Architectural Component: Service Orchestration

- The resource abstraction and control layer contains the system components that Cloud Providers use to provide and manage access to the physical computing resources through software abstraction. E.g. hypervisors, virtual machines, virtual data storage etc.
- The resource abstraction needs to ensure efficient, secure, and reliable usage of the underlying physical resources.
- 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.



NIST Cloud Computing Reference Architectural Component: Service Orchestration

- 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.



NIST Cloud Computing Reference Architectural Component: Security

- 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.
- 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, analyze and implement security in a cloud system.

NIST Cloud Computing Reference Architectural Component: Security

- Cloud Service Model Perspectives: The three service models 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. So, It is important to consider the impact of cloud service models and their different issues in security design and implementation.

NIST Cloud Computing Reference Architectural Component: Security

- Implications of Cloud Deployment Models:
  - The variations of cloud deployment models have important security implication. One way to look at the security implications from the deployment model perspective is the differing level of exclusivity of tenants in a deployment model. A private cloud is dedicated to one consumer organization, whereas 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.

NIST Cloud Computing Reference Architectural Component: Security

- Shared Security Responsibilities:
    - Compared to traditional IT systems, where one organization has control over the whole stack of computing resources and the entire life-cycle of the systems, the Cloud Provider and the Cloud Consumer have differing degrees of control over the computing resources in a cloud system.
    - Cloud Providers and Cloud Consumers collaboratively design, build, deploy, and operate cloud-based systems.
    - Security controls, i.e., measures used to provide protections, need to be analyzed to determine which party is in a better position to implement.

NIST Cloud Computing Reference Architectural Component: Privacy

- 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 providers must ensure the privacy of the collected personally identifiable information (PII).
- 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.

NIST Cloud Computing Reference Architectural Component: Cloud Service Management

- Cloud Service Management includes all the service-related functions that are necessary for the management and operation of those services required by cloud consumers. Broadly these functions can be divided into three categories:
  - Business support
  - Provisioning/Configuration
  - Portability/Interoperability

NIST Cloud Computing Reference Architectural Component: Cloud Service Management

- Business support: It includes 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 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.

NIST Cloud Computing Reference Architectural Component: Cloud Service Management

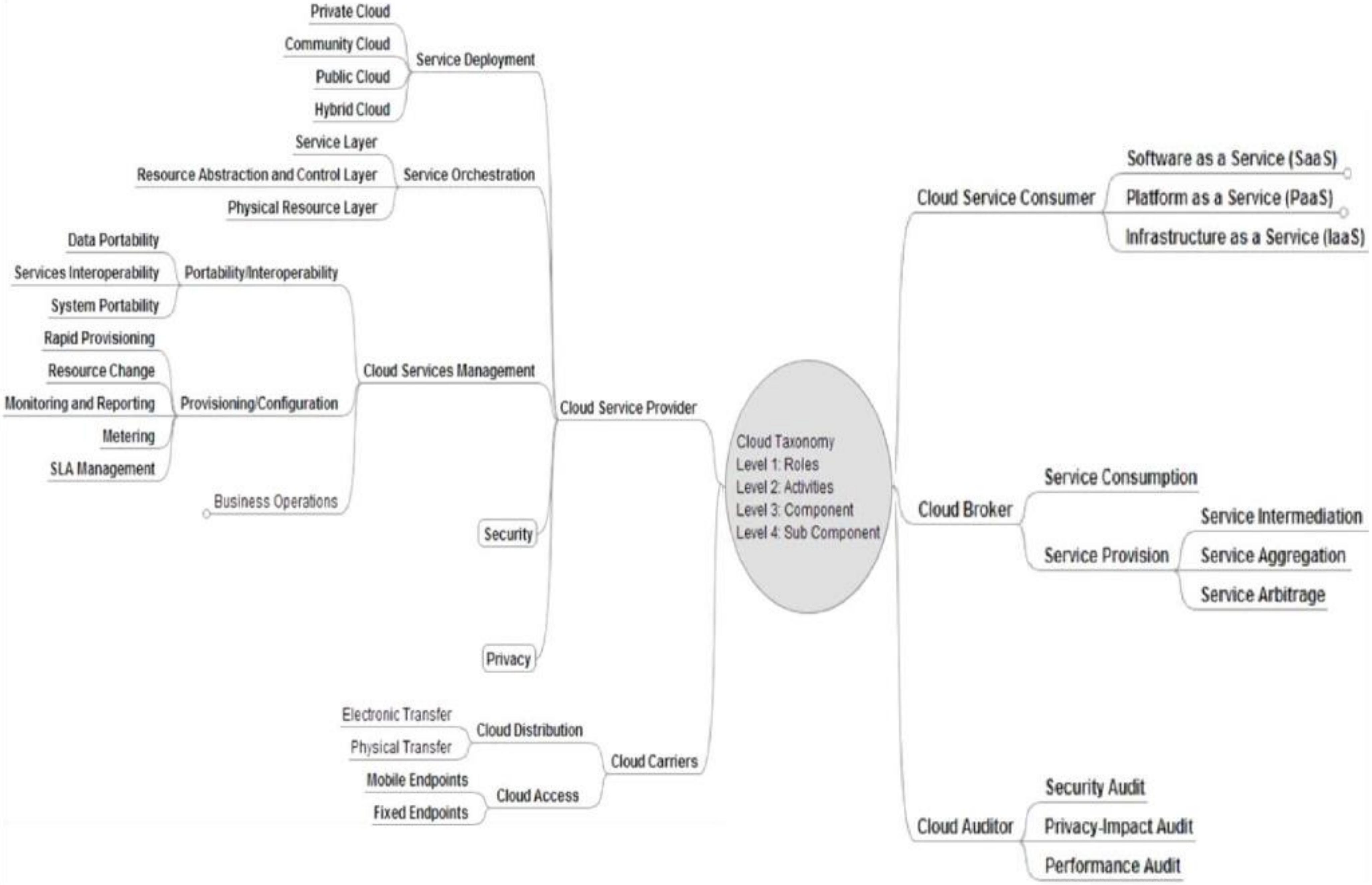
- Provisioning/Configuration:
  - Rapid provisioning: Automatically deploying cloud systems based on the requested service/resources/capabilities.
  - Resource changing: Adjusting configuration/resource assignment for repairs, upgrades and joining new nodes into the cloud.
  - Monitoring and Reporting: 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.

NIST Cloud Computing Reference Architectural Component: Cloud Service Management

- Portability & Interoperability:
  - Portability means whether cloud consumer can move their data or applications across multiple cloud environments at low cost and minimal disruption.
  - Interoperability means 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.

Cloud Taxonomy

- Taxonomy is the science of categorization or classification of things based on a predefined system. Typically, taxonomy contains a controlled vocabulary with a hierarchical tree-like structure. A four-level taxonomy is presented by NIST to describe the key concepts about cloud computing.
  - Level 1: **Role**, which indicates a set of **obligations** and behaviors as conceptualized by the associated actors in the context of cloud computing.
  - Level 2: **Activity**, which entails the general behaviors or **tasks** associated to a specific role.
  - Level 3: **Component**, which refer to the specific processes, actions, or tasks that must be performed to meet the objective of a specific activity.
  - Level 4: Sub-component, which present a modular part of a component.


Cloud Taxonomy
Level 1: Roles
Level 2: Activities
Level 3: Component
Level 4: Sub Component
Cloud Service Provider
Service Deployment
Private Cloud
Community Cloud
Public Cloud
Hybrid Cloud
Service Orchestration
Service Layer
Resource Abstraction and Control Layer
Physical Resource Layer
Cloud Services Management
Portability/Interoperability
Data Portability
Services Interoperability
System Portability
Provisioning/Configuration
Rapid Provisioning
Resource Change
Monitoring and Reporting
Metering
SLA Management
Business Operations
Security
Privacy
Cloud Carriers
Cloud Distribution
Electronic Transfer
Physical Transfer
Cloud Access
Mobile Endpoints
Fixed Endpoints
Cloud Service Consumer
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Cloud Broker
Service Consumption
Service Provision
Service Intermediation
Service Aggregation
Service Arbitrage
Cloud Auditor
Security Audit
Privacy-Impact Audit
Performance Audit