Module 5
Cloud Computing Security

Submodule 1: Cloud Computing Fundamentals

Cloud Computing

- NIST defines cloud computing, in NIST SP-800-145 (*The NIST Definition of Cloud Computing,* September 2011*)* as follows:
    - “**Cloud computing:** A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.”

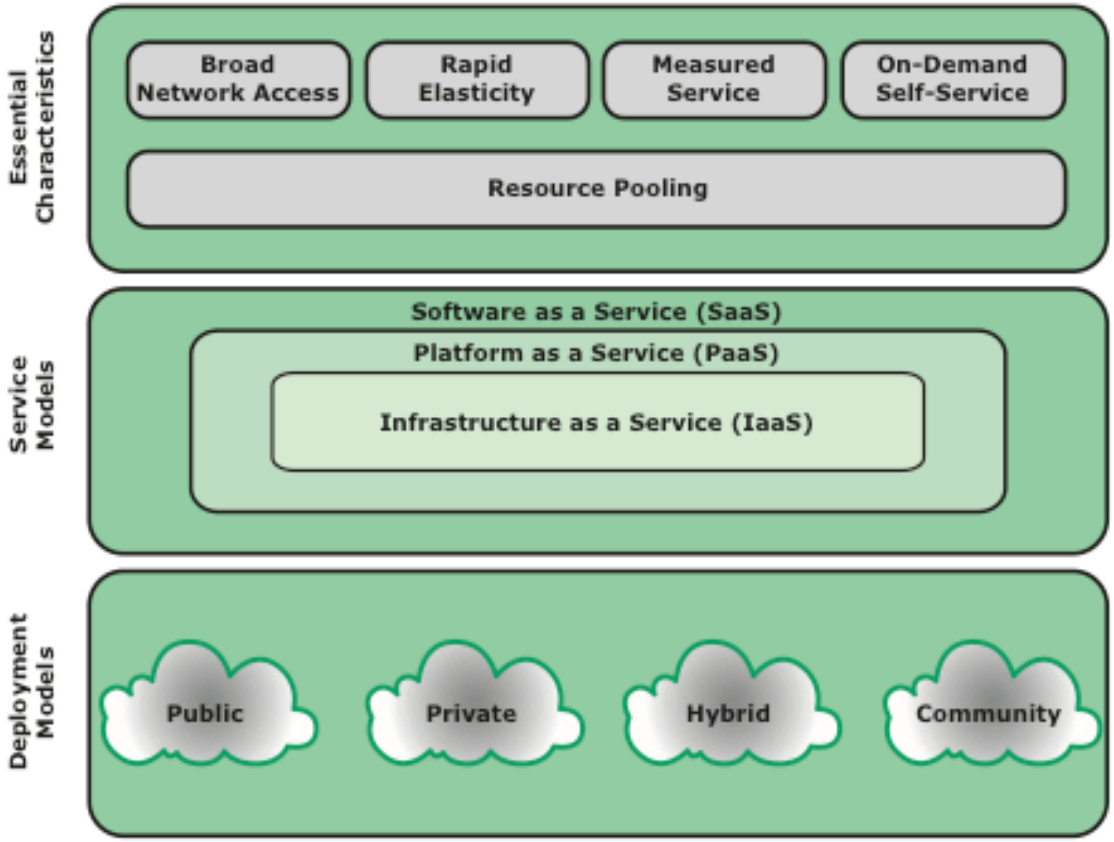


Figure 13.1 Cloud Computing Elements

Cloud Service Models

- NIST defines three service models, which can be viewed as nested service alternatives
  - Software as a service (SaaS)
  - Platform as a service (PaaS)
  - Infrastructure as a service (IaaS)

Software as a Service (Saas)

- SaaS provides service to customers in the form of software, specifically application software, running on and accessible in the cloud
- It enables the customer to use the cloud provider's applications running on the provider's cloud infrastructure
  - The applications are accessible from various client devices through a simple interface, such as a Web browser
  - Instead of obtaining desktop and server licenses for software products it uses, an enterprise obtains the same functions from the cloud service
- The use of SaaS avoids the complexity of software installation, maintenance, upgrades, and patches
- Examples of this service are Google Gmail, Microsoft 365, Salesforce, Citrix GoToMeeting, and Cisco WebEx

Platform as a Service (PaaS)-I

- A PaaS cloud provides service to customers in the form of a platform on which the customer’s applications can run
- PaaS enables the customer to deploy onto the cloud infrastructure customer-created or acquired applications
- A PaaS cloud provides useful software building blocks, plus a number of development tools, such as programming language tools, run-time environments, and other tools that assist in deploying new applications

Platform as a Service (PaaS)-II

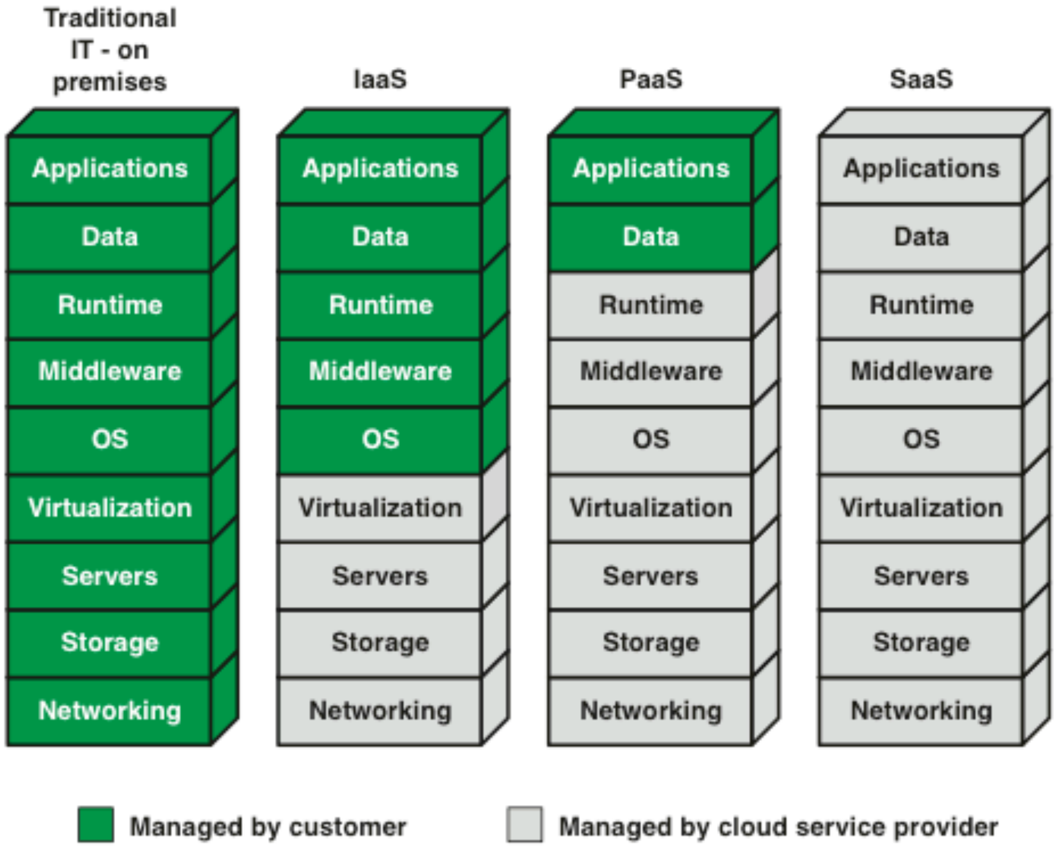
- In effect, PaaS is an operating system in the cloud
- It is useful for an organization that wants to develop new or tailored applications while paying for the needed computing resources only as needed, and only for as long as needed
- Examples of PaaS include AppEngine, Engine Yard, Heroku, Microsoft Azure, Force.com, and Apache Stratos

Infrastructure as a Service (IaaS)-I

- With IaaS, the customer has access to the resources of the underlying cloud infrastructure
- The cloud service user does not manage or control the resources of the underlying cloud infrastructure, but has control over operating systems, deployed applications, and possibly limited control of select networking components
- IaaS provides virtual machines and other virtualized hardware and operating systems

Infrastructure as a Service (IaaS)-II

- IaaS offers the customer processing, storage, networks, and other fundamental computing resources so the customer is able to deploy and run arbitrary software, which can include operating systems and applications
- IaaS enables customers to combine basic computing services, such as number crunching and data storage, to build highly adaptable computer systems
- Examples of IaaS are Amazon Elastic Compute Cloud, Microsoft Windows Azure, Google Compute Engine, and Rackspace



Traditional IT - on premises	IaaS	PaaS	SaaS
🟩 Applications	🟩 Applications	🟩 Applications	⬜ Applications
🟩 Data	🟩 Data	🟩 Data	⬜ Data
🟩 Runtime	🟩 Runtime	⬜ Runtime	⬜ Runtime
🟩 Middleware	🟩 Middleware	⬜ Middleware	⬜ Middleware
🟩 OS	🟩 OS	⬜ OS	⬜ OS
🟩 Virtualization	⬜ Virtualization	⬜ Virtualization	⬜ Virtualization
🟩 Servers	⬜ Servers	⬜ Servers	⬜ Servers
🟩 Storage	⬜ Storage	⬜ Storage	⬜ Storage
🟩 Networking	⬜ Networking	⬜ Networking	⬜ Networking

🟩 Managed by customer ⬜ Managed by cloud service provider

Figure 13.2 Separation of Responsibilities in Cloud Service Models

Cloud Deployment Models

- The four most prominent deployment models for cloud computing are:
  - Public cloud
  - Private cloud
  - Hybrid cloud
  - Community cloud

Public Cloud-I

- A public cloud infrastructure is made available to the general public or a large industry group, and is owned by an organization selling cloud services
  - The cloud provider is responsible both for the cloud infrastructure and for the control of data and operations within the cloud

Public Cloud-II

- A public cloud may be owned, managed, and operated by a business, academic, or government organization, or some combination of them
  - All major components are outside the enterprise firewall, located in a multitenant infrastructure
  - Applications and storage are made available over the Internet via secured IP, and can be free or offered at a pay-per-usage fee
- The major advantage of the public cloud is cost
- The principal concern is security

Private Cloud-I

- A private cloud is implemented within the internal IT environment of the organization
- The organization may choose to manage the cloud in house or contract the management function to a third party
- The cloud servers and storage devices may exist on premise or off premise
- Private clouds can deliver IaaS internally to employees or business units through an intranet or the Internet via a virtual private network (VPN), as well as software or storage as services to its branch offices

Private Cloud-II

- Examples of services delivered through the private cloud include database on demand, email on demand, and storage on demand
- A key motivation for opting for a private cloud is security
- Other benefits include easy resource sharing and rapid deployment to organizational entities

Community Cloud-I

- A community cloud shares characteristics of private and public clouds
  - Has restricted access like a private cloud
  - The cloud resources are shared among a number of independent organizations like a public cloud
- The organizations that share the community cloud have similar requirements and, typically, a need to exchange data with each other
  - An example would be the health care industry

Community Cloud-II

- The cloud infrastructure may be managed by the participating organizations or a third party, and may exist on premise or off premise
  - In this deployment model, the costs are spread over fewer users than a public cloud so only some of the cost savings potential of cloud computing are realized

Hybrid Cloud-I

- The hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability
- With a hybrid cloud solution, sensitive information can be placed in a private area of the cloud, and less sensitive data can take advantage of the benefits of the public cloud

Hybrid Cloud-II

- A hybrid public/private cloud solution can be particularly attractive for smaller business
- Many applications for which security concerns are less can be offloaded at considerable cost savings without committing the organization to moving more sensitive data and applications to the public cloud

	Private	**Community**	**Public**	**Hybrid**
Scalability	Limited	Limited	Very high	Very high
Security	Most secure option	Very secure	Moderately secure	Very secure
Performance	Very good	Very good	Low to medium	Good
Reliability	Very high	Very high	Medium	Medium to high
Cost	High	Medium	Low	Medium

Cloud Computing Architecture

- NIST SP-500-292 (*NIST Cloud Computing Reference Architecture)* establishes reference architecture, described as follows:
  - “The NIST cloud computing reference architecture focuses on the requirements of “what” cloud services provide, not a “how to” design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference.”

Reference Architecture Objectives

- NIST developed the reference architecture with the following objectives in mind:
  - To illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model
  - To provide a technical reference for CSCs to understand, discuss, categorize, and compare cloud services
  - To facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations

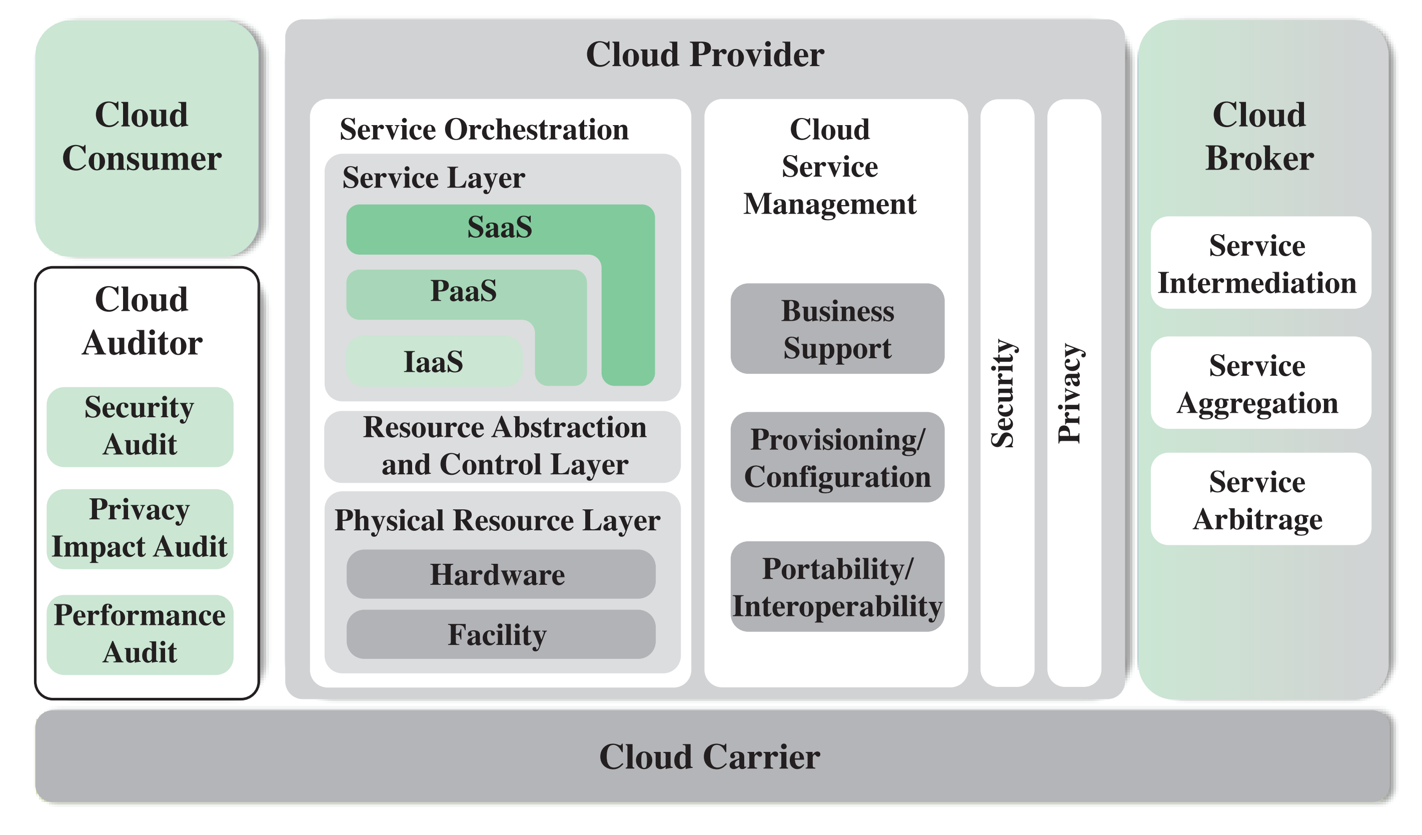


Figure 13.3 NIST Cloud Computing Reference Architecture

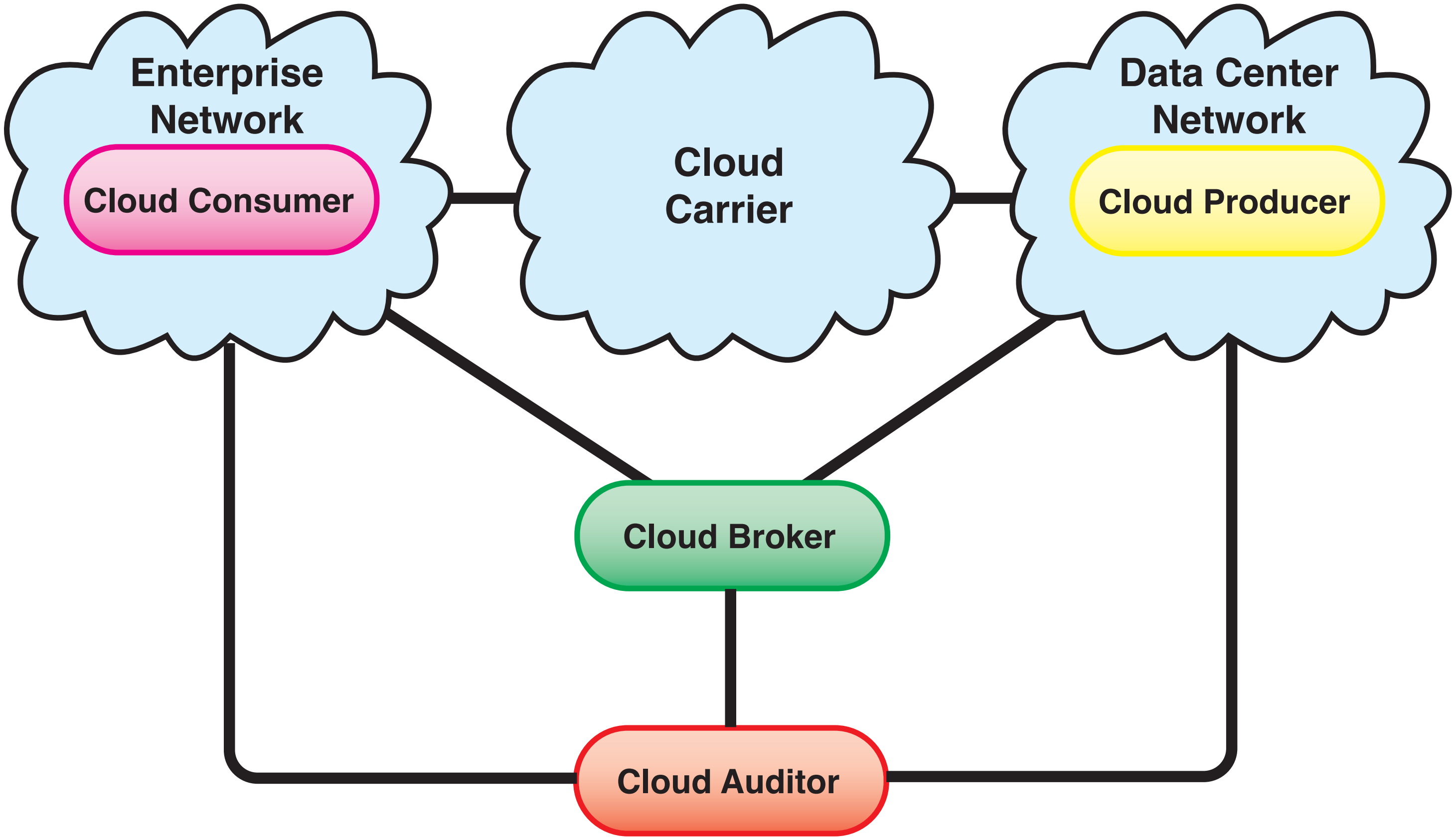


Figure 13.4 Interactions Between Actors in Cloud Computing