Cloud Security: Part 2

Gaurav S. Kasbekar

Dept. of Electrical Engineering

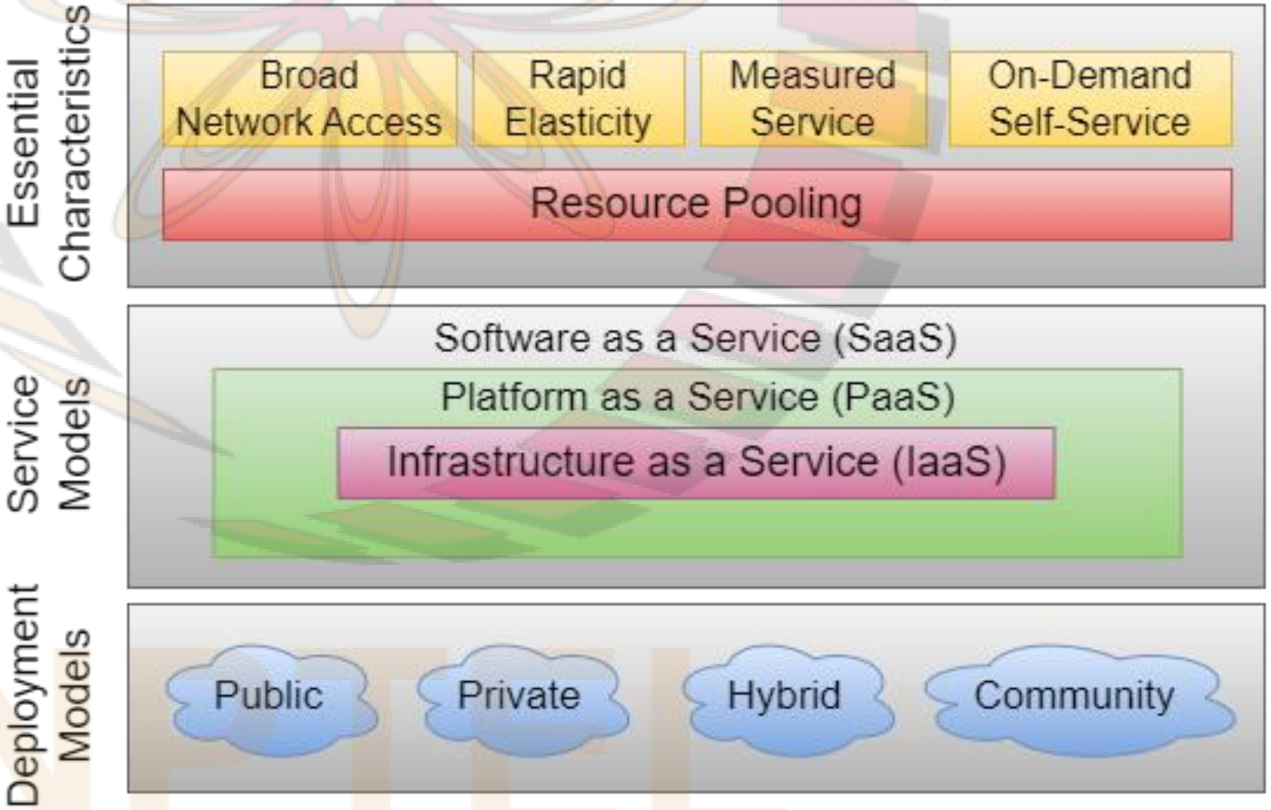
IIT Bombay

References

- W. Stallings, "*Cryptography and Network Security*", 8th edition, Pearson Education, 2023
- C. Kaufman, R. Perlman, M. Speciner, R. Perlner, "*Network Security: Private Communication in a Public World*", Pearson Education, 3rd edition, 2023

Cloud Deployment Models

- There are the following four deployment models:
  - ❑Public Cloud
  - ❑Private Cloud
  - ❑Community Cloud
  - ❑Hybrid Cloud



Essential Characteristics

Broad Network Access

Rapid Elasticity

Measured Service

On-Demand Self-Service

Resource Pooling

Service Models

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Deployment Models

Public

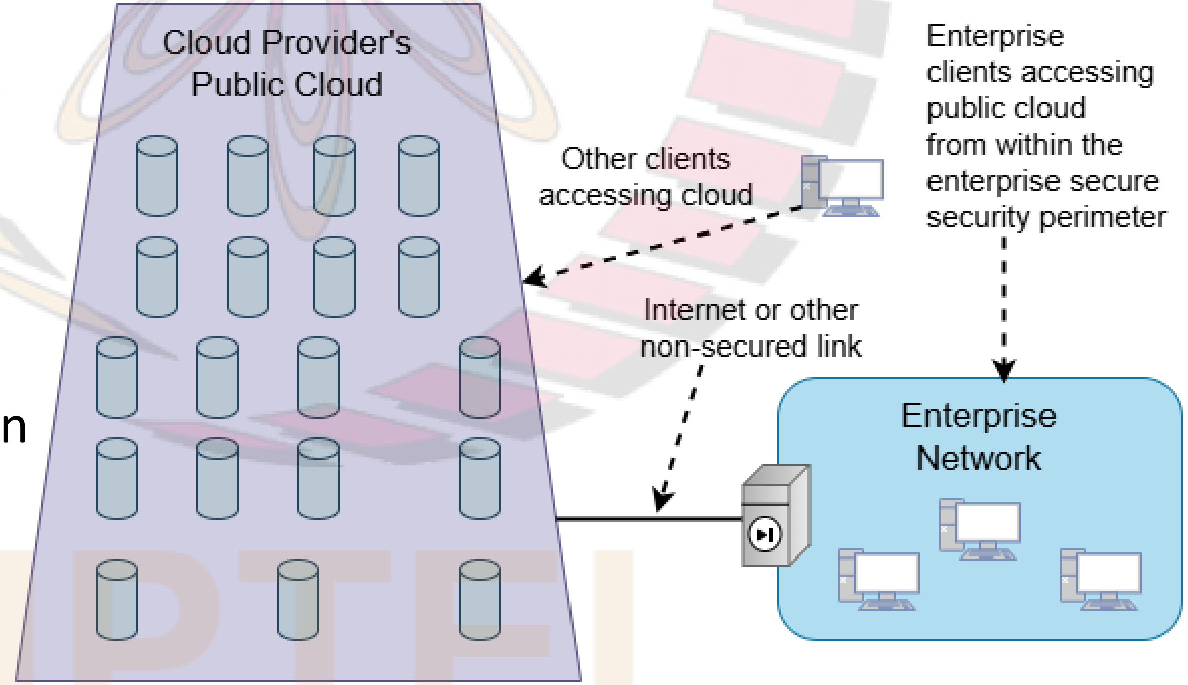
Private

Hybrid

Community

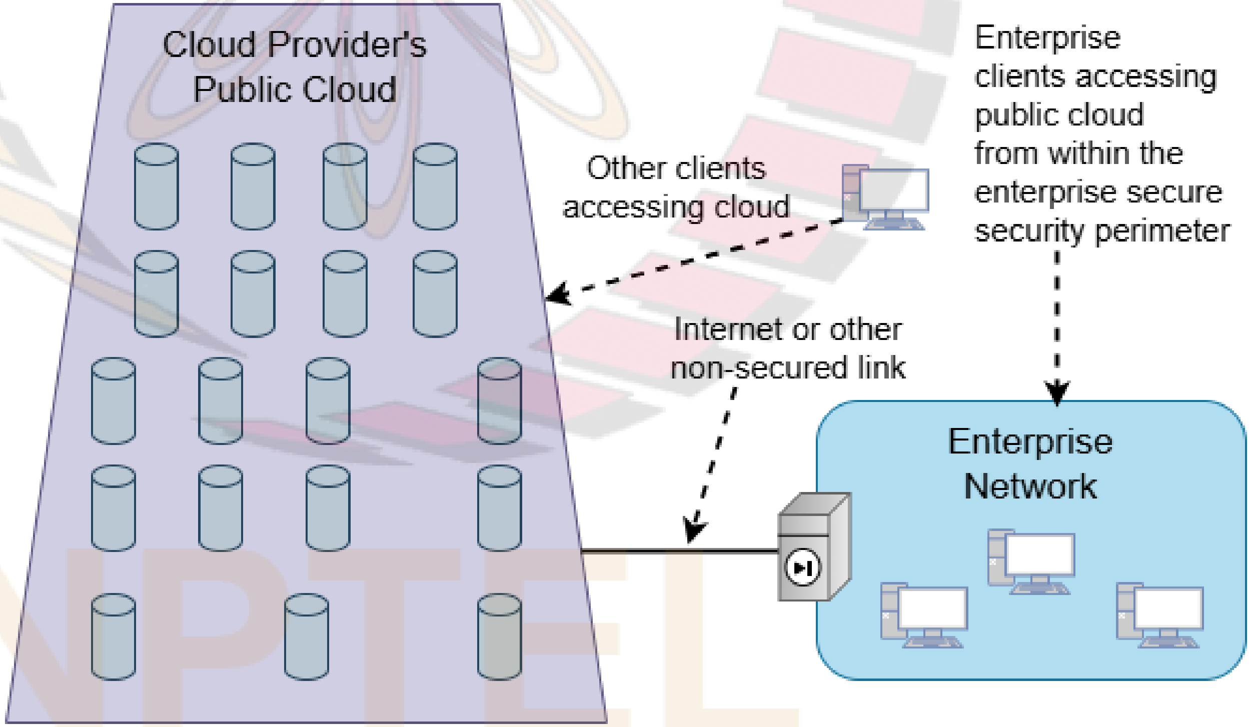
Public Cloud

- Public cloud infrastructure is:
  - ❑made available to general public and/ or a large industry group
  - ❑owned by an organization selling cloud services
- May be owned, managed, and operated by a business, academic, or government organization, or some combination of them
- Exists on the premises of the cloud service provider
- E.g.:
  - ❑ Amazon and Google on-demand Web applications or capacity
  - ❑ Yahoo mail
  - ❑ Facebook or LinkedIn social media applications


Cloud Provider's Public Cloud
Other clients accessing cloud
Enterprise clients accessing public cloud from within the enterprise secure security perimeter
Internet or other non-secured link
Enterprise Network

Public Cloud (contd.)

- Public clouds are inexpensive and can scale to meet needs
- However, they:
  - ❑provide no or lower service level agreements (SLAs) and may not offer the guarantees against data loss or corruption found with private or hybrid cloud offerings
  - ❑do not necessarily provide for compliance with privacy laws, which remain the responsibility of the subscriber or corporate end user

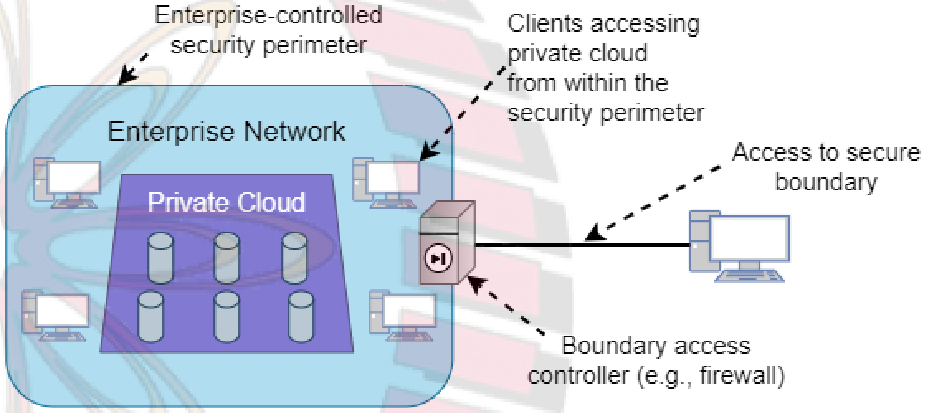

Cloud Provider's Public Cloud
Other clients accessing cloud
Enterprise clients accessing public cloud from within the enterprise secure security perimeter
Internet or other non-secured link
Enterprise Network

Private Cloud

- Implemented within the internal IT environment of the organization
- Organization may choose to:
  - ❑manage the cloud in house or
  - ❑contract the management function to a third party
- Cloud servers and storage devices may exist on premise or off premise
- E.g. services delivered through private clouds:
  - ❑Database on demand
  - ❑Email on demand
  - ❑Storage on demand

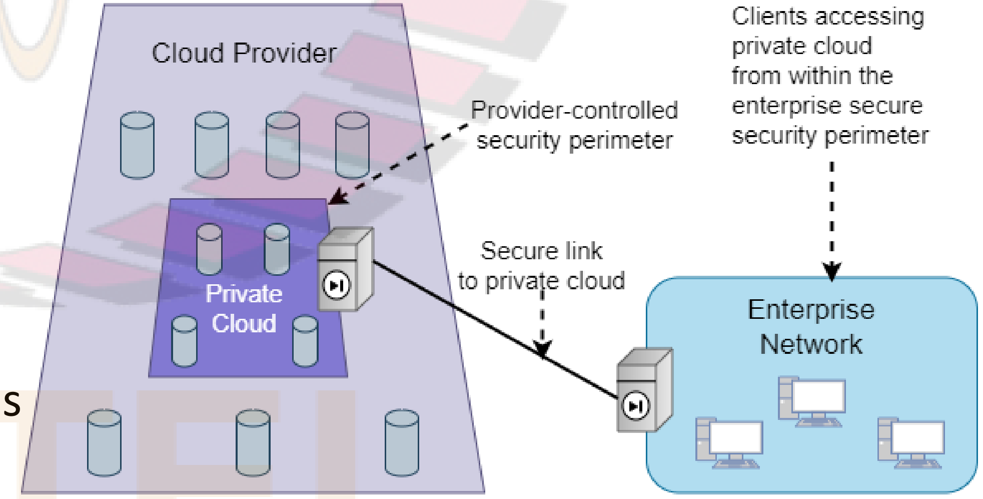
Private Cloud (contd.)

- Fig. illustrates the two typical private cloud configurations
- On-premises private cloud:
  - ❑Consists of an interconnected collection of servers and data storage devices hosting enterprise applications and data
  - ❑Local workstations have access to cloud resources from within the enterprise security perimeter
  - ❑Remote users (e.g., from satellite offices, working from home, travelling, etc.) have access through a secure link, e.g., VPN
- Outsourced private cloud:
  - ❑Cloud provider establishes and maintains the private cloud
  - ❑Consists of dedicated infrastructure resources not shared with other cloud provider clients
  - ❑Typically, a secure link between boundary controllers (e.g., dedicated leased line, VPN over Internet) provides communications between enterprise client systems and the private cloud



Enterprise-controlled security perimeter
Clients accessing private cloud from within the security perimeter
Enterprise Network
Private Cloud
Access to secure boundary
Boundary access controller (e.g., firewall)

(a) On-premises private cloud



Cloud Provider
Provider-controlled security perimeter
Clients accessing private cloud from within the enterprise secure security perimeter
Private Cloud
Secure link to private cloud
Enterprise Network

(b) Outsourced private cloud

Community Cloud

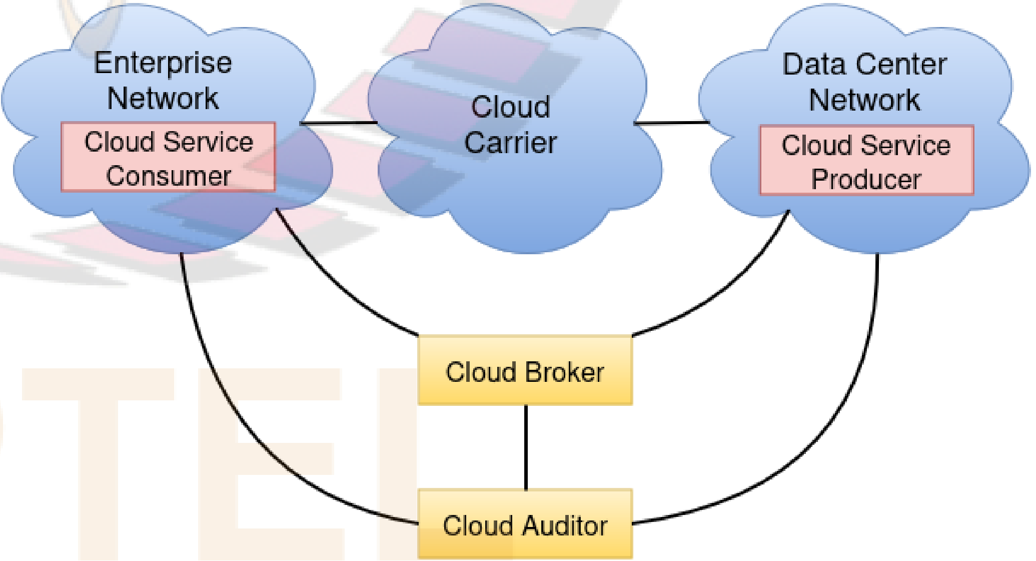
- Shares characteristics of private and public clouds
- Like a private cloud, it has restricted access
- Like a public cloud, the cloud resources are shared among a number of independent organizations
- The organizations that share the community cloud have similar requirements and, typically, a need to exchange data with each other
- E.g.: healthcare industry uses the community cloud concept

Hybrid Cloud

- 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 (e.g., for load balancing between clouds)
- Sensitive information can be placed in a private area of the cloud
- Less sensitive data can be placed in the public cloud

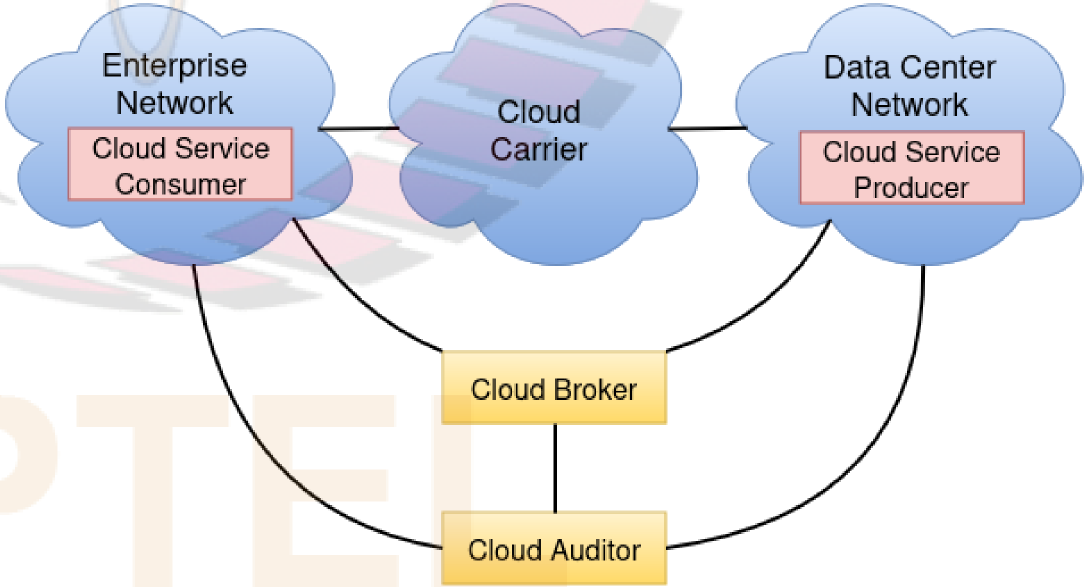
Cloud Computing Reference Architecture

- There are five major actors, which are as follows
- **Cloud Service Customer (CSC)**:
  - ❑Person or organization that maintains a business relationship with, and uses services from, cloud providers
- **Cloud Service Provider (CSP)**:
  - ❑Person, organization, or entity responsible for making a cloud service available to interested parties
- **Cloud Auditor**:
  - ❑Party that can conduct independent assessment of cloud services, information system operations, performance, and security of cloud implementation
- **Cloud Broker**:
  - ❑Entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between CSPs and cloud consumers
- **Cloud Carrier**:
  - ❑ Intermediary that provides connectivity and transport of cloud services from CSPs to cloud consumers



Cloud Computing Reference Architecture: Additional Details

- **Cloud Carrier**:
  - ❑ is a networking facility that provides connectivity and transport of cloud services between CSCs and CSPs
  - ❑ Typically, a CSP will set up SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to CSCs
- **Cloud Broker**:
  - ❑ Useful when cloud services are too complex for a cloud consumer to easily manage
  - ❑ Following areas of support may be offered by cloud broker:
    - ○ *Service intermediation*: value-added services, such as identity management, performance reporting, and enhanced security
    - ○ *Service aggregation*: broker combines multiple cloud services to meet consumer needs not addressed by a single CSP, or to optimize performance or minimize cost
- **Cloud Auditor**:
  - ❑ Can evaluate the services provided by CSP in terms of security controls, privacy impact, performance, etc.
  - ❑ Auditor is an independent entity that can assure that the CSP conforms to a set of standards



Enterprise Network
Cloud Service Consumer
Cloud Carrier
Data Center Network
Cloud Service Producer
Cloud Broker
Cloud Auditor