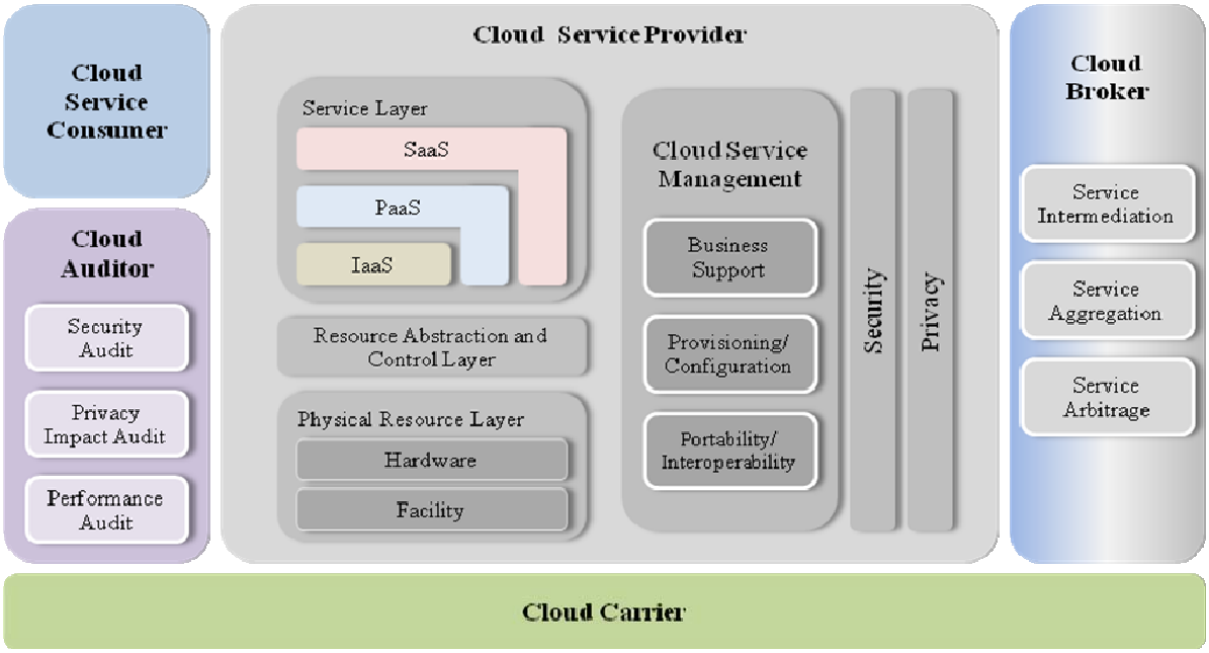
Day 2

“CLOUD SECURITY”

NIST Cloud Computing Reference Architecture

The NIST Cloud Computing Reference Architecture, developed by the National Institute of Standards and Technology (NIST), provides a high-level framework for understanding cloud computing roles, responsibilities, and components. It promotes standardization, interoperability, and secure deployment.



Key Components and Roles:

1. Cloud Consumer
    a. Uses cloud services (IaaS, PaaS, SaaS).
    b. Interacts with service management interfaces.
2. Cloud Provider
    a. Delivers cloud services (computing, storage, networking).
    b. Manages infrastructure and service provisioning.
3. Cloud Broker
    a. Acts as an intermediary between consumer and provider.
    b. Manages service delivery, aggregation, and customization.
4. Cloud Carrier
    a. Provides connectivity and transport of services between provider and consumer.
    b. Ensures secure and reliable access to cloud resources.
5. Cloud Auditor
    a. Evaluates cloud services’ security, compliance, and performance.
    b. Provides independent assessment and monitoring.

Core Security Objectives:

The core security objectives of an organization while migrating its workloads to the cloud environment should be the following:

1. Data Security- it means the data be encrypted while transferring to the cloud.
2. Compliance-Data should be classified on the basis of standard compliance.
3. Cost-it should be minimal cost.
4. Scalability-security concerns should not hamper scalability.

Cloud Security Concerns:

1. Security controls and compliance in cloud environments are similar to traditional IT setups, but follow a shared responsibility model between the provider and consumer.
2. Data security is a major concern, as critical data may be geographically dispersed and beyond the full control of the organization.
3. Additional risks arise based on deployment models, operational practices, and underlying cloud technologies, making cloud security more complex.

Cloud Security Issues:

1. Security Categories

- **Cloud Providers**: Must secure physical infrastructure against external threats and natural disasters to ensure service availability.
- **Cloud Consumers**: Face concerns over **data security, integrity, and regulatory compliance** due to dispersed data storage.

2. Security Models

- **SaaS**: Vulnerable to **identity theft, unauthorized data access, and data breaches**.
- **PaaS**: Susceptible to **phishing attacks, brute-force attacks**, and code injection risks.
- **IaaS**: Exposed to **data loss, compliance issues**, and insecure virtual environments.

3. Security Dimensions

- **Vulnerabilities**: Caused by **misconfiguration, weak access control**, and unpatched systems.
- **Risks**: Include **identity theft, malware, and compliance violations**.
- **Threats**: Include **data loss, DDoS attacks, and service disruptions**.

Core Cloud Security Risk, Threats, and Vulnerabilities:

- Unknown risk profiles prevent organizations from identifying and mitigating potential threats effectively.
- Account hijacking, data loss, insecure APIs, and insider threats are major cloud-specific threats.
- Vulnerabilities include weak access controls, lack of MFA, shared infrastructure flaws, and improper cloud configurations.

--The End--