Cloud Computing

Cloud computing is the on-demand delivery of IT resources—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet. Instead of owning, operating, and maintaining your own physical data centers and servers, you can access these services from a cloud provider like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud. This model typically follows a "pay-as-you-go" pricing structure, meaning you only pay for the resources you consume.

Characteristics of Cloud Computing

The essential characteristics that define a cloud computing environment are:

1. **On-Demand Self-Service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
2. **Broad Network Access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
3. **Resource Pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources.
4. **Rapid Elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
5. **Measured Service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and the consumer of the utilized service.

Cloud Deployment Models (Types of Cloud)

This describes the environment in which the cloud services are deployed.

1. ## Public Cloud:

   The cloud infrastructure is provisioned for open use by the general public. It is owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

   - **Examples:** Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

2. ## Private Cloud:

   The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

3. ## Hybrid Cloud:

   The cloud infrastructure is a composition of two or more distinct cloud infrastructures (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., cloud bursting for load balancing between clouds).

4. ## Community Cloud:

   The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

Cloud Service Models

This defines the different levels of service and management you can obtain from a cloud provider.

1. ## Infrastructure as a Service (IaaS):
   - It Provides the most basic building blocks for cloud IT. It offers access to networking features, computers (virtual or on dedicated hardware), and data

storage space. IaaS gives you the highest level of flexibility and management control over your IT resources.

- We can manage Applications, Data, Runtime, Middleware, Operating System.
- Provider manages Virtualization, Servers, Storage, Networking.
- Examples: Amazon EC2, Google Compute Engine, Microsoft Azure Virtual Machines.

2. Platform as a Service (PaaS):
   - **It** removes the need for you to manage the underlying infrastructure (usually hardware and operating systems) and allows you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, or patching.
   - We can manage Applications, Data.
   - Provider manages Runtime, Middleware, Operating System, Virtualization, Servers, Storage, Networking.
   - Examples: AWS Elastic Beanstalk, Heroku, Google App Engine, Microsoft Azure App Services.
3. Software as a Service (SaaS):
   - It Provides you with a completed product that is run and managed by the service provider. In most cases, people referring to SaaS are referring to end-user applications. With a SaaS offering, you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece of software.
   - We don’t manage anything. It's a fully managed service.
   - Provider manages Everything from the application down to the networking.
   - Examples: Google Workspace, Microsoft Office 365, Salesforce, Dropbox.

Key Cloud Providers

There are three major cloud providers, often referred to as "hyperscalers".

1. Amazon Web Services (AWS):
   - **Provider:** Amazon.
   - It was launched in 2006, AWS is the oldest and most dominant player in the cloud market. It has the largest global market share and offers an extensive and mature portfolio of over 200 fully featured services from data centers globally.
   - Key Services are:
     - **Compute:** EC2 (Elastic Compute Cloud) for virtual servers.
     - **Storage:** S3 (Simple Storage Service) for object storage.
     - **Database:** RDS (Relational Database Service), DynamoDB (NoSQL).

        - **Networking:** VPC (Virtual Private Cloud).

2. Microsoft Azure:
    - **Provider:** Microsoft.
    - It was launched in 2010, Azure is the second-largest cloud provider and is growing rapidly. Its key strength lies in its integration with Microsoft's existing enterprise software ecosystem (like Windows Server, Office 365, and Active Directory), making it a popular choice for large enterprises that are already heavily invested in Microsoft products.
    - **Key Services:**
        - **Compute:** Azure Virtual Machines.
        - **Storage:** Azure Blob Storage.
        - **Database:** Azure SQL Database, Cosmos DB.
        - **Identity:** Azure Active Directory (Azure AD).
3. Google Cloud Platform (GCP):
    - **Provider:** Google.
    - It was launched in 2008, GCP is the third major player. It is highly regarded for its expertise in areas like big data, machine learning (ML), artificial intelligence (AI), analytics, and containerization (especially with its development of Kubernetes). It leverages the same infrastructure that powers Google's own products like Search and YouTube.
    - **Key Services:**
        - **Compute:** Compute Engine.
        - **Storage:** Cloud Storage.
        - **Database:** Cloud SQL, Bigtable.
        - **Big Data & ML:** BigQuery (data warehousing), AI Platform.

Other notable providers include Alibaba Cloud, Oracle Cloud Infrastructure (OCI), and IBM Cloud.

Cloud Security

Cloud security is a collection of policies, technologies, controls, and procedures designed to protect cloud-based systems, data, and infrastructure from threats. It is a critical aspect of cloud computing.

Shared Responsibility Model

This is a fundamental concept in cloud security. It defines the division of security obligations between the cloud service provider (CSP) and the customer.

- **Provider's Responsibility (Security *of* the Cloud):** The cloud service provider is responsible for protecting the infrastructure that runs all of the services offered. This includes the hardware, software, networking, and physical facilities that run the cloud services. For example, they are responsible for the physical security of the data centers.

- **Customer's Responsibility (Security *in* the Cloud):** The customer is responsible for managing and securing their data, applications, identity, and access management. This includes configuring network firewalls, encrypting data, managing user access, and securing the operating systems and applications they deploy.

The extent of the customer's responsibility varies by service model:

- **In Infrastructure as a Service** the customer has the most responsibility, including securing the operating system, middleware, and application data.
- **In Platform as a Service** the customer is responsible for securing their applications and data, while the provider manages the platform (OS, runtime, etc.).
- **In Software as a Service** the customer has the least responsibility, primarily managing user access and data within the application.

Key Pillars of Cloud Security

1. **Identity and Access Management (IAM)**
2. **Data Protection**
3. **Network Security**
4. **Threat Detection and Monitoring**
5. **Compliance**