Name: Prathamesh Arvind Jadhav

UNIT-3 – Cloud Architecture, Services and Storage

Cloud Architecture:

What is Cloud Architecture?

Cloud architecture refers to the **components** and **subcomponents** required for cloud computing. It's the structure that brings together **databases, software capabilities, applications, and services** that are accessed over the internet.

Just like building architecture has a foundation, walls, and a roof — cloud architecture has layers and components that work together to deliver services.

□ Key Components of Cloud Architecture

1. Front-End (Client Side)

This is what users interact with — typically a **web browser or app**.

- Examples: Chrome browser, mobile apps
- Interfaces with: Web servers, APIs
- Technologies: HTML, CSS, JavaScript

2. Back-End (Server Side)

This is the backbone of cloud architecture. It manages all **resources and services**.

Core Elements:

- **Servers** – Provide computing power (physical or virtual).
- **Storage** – Stores data persistently (e.g., Amazon S3, Google Cloud Storage).
- **Databases** – Manage structured data (e.g., MySQL, MongoDB).
- **Application Logic** – The business logic layer that performs processing.
- **Virtual Machines & Containers** – Isolated environments to run applications.

3. Cloud-Based Delivery Models

a. IaaS (Infrastructure as a Service)

You get virtual servers, storage, and networking.

- Example: AWS EC2, Google Compute Engine

b. PaaS (Platform as a Service)

You get an environment for app development without managing infrastructure.

- Example: Google App Engine, Heroku

c. SaaS (Software as a Service)

You use ready-made software via a browser.

- Example: Google Workspace, Dropbox, Salesforce

4. Cloud Deployment Models

Model	Description	Example
Public Cloud	Services offered over the public internet	AWS, Azure, GCP
Private Cloud	Services used exclusively by one organization	VMware, OpenStack
Hybrid Cloud	Mix of public and private	AWS Outposts, Azure Stack
Multi-cloud	Using services from multiple cloud providers	AWS + Azure + GCP

 Building Blocks of Cloud Architecture

1. Virtualization

Enables running multiple operating systems and applications on a single machine.

2. Scalability

The ability to automatically **scale resources** up or down based on demand.

3. Elasticity

Dynamic allocation of resources to handle varying workloads.

4. Redundancy and Fault Tolerance

Backup systems and failovers ensure the system is available even if parts fail.

5. Load Balancing

Distributes incoming traffic across multiple servers to ensure no single server is overwhelmed.

6. Security

Includes identity management, encryption, firewalls, and compliance policies.

Name: Prathamesh Arvind Jadhav

□ Benefits of Cloud Architecture

- □ Cost-effective (pay-as-you-go)
- □ Scalable and Elastic
- □ High Availability
- □ Disaster Recovery
- □ Fast Deployment

□ Security in Cloud Architecture

- Authentication (OAuth, IAM roles)
- Authorization (Access Control Lists)
- Encryption (in-transit and at-rest)
- Monitoring and Incident Response

Services and Storage Layered Cloud Architecture Design:

What is Layered Cloud Architecture?

Layered architecture in the cloud separates concerns into different layers for **modularity**, **scalability**, **manageability**, and **security**. Each layer has a specific function and interacts with others.

□ Major Layers in Cloud Architecture (Focused on Services & Storage)

Here's a breakdown of a **typical layered cloud architecture** with focus on **Services** and **Storage**:

□ 1. Infrastructure Layer (Base Layer)

□ Purpose:

Provides the physical or virtual **compute**, **network**, and **storage resources**.

□ Components:

- Physical servers
- Virtual Machines (VMs)
- Networking (routers, switches, firewalls)
- Disk storage (block storage like Amazon EBS)

 Think of it as:

The engine room — everything runs on this foundation.

---

 2. Storage Layer (Data Storage & Management)

 Purpose:

Handles **persistent storage**, **data organization**, and **data lifecycle**.

 Types of Storage:

Type	Description	Examples
Block Storage	Like hard drives	Amazon EBS, Azure Disks
File Storage	Hierarchical, file-based	Amazon EFS, Google Filestore
Object Storage	Store as objects (scalable & distributed)	Amazon S3, Azure Blob
Database Storage	Structured or unstructured	Amazon RDS, MongoDB Atlas

 Think of it as:

The digital warehouse where all data is kept and accessed by apps.

---

 3. Platform Layer (Platform Services)

 Purpose:

Provides **development tools**, **middleware**, and **runtime environments**.

 Services:

- Application hosting (e.g., AWS Elastic Beanstalk, Azure App Services)
- Container orchestration (e.g., Kubernetes, ECS, AKS)
- DevOps tools (CI/CD pipelines)
- API gateways and service mesh
- Data analytics platforms

 Think of it as:

The builder’s workshop – tools to build, run, and manage apps.

Name: Prathamesh Arvind Jadhav

□ 4. Service Layer (Cloud Services / SaaS Layer)

□ **Purpose:**

Provides **user-facing services** and **business logic**.

□ **Categories:**

Service Type	Examples
Compute	AWS Lambda, Azure Functions, EC2
Storage	S3, Blob Storage
Database	Amazon RDS, Firebase
AI/ML	AWS SageMaker, Google Vertex AI
Monitoring	CloudWatch, Datadog
Messaging	SNS, SQS, Pub/Sub

□ **Think of it as:**

The app store – cloud-native services available to developers and users.

□ 5. Management Layer

□ **Purpose:**

Enables **monitoring**, **orchestration**, **security**, and **resource management**.

□ **Includes:**

- Identity and Access Management (IAM)
- Billing and Cost Management
- Logs and Metrics
- Auto-scaling and Load Balancing

□ **Think of it as:**

The control tower — overseeing everything that happens in the cloud.

6. User Layer (Front-End)

□ **Purpose:**

User interfaces to interact with services — web/mobile apps, dashboards, terminals.

Name: Prathamesh Arvind Jadhav

Security and Compliance Across Layers

Security isn't a single layer — it spans **all layers**:

- Data encryption at storage and in transit
- Access controls at service and platform levels
- Firewall rules and network segmentation at infrastructure level

---

Benefits of Layered Architecture

- **Separation of concerns** (clear boundaries)
- **Easier scalability** (scale specific layers)
- **Better security management**
- **Simplified development and maintenance**

NIST Cloud Computing Reference Architecture

Introduction

The **National Institute of Standards and Technology (NIST)** defines a **Cloud Computing Reference Architecture (CCRA)** to provide a structured framework for understanding cloud computing services and their interactions. It helps organizations adopt cloud technology by defining **key roles, components, and interactions** within a cloud environment.

Key Components of NIST Cloud Computing Reference Architecture

The NIST model consists of **five major actors**:

1.Cloud Consumer

- The **end-user or business** that uses cloud services.
- Requests and manages cloud resources like computing, storage, and applications.
- Example: A company using **AWS EC2 instances** for hosting applications.

2.Cloud Provider

- The entity that **delivers cloud services** (IaaS, PaaS, SaaS) to consumers.
- Manages infrastructure, security, and availability.
- Example: **Amazon Web Services (AWS), Microsoft Azure, Google Cloud**.

3.Cloud Auditor

- An **independent party** that assesses cloud security, compliance, and performance.
- Ensures cloud providers meet industry standards (ISO 27001, GDPR, etc.).
- Example: **Third-party security firms conducting cloud audits**.

4.Cloud Broker

- Acts as an **intermediary** between cloud consumers and providers.
- Helps in **service selection, cost optimization, and integration**.
- Example: **Cloud management platforms like RightScale and Cloudability**.

5.Cloud Carrier

- The **network provider** that connects cloud consumers and providers.
- Ensures secure and reliable **data transmission**.
- Example: **Internet Service Providers (ISPs), VPN providers**.

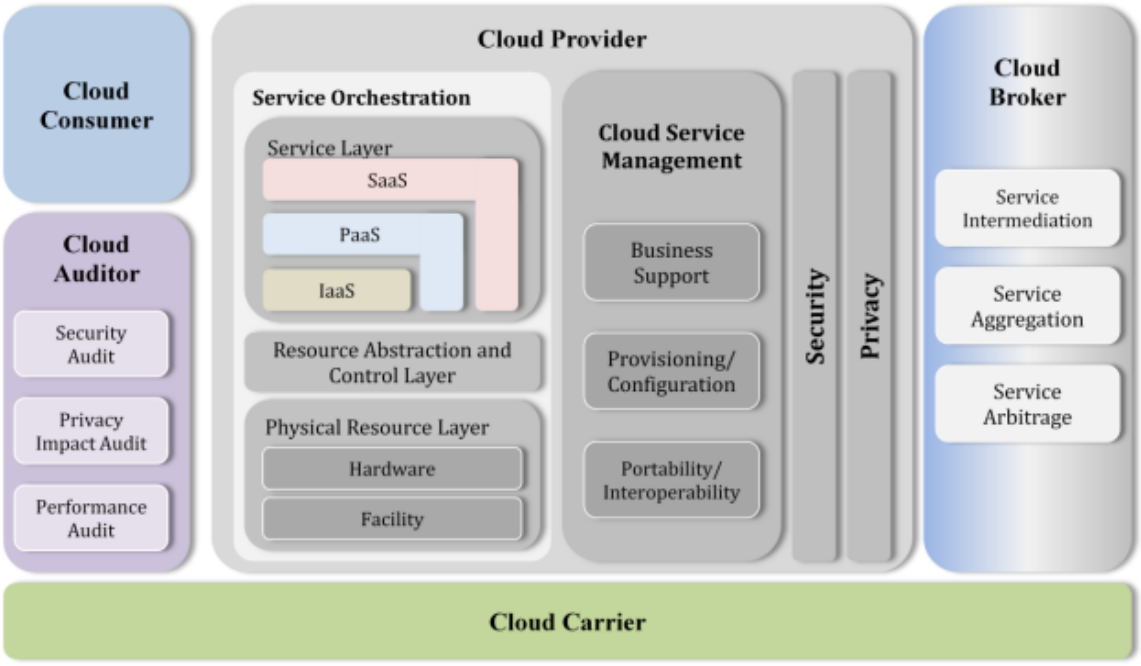

Figure 1: The Conceptual Reference Model

Cloud Deployment Models

Introduction

A **Cloud Deployment Model** defines how cloud services are hosted, managed, and accessed by users. It determines the **ownership, security, and accessibility** of cloud resources. There are four primary cloud deployment models:

Name: Prathamesh Arvind Jadhav

---

1. Public Cloud

✔ Owned and operated by **third-party cloud providers** (AWS, Google Cloud, Microsoft Azure).
✔ Resources like servers and storage are shared **among multiple users (multi-tenancy)**.
✔ **Highly scalable** with pay-as-you-go pricing.

 Use Cases:
✔ Website hosting
✔ SaaS applications (Google Drive, Microsoft 365)
✔ Cloud-based email services

 Advantages:
✔ Cost-effective (no hardware maintenance)
✔ Easy scalability
✔ High availability

 Disadvantages:
 Less control over security
 Performance depends on network speed

---

2. Private Cloud

✔ Owned and used **exclusively** by a **single organization**.
✔ Provides **higher security, control, and customization**.
✔ Can be hosted **on-premises** or by a third-party provider.

 Use Cases:
✔ Financial institutions
✔ Government organizations
✔ Enterprises needing **strict data privacy**

 Advantages:
✔ High security and compliance
✔ Better performance and reliability

 Disadvantages:
 High cost of maintenance
 Requires IT expertise

Name: Prathamesh Arvind Jadhav

---

3. Hybrid Cloud

✔ **Combination of public and private clouds** for flexibility and cost savings.
✔ Sensitive data is kept in **private cloud**, while less critical workloads use **public cloud**.
✔ Supports **cloud bursting** (scaling workloads to the public cloud during high demand).

 Use Cases:
✔ Businesses needing **secure data storage** but **scalable computing power**
✔ Disaster recovery and backup

 Advantages:
✔ Optimized cost and performance
✔ Better flexibility and scalability

 Disadvantages:
 Complex management and integration
 Higher security risks than private cloud

---

4. Community Cloud

✔ Shared by **multiple organizations** with common concerns (security, compliance).
✔ Managed by one or more organizations or a third party.

 Use Cases:
✔ Government agencies
✔ Healthcare institutions with shared regulations

 Advantages:
✔ Improved security compared to the public cloud
✔ Cost-sharing among users

 Disadvantages:
 Limited scalability
 Complex governance

Name: Prathamesh Arvind Jadhav

Cloud Service Models

Introduction

Cloud computing provides three primary **service models** that define how resources are delivered and managed over the internet. These are:

1.**Infrastructure as a Service (IaaS)**
2.**Platform as a Service (PaaS)**
3.**Software as a Service (SaaS)**

Each model offers a different level of control, flexibility, and management for users.

---

1. Infrastructure as a Service (IaaS)

✔ Provides **virtualized computing resources** over the internet.
✔ Includes **virtual machines, storage, networking, and operating systems**.
✔ Users control the infrastructure but outsource hardware maintenance.

 Examples:
✔ **Amazon Web Services (AWS) EC2**
✔ **Microsoft Azure Virtual Machines**
✔ **Google Cloud Compute Engine**

 Use Cases:
✔ Hosting websites and applications
✔ Running big data and analytics workloads
✔ Disaster recovery solutions

 Advantages:
✔ **Scalable and flexible** resources
✔ **Cost-efficient (pay-as-you-go model)**
✔ **No need to maintain physical hardware**

 Disadvantages:
 Requires technical expertise for management
 Security concerns (as infrastructure is managed by third-party providers)

---

2. Platform as a Service (PaaS)

✔ Provides a **managed platform for developers** to build, test, and deploy applications.
✔ Includes **operating systems, development tools, databases, and runtime environments**.
✔ Developers focus on coding without managing underlying infrastructure.

 Examples:
✔ **Google App Engine**
✔ **Microsoft Azure App Services**
✔ **AWS Elastic Beanstalk**

 Use Cases:
✔ Web and mobile application development
✔ API development and management
✔ Automating DevOps tasks

 Advantages:
✔ **Faster development and deployment**
✔ **No need to manage servers and databases**
✔ **Automatic scaling and security updates**

 Disadvantages:
 Limited control over underlying infrastructure
 Compatibility issues with legacy applications

---

3. Software as a Service (SaaS)

✔ Provides **ready-to-use software applications** over the internet.
✔ Users **don't need to install or maintain software**; everything is managed by the provider.
✔ Available via **web browsers** on any device.

 Examples:
✔ **Google Workspace (Docs, Sheets, Gmail)**
✔ **Microsoft Office 365**
✔ **Salesforce CRM**

 Use Cases:
✔ Cloud-based email services
✔ Customer relationship management (CRM)
✔ Collaboration and productivity tools

 Advantages:
✔ **No installation or maintenance required**

✔ **Accessible from anywhere**
✔ **Automatic updates and security patches**

 Disadvantages:
 Limited customization options
 Data privacy and security concerns

Cloud Storage and Storage Providers

Introduction

Cloud storage is a **service that allows users to store data remotely** and access it via the internet. It eliminates the need for physical storage devices and provides **scalability, security, and accessibility**.

Cloud storage providers **manage the infrastructure**, ensuring data availability, backup, and disaster recovery.

Key Features of Cloud Storage

✔ **Scalability** – Easily increase or decrease storage space as needed.
✔ **Accessibility** – Access data from anywhere using an internet connection.
✔ **Cost Efficiency** – Pay for only the storage space used.
✔ **Security** – Data is encrypted and protected from cyber threats.
✔ **Backup and Recovery** – Automatic backups ensure data is never lost.

Types of Cloud Storage

1.Object Storage

- Stores data as objects in a **flat address space**.
- Used for storing **unstructured data** like images, videos, and backups.
- Example: **Amazon S3, Google Cloud Storage, Azure Blob Storage**

2.File Storage

- Uses a **hierarchical structure (folders and files)** like traditional storage.
- Supports **file-sharing applications** and **network file systems (NFS, SMB)**.
- Example: **Google Drive, Dropbox, OneDrive**

Name: Prathamesh Arvind Jadhav

3.Block Storage

- Stores data in **fixed-size blocks**, similar to hard drives.
- Used for **database storage and virtual machine disks**.
- Example: **Amazon EBS (Elastic Block Store), Azure Disk Storage**

Popular Cloud Storage Providers

1.Amazon Web Services (AWS) - S3 (Simple Storage Service)

✔ Highly scalable **object storage**.
✔ Supports **backup, disaster recovery, and data archiving**.
✔ Integrated with other AWS services.

2.Google Cloud Storage

✔ Provides **multi-regional storage** with high availability.
✔ Offers **Coldline and Nearline storage** for cost-effective archiving.
✔ Supports machine learning and data analytics.

3.Microsoft Azure Storage

✔ Offers **Blob Storage (object storage)**, **File Storage**, and **Disk Storage**.
✔ Ideal for enterprise applications and hybrid cloud solutions.
✔ Secure encryption and compliance with industry standards.

4.Dropbox

✔ Simple **file-based cloud storage** for individuals and teams.
✔ Supports **file synchronization and sharing**.
✔ Used for collaboration and document management.

5.Google Drive

✔ Personal and business **file storage and sharing**.
✔ Offers **15GB of free storage** with integration into Google Workspace.
✔ Supports **collaboration with real-time editing**.

Advantages of Cloud Storage

Name: Prathamesh Arvind Jadhav

✔ **No hardware maintenance** – No need to invest in physical storage devices.
✔ **Scalability** – Easily upgrade or downgrade storage as per needs.
✔ **Data protection** – Encrypted storage with backup and recovery options.
✔ **Collaboration** – Multiple users can access and share data from anywhere.

Disadvantages of Cloud Storage

 Internet dependency – Requires a stable internet connection.
 Security risks – Potential vulnerabilities if not properly managed.
 Ongoing costs – Long-term cloud storage may be expensive compared to local storage.