Unit-1 Cloud Layers

Application Layer: End-user applications and SaaS solutions.
Platform Layer: Development and middleware services (PaaS).
Infrastructure Layer: Virtualized computing, storage, and network services (IaaS).
Physical Layer: Underlying hardware, data centers, and networking infrastructure.

Ethical Issues in Cloud Computing

Cloud computing brings numerous benefits but also raises significant ethical concerns:

Privacy & Data Protection
Cloud providers store vast amounts of personal and sensitive data, raising concerns about unauthorized access, misuse, and surveillance. Ethical questions arise regarding who owns the data—the user, the cloud provider, or the government? Regulations like GDPR and CCPA attempt to enforce ethical data handling, but compliance varies.
Security & Cybercrime
Ethical issues arise when cloud service providers fail to implement adequate security measures, leading to data breaches and cyberattacks.
Ransomware attacks and unauthorized monitoring by third parties pose serious ethical risks.
Vendor Lock-in & Monopoly Concerns
Large cloud providers (AWS, Google Cloud, Azure) dominate the industry, raising concerns about monopoly power and lack of fair competition.
Vendor lock-in limits customer choices, forcing them to stay with a provider even if costs increase or services degrade.
Environmental Impact
Cloud data centers consume massive amounts of electricity, contributing to carbon emissions and electronic waste Ethical responsibility demands providers shift toward renewable energy and green computing strategies.

AI & Algorithmic Bias

Cloud services often integrate AI and machine learning, which can amplify bias in decision-making (e.g., discriminatory hiring algorithms). Ethical cloud computing requires transparency and fairness in AI model training and data processing.

Future of Cloud Computing

1. Edge Computing & Decentralization

Edge computing reduces latency by processing data closer to the user.Will enable faster real-time applications (e.g., autonomous vehicles, smart cities).

2. AI & Cloud Integration

AI-powered cloud automation will enhance cybersecurity, workload management, and analytics.Cloud services will embed AI-driven decision-making and forecasting capabilities.

3. Quantum Computing in the Cloud

Companies like IBM and Google are investing in quantum cloud computing.This will accelerate complex computations in drug discovery, encryption, and AI.

4. Sustainable & Green Cloud Computing

Providers will adopt renewable energy and carbon-neutral data centers.Energy-efficient liquid cooling and serverless computing will become more common.

5. Hybrid & Multi-Cloud Strategies

Businesses will increasingly adopt multi-cloud strategies to avoid vendor lock-in.Cloud interoperability will improve, enabling seamless cross-platform integration.

Ubiquitous Cloud and the Internet of Things (IoT)

The Ubiquitous Cloud refers to cloud computing anytime, anywhere, seamlessly integrating with devices like smartphones, IoT sensors, and autonomous systems.

1. IoT and Cloud Integration

IoT generates massive amounts of real-time data, requiring cloud storage and processing.Cloud platforms (AWS IoT, Azure IoT Hub, Google Cloud IoT) enable remote monitoring, automation, and analytics.

2. Fog Computing & Edge Processing

Fog computing processes IoT data closer to the source to reduce latency and bandwidth usage.Useful in applications like smart homes, industrial automation, and connected healthcare.

3. Smart Cities & Cloud-Based AI

IoT devices in traffic systems, surveillance, and utilities use cloud AI for optimization.Cloud-based AI analyzes data for predictive maintenance, energy savings, and security.

4. Security Challenges in IoT & Cloud

IoT devices have weak security protocols, making them vulnerable to attacks.Cloud-based AI-driven security will enhance IoT device authentication and encryption.

Cloud computing layers

Physical Layer

- Foundation layer of the cloud infrastructure.
- Specifies entities that operate at this layer : Compute systems, network devices and storage devices. Operating environment, protocol, tools and processes.

Functions of physical layer : Executes requests generated by the virtualization and control layer.

Virtual Layer

- Deployed on the physical layer.
- Specifies entities that operate at this layer : Virtualization software, resource pools, virtual resources.

Functions of virtual layer : Abstracts physical resources and makes them appear as virtual resources (enables multitenant environment). Executes the requests generated by control layer.

Control Layer

- Deployed either on virtual layer or on physical layer

- Specifies entities that operate at this layer : control software
- **Functions of control layer** : Enables resource configuration, resource pool, configuration and resource provisioning. Executes requests generated by **service layer.** Exposes resources to and supports the service layer. Collaborates with the virtualization software and enables resource pooling and creating virtual resources, dynamic allocation and optimizing utilization of resources.

Service Orchestration Layer

- Specifies the entites that operate at this layer : Orchestration software.

Functions of orchestration layer : Provides workflows for executing automated tasks. Interacts with various entities to invoke provisionning tasks.

Service Layer

- Consumers interact and consume cloud resources via thos layer.
- Specifies the entities that operate at this layer : Service catalog and self-service portal.
-

Functions of service layer : Store information about cloud services in service catalog and presents them to the consumers. Enables consumers to access and manage cloud services via a self-service portal.

Cross-layer function

Business continuity

- Specifies adoption of proactive and reactive measures to mitigate the impact of downtime.
- Enables ensuring the availability of services in line with SLA.
- Supports all the layers to provide uninterrupted services.

Security

- Specifies the adoption of : Administrative mechanisms (security and personnel policies, standard procedures to direct safe execution of operations) and technical mechanisms (firewall, intrusion detection and prevention systems, antivirus).
- Deploys security mechanisms to meet GRC requirements.
- Supports all the layers to provide secure services.

GRC (Governance, Risk, and Compliance) Requirements in Cloud Computing

Governance, Risk, and Compliance (GRC) in cloud computing refers to the policies, frameworks, and controls necessary to ensure security, regulatory compliance, and risk management in cloud environments. Cloud GRC ensures that organizations meet legal, regulatory, and business objectives while maintaining security and operational efficiency.

Key Governance Aspects:

Cloud Strategy & Policies: Define cloud adoption, usage policies, and service models (SaaS, PaaS, IaaS).

Roles & Responsibilities: Assign clear responsibilities for cloud management (e.g., IT admins, security teams).

Data Ownership & Accountability: Determine who controls, accesses, and manages cloud data.

Resource Management: Establish cost controls, performance monitoring, and provisioning policies.

Cloud Provider Oversight: Evaluate and monitor cloud vendors for compliance with service agreements (SLAs).

Service Management

Specifies adoption of activities related to service portfolio management and service operation management.

Service portfolio management :

• Define the service roadmap, service features, and service levels

• Assess and prioritize where investments across the service portfolio are most needed

• Establish budgeting and pricing

• Deal with consumers in supporting activities such as taking orders, processing bills, and collecting payments

Service operation management :

- Enables infrastructure configuration and resource provisioning
- Enable problem resolution
- Enables capacity and availability management
- Enables compliance conformance

- Enables monitoring cloud services and their constituent elements

1. Cloud Service Models (SPI Model)

1.1 Software as a Service (SaaS)

Provides fully functional software applications over the internet.
Users access the service via web browsers without installing software.
Examples: Google Workspace, Microsoft 365, Salesforce.

1.2 Platform as a Service (PaaS)

Provides a platform for developers to build, test, and deploy applications.Eliminates the need to manage infrastructure.
Examples: Microsoft Azure App Services, Google App Engine, AWS Lambda.

1.3 Infrastructure as a Service (IaaS)

Provides virtualized computing resources (servers, storage, networking).Users control OS, applications, and configurations.

Examples: AWS EC2, Google Compute Engine, Microsoft Azure Virtual Machines.

1.4 Other Cloud Service Models

Function as a Service (FaaS): Serverless computing model (e.g., AWS Lambda).

Database as a Service (DBaaS): Cloud-managed databases (e.g., Amazon RDS).

Storage as a Service (STaaS): Cloud-based storage solutions (e.g., Google Drive, AWS S3).

2. **Data Center Design and Interconnection Network**

2.1 Data Center Design Considerations

Location: Should be in areas with stable climate, low disaster risk, and proximity to users.

Power Supply: Reliable power with backup generators and UPS systems.

Cooling Systems: Efficient cooling to manage heat from servers (e.g., liquid cooling).

Security: Physical security (biometrics, surveillance) and cybersecurity.

2.2 Data Center Tiers (Uptime Institute Classification)

Tier 1: Basic infrastructure with minimal redundancy (99.67% uptime).

Tier 2: Redundant power and cooling systems (99.75% uptime).

Tier 3: Concurrently maintainable infrastructure (99.98% uptime).

Tier 4: Fault-tolerant infrastructure with multiple redundancies (99.995% uptime).

2.3 Interconnection Network in Data Centers

Core Layer: High-speed backbone network connecting multiple data centers.
Aggregation Layer: Distributes traffic between servers and core network.
Access Layer: Connects individual servers to the network.

Networking Technologies:

Ethernet, Fiber Optic, InfiniBand for high-speed data transfer.
Software-Defined Networking (SDN): Dynamic network control and automation.
Network Function Virtualization (NFV): Virtualized network services for scalability.

3. Architectural Design of Compute and Storage Clouds

3.1 Compute Cloud Architecture

Virtualization: Uses Hypervisors (VMware, KVM, Xen) to run multiple virtual machines (VMs) on a single physical server.

Containerization: Uses Docker, Kubernetes for lightweight application deployment.

Scalability: Supports horizontal (adding more servers) and vertical (upgrading hardware) scaling.

Orchestration: Tools like Kubernetes and OpenStack manage compute resources.

3.2 Storage Cloud Architecture

Block Storage: Works like a traditional hard drive (e.g., Amazon EBS, Google Persistent Disk).

Object Storage: Stores data as objects (e.g., AWS S3, Azure Blob Storage).

File Storage: Network-based file storage (e.g., AWS EFS, Google Filestore).

Redundancy & Backup:

RAID configurations for fault tolerance.

Geo-replication for disaster recovery.

3.3 Key Components of Cloud Architecture

Front-end Layer: User interface (Web UI, Mobile App, API).

Back-end Layer: Compute resources, storage, and networking.

Middleware: Manages communication between components (e.g., API gateways, load balancers).

Security Layer: Encryption, identity & access management, firewalls.