**Cloud Provider and User Responsibilities in Cloud Security**

Cloud security is a **shared responsibility**. This means both the **cloud provider** (like AWS, Azure, GCP) and the **user or customer** (your company) have roles to play.

**Cloud Provider Responsibilities**

These are the things the **cloud provider** handles. These protections are already built into the cloud service.

**✅ Definition**

Cloud providers build security directly into their infrastructure to keep customer data and systems safe.

**🔒 1. Physical Data Centers**

The provider is responsible for securing the actual buildings and hardware where data is stored.

* They manage **who can physically enter** the data center (access control).
* They have **surveillance cameras** and security guards.
* **Environmental controls** like fire suppression and climate control are also in place.

**🌐 2. Network Infrastructure Security**

The provider protects the cloud network.

* **DDoS Protection** – Stops hackers from overwhelming your servers.
* **IDS/IPS** – Intrusion Detection/Prevention Systems to catch attacks.
* **Encrypted Data Transmission** – Keeps data secure while it moves over the internet.

**🛡 3. Compliance and Certifications**

Cloud providers follow global standards and get certified to prove they meet strict security rules (like ISO, SOC, etc.).

**User (Customer) Responsibilities**

These are the things **you** (the cloud customer) must manage to keep your environment secure.

**👤 1. Access Management**

Control **who can access** your cloud resources.

* Use **strong passwords and authentication methods**.
* Implement **MFA (Multi-Factor Authentication)**.
* Use **IAM (Identity and Access Management)** to define what users can do.
* Create and apply **access policies**.

**🔐 2. Data Encryption**

Protect your data when stored or moving across the network.

* **Encrypt at rest** (when stored) and **in transit** (while moving).
* Use tools like:
  + **AWS KMS** (Key Management Service)
  + **Azure Key Vault**

to manage encryption keys securely.

**🌍 3. Network Configuration**

Secure your virtual cloud network.

* Set up **security groups** and **firewall rules** to control traffic.
* Make sure your **VPC (Virtual Private Cloud)** is properly configured.
  + Only allow necessary traffic in and out.
  + Block everything else.