**Day 7**





**“CLOUD SECURITY”**

**Security of Physical and Environment Component:**

1. **Strict Physical Access Control & Monitoring**

* Use biometric IDs, metal detectors, surveillance cameras, and intrusion detection systems (IDS).
* Maintain detailed access logs and conduct regular audits.

1. **Environmental Safeguards & Redundancy**

* Ensure 24/7 power supply, fire detection/suppression, and climate control to prevent overheating or outages.

1. **Secure Lifecycle & Compliance Management**

* Enforce data sanitization and secure decommissioning of hardware.
* Maintain compliance with global/industry standards and automate patching and issue remediation

**Security of Management Component:**

1. **Identity & Access Management (IAM)**
   * Enforce least privilege access and multi-factor authentication (MFA).
   * Use a hierarchy of accounts: Root/Master (rarely used), Super-admin, and Service Admins with scoped permissions.
2. **Cloud Provider Responsibilities**
   * Implement perimeter security for APIs and consoles.
   * Use strong authentication standards (e.g., OAuth) and secure internal credential handling.
   * Provide granular authorization for both internal admins and customer-facing roles.
3. **Logging, Monitoring & Alerts**
   * Maintain detailed logs of user and admin actions on cloud resources.
   * Enable real-time monitoring and alerting for unusual activities, and provide log access via APIs for customers.

**Security of Network Component:**

1. **Access Control & Traffic Encryption**
   * Enforce network access control (ACLs) to limit access to VMs/services.
   * Encrypt all outbound traffic leaving physical boundaries, and authenticate traffic between VMs.
2. **Monitoring & Segmentation**
   * Use access points to monitor inbound/outbound traffic.
   * Continuously monitor network devices, firewall rules, usage, scans, and anomalies with automated tools.
   * Physically segregate networks for operations and security.
3. **Resilience & Secure Management**
   * Use geographically distributed data centers for failover.
   * Secure remote management with SSL/HTTPS to prevent tampering and eavesdropping on the management plane.

--The End--