Question3:

Security Considerations:

Write your common security practices and tools for securing cloud infrastructure and deployments. Include considerations for access control, data protection, and network security.

Answer:

Here are some common security practices and tools for securing cloud infrastructure and deployments, focusing on access control, data protection, and network security.

1. Access Control

- Implement **Least Privilege Access (LPA)** to restrict permissions to only what is necessary.
- Use **Role-Based Access Control (RBAC)** and **Attribute-Based Access Control (ABAC)** for fine-grained access control.
- Enforce **Multi-Factor Authentication (MFA)** for all privileged accounts.
- Monitor and rotate **IAM credentials**, **API keys**, and **secrets** periodically.

Tools & Services:

- **AWS IAM** – Identity and Access Management
- **HashiCorp Vault** – Secrets management
- **AWS Security Hub** – Centralized security management

2. Data Protection

- **Encrypt data at rest and in transit** using AES-256 and TLS 1.2/1.3.
- Implement **key management** with services like AWS KMS or HashiCorp Vault.
- Enable **backup and disaster recovery** strategies with automated snapshots.
- Apply **logging and monitoring** to track data access and modifications.

Tools & Services:

- **AWS KMS** – Encryption key management
- **ELK Stack / AWS CloudTrail –** Logging and monitoring

3. Network Security

- **Restrict inbound and outbound traffic** using security groups and firewall rules.
- Use **Network Access Control Lists (NACLs)** and **VPC segmentation** to control traffic flow.
- Enable **DDoS protection** via services like AWS Shield or Azure DDoS Protection.
- Apply **container and API security** with Web Application Firewalls (WAFs) and API gateways.

Tools & Services:

- **AWS VPC Security Groups** – Network access controls
- **AWS Shield / Cloudflare** – DDoS mitigation
- **AWS WAF / Cloudflare WAF** – Web Application Firewall
- **AWS API Gateway / Nginx** – API security and rate limiting