**Module – 5**

**Cloud Security Essentials**

**1. How to Configure, Develop, and Maintain Security and Privacy in Cloud**

**A. Configuration:**

* **Use IAM Policies:** Implement least privilege access (roles, groups, policies).
* **Network Segmentation:** Create Virtual Private Clouds (VPC), subnets, and use firewalls.
* **Encrypt Data:** Use encryption at rest and in transit with managed keys (KMS).
* **Enable Logging:** Activate services like AWS CloudTrail, Azure Monitor, or GCP Cloud Audit Logs.

**B. Development:**

* **Secure Code Practices:** Use static code analysis, secrets management, and patch libraries.
* **CI/CD Integration:** Scan for vulnerabilities in the deployment pipeline.
* **DevSecOps:** Shift security left into development with tools like AWS CodeGuru, GitHub Advanced Security.

**C. Maintenance:**

* **Regular Audits:** Conduct compliance checks (e.g., using AWS Config or Azure Security Center).
* **Auto-Patching:** Use cloud-native patch management for OS and applications.
* **Incident Response:** Implement detection and alerting with services like AWS GuardDuty, Azure Sentinel.

**2. What is Portability in Cloud?**

**Cloud Portability** refers to the ability to move applications and data between cloud providers or between on-premise and cloud environments with minimal disruption.

* **Example:** Migrating a containerized app from AWS ECS to Google Kubernetes Engine (GKE).
* **Challenges:** Proprietary services (e.g., DynamoDB, Azure Cosmos DB), data formats, APIs.
* **Solution:** Use standard platforms like Kubernetes, Docker, and multi-cloud management tools (e.g., Terraform, Anthos).

**3. What is Reliability and High Availability in Cloud?**

**Reliability:** The system’s ability to operate consistently over time without failure.

**High Availability (HA):** Ensuring a system remains operational even during failure by:

* **Using multiple availability zones (AZs)**
* **Load balancing traffic across instances**
* **Auto-scaling infrastructure**
* **Replication of databases and services**

**Example:** AWS S3 offers 99.999999999% durability and replicates data across multiple AZs.

**4. Describe Mobility in Cloud Computing**

**Cloud Mobility** refers to the ability for users and applications to access data and services from anywhere, on any device.

* **Mobile Backend as a Service (MBaaS):** Firebase (GCP), AWS Amplify, Azure Mobile Apps
* **Benefits:**
  + Always-on access to cloud-hosted applications
  + Real-time data synchronization across devices
  + Device-independent experience
* **Use Case:** A mobile app using AWS Amplify to store user photos in S3, authenticated via Cognito.

**5. Describe AWS, Azure, and Google Cloud Platforms**

| **Feature** | **AWS** | **Azure** | **Google Cloud** |
| --- | --- | --- | --- |
| Launched | 2006 | 2010 | 2008 |
| Strength | Market leader, broadest services | Seamless Microsoft integration | Strong in data, AI, open-source |
| Compute | EC2, Lambda | VM, Functions | Compute Engine, Cloud Functions |
| Storage | S3, EBS | Blob, Disk | Cloud Storage, Persistent Disk |
| Database | RDS, DynamoDB | SQL Database, Cosmos DB | Cloud SQL, BigQuery |
| Networking | VPC, CloudFront | VNet, ExpressRoute | VPC, Cloud CDN |
| Identity | IAM, Cognito | Azure AD | Cloud IAM |

**6. Accessing AWS, Azure, and Google Cloud (Choose One: AWS Portal)**

**Accessing AWS via AWS Management Console:**

1. Go to <https://console.aws.amazon.com>
2. Sign in with AWS account credentials.
3. Use the **Search bar** to find services like EC2 (compute), S3 (storage), and VPC (network).
4. Navigate through the dashboard, billing, and support options.

**7. Create Compute, Network, Storage on AWS, Azure, and GCP**

| **Cloud** | **Compute** | **Network** | **Storage** |
| --- | --- | --- | --- |
| **AWS** | **EC2**: Launch via AMI, set instance type, key pair | **VPC**: Define CIDR, subnets, route tables | **S3 / EBS**: Object or block storage |
| **Azure** | **Virtual Machines**: Define OS, size, region | **VNet**: Create subnet, NSG, routing | **Blob / Disk Storage** |
| **GCP** | **Compute Engine**: Select image, zone, machine type | **VPC Network**: Configure firewall, subnets | **Cloud Storage / Persistent Disk** |

**8. Compare Cloud Pricing (Amazon Web Services Focus)**

Here’s a **basic comparison** of compute and storage pricing across AWS, Azure, and GCP (approximate as of 2024, varies by region):

| **Resource** | **AWS** | **Azure** | **GCP** |
| --- | --- | --- | --- |
| **Compute (2 vCPU, 8 GB)** | ~$0.092/hr (t3.medium) | ~$0.096/hr (B2ms) | ~$0.084/hr (e2-standard-2) |
| **Storage (S3 / Blob / Cloud Storage)** | ~$0.023/GB/mo | ~$0.0184/GB/mo | ~$0.020/GB/mo |
| **Data Transfer (Out)** | $0.09/GB (first 10 TB) | $0.087/GB | $0.12/GB |