Module - 5

1-How to configure, develop and maintain Security and Privacy in cloud?
- Identity and Access Management (IAM): Implement IAM to control user access to resources. Each user should have their own credentials, and access should be granted based on roles.
- Encryption: Encrypt data both at rest and in transit using advanced encryption standards such as AES-256.
- Network Security: Use firewalls, virtual private networks (VPNs), and security groups to control traffic and prevent unauthorized access.
- Compliance and Auditing: Make sure the cloud service complies with industry standards (e.g., GDPR, HIPAA). Implement auditing and monitoring tools to track changes and potential security breaches.
- Data Backup and Disaster Recovery: Regularly back up your data and implement disaster recovery mechanisms.
- Multi-factor Authentication (MFA): Always use MFA for administrative and sensitive accounts.
- Automated Patch Management: Regularly update and patch systems to minimize vulnerabilities.

2-What is Portability in cloud?
- Portability in the cloud refers to the ability to move applications, data, and workloads across different cloud environments (e.g., from one cloud provider to another) or from on-premises to the cloud and vice versa. It enables organizations to avoid vendor lock-in by ensuring that they can easily migrate between different platforms or use hybrid cloud setups. This is achieved by using standardized formats and APIs (Application programming interface) , such as containers (Docker) and microservices architectures.

3-What is Reliability and high Availability in cloud?
- Reliability: In cloud computing, reliability refers to the system's ability to consistently perform its intended functions without

failures. Cloud providers ensure reliability by using fault-tolerant infrastructures and distributed systems to minimize downtime.

- High Availability (HA): High availability ensures that a system or service remains operational and accessible even if a failure occurs in part of the infrastructure. Cloud providers achieve this by offering redundancy (replicating systems, databases, etc.) and failover mechanisms to ensure that if one component fails, another takes over without affecting service.

4-Describe Mobility Cloud Computing

- **Mobility Cloud Computing** refers to the ability to access and manage cloud services and resources from mobile devices (smartphones, tablets, laptops). This technology facilitates the management of cloud-based applications, storage, and compute resources while on the go. The goal of mobility cloud computing is to offer flexibility, scalability, and convenience for users to perform cloud-related tasks remotely, whether it's accessing data, monitoring systems, or performing administrative tasks.

Key Features of Mobility Cloud Computing:

- Access Anywhere: Users can access cloud resources from mobile devices, enhancing flexibility.
- Real-Time Synchronization: Information is constantly synchronized across devices.
- Scalability: Cloud platforms offer the ability to scale resources based on the needs of mobile users.
- Security: Cloud service providers implement strict security measures to ensure that mobile access is secure, including encryption and multi-factor authentication.

5-Describe AWS, Azure, Google cloud Platforms

- Amazon Web Services (AWS) :- AWS is the leading cloud platform, offering a wide array of services across compute, storage, networking, databases, machine learning, and more. It is known for its scalability, reliability, and large global presence. AWS offers services like EC2 (Elastic Compute Cloud) for computing, S3 (Simple Storage Service) for storage, and RDS (Relational Database Service) for databases. It's often chosen for large-scale

enterprise applications and startups due to its broad range of services and extensive ecosystem.

- Microsoft Azure :- Azure is Microsoft's cloud platform, offering a similar range of services to AWS but with a strong emphasis on integrating with Microsoft products such as Windows Server, Active Directory, SQL Server, and Office 365. Azure supports both Windows and Linux environments, providing flexibility for organizations with mixed OS environments. It also excels in hybrid cloud scenarios, where on-premises infrastructure is integrated with cloud services.

- Google Cloud Platform (GCP) :- GCP is known for its strong emphasis on data analytics, artificial intelligence (AI), machine learning, and containerized applications (with services like Kubernetes Engine). Google Cloud's primary advantages are its high-performance computing, big data analytics capabilities, and its integration with Google's ecosystem (like Google Workspace and Android). GCP's services include Compute Engine, Google Cloud Storage, BigQuery (data analytics), and TensorFlow (AI/ML).

6-Accessing AWS, Azure and Google cloud Platforms (any one portal)

- Done in lab.

7-Create compute, create network, create storage on AWS , Azure and GCP

- Done in lab.

8-Compare Cloud pricing of resources and services on all platform Amazon Web Services (AWS)

- AWS Pricing: AWS pricing is typically based on a pay-as-you-go model, where you pay for what you use. Services like EC2 (compute), S3 (storage), and RDS (databases) charge per usage metrics such as instance hours, storage size, and I/O operations.
- Pricing models:

- Pay-as-you-go: Users pay for the services they use, with no long-term commitments. Prices are usually charged per hour or per second.
- Reserved instances (RIs): Users commit to a specific amount of computing capacity for a set period of time, in exchange for a discount.
- Savings plans (SPs): Users commit to a consistent amount of usage for a set period of time, in exchange for a discount.
- Spot instances (SIs): Users can use unused computing capacity in the AWS cloud at a discount.
- Free trials: Users can test a service for a set period of time.
- 12-month free usage: Users can use various services with different limits for 12 months.
- Always free: Users can enjoy some services free of charge forever.