U23CST71 - CLOUD COMPUTING

Question Bank: 2 Mark Q&A + 16 Mark Questions (Unit I to V)

UNIT I – CLOUD ARCHITECTURE MODELS AND INFRASTRUCTURE

PART A – 2 Mark Questions with Answers

1. Define Cloud Computing.

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications) that can be rapidly provisioned and released with minimal management effort. (NIST Definition)

2. What are the essential characteristics of Cloud Computing?

The five essential characteristics are: (i) On-demand self-service, (ii) Broad network access, (iii) Resource pooling, (iv) Rapid elasticity, and (v) Measured service.

3. What is a Cloud Reference Architecture?

Cloud Reference Architecture is a standard framework defined by NIST that describes the major actors (Cloud Consumer, Provider, Auditor, Broker, Carrier) and their activities and functions in cloud computing.

4. List the Cloud Service Models.

The three cloud service models are: (i) Infrastructure as a Service (IaaS), (ii) Platform as a Service (PaaS), and (iii) Software as a Service (SaaS).

5. What are Cloud Deployment Models?

The four deployment models are: (i) Public Cloud, (ii) Private Cloud, (iii) Hybrid Cloud, and (iv) Community Cloud.

6. What is IaaS?

Infrastructure as a Service (IaaS) provides virtualized computing resources over the internet such as virtual machines, storage, and networking. Examples: Amazon EC2, Microsoft Azure VMs, Google Compute Engine.

7. What is PaaS?

Platform as a Service (PaaS) provides a platform allowing customers to develop, run, and manage applications without dealing with infrastructure. Examples: Google App Engine, Microsoft Azure App Service, Heroku.

8. What is SaaS?

Software as a Service (SaaS) delivers software applications over the internet on a subscription basis. Users access software via web browser. Examples: Gmail, Salesforce, Microsoft 365.

9. What is a Compute Cloud?

A Compute Cloud provides scalable processing power as a service, allowing users to run applications on virtual machines hosted in data centers, paying only for the resources used.

10. What is a Storage Cloud?

A Storage Cloud provides scalable, on-demand data storage over the internet. Users can store, retrieve and manage data remotely. Examples: Amazon S3, Google Cloud Storage, Azure Blob Storage.

PART B – 16 Mark Questions

1. Explain the NIST Cloud Computing Reference Architecture in detail with a neat diagram. Describe the roles of Cloud Consumer, Cloud Provider, Cloud Auditor, Cloud Broker, and Cloud Carrier.

2. Describe the Cloud Service Models (IaaS, PaaS, SaaS) with examples. Compare these models in terms of control, flexibility, and management responsibilities.

3. Explain the Cloud Deployment Models (Public, Private, Hybrid, Community) with their advantages and disadvantages. When should each model be used?

4. Describe the Architectural Design of Compute and Storage Clouds. Explain the design challenges involved in building cloud systems.

5. Explain the System Models for Distributed and Cloud Computing. Discuss how cloud infrastructure is designed to support scalability and availability.

UNIT II – VIRTUALIZATION BASICS

PART A – 2 Mark Questions with Answers

1. Define Virtualization.

Virtualization is the process of creating a virtual (rather than actual) version of computing resources such as hardware, OS, storage, or network. It allows multiple virtual instances to run on a single physical machine.

2. What is a Virtual Machine (VM)?

A Virtual Machine is an emulation of a computer system that runs on a host machine using virtualization software. It behaves like a real computer and can run its own OS and applications independently.

3. What is a Hypervisor?

A Hypervisor (Virtual Machine Monitor - VMM) is software that creates and manages virtual machines. It allows multiple OS instances to share hardware resources. Types: Type 1 (bare-metal) and Type 2 (hosted).

4. Differentiate Type 1 and Type 2 Hypervisors.

Type 1 (Bare-metal) hypervisor runs directly on hardware (e.g., VMware ESXi, Hyper-V). Type 2 (Hosted) hypervisor runs on top of a host OS (e.g., VMware Workstation, VirtualBox). Type 1 is faster and more secure.

5. What is Full Virtualization?

Full Virtualization allows an unmodified guest OS to run on virtual hardware. The hypervisor fully emulates the underlying hardware, making guest OS unaware it is virtualized. Example: VMware, VirtualBox.

6. What is Para-Virtualization?

Para-Virtualization requires modification of the guest OS to work cooperatively with the hypervisor. The guest OS is aware of the virtualization layer, which improves performance. Example: Xen hypervisor.

7. What is Hardware Virtualization?

Hardware Virtualization (Hardware-assisted Virtualization) uses CPU hardware features like Intel VT-x or AMD-V to improve virtualization performance. It allows the hypervisor to run guest OS without full software emulation.

8. What are the key concepts of Virtualization?

Key concepts include: (i) Partitioning – dividing resources, (ii) Isolation – VMs are independent, (iii) Encapsulation – VM state saved as files, (iv) Hardware independence – VM portable across hardware.

9. What is CPU Virtualization?

CPU Virtualization allows multiple VMs to share a single physical CPU. The hypervisor multiplexes CPU time among VMs, ensuring each VM gets processing time and is isolated from others.

10. What is Memory Virtualization?

Memory Virtualization abstracts physical memory and presents each VM with its own virtual address space. Techniques include shadow page tables, memory ballooning, and hardware-assisted page table management (e.g., Intel EPT).

PART B – 16 Mark Questions

1. Explain the Taxonomy of Virtual Machines with neat diagrams. Describe different types of VMs and their characteristics.

2. Describe the Virtualization Structure in detail. Explain the implementation levels of virtualization with examples.

3. Explain Full Virtualization, Para-Virtualization, and Hardware-Assisted Virtualization. Compare these techniques with suitable examples.

4. Describe the Virtualization of CPU, Memory, and I/O Devices. Explain the techniques used to virtualize each resource.

5. Explain the key concepts and benefits of virtualization in cloud computing. How does virtualization support resource pooling and elasticity?

UNIT III – VIRTUALIZATION INFRASTRUCTURE AND DOCKER

PART A – 2 Mark Questions with Answers

1. What is Desktop Virtualization?

Desktop Virtualization (VDI - Virtual Desktop Infrastructure) delivers a desktop OS to end users from a centralized server. Users access their virtual desktop remotely. Examples: Citrix Virtual Apps, VMware Horizon.

2. What is Network Virtualization?

Network Virtualization combines hardware and software network resources into a single, software-based administrative entity called a Virtual Network. It decouples network services from the underlying hardware. Example: VLAN, SDN.

3. What is Storage Virtualization?

Storage Virtualization abstracts physical storage from multiple network storage devices into a single logical storage device managed from a central console. Example: SAN virtualization, NAS virtualization, RAID.

4. What is Application Virtualization?

Application Virtualization encapsulates an application from the underlying OS, allowing it to run in an isolated virtual environment without installation. Example: VMware ThinApp, Microsoft App-V.

5. What is a Container?

A Container is a lightweight, standalone, executable package that includes everything needed to run an application: code, runtime, libraries, and settings. Containers share the host OS kernel, unlike VMs which have their own OS.

6. Differentiate Containers and Virtual Machines.

VMs include full OS + application + hypervisor layer (heavy, ~GBs). Containers share host OS kernel, include only app + dependencies (lightweight, ~MBs). Containers start faster and are more portable than VMs.

7. What is Docker?

Docker is an open-source platform that automates the deployment of applications inside software containers. It provides tools to build, ship, and run containers efficiently. Docker uses a client-server architecture.

8. What are Docker Components?

Key Docker components are: (i) Docker Engine (server), (ii) Docker Client (CLI), (iii) Docker Image (read-only template), (iv) Docker Container (running instance of image), (v) Docker Registry (image repository).

9. What is a Docker Image?

A Docker Image is a read-only template used to create Docker containers. It contains application code, runtime, libraries and dependencies. Images are built from Dockerfiles and stored in Docker registries like Docker Hub.

10. What is a Docker Registry?

A Docker Registry is a storage and distribution system for Docker images. Docker Hub is the default public registry. Organizations can use private registries. Users push/pull images using docker push and docker pull commands.

PART B – 16 Mark Questions

1. Explain Docker architecture in detail. Describe Docker Engine, Docker Client, Docker Images, Docker Containers, and Docker Registries with neat diagrams.

2. Describe Desktop Virtualization, Network Virtualization, and Storage Virtualization with suitable examples and use cases.

3. Compare Virtual Machines and Containers. Explain the architecture of containerization and how Docker achieves OS-level virtualization.

4. Explain Application Virtualization and Virtual Clusters. Describe Resource Management techniques in virtualized environments.

5. Describe the Docker Container lifecycle. Explain Docker Images and Repositories with examples of Docker commands.

UNIT IV – CLOUD DEPLOYMENT ENVIRONMENT

PART A – 2 Mark Questions with Answers

1. What is Google App Engine?

Google App Engine is a PaaS cloud offering by Google that allows developers to build and run applications on Google's infrastructure. It supports Python, Java, Go, PHP, and Node.js, with automatic scaling and management.

2. What is Amazon AWS?

Amazon Web Services (AWS) is a comprehensive cloud platform by Amazon offering over 200 services including IaaS (EC2, S3), PaaS (Elastic Beanstalk), and SaaS. It is the world's most widely adopted cloud platform.

3. What is Microsoft Azure?

Microsoft Azure is a cloud computing platform by Microsoft offering services including virtual machines, databases, analytics, AI, and networking. It integrates well with Microsoft products and supports hybrid cloud deployments.

4. What is Amazon EC2?

Amazon Elastic Compute Cloud (EC2) is an IaaS service that provides resizable virtual servers (instances) in the cloud. Users can choose instance types, OS, and configure security. EC2 supports auto-scaling and load balancing.

5. What is Amazon S3?

Amazon Simple Storage Service (S3) is an object storage service offering scalability, availability, and durability. It stores data as objects in buckets and is used for backup, archiving, data lakes, and static website hosting.

6. What is Eucalyptus?

Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems) is an open-source cloud platform that enables building private and hybrid clouds compatible with AWS APIs.

7. What is OpenStack?

OpenStack is a free, open-source cloud operating system that controls large pools of compute, storage, and networking resources throughout a data center. It is managed through a dashboard or REST API.

8. What are Cloud Software Environments?

Cloud Software Environments are platforms and tools that enable development, deployment, and management of cloud applications. Examples include Google App Engine, AWS Elastic Beanstalk, Microsoft Azure App Service.

9. What is Auto Scaling in AWS?

Auto Scaling in AWS automatically adjusts the number of EC2 instances in response to traffic demand. It ensures application availability and reduces costs by scaling in when demand decreases and scaling out when demand increases.

10. What is Azure Active Directory?

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. It enables employees to sign in and access resources. It supports Single Sign-On (SSO), Multi-Factor Authentication (MFA), and conditional access.

PART B – 16 Mark Questions

1. Explain Amazon Web Services (AWS) in detail. Describe key AWS services like EC2, S3, RDS, Lambda, and VPC with their use cases.

2. Describe Microsoft Azure cloud platform. Explain its core services including Azure VMs, Azure Storage, Azure SQL Database, and Azure Active Directory.

3. Explain Google App Engine architecture and features. Describe how it supports application deployment, scaling, and management.

4. Compare OpenStack and Eucalyptus as open-source cloud platforms. Explain their architecture, components, and use cases.

5. Describe the various Cloud Software Environments available. Compare AWS, Azure, and Google Cloud in terms of services, pricing, and target use cases.

UNIT V – CLOUD SECURITY

PART A – 2 Mark Questions with Answers

1. What is Cloud Security?

Cloud Security refers to the set of policies, controls, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure from threats, unauthorized access, and data breaches.

2. What is Guest Hopping?

Guest Hopping (VM Escape) is a virtualization-specific attack where an attacker in one VM escapes the VM boundary and gains access to the host hypervisor or other VMs on the same physical host, compromising isolation.

3. What is a VM Migration Attack?

A VM Migration Attack exploits the live migration process of virtual machines between physical hosts. Attackers can intercept migrating VM data, redirect migration to a malicious host, or perform man-in-the-middle attacks during migration.

4. What is Hyperjacking?

Hyperjacking is an attack where an attacker installs a rogue hypervisor (rootkit hypervisor) that takes control of the physical server. The legitimate hypervisor and all its VMs run under the attacker's malicious hypervisor undetected.

5. What is Identity and Access Management (IAM)?

IAM is a framework of policies and technologies that ensures the right people (identity) have appropriate access (authorization) to technology resources. It manages user identities, roles, and permissions in cloud environments.

6. What are IAM Challenges?

IAM challenges include: (i) Managing identities across multiple cloud providers, (ii) Enforcing least privilege principle, (iii) Handling federated identities, (iv) Securing privileged accounts, (v) Compliance and audit requirements.

7. What is IAM Architecture?

IAM Architecture consists of: (i) Identity Store (user directory), (ii) Authentication service (verifying identity), (iii) Authorization service (access control), (iv) Federation service (SSO across domains), and (v) Audit and Compliance module.

8. What is Data Security in Cloud?

Data Security in Cloud involves protecting data from unauthorized access, corruption, or theft throughout its lifecycle. It includes encryption (at rest and in transit), access controls, data masking, and data loss prevention (DLP).

9. What is a Virtualization System-Specific Attack?

Virtualization System-Specific Attacks target vulnerabilities unique to virtualized environments. Examples include VM escape, hyperjacking, VM migration attacks, side-channel attacks, and denial-of-service attacks on the hypervisor.

10. What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication (MFA) requires users to provide two or more verification factors to gain access. Factors include: Something you know (password), Something you have (OTP token), and Something you are (biometrics).

PART B – 16 Mark Questions

1. Describe Virtualization System-Specific Attacks in detail. Explain Guest Hopping, VM Migration Attack, and Hyperjacking with preventive measures.

2. Explain Identity and Access Management (IAM) in cloud computing. Describe IAM architecture, components, challenges, and best practices.

3. Describe Data Security and Storage security issues in the cloud. Explain encryption techniques, access control mechanisms, and compliance requirements.

4. Explain the IAM challenges faced in cloud environments. Describe IAM practices to overcome identity management issues in multi-cloud deployments.

5. Write a detailed note on Cloud Security threats and countermeasures. Cover data breaches, account hijacking, insecure APIs, and denial-of-service attacks.