**IMP Questions!!**

**UNIT - I: Introduction to Cloud Computing**

**Short Answers:**

1. Define cloud computing.
2. characteristics of cloud computing.
3. What is the NIST cloud computing reference architecture?
4. Briefly explain the evolution of cloud computing.
5. What are the key components of cloud computing?
6. Differentiate between single-cloud and multi-cloud environments.
7. Explain the concept of threat assessment in cloud computing.
8. Analyse the risks associated with migrating to the cloud and propose mitigation strategies.
9. Evaluate the security issues in multi-cloud environments.
10. Provide an overview of computer security and its relevance in cloud computing.
11. Explore the threats in cloud computing, categorizing them into infrastructure and service provider threats.
12. Explain the research challenges in the field of cloud computing.
13. Types of cloud and their characteristics.
14. Risks and approaches of migration into the cloud.
15. Infrastructure and host threats in cloud computing.
16. Privacy and security in multi-clouds.
17. Cloud computing research challenges.
18. What are the characteristics and advantages of cloud computing?
19. Explain the concept of cloud computing security baseline.
20. Discuss the vulnerabilities and attacks associated with cloud storage services.

**UNIT - II: Cloud Computing Architecture**

1. Define object storage and its applications in cloud computing.
2. Types of virtualization.
3. What is para virtualization?
4. Compare full virtualization, paravirtualization, and containerization.
5. Discuss the criteria for choosing a hypervisor in a cloud computing environment.
6. Explain hypervisor memory optimization.
7. hypervisor hardening.
8. Explain the security measures for hypervisors, focusing on memory optimization and additional security features.
9. What is Docker, and how does it relate to cloud computing?
10. virtual hardware with Quick Emulator?
11. Discuss the impact of team expertise, project maturity, certifications, and features on the selection of a hypervisor.
12. Compare and contrast various types of virtualization, including full virtualization, paravirtualization, and containerization.
13. Discuss the concept of hardening in the context of physical hardware and host operating systems.
14. Compare Docker and Linux Containers. Highlight their advantages and use cases.
15. Discuss hardware concerns in the context of hypervisor selection.

**UNIT - III: Cloud Service Models**

1. PaaS, SaaS, and IaaS, and provide examples for each. Discuss their working principles.
2. Provide examples of cloud services for each model.
3. Explain the importance of Service Level Agreements (SLAs) in cloud computing.
4. What are recent service models like BMaaS and XaaS?
5. Discuss the design considerations for datacenter and interconnection networks.
6. Explain the concept of billing and accounting in cloud computing.
7. What are recent service models like BMaaS and XaaS, and how do they differ from traditional models?
8. Explain the importance of service management in the cloud. Discuss Service Level Agreements (SLAs) and their components.
9. Explore billing and accounting processes in cloud computing. Highlight challenges and best practices.
10. Compare different scaling techniques used in cloud services.
11. Discuss the design considerations for datacenter and interconnection networks in cloud computing.

**UNIT - IV: Securing Cloud Communications and API**

**Short Answers:**

1. Explain symmetric and asymmetric encryption and their applications in securing cloud communications.
2. Compare stream cipher and block cipher. Highlight their strengths and weaknesses.
3. Identification, authentication, and authorization. Discuss the principles of identification, authentication, and authorization in cloud computing.
4. What is mandatory access control, and how does it enhance cloud security?
5. Define and compare mandatory access control, discretionary access control, and role-based access control in cloud security.
6. Explain the concept of session management in the context of cloud security.
7. Discuss the importance of federated identity in cloud computing.
8. What are signed certificates versus self-signed certificates?
9. Elaborate on the concepts of public key infrastructure, signed certificates, and self-signed certificates.
10. Secure API environment. Discuss the components of a secure API environment.
11. Discuss the components of a secure API environment. What are the key components of a secure API environment?

**UNIT - V: Emerging Cloud Environments and Cloud Forensics**

**Short Answers:**

1. Provide a case study on an open-source cloud environment and a commercial cloud service.
2. Cloud forensics and its significance in modern computing environments.
3. Define and discuss the dimensions of cloud forensics. Highlight the challenges associated with cloud crime investigations.
4. Explain the challenges in cloud crime investigations.
5. Discuss the usages of cloud forensics.
6. Name some cloud forensics tools.

**Long Answers:**

1. Explain the architecture of Eucalyptus and Open Nebula. Discuss their contributions to cloud computing.
2. Explore the usages of cloud forensics and its significance in modern computing environments.
3. Discuss the tools and frameworks used in cloud forensic investigations.
4. Analyze the role of digital forensic investigation in the context of cloud computing.
5. Compare different cloud computing environments, such as Google App Engine, IBM Cloud, and VMWare Cloud. Highlight their features and use cases.
6. Cloud forensics tools.
7. Google App Engine, IBM Cloud, VMWare Cloud.
8. Analyze the role of digital forensic investigation in the context of cloud computing.