0904E0100

Candidate's Seat No :_____

IM.B.A. (CSM) Sem.-6 Examination

CSM-BBA-CC-308

Cloud Architecture & Security Fundamentals

April-2025

Time : 2-30 Hours] **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Discuss the different types of cloud computing services (IaaS, PaaS, SaaS) with examples. 7Marks

ii. Compare and contrast public, private, hybrid, and community cloud deployment models. 7Marks

OR

i. Discuss the role of virtualization in enabling cloud computing services. 7Marks

ii. Describe the shared responsibilities model in cloud computing and its importance for security. 7Marks

Question 2 Answer the following questions:

i. Explain the evolution of cluster, grid, and cloud computing technologies with examples. 7Marks

ii. Explain the key components of infrastructure in cloud computing: compute, storage, and networking layers. 7Marks

OR

i. Analyse the advantages and disadvantages of serverless computing within a web service implementation context. 7Marks

ii. Describe virtualization technologies and their role in enabling cloud infrastructure components (compute, storage, networking). 7Marks

Question 3 Answer the following questions:

i. Discuss the concepts of reliability, availability, and security in cloud-based services and their interdependencies. 7Marks

ii. What are the key components of cloud economics, and how can organizations optimize costs associated with cloud services? 7Marks

OR

i. Explain the process of vulnerability assessment and penetration testing in cloud environments. Why are they critical for security? 7Marks

ii. Describe how service-level agreements (SLAs) impact the reliability and performance expectations of cloud services. 7Marks

Questions 4 Answer the following questions:

i. Identify and discuss emerging threats in cloud security, including potential attack vectors and mitigation strategies. 7Marks

ii. Examine the potential role of blockchain technology in enhancing security within cloud environments, including use cases and benefits. 7Marks

OR

E100-2

i. Define Confidential Computing and explain how it enhances data protection within cloud environments through secure enclaves or trusted execution environments (TEEs). 7Marks

ii. Explore how organizations can adapt their security strategies to address emerging technologies such as IoT within their cloud infrastructure frameworks. 7Marks

Questions 5: Attempt any Seven out of Twelve. 14Marks

1. Name the three primary service models of cloud computing and briefly explain one of them.
2. Mention one example of Infrastructure as a Service (IaaS).
3. State one security consideration for implementing web services in the cloud.
4. Define grid computing and mention one difference between grid and cloud computing.
5. What is virtualization in the context of cloud computing?
6. Define reliability in the context of cloud-based services.
7. State one metric used to measure scalability in cloud services.
8. What is meant by "service-level agreement" (SLA) in a cloud environment?
9. Name one dimension of cloud security controls and briefly explain its purpose.
10. What is continuous monitoring, and why is it important for maintaining security in the cloud?
11. Name one regulation or framework that governs data privacy in the context of global cloud usage (e.g., GDPR).
12. State one challenge organizations face when integrating new security technologies into

.....X.....X.....