School of Computing Science and Engineering

Department of Computer Application
Mid Term Examination

Exam Date: 01 Oct 2023
Time : 90 Minutes
Marks : 50

Sem III - MCAE2332 - Cloud Security and Management

Your answer should be specific to the question asked
Draw neat labeled diagrams wherever necessary

1)	Compare the data privacy implications of using SaaS applications versus on-premises software.	K2 (2)
2)	Evaluate the scalability Considerations for SaaS applications in the Context of varying user demands.	K1 (3)
3)	Analyze the potential security risks associated with virtualization.	K2 (4)
4)	Zero Trust Network Architecture (ZTNA) Implementation in a Hybrid Cloud: Detail how a company leveraged Zero Trust principles to secure access to its applications and resources across both on-premises and cloud environments. Highlight the benefits of ZTNA in enhancing security and simplifying management in a hybrid cloud setup.	K2 (6)
5)	Describe the benefits and challenges of implementing storage virtualization, emphasizing its role in simplifying storage management.	K3 (6)
6)	Discuss why scalability and performance are important factors to Consider when implementing cloud solutions, and provide examples of how they can positively impact an organization's operations and growth.	K3 (9)
7)	Create a novel approach for ensuring data privacy and Confidentiality in a cloud environment that employs serverless Computing. Integrate Concepts of data masking, tokenization, and secure key management to protect sensitive information while allowing seamless data processing within serverless functions.	K4 (8)
8)	Develop a Comprehensive training program for cloud security professionals, focusing on advanced virtualization techniques and their impact on security. Create a curriculum that Covers topics such as hypervisor security, Container runtime protection, secure orchestration, and Compliance management, and outline hands-on exercises and assessments to validate participants' skills.	K4 (12)

OR

	Design a cloud-native intrusion detection and prevention system that leverages artificial intelligence and machine learning techniques. Integrate behavior analysis, anomaly detection, and real-time threat intelligence to proactively identify and mitigate security threats within virtualized cloud environments.	K4 (12)