Register No : _____

THE KAVERY ENGINEERING COLLEGE

(An Autonomous Institution)

B.E/B.TECH DEGREE END SEMESTER THEORY EXAMINATIONS, NOV /DEC 2024

Seventh Semester

Computer Science and Engineering

CCS362 - Security and Privacy in Cloud

Regulations - 2021

Duration : 3 Hrs *Maximum : 100 Marks*

*PART – A (ANSWER ALL QUESTIONS) (Marks 10*2=20)*

Q.No	*Questions*	*BLT*	*CO*	*Marks*
1.	Define confidentiality in cloud security.	RE	1	2
2.	What is the main difference between symmetric and asymmetric cryptography?	UN	1	2
3.	Name two common attack vectors in cloud environments.	UN	2	2
4.	What is data tokenization in the context of data protection?	RE	2	2
5.	List the purpose of Multi-Factor Authentication (MFA) in cloud security.	UN	3	2
6.	What is the role of an identity provider in identity federation?	RE	3	2
7.	Explain geo-tagging and one of its common applications.	UN	4	2
8.	What is cloud resource access control, and why is it important in cloud computing?	UN	4	2
9.	How does detecting malicious traffic contribute to system security?	UN	5	2
10.	Why is tamper-proofing audit logs important in security management?	UN	5	2

*PART – B (ANSWER ALL QUESTIONS) (Marks 5*13 = 65)*

Q.No		*Questions*	*BLT*	*CO*	*Marks*
11.	a	Explain the role of the following security services in cloud computing: confidentiality, integrity, and authentication.	UN	1	13
		Or			
	b	Describe the role of hash functions in cryptography and their applications in security.	UN	1	13
12.	a	Demonstrate end-to-end access control in cloud environments and its importance in preventing unauthorized access.	UN	2	13
		Or			
	b	Illustrate various data protection strategies for tenant data, focusing on encryption, data redaction, and key management.	UN	2	13

13.	a	Implement a multi-factor authentication (MFA) and single sign-on (SSO) strategy for a cloud infrastructure. Describe how this approach enhances security while simplifying the user experience.	AP	3	13
		Or			
	b	Design a secure cloud infrastructure by applying OS hardening, verified and measured boot, and intruder detection and prevention mechanisms.	AP	3	13
14.	a	Explain cloud bursting, geo-tagging, and secure cloud interfaces, discussing their roles and significance in cloud computing environments.	UN	4	13
		Or			
	b	Explain the concept of design patterns in software development, and discuss its relevance in cloud-based systems.	UN	4	13
15.	a	Explain proactive activity monitoring and its importance in cybersecurity.	AN	5	13
		Or			
	b	Discuss the importance of secure record generation, reporting, and management in cybersecurity.	AN	5	13

*PART – C (Marks 1*15 = 15)*

Q.No		*Questions*	*BLT*	*CO*	*Marks*
16.	a	Analyze the impact of common attack vectors and threats on network and storage security, and evaluate how secure isolation strategies and virtualization techniques can mitigate these risks. Discuss the strengths and limitations of these approaches in enhancing overall system security.	AN	2	15
		Or			
	b	Analyze the effectiveness of roles-based access control (RBAC) combined with multi-factor authentication (MFA) in enhancing security within an organization.	AN	3	15