OR	iii.	Explain the architecture and best practices for implementing an effective Identity and Access Management (IAM) system in a cloud environment. How do these practices help secure cloud services?	**7**	3	4	2
Q.5	i.	Describe the role of patch and configuration management in maintaining cloud security. How do these practices help prevent security vulnerabilities in cloud environments?	**4**	2	3	4
	ii.	Compare and contrast availability management strategies for Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) in cloud computing. What are some common techniques used to ensure availability in each service model?	**6**	3	4	4
OR	iii.	Explain the importance of access control in cloud security management. Discuss at least three access control methods that can be applied to protect cloud resources and ensure authorized access.	**6**	2	5	4
Q.6		Attempt any two:				
	i.	Discuss the responsibilities of cloud service providers and customers regarding data ownership and compliance with local laws. How can both parties ensure that they meet their legal obligations?	**5**	2	4	4
	ii.	Explain the significance of the right to conduct penetration tests in cloud environments. What are the potential legal and compliance implications if a customer performs penetration testing without proper authorization from the cloud provider?	**5**	2	5	5
	iii.	Examine how modern security standards, such as PCI DSS, address the challenges of cloud services and virtualization. What key requirements must cloud service providers meet to ensure compliance with these standards?	**5**	3	6	5

******

Total No. of Questions: 6 *Total No. of Printed Pages:4*

Enrollment No......................................

Faculty of Engineering
End Sem Examination Dec 2024
CA5EL13 Cloud Security

Programme: MCA / BCA-MCA (Integrated) Branch/Specialisation: Computer Application

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d. Assume suitable data if necessary. Notations and symbols have their usual meaning.

			Marks	**BL**	**PO**	**CO**	**PSO**
Q.1	i.	Which of the following cloud security principles ensures that data is only accessible to authorized users and is protected from unauthorized disclosure? (a) Integrity (b) Availability (c) Confidentiality (d) Non-repudiation	**1**	1	1	1	
	ii.	How does the concept of "Defense in Depth" apply to cloud security, especially in PaaS environments? (a) By implementing multiple layers of security controls to protect data and applications (b) By ensuring high availability of services across multiple data centers (c) By using multi-factor authentication for all user accounts (d) By applying encryption to all stored data	**1**	1	2	2	
	iii.	Which of the following principles is included in the CIA triad for cloud security and focuses on ensuring that data is protected from unauthorized modifications? (a) Confidentiality (b) Availability (c) Integrity (d) Compliance	**1**	1	1	2	
	iv.	In the context of cloud computing, which of the following best describes "Business Continuity and Disaster Recovery" (BC/DR)? (a) Ensuring that cloud services are designed to scale dynamically according to workload demands (b) Developing and implementing strategies to maintain operations and recover data during and after a disruption (c) Applying encryption techniques to protect data at rest and in transit (d) Establishing policies for user authentication and access control in the cloud	**1**	1	3	2	

v. Which of the following is a key challenge associated with Identity and Access Management (IAM) in cloud environments? **1** 1 3 3

(a) Ensuring data replication across multiple cloud regions

(b) Implementing hardware firewalls for network security

(c) Optimizing server load balancing for high availability

(d) Managing user identities and access across multiple trust boundaries

vi. Which protocol is commonly used in cloud services for federated identity management, allowing users to access multiple services using a single set of credentials? **1** 1 2 2

(a) SAML (b) TCP (c) SMTP (d) DNS

vii. Which of the following is a key aspect of availability management in Infrastructure as a Service (IaaS)? **1** 1 3 3

(a) Managing software updates for the cloud provider's applications

(b) Ensuring data encryption during transmission over the network

(c) Implementing failover strategies and redundancy for virtual machines

(d) Monitoring user activity for potential insider threats

viii. Which security management standard is commonly used for establishing a framework for information security management in cloud environments? **1** 1 2 5

(a) ISO/IEC 27001 (b) IEEE 802.11

(c) ITIL v3 (d) COBIT 5

ix. Which of the following statements accurately reflects the ownership of data in cloud environments? **1** 1 3 4

(a) The cloud service provider owns all data stored in their services

(b) Customers retain ownership of their data, but the cloud provider may have access for management purposes

(c) Data ownership automatically transfers to the cloud provider upon upload

(d) Ownership of data is irrelevant as long as it is stored in the cloud

x. What is the primary focus of the Payment Card Industry Data Security Standard (PCI DSS) concerning cloud services? **1** 1 3 4

(a) Ensuring that cloud providers have physical security measures in place

(b) Regulating the pricing structure of cloud services

(c) Mandating the use of specific cloud service providers for financial institutions

(d) Establishing requirements for securely storing and processing credit card information in the cloud

Q.2 i. Define "Confidentiality" in the context of cloud computing. Why is it important for cloud service models like SaaS and IaaS? **4** 1 2 1

ii. Discuss the role of "Authentication" and "Non-repudiation" in ensuring the integrity of data in cloud environments. How are these concepts applied differently in IaaS and SaaS? **6** 2 3 1

OR iii. Describe how "Defense in depth" and "Availability" can be integrated into a comprehensive security strategy for cloud-based services. What challenges might arise when applying these concepts to multi-cloud or hybrid cloud environments? **6** 2 2 2

Q.3 i. What are the three core components of the CIA triad in cloud information security? Why are they important? **2** 1 3 3

ii. Discuss the role of cloud security design principles in mitigating risk issues in cloud environments. Provide examples of at least three design principles and explain how they help address specific security challenges. **8** 2 2 4

OR iii. Analyze the importance of implementing security policies and their decomposition in cloud environments. How do these policies support cloud information security objectives such as confidentiality, integrity, and availability (CIA triad)? Discuss the key steps involved in designing and implementing effective security policies for cloud computing. **8** 3 3 4

Q.4 i. Explain the concept of "Trust boundaries" in Identity and Access Management (IAM). Why is it important to consider these boundaries when designing IAM solutions for cloud environments? **3** 2 4 3

ii. Discuss the key challenges associated with implementing Identity and Access Management (IAM) in cloud environments. How do these challenges differ from traditional on-premises IAM? What strategies can be used to address them? **7** 3 3 3

Marking Scheme

CA5EL13 (T) Cloud Security (T)

Q.1 i) C. Confidentiality **1**

ii) A. By implementing multiple layers of security controls to protect data and applications. **1**

iii) C. Integrity **1**

iv) B. Developing and implementing strategies to maintain operations and recover data during and after a disruption. **1**

v) D. Managing user identities and access across multiple trust boundaries. **1**

vi) A. SAML (Security Assertion Markup Language) **1**

vii) C. Implementing failover strategies and redundancy for virtual machines. **1**

viii) A. ISO/IEC 27001 **1**

ix) B. Customers retain ownership of their data, but the cloud provider may have access for management purposes. **1**

x) D.Establishing requirements for securely storing and processing credit card information in the cloud. **1**

Q.2 i. Define "Confidentiality" in the context of cloud computing. **2M** **4**

Why is it important for cloud service models like SaaS and IaaS? **2M**

ii. Discuss the role of "Authentication" and "Non-repudiation" in ensuring the integrity of data in cloud environments. **3M** **6**

How are these concepts applied differently in IaaS and SaaS? **3M**

OR iii. Describe how "Defense in depth" and "Availability" can be integrated into a comprehensive security strategy for cloud-based services. **3M** **6**

What challenges might arise when applying these concepts to multi-cloud or hybrid cloud environments? **3M**

Q.3 i. What are the three core components of the CIA triad in cloud information security? **2M** **2**

Why are they important? **2M**

ii. Discuss the role of cloud security design principles in mitigating risk issues in cloud environments. **4M** **8**

Provide examples of at least three design principles and explain how they help address specific security challenges. **4M**

OR iii. Analyze the importance of implementing security policies and their decomposition in cloud environments. **4M** **8**

How do these policies support cloud information security objectives such as confidentiality, integrity, and availability (CIA triad)? Discuss the key steps involved in designing and implementing effective security policies for cloud computing. **4M**

Q.4 i. Explain the concept of "Trust boundaries" in Identity and Access Management (IAM). **1.5M** **3**

Why is it important to consider these boundaries when designing IAM solutions for cloud environments? **1.5M**

ii. Discuss the key challenges associated with implementing Identity and Access Management (IAM) in cloud environments. **3.5M** **7**

How do these challenges differ from traditional on-premises IAM? What strategies can be used to address them? **3.5M**

OR iii. Explain the architecture and best practices for implementing an effective Identity and Access Management (IAM) system in a cloud environment. **7**

3.5M

How do these practices help secure cloud services? **3.5M**

Q.5 i. Describe the role of patch and configuration management in maintaining cloud security. **2M** **4**

How do these practices help prevent security vulnerabilities in cloud environments? **2M**

ii. Compare and contrast availability management strategies for Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) in cloud computing. **3M** **6**

What are some common techniques used to ensure availability in each service model? **3M**

OR iii. Explain the importance of access control in cloud security management. **3M** **6**

Discuss at least three access control methods that can be applied to protect cloud resources and ensure authorized access. 3M

Q.6 Attempt any two:

i. Discuss the responsibilities of cloud service providers and **5**

P.T.O.

customers regarding data ownership and compliance with local laws. **2.5M**

How can both parties ensure that they meet their legal obligations? **2.5M**

ii. Explain the significance of the right to conduct penetration tests in cloud environments. **2.5M** **5**

What are the potential legal and compliance implications if a customer performs penetration testing without proper authorization from the cloud provider? **2.5M**

iii. Examine how modern security standards, such as PCI DSS, address the challenges of cloud services and virtualization. **2.5M** **5**

What key requirements must cloud service providers meet to ensure compliance with these standards? **2.5M**

******