19CS416 – CLOUD SECURITY

PART A **(10 x 2 = 20 marks)**

		CO
1.	Name any two key milestones in the evolution of cloud computing.	CO1
2.	How does cloud computing enhance business continuity?	CO1
3.	Enumerate the benefits of cloud computing.	CO1
4.	Define Private Cloud.	CO1
5.	Name two companies that significantly contributed to the growth of cloud computing	CO1
6.	Differentiate between Cloud Service Models and Cloud Deployment Models with suitable examples	CO1
7.	Define the three primary objectives of cloud information security.	CO2
8.	What are the key components of cloud security services?	CO2
9.	Why is auditing important in cloud security?	CO2
10.	Differentiate authentication and authorization in cloud security.	CO2
11.	What is Role-Based Access Control (RBAC) in cloud security?	CO2
12.	What are the 4 A's in Cloud Computing security, and what do they signify?	CO2
13.	Define eavesdropping. How it poses a threat to data security in cloud environments?	CO3
14.	What is a Denial of Service (DoS) attack? How can it impact the availability of cloud services?	CO3
15.	Write short notes on network intrusion and its potential impact on cloud infrastructure.	CO3
16.	List the significance of privilege escalation as a threat to cloud security.	CO3
17.	Why are inactive virtual machines a security risk in cloud environments?	CO3
18.	What is the risk of poor access control in cloud security, and how can it be mitigated?	CO3
19.	Define policy types in cloud security.	CO4
20.	What is virtualization security management?	CO4
21.	Define VM threat level.	CO4
22.	What are the risks associated with hypervisors?	CO4
23.	State the importance of security policy implementation?	CO4
24.	Why is VM isolation important in virtualization security, and how can it be achieved	CO4
25.	What are architectural considerations in cloud computing?	CO5
26.	What is the importance of security awareness in cloud computing?	CO5
27.	Define compliance in cloud security.	CO5
28.	How is identity management implemented in cloud environments?	CO5
29.	How does information classification enhance cloud security?	CO5
30.	Why is identity management critical in cloud security?	CO5

PART B **(5 x 13 = 65 marks)**

		CO
11.	Describe the essential characteristics of cloud computing and discuss why they are fundamental to the concept.	CO1
	Compare and contrast the three cloud delivery models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Provide examples of each.	CO1
	Evaluate the suitability of different cloud deployment models (public, community, private, hybrid) for various types of organizations and applications. Discuss the advantages and disadvantages of each deployment model.	CO1
	Discuss how cloud computing architecture enables scalability, elasticity, and resource pooling. Provide real-world examples to support your explanation.	CO1
	Analyze the evolution of cloud computing and evaluate its impact on modern businesses by examining how it has transformed traditional IT infrastructure and operational models.	CO1
	Discuss how cloud computing architecture enables scalability, elasticity, and resource pooling. Provide real-world examples to support your explanation.	CO1
12.	Explain the Confidentiality, Integrity, and Availability (CIA) Triad in cloud security. How does the CIA model help ensure secure cloud computing?	CO2
	What are the major security threats in cloud computing? Explain strategies to mitigate risks associated with unauthorized access, data breaches, and account hijacking.	CO2
	Describe the process of authentication in cloud computing. Illustrate different authentication mechanisms commonly used in cloud environments and their strengths and weaknesses.	CO2
	Explain at least four cloud security design principles. Discuss how these principles contribute to the development of secure cloud-based systems.	CO2
	Identify the key obstacles to maintaining data confidentiality in cloud environments and evaluate recommended strategies, including the use of encryption techniques and access control mechanisms, to safeguard sensitive information.	CO2
	Describe the concept of cloud availability, analyze common hazards that threaten it (e.g., hardware failures, network outages, cyberattacks, misconfigurations), and evaluate strategies to ensure robustness and continuity in cloud-based systems.	CO2
13.	Describe the impact of eavesdropping on the confidentiality of data transmitted over cloud networks. Provide examples of encryption techniques that can mitigate this threat.	CO3
	Analyze the various types of Denial of Service (DoS) attacks commonly encountered in cloud environments, and evaluate mitigation strategies at both the network and application levels to protect against these threats.	CO3
	Analyze the anatomy of a network intrusion in a cloud environment. How intrusion detection and prevention systems (IDPS) can help mitigate the risks associated with network-based attacks?	CO3
	Evaluate the impact of inactive virtual machines on cloud infrastructure security. What are the risks associated with unused or abandoned VMs and outline strategies for identifying and mitigating these risks through proactive resource management practices?	CO3
	Examine the role of access control in cloud security and analyze the potential consequences of weak or poorly enforced access policies. Evaluate how the principles	CO3

	of least privilege and separation of duties can be applied to strengthen access control in cloud-based systems.	
	Analyze the complexities of configuring cloud services and the security risks associated with misconfigurations. Discuss the challenges that organizations face in maintaining secure configurations and propose strategies for adopting secure-by-default practices to minimize these risks.	CO3
14.	Analyze the role of Computer Security Incident Response Teams (CSIRTs) in managing security incidents in cloud computing.	CO4
	Assess the significance of security policy implementation in addressing cloud computing security challenges.	CO4
	Discuss the challenges and best practices associated with virtualization security management in cloud environments.	CO4
	Enumerate the various threat levels associated with virtual machines (VMs) and their impact on cloud security.	CO4
	Analyze the performance and management challenges of hypervisors in large-scale cloud infrastructures. Propose strategies to balance efficiency with security.	CO4
	Examine the key security risks associated with hypervisors in cloud environments. How do vulnerabilities in the hypervisor affect virtual machines and overall cloud security?	CO4
15.	Discuss multi-tenancy, resource isolation, and scalability in cloud security.	CO5
	Evaluate the significance of architectural considerations in designing secure cloud infrastructures.	CO5
	Analyze the importance of secure execution environments in protecting cloud workloads from malicious attacks and unauthorized access.	CO5
	Explain the role of access control mechanisms in enforcing security policies and protecting sensitive data in cloud computing environments.	CO5
	Analyze the key challenges in establishing secure execution environments within multi-tenant cloud infrastructures, and examine how these challenges influence overall system reliability and user trust.	CO5
	Critically assess how shared responsibility models in cloud computing affect compliance obligations of cloud service providers and customers	CO5

PART C (1 x 15 = 15 marks)

(Case study/Comprehensive type Questions)

		CO
16.	A large enterprise with an on-premises data center plans to migrate to the cloud for better scalability and cost efficiency. However, they are concerned about data security and downtime during migration. i. What challenges might the enterprise face during cloud migration? (8) ii. Which cloud service and deployment model would best suit their requirements? (7)	CO1
	A hospital wants to adopt a Software as a Service (SaaS) solution for patient record management. However, they are concerned about data security, compliance, and integration with existing systems. i. What are the advantages and risks of using SaaS in a healthcare setting? (7) ii. What access control and encryption measures should be implemented? (8)	CO1

	A financial services company is using a cloud-based document management system to store confidential customer data. A recent security audit reveals that several unauthorized users accessed sensitive files due to misconfigured access controls. i. What security principles were violated? (5) ii. How can authentication and authorization mechanisms prevent such incidents? (5) iii. What role does role-based access control (RBAC) play in mitigating unauthorized access? (5)	CO2
	A cloud administrator at a healthcare company misuse privileged access to delete critical patient records from a cloud storage system. There are no proper logs to track the changes. i. How can auditing and accountability help prevent such insider threats? (5) ii. What security services (e.g., AWS CloudTrail, Azure Monitor) can track and log user activities? (5) iii. How does the principle of least privilege (PoLP) help mitigate insider threats? (5)	C02
	A finance company uses cloud-based virtual machines for processing financial transactions. One day, an employee with basic user privileges gains unauthorized access to an administrative VM, allowing them to manipulate financial data. i. What security policies and access control mechanisms were missing? (5) ii. How can role-based access control (RBAC) and least privilege principles prevent such incidents? (5) iii. What virtualization security best practices (e.g., MFA, logging, auditing) should be implemented? (5)	CO5
	A cloud service provider hosts multiple VMs on a shared infrastructure. A security analyst discovers that an attacker has successfully executed a VM escape attack, allowing them to access the underlying hypervisor and manipulate other virtual machines. i. What security vulnerability does a VM escape attack exploit? (5) ii. How can hypervisor security hardening prevent such attacks? (5) iii. What security policies should cloud providers implement to protect multi-tenant environments? (5)	CO5