Reg. No.															

Question Paper Code	13597

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2025

Sixth Semester

Computer Science and Engineering (Cyber Security)

20SCPC601 - DISTRIBUTED AND CLOUD SECURITY

Regulations - 2020

Duration: 3 Hours Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	*K – Level*	*CO*
1.	In distributed systems, what is transparency (a) Users must manage resources manually. (b) The system hides the complexity of distribution from users. (c) The system always shows the location of resources. (d) Systems are slower and less reliable.	*1*	*K1*	*CO1*
2.	Which of these is a Platform as a Service (PaaS) provider? (a) Microsoft Azure App Service (b) Amazon EC2 (c) Google Docs (d) Dropbox	*1*	*K1*	*CO1*
3.	In federated identity management, identities are managed by which of the following (a) A single centralized server only (b) Each service provider separately (c) Different trusted organizations collaboratively (d) Only the cloud provider	*1*	*K1*	*CO2*
4.	Which of the following is considered a best practice for securing authentication in cloud environments? (a) Using single passwords for all services (b) Disabling multi-factor authentication (c) Enabling multi-factor authentication (MFA) (d) Sharing user credentials via email	*1*	*K1*	*CO2*
5.	Where is data residency primarily concerned? (a) In the process of data encryption (b) The physical or geographical location of data storage (c) The encryption of transferred data (d) The management of user access	*1*	*K1*	*CO3*
6.	Contrast tokenization and data masking. Which of the following is true? (a) Tokenization replaces sensitive data with non-sensitive substitutes, while data masking obscures sensitive data to make it unrecognizable. (b) Tokenization encrypts sensitive data, while data masking stores data in plain text. (c) Tokenization is used for securing data during transfer, while data masking is used for data storage. (d) Both tokenization and data masking completely anonymize data for public use.	*1*	*K2*	*CO3*
7.	How does network segmentation enhance security in cloud environments? (a) By isolating critical resources from other parts of the network to limit the impact of a potential attack (b) By encrypting all network traffic between devices (c) By enabling automatic updates of security patches (d) By preventing any traffic from entering the network	*1*	*K1*	*CO4*

8.	Which of the following is a technique used for securing virtual networks in cloud environments? (a) Network segmentation (b) FTP file transfer (c) Public key infrastructure (PKI) (d) Data redundancy	*1*	*K1*	*CO4*
9.	Choose the type of transactions PCI DSS compliance is related to (a) Social media accounts (b) Credit card transactions (c) Public records (d) Government documents	*1*	*K1*	*CO5*
10.	Tell what Disaster Recovery Planning ensures: (a) New application development (b) Rapid restoration of services after disruption (c) Hiring new employees (d) Selling company assets	*1*	*K1*	*CO6*

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11.	Outline the characteristics of distributed systems.	*2*	*K2*	*CO1*
12.	Differentiate virtualization and containerization.	*2*	*K2*	*CO1*
13.	Illustrate with an example how Single Sign-On (SSO) can improve user experience across multiple platforms.	*2*	*K2*	*CO2*
14.	Summarize the key concept behind Role-Based Access Control (RBAC).	*2*	*K2*	*CO2*
15.	Infer the potential risks associated with insecure data transfer in cloud environments. What are the possible consequences of failing to implement secure protocols like SSL/TLS?	*2*	*K2*	*CO3*
16.	Outline the steps involved in implementing data encryption in a distributed system to ensure both confidentiality and integrity of sensitive data.	*2*	*K2*	*CO3*
17.	Illustrate the process of DDoS mitigation. Explain at least two methods used to defend against DDoS attacks in cloud environments and their effectiveness.	*2*	*K2*	*CO4*
18.	Outline the key differences between intra-cloud and inter-cloud communication. What secure protocols are typically used in each scenario to protect data during transmission?	*2*	*K2*	*CO4*
19.	Illustrate the steps involved in incident response planning in a distributed cloud environment.	*2*	*K2*	*CO5*
20.	Interpret the role of audit trails in cloud forensic investigations.	*2*	*K2*	*CO5*
21.	Classify different types of evidence collected during a cloud forensic investigation.	*2*	*K2*	*CO6*
22.	Infer the potential impact on a business if disaster recovery plans are not in place.	*2*	*K2*	*CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Discuss the differences between IaaS, PaaS, and SaaS, with real-world examples.	*11*	*K2*	*CO1*
		OR			
	b)	Experiment with different containerization and virtualization tools for a cloud-based application. Which one provides faster deployment and better resource efficiency?	*11*	*K2*	*CO1*
24.	a)	Discuss Single Sign-On (SSO) and its advantages and disadvantages with neat diagram.	*11*	*K2*	*CO2*
		OR			
	b)	Compare Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).	*11*	*K2*	*CO2*
25.	a) i)	Apply the principles of secure data transfer protocols to a real-world scenario where you need to transmit sensitive financial data over the internet. Discuss how SSL/TLS and SSH can be implemented to secure this transfer and prevent unauthorized access during transmission.	*6*	*K2*	*CO3*

	ii)	Compare and contrast data masking and tokenization.	*5*	*K2*	*CO3*
		OR			
	b) i)	Construct a security model for ensuring data integrity in a cloud-based distributed storage system.	*6*	*K2*	*CO3*
	ii)	Explain the challenges associated with data residency and compliance in distributed systems.	*5*	*K2*	*CO3*
26.	a) i)	Explain the role of network segmentation in securing cloud environments.	*6*	*K2*	*CO4*
	ii)	Explain the role of cloud-based Web Application Firewalls (WAF) in preventing attacks.	*5*	*K2*	*CO4*
		OR			
	b) i)	Examine the motives behind attackers attempting to exploit virtual network vulnerabilities. How do intrusion detection/prevention systems (IDS/IPS) function to identify and stop malicious activities that target these vulnerabilities?	*6*	*K2*	*CO4*
	ii)	Evaluate the effectiveness of secure communication protocols in protecting data during inter-cloud and intra-cloud communication. What are the strengths and weaknesses of these protocols in preventing unauthorized access?	*5*	*K2*	*CO4*
27.	a)	Estimate the risks of non-compliance with GDPR in cloud deployments and suggest mitigation strategies.	*11*	*K2*	*CO5*
		OR			
	b)	Explain in detail about Incident response planning in cloud environments.	*11*	*K2*	*CO5*
28.	a)	Explain in detail about Cloud auditing and monitoring tools.	*11*	*K1*	*CO6*
		OR			
	b)	Formulate a theory explaining how integrating AI-based monitoring could improve forensic investigations and disaster recovery in cloud systems.	*11*	*K1*	*CO6*