(33)

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATIONS- 2026

B.Tech-8th Semester (CSE/IT)

COURSE CODE (CREDITS): 19B1WCI835 (3) MAX MARKS: 35

COURSE NAME: CLOUD COMPUTING SECURITY

COURSE INSTRUCTOR: Dr Pankaj Dhiman, Ms Nitika MAX. TIME: 2 Hours

Note: (a) All questions are compulsory.

(b) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

(c) Use of calculator is allowed

Q.No	Question	CO	Marks
Q1	Cloud environments are vulnerable to various attack vectors such as hypervisor compromise, tenant hopping, malicious virtual machines, and storage leakage attacks. Critically analyze these attack vectors and discuss mitigation mechanisms for securing cloud infrastructures.	2	5
Q2	In a multi-tenant cloud network, 500 packets/sec are generated by Tenant A and 700 packets/sec by Tenant B. During a DDoS attack, malicious traffic increases Tenant B's traffic by 250%. Calculate the total traffic after the attack. If the IDS can handle only 2200 packets/sec, determine whether congestion will occur.	3	5
Q3	A cloud service provider guarantees annual service availability of 99.95% under its Service Level Agreement (SLA). Calculate the maximum downtime allowed annually and monthly. Discuss the relationship between Quality of Service (QoS), service availability, and security monitoring in cloud infrastructures.	4	5
Q4	Compare compute isolation, network isolation, and storage isolation strategies in cloud environments. Which isolation mechanism is most critical in multi-tenant public clouds and why?	3	5
Q5	Cloud Security Alliance (CSA), NIST, and ENISA provide important security guidelines for cloud computing. Compare these frameworks and critically analyze their contributions toward improving cloud security governance and risk management.	2	5
Q6	Explain the working of Multi-Factor Authentication (MFA) in cloud environments. How does MFA mitigate phishing and credential theft attacks?	4	5
Q7	Cloud computing introduces scalability and elasticity as major advantages over traditional systems. Critically discuss how dynamic scaling affects security monitoring, access control enforcement, and incident response mechanisms.	1	5