(159)

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATIONS- 2026

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

COURSE CODE (CREDITS): 19B1WCI835 (3) MAX MARKS: 25

COURSE NAME: CLOUD COMPUTING SECURITY

COURSE INSTRUCTOR: Dr Pankaj Dhiman, Ms Nitika MAX. TIME: 1 Hour 30 Min

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 not allowed

Q.No	Question	CO	Marks
Q1	In a distributed healthcare system, maintaining both confidentiality and integrity is critical. Critically analyze the trade-offs between confidentiality and integrity and propose a hybrid mechanism using encryption, hashing, and digital signatures. Evaluate performance overhead and scalability issues.	2	5
Q2	A virtual machine has 120 services running, out of which 45 are unnecessary. Each unnecessary service introduces a 0.02 probability of exploitation. After OS hardening, all unnecessary services are removed. Calculate the total risk reduction achieved. If each remaining service still has a baseline vulnerability probability of 0.005, compute the residual system risk.	3	5
Q3	Explain the concept of Zero Trust Architecture. Design a Zero Trust model for cloud systems and compare it with traditional perimeter-based security	2	3
Q4	In an organization, the probability of an insider data leak per employee is 0.001, and there are 500 employees. Calculate the probability that at least one data leak occurs. Based on your result, suggest appropriate data protection strategies to mitigate insider threats.	3	5
Q5	Differentiate between authentication and authorization in cloud systems. Design a secure framework integrating multi-factor authentication (MFA) and role-based access control (RBAC). Analyze how the system prevents unauthorized access even if credentials are compromised.	2	4
Q6	Explain the concepts of OS hardening and system minimization in the context of cloud and IoT environments.	3	3