JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2025

B.Tech-II Semester (CSE/IT/ECE/CE/BT/BI)

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

COURSE NAME: Cloud Computing Security

COURSE INSTRUCTORS: Er. 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

Q.No	Question	CO	Marks
Q1	Explain how proactive activity monitoring and identity management work together to enhance cloud security. Discuss with reference to intrusion detection, system privilege abuse, and the role of Single Sign-On (SSO) in access control.	CO4	[7]
Q2	What is the role of encryption in ensuring data confidentiality in cloud computing? Briefly explain how encryption and key management help protect tenant data in the cloud.	CO4	[7]
Q3	An organization stores 500 GB of sensitive customer data on a cloud platform. As part of its data protection policy, the data is encrypted using a 256-bit AES algorithm. To ensure secure key management, the organization uses a Key Management Service (KMS) that supports automated key rotation every 90 days. Given the following: • The cloud provider charges ₹0.15 per GB per month for encrypted storage. • There is an additional ₹0.05 per GB per key rotation (as a processing overhead). • The organization retains data for 12 months. Calculate the total annual cost of encrypted storage including key rotation overhead.	CO4	[7]
Q4	Cloud security must address both architectural complexity and multitenancy risks. Critically evaluate how secure isolation strategies in compute, network, and storage layers help mitigate threats in a multitenant environment. Reference at least one guideline (CSA, NIST, or ENISA) and relate it to a real-world scenario where isolation failure led to a breach or security compromise.	CO2	[7]
Q5	A cloud storage provider manages tenant data across three lifecycle stages: Active, Archived, and To-be-deleted. The data volume and protection techniques applied at each stage are as follows:	CO3	[7]

Stage	Data Volume (TB)	Encryption Overhead (%)	Tokenization Applied	Deletion Cost ($/TB)
Active	4	20	Yes	N/A
Archived	6	10	No	N/A
To-be-deleted	2	15	Yes	25

1) Calculate the total effective data volume after applying encryption overhead.
2) Determine the total deletion cost for the "To-be-deleted" stage.
3) Identify the total amount of data that is tokenized.