

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

B.Tech.-V SEMESTER | T1 EXAM - AUGUST 2026

COURSE CODE (CREDITS): 25B11CI513 (3)

MAX. MARKS: 15

COURSE NAME: Cloud Computing and Security

MAX. TIME: 60 Min.

COURSE INSTRUCTORS: D. Gupta

Note: 1) All questions are compulsory. Marks and COs for each question are indicated. 2) Answer the questions in the given order. 3) Be concise and write neatly. 4) Use of calculators is not allowed.

Q. No.	Question	CO	Marks
Q. 1	Define Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). For each model, state one real-world example, one type of user who would typically use it, and one key benefit and one key limitation it offers compared to a traditional on-premises setup.	1	3
Q. 2	Compare Full Virtualization and Para-Virtualization on the basis of isolation, security, technique used, speed, portability, and give one example hypervisor/product for each. Based on your comparison, justify which approach is better suited for a security-sensitive, multi-tenant public cloud environment.	1	3
Q. 3	A retail company runs a real-time fraud-detection pipeline (e.g. Apache Kafka → Apache Spark → Delta Lake) on a hybrid cloud, keeping sensitive transaction data on its private cloud while bursting non-sensitive processing to the public cloud. a) Explain how the security design principles of Least Privilege, Defense in Depth, and Fail-Safe Defaults would each be applied in this pipeline. b) Identify one benefit and one limitation of using a hybrid deployment model in this scenario.	2	3
Q. 4	a) Compare Public Cloud and Private Cloud on ownership, tenancy, cost, control/security, and scalability. Give one real-world use case for each. b) List and briefly explain the four key properties of a Virtual Machine: Partitioning, Isolation, Encapsulation, and Hardware Independence. c) Data protection must cover the entire data lifecycle. Explain the security approach used for data at rest, data in transit, and data in use, naming one relevant technology/standard for each (e.g., AES-256, TLS, TEE).	2	6 (2+2+2)