| QP Code: D154042 | Total Pages: 1 | Name: |
|---|---|---|
| | | Register No. |

**FIFTH SEMESTER (CUFYUGP) DEGREE EXAMINATION, NOVEMBER 2026**

**COMPUTER SCIENCE**

**CSC5EJ306(3) – SECURITY AND PRIVACY IN CLOUD**

**2024 Admission onwards**

**Maximum Time: 2 Hours** | **Maximum Marks: 70**

## Section A

**All Questions can be answered. Each Question carries 3 marks (Ceiling: 24 Marks)**

| | |
|---|---|
| 1 | What is non-repudiation? How is it achieved in cloud security? |
| 2 | Define a hash function. Mention any two properties of a secure hash function. |
| 3 | What is authentication? Why is it important in cloud computing? |
| 4 | What is end-to-end access control? |
| 5 | Define virtualization security in a cloud environment. |
| 6 | Differentiate between encryption and obfuscation. |
| 7 | What is an Identity Provider? State its role in cloud computing. |
| 8 | What is Multi-Factor Authentication? Give two examples of authentication factors. |
| 9 | What is OS hardening? Why is it required in cloud infrastructure? |
| 10 | What is geo-tagging in cloud computing? |

## Section B

**All Questions can be answered. Each Question carries 6 marks (Ceiling: 36 Marks)**

| | |
|---|---|
| 11 | Explain hash functions and their applications in cloud security. |
| 12 | Describe digital signatures and explain how they provide authentication and non-repudiation. |
| 13 | Explain comprehensive data protection and end-to-end access control as security design principles. |
| 14 | Describe data retention, detection and archiving procedures for tenant data. |
| 15 | Explain encryption, redaction, tokenisation and obfuscation as cloud data protection techniques. |
| 16 | Explain RBAC and discuss its advantages in managing access to cloud resources. |
| 17 | Explain the relationship between identity providers and service consumers in cloud computing. |
| 18 | Describe intruder detection and prevention mechanisms used in cloud environments. |

## Section C

**Answer any ONE. Each Question carries 10 marks (1x10=10 Marks)**

| | |
|---|---|
| 19 | Explain cloud access-control architecture, covering identification, authentication, authorization, RBAC, MFA and SSO. |
| 20 | Analyse cloud security design patterns, including cloud bursting, geo-tagging, secure interfaces and resource access control, with suitable examples. |