

# CLOUD SECURITY

|                                   |                                         |                                                          |                         |
|-----------------------------------|-----------------------------------------|----------------------------------------------------------|-------------------------|
| <b>Subject Code:</b><br>CS35325CS | <b>Subject Type:</b> DE<br>(Elective-4) | <b>Evaluation Scheme:</b><br>MSE (30), TA (20), ESE (50) | <b>L-T-P:</b> 3-0-0 (3) |
|-----------------------------------|-----------------------------------------|----------------------------------------------------------|-------------------------|

**Pre-Requisites:** Computer Networks, Cloud Computing, Cryptography & Network Security

**Course Objective:** To provide an in-depth understanding of security challenges and solutions in cloud computing environments, enabling students to design, analyze, and implement secure cloud architectures while addressing issues related to data protection, privacy, identity management, and compliance in distributed systems.

**Course Outcomes:** At the end of the course, the student will be able to

| CO   | Course Outcomes                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------|
| CO-1 | Analyze security threats, vulnerabilities, and risk models specific to cloud computing environments                        |
| CO-2 | Design secure cloud architectures incorporating identity management, encryption, and access control mechanisms             |
| CO-3 | Evaluate cloud security solutions including virtualization security, container security, and network protection techniques |
| CO-4 | Apply security governance, compliance frameworks, and privacy-preserving techniques in real-world cloud deployments        |

## Syllabus:

### Unit-1: Introduction to Cloud Security

Cloud computing models (IaaS, PaaS, SaaS) and deployment models (public, private, hybrid), shared responsibility model, cloud threat landscape, attack surfaces in cloud environments, risk assessment and threat modeling, security challenges in multi-tenant environments, data lifecycle in cloud, fundamentals of trust and security requirements.

### Unit-2: Identity, Access Control and Data Security

Identity and Access Management (IAM), authentication mechanisms (multi-factor authentication, federated identity), authorization models (RBAC, ABAC), cryptographic techniques for cloud (encryption at rest and in transit), key management systems, secure data storage, data masking, tokenization, and privacy preservation in cloud systems.

### Unit-3: Infrastructure and Network Security in Cloud

Virtualization security, hypervisor vulnerabilities, container security and orchestration platforms (Docker, Kubernetes), network security in cloud (VPCs, firewalls, intrusion detection/prevention systems), secure API design, zero-trust architecture, security monitoring and incident response in cloud environments.

### Unit-4: Advanced Cloud Security and Governance

Cloud security frameworks (CSA, NIST), compliance standards (ISO 27001, GDPR), security auditing and logging, DevSecOps practices, secure software development in cloud, cloud forensics, privacy-preserving techniques (homomorphic encryption, differential privacy), emerging trends such as confidential computing and secure multi-party computation.

## Learning Resources:

### Text Books:

1. Ronald L. Krutz & Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley.
2. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy, O'Reilly.
3. NIST Special Publications on Cloud Security.