ELECTIVE-4

CLOUD SECURITY

Subject Code: CS34324CS	Subject Type: Elective
Evaluation Scheme: MSE(30), TA(20), ESE(50)	L-T-P: 3-0-0

Pre-Requisites: Computer Networks, Operating Systems, Cryptography, Information Security Fundamentals

Course Objective: To provide a comprehensive understanding of cloud computing security concepts, threats, defensive mechanisms, and secure management strategies across different cloud service models.

Course Outcomes:

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

CO-1	Understand and analyze the fundamental concepts, architectures, and security challenges in cloud computing.
CO-2	Evaluate security mechanisms across network, host, and application layers in cloud environments.
CO-3	Understand and implement data security, storage protection, and encryption techniques in the cloud.
CO-4	Analyze availability, risk management, and compliance strategies across SaaS, PaaS, and IaaS models.
CO-5	Evaluate cloud security tools, techniques, and real-world challenges in securing cloud infrastructures.

Course Articulation Matrix:

CO/PO	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	2	2	1	2	1
CO-2	3	3	2	2	2	2
CO-3	3	2	2	1	2	1
CO-4	2	3	2	2	3	2
CO-5	2	2	3	1	3	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Introduction to Cloud Security

Introduction to cloud computing; service models (SaaS, PaaS, IaaS); deployment models (public, private, hybrid); concepts of security; system security assessment; information-theoretic vs computational security; key drivers and barriers to cloud adoption; shared responsibility model; threat landscape in cloud environments.

Unit-2: Infrastructure Security

Network-level security: confidentiality, integrity, access control, mitigation techniques; host-level security in SaaS, PaaS, IaaS; virtualization security and hypervisor risks; application-level threats and vulnerabilities; privacy and compliance risks; threats to infrastructure, data, and identity; case study: Amazon EC2 infrastructure security.

Unit-3: Data Security and Storage

Data security in cloud environments; data classification and lifecycle; data dispersal and redundancy techniques; high availability and integrity mechanisms; encryption (at rest, in transit); key management systems (KMS); cloud forensics; data location and jurisdiction issues; backup and recovery strategies.

Unit-4: Security Management and Availability

Security management standards (ISO 27001, NIST); identity and access management (IAM); availability management strategies; SLA considerations; SaaS, PaaS, IaaS availability models; risk assessment and mitigation; compliance and governance; incident response and disaster recovery planning.Cloud Security Tools and Emerging Trends: Cloud security tools and techniques; data encryption/decryption methods; intrusion detection and prevention in cloud; SIEM integration; trusted cloud infrastructures; DevSecOps practices; regulatory and compliance issues (GDPR, HIPAA); emerging trends: Zero Trust Architecture, container security, serverless security.

Learning Resources:

Text and Reference Books:

1. Mather, T., Kumaraswamy S., and Latif, S. *Cloud Security and Privacy*, O'Reilly, 2009.
2. Stallings, William. *Cryptography and Network Security*, Pearson, 2022.
3. Krutz, Ronald L., and Russell Dean Vines. *Cloud Security*, Wiley, 2010.
4. Rittinghouse, John W. *Cloud Computing: Implementation, Management, and Security*, CRC Press, 2009.
5. Menezes, A., et al. *Handbook of Applied Cryptography*, CRC Press, 1996.