SECURITY AND PRIVACY IN CLOUD COMPUTING
ENCTNS 571

Credits: 4 **Year: I** **Part: II**

Course Objectives

This course presents comprehensive introduction to cloud computing, cloud computing architecture, Cloud management, Security Management in the Cloud, Monitoring, Auditing and Management, Cloud security. It Focus on the Real-world goals for services provided by security and privacy in cloud Computing, the constrains on cloud computing infrastructure security and addresses regulatory compliance requirements critical to design, implement, deliver and manage secure cloud-based services.

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
• Understand the history and evolution of cloud computing. • Identify key features and service requirements of cloud computing. • Analyze cloud and dynamic infrastructure. • Evaluate the challenges of cloud computing.	**1 Introduction to cloud computing** 1.1 History of Cloud Computing 1.2 Features of cloud computing 1.3 Cloud services requirements 1.4 Cloud and dynamic infrastructure 1.5 Challenges of cloud computing	8	• Lectures: Introduction to cloud computing concepts and trends. • Case Studies: Real-world examples of cloud adoption. • Hands-on Labs: Exploring cloud platforms (AWS, Azure, GCP). • Group Discussions: Challenges and benefits of cloud adoption.
• Understand cloud computing characteristics and models (PaaS, SaaS, IaaS).	**2 Cloud Computing Architecture** 2.1 Cloud computing Characteristics 2.2 Cloud reference model -platform as service 2.3 Software as a service, infrastructure as service	12	• Lectures: Explanation of cloud models and architectures. • Lab Sessions: Implementing cloud

• Compare different cloud deployment models (Public, Private, Hybrid, Community). • Design and implement cloud architecture using SOA principles. • Evaluate security, trust, and privacy in cloud environments.	2.4 Cloud deployment models 2.4.1 Public clouds 2.4.2 Private clouds 2.4.3 Community cloud, hybrid clouds 2.5 Cloud design and implementation using SOA 2.6 Security, trust and privacy		environments in AWS or Azure. • Case Studies: Cloud adoption strategies for businesses. • Hands-on Projects: Deploying applications on different cloud models.
• Understand security management standards for cloud computing. • Implement availability management for SaaS, PaaS, and IaaS. • Analyze access control mechanisms and security vulnerabilities. • Apply patch management and configuration best practices.	**3 Security Management in the Cloud** 3.1 Security Management Standards, 3.2 Security Management in the Cloud Availability Management, 3.3 SaaS Availability Management 3.4 PaaS Availability Management, 3.5 IaaS Availability Management, 3.6 Access Control, 3.7 Security Vulnerability 3.8 Patch, and Configuration Management	10	• Lectures: Security management frameworks (ISO 27001, NIST). • Workshops: Implementing access control in cloud environments. • Practical Demonstrations: Patch management in AWS/Azure. • Case Studies: Cloud security incidents and mitigation strategies.
• Understand the cloud-based information life cycle. • Apply data	**4 Data Privacy for Cloud Infrastructure and Services** 4.1 Cloud based Information Life Cycle 4.2 Data protection for Confidentiality and Integrity 4.3 Common attack vectors and threats	12	• Hands-on Labs: Implementing encryption and data protection techniques. • Lectures: Cloud data

protection techniques for confidentiality and integrity. • Identify common attack vectors and threats in cloud environments. • Implement encryption, tokenization, PKI, and key management strategies. • Develop data retention, deletion, and archiving procedures.	4.4 Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key 4.5 Management, Assuring data deletion 4.6 Data retention, deletion and archiving procedures for tenant data 4.7 Data Protection plan and Strategies.		privacy regulations and compliance. • Case Studies: Real-world breaches and data privacy failures. • Group Activities: Designing secure cloud storage strategies.
• erform proactive monitoring and incident response in cloud environments. • Detect unauthorized access, malicious traffic, and privilege abuse. • Implement intrusion detection and security event management. • Audit logs and ensure tamper-proof security	**5 Monitoring, Auditing and Management** 5.1 1Proactive activity monitoring 5.2 Incident Response 5.3 Monitoring for unauthorized access, malicious traffic, abuse of system privileges, intrusion 5.4 Detection, events and alerts auditing 5.5 Tamper-proofing audit logs 5.6 Quality of Services 5.7 Secure Management 5.8 User management 5.9 Identity management 5.10 Security Information and Event Management	12	• Lab Exercises: Implementing SIEM (Security Information and Event Management). • Lectures: Incident response planning and auditing best practices. • Simulations: Security breach and forensic investigation scenarios. • Hands-on Labs: Analyzing cloud security events in real-time.

compliance. • Evaluate Quality of Service (QoS) and secure user management.			
• Identify security challenges and risks in cloud computing. • Implement security monitoring techniques for cloud-based applications. • Design security architecture for cloud deployments. • Apply data security and application security principles. • Implement identity management and access control for virtual environments.	**6 Cloud Security** 6.1 Cloud Security challenges and Risks 6.2 Software-as-a-Service Security 6.3 Security Monitoring 6.4 Security Architecture Design 6.5 Data Security 6.6 Application Security 6.7 Virtual Machine Security 6.8 Identity Management and Access Control	6	• Lectures: Cloud security threats and risk management. • Workshops: Implementing identity management in cloud environments. • Practical Demonstrations: Configuring virtual machine security. • Case Studies: Cloud security failures and lessons learned.

Lab Activities

1. Information Security Gap Assessment through ISO 27001
2. Cyber Security Maturity Assessment thorough NIST Cyber Security Framework.
3. IT Governance Audit through Control Objective for Related Technologies.

4. Develop IS Audit Terms of Reference
5. IS Audit Case Studies and Practical Exercises

Evaluation Schemes

a. Internal Evaluation

Type	**Weightage**
Minor tests	70%
Assignments	30%

b. Final Exam

The questions will cover all chapters of the syllabus. The evaluation scheme will be as indicated in the table:

Chapter	**Hours**	**Mark distribution***
1	8	8
2	12	12
3	10	10
4	12	12
5	12	10
6	6	8
		60

*There may be minor deviation in marks distribution.

References

1. Vacca, J. R. (Ed.). (2013). *Network and system security*. Elsevier.
2. Subramanian, M., Gonsalves, T. A., & Rani, N. U. (2010). *Network management: principles and practice*. Pearson Education India.
3. Buyya, R., Vecchiola, C., & Selvi, S. T. (2013). *Mastering cloud computing: foundations and applications programming*. Newnes.
4. Mather, T. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.