Cloud Computing Security

Coursetitle& Code	Credits	Creditdistributionofthecourse			Eligibility criteria	Pre-requisiteofthe course (if any)
		Lectur	Tutorial	Practical/Pract		
Cloud Computing Security	4	3	0	1	Class XII Pass	NA

COURSE OBJECTIVE

- To understand the fundamental concepts of Cloud Computing, including delivery models (SaaS, PaaS, IaaS) and deployment models (Public, Private, Community, Hybrid).
- To gain insights into Cloud Computing architecture and the benefits of implementing Cloud solutions across different business environments.
- To learn about Cloud security principles, including confidentiality, integrity, availability, and secure development practices.
- To explore the risks and security challenges in Cloud Computing, including privacy, compliance, and service provider risks.
- To understand Cloud Computing security architecture, focusing on identity management, access control, and autonomic security in Cloud environments.

COURSE OUTCOME

After completion of this course, students will be able to:

- Explain the core concepts of Cloud Computing, including different delivery and deployment models.
- Design and implement Cloud Computing architectures to meet business and security requirements.
- Apply Cloud security principles to ensure data confidentiality, integrity, and availability in Cloud environments.
- Identify and mitigate risks and security challenges associated with Cloud services and infrastructure.
- Implement security measures in Cloud systems, including identity management, access control, and autonomic security.

SYLLABUS

Unit 1: Cloud Computing Fundamentals (9 Hours)

Introduction to Cloud Computing, Cloud Delivery Models: SaaS, PaaS, IaaS, Cloud Deployment Models: Public, Private, Community, Hybrid, Expected Benefits of Cloud Computing

Unit 2: Cloud Computing Architecture (8 Hours)

Overview of Cloud Computing Architecture, Cloud Delivery Models: SaaS, PaaS, IaaS, Cloud Deployment Models: Public, Private, Community, Hybrid

Unit 3: Cloud Computing Software Security Fundamentals (9 Hours)

Cloud Information Security Objectives: Confidentiality, Integrity, Availability, Cloud Security Services and Design Principles, Secure Cloud Software Requirements, Secure Development Practices

Unit 4: Cloud Computing Risk Issues and Security Challenges (9 Hours)

Privacy and Compliance Risks in Cloud Computing, Threats to Infrastructure, Data, and Access Control, Cloud Access Control Issues, Security Policy Implementation and Types, Cloud Service Provider Risks

Unit 5: Cloud Computing Security Architecture (10 Hours)

Architectural Considerations in Cloud Security, Trusted Cloud Computing, Secure Execution Environments, Identity Management and Access Control, Autonomic Security in Cloud Computing

REFERENCE BOOKS

1. Ronald L. Krutz, Russell Dean Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Wiley.
2. John W. Ittinghouse, James F. Ransome, *Cloud Computing: Implementation, Management, and Security*, CRC Press.
3. Borko Furht, Armando Escalante, *Handbook of Cloud Computing*, Springer.
4. Charles Badcock, *Cloud Revolution*, TMH.

PRACTICAL COMPONENT (IF ANY)

The practicals are based on open-source tools like OpenStack, CloudStack, Eucalyptus, and Minikube for Kubernetes.

LIST OF PRACTICALSPractical (30 Hours)

1. Setting Up a Private Cloud with OpenStack
2. Creating and Managing Virtual Machines in CloudStack
3. Deploying a Containerized Application Using Kubernetes (Minikube)
4. Setting Up Multi-Tier Applications in OpenStack using Heat Orchestration
5. Simulating Cloud Storage Using OpenStack Swift
6. Configuring and Managing Virtual Networks in OpenStack Neutron
7. Cloud Monitoring Using OpenStack Ceilometer