NIRMA UNIVERSITY

Institute:	Institute of Technology, School of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	6CS405CC22
Course Title:	Secured Cloud Computing
Course Type:	Department Elective-I
Year of Introduction:	2022-23

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLOs):

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

1. explain the fundamentals of cloud computing architectures based on current standards, protocols, and best practices (BL2)
2. experiment with the concepts and guiding principles for designing and implementing security in Cloud Computing (BL3)
3. discover threats, risks, vulnerabilities, and privacy issues associated with cloud-based IT services (BL4)
4. conclude the safeguards and countermeasures for Cloud-based IT services. (BL5)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Fundamental of Cloud and its security aspects:** Understand what is Cloud computing, the Architectural and Technological Influences of Cloud Computing, Understand the Cloud deployment models Public, Private, Community, and Hybrid models, Scope of Control, Software as a Service (SaaS) Platform as a Service (PaaS) Infrastructure as a Service (IaaS) Cloud Computing Roles, Risks and Security Concerns. Industry-Specific Cloud Security Standards	08
Unit-II	**Cloud Virtualization:** Virtual machines and virtualization of clusters and data centers automation, Applications of Virtual Machines, Implementation levels of virtualization, Virtualization Introspection, monitoring for unauthorized access, and safeguarding hypervisors against potential vulnerabilities and exploits	07
Unit-III	**Guiding Security design principles:** Data center design and interconnection networks, InterCloud resource management, Cloud Security and trust management, Cloud Infrastructure and SLA. Secure isolation, comprehensive data protection, and end-to-end access control, monitoring, and auditing. Common attack vectors and threats. Multitenancy, Inter-tenant network segmentation strategies, Storage isolation strategies	05
Unit-IV	**Data Protection for Cloud Infrastructure and Services:** Understand the Cloud-based Information Life Cycle, Data protection for Confidentiality and Integrity, Common attack vectors and threats, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key Management, and Data Protection Strategies. Securing Compute	07

	service, Securing Storage, Securing Network services, Case-study: Cloud Data Loss Prevention (DLP)	
Unit-V	**Security Parameters in Cloud:** Authentication and Authorization, Roles-based Access Control, Multi-factor authentication, Host, storage, and network access control options, OS Hardening and minimization, securing remote access, Firewalls, IDS, IPS, and honeypots. Proactive activity monitoring, Incident Response, Monitoring for unauthorized access, malicious traffic, Quality of Services, Secure Management, User management, and Identity access management	06
Unit-VI	**Cloud Security Essentials:** Single Sign-on, Identity Federation, Identity providers, and service consumers, The role of Identity provisioning, Security Patterns for Cloud Computing, Trusted Platform, Geo-tagging, Cloud VM Platform Encryption, Trusted Cloud Resource Pools, Secure Cloud Interfaces.	07
Unit-VII	**Security Patterns for Cloud Computing:** Data Sovereignty, AI-driven threat Detection, Data Security pattern, storage On-Premise Internet Access, Secure External Cloud Connection, Denial-of-Service, Cloud Traffic Hijacking Protection, Trust Attestation Service, Collaborative Monitoring and Logging, Independent Cloud Auditing, Protecting serverless architectures and microservices through API security, secure CI/CD pipelines, and runtime application self-protection (RASP).	05

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study content.

Suggested Readings/ References:

1. Kai Hwang, Geoffrey C. Fox, Jack J Dongarra, Distributed and Cloud Computing, Morgan Kaufmann
2. Mather, T., Kumaraswamy, S., & Latif, S., Cloud security and privacy: an enterprise perspective on risks and compliance. O'Reilly
3. Vacca, J. R., Cloud computing security: foundations and challenges. CRC Press
4. Gupta, B. B., Cloud Security: Concepts, Applications and Perspectives. CRC Press.

Suggested List of Experiments:

Sr. No.	Name of Experiments/Exercises	Hours
1	Working with AWS IAM (Identity Access Management) to assign various rights to the cloud user for dedicated services.	02
2	Identification and observations of the phishing attack in the Cloud eco-system.	02
3	Understanding and handling of Cloud Security breaches to manage safety in the cloud eco-system.	02
4	To classify the cloud security parameters and analyse them for network security.	04
5	Understanding the Cloud network topology and analysing its network behaviour with different Cloud-based tasks	04

6	Exploring and implementing the open-source cloud security tools. Understanding and analysing its impact to the cloud resources components. https://blog.runpanther.io/open-source-cloud-security-tools	04
7	Performing a DDoS simulation attack and identifying its pattern using Wireshark tool/ or any other networking tool (Goldeneye simulator)	04
8	Implementing the cloud monitoring strategy on any public/private cloud and identify the traces of the attack (DDoS Attack scenario can be considered)	04
9	Identifying the SLA violation using Rally and analysing its results in terms of a graph representation and tracing the anomaly detection.	04