NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	B.Tech. Computer Science and Engineering
Course Code:	2CSDE79
Course Title:	Cloud Security and Frameworks
Course Type:	Departmental Elective
Year of Introduction:	2021-22

Credit Scheme

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

Course Learning Outcomes (CLO):

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

1. classify cloud architectural aspects
2. recognize the trusted platform for cloud computing.
3. identify the security risks associated with the cloud platforms
4. inspect the cloud computing security design patterns

Syllabus: **Total Teaching hours: 45**

Unit	Syllabus	Teaching hours
Unit-I	**Fundamentals of cloud computing architecture and security issues:** Current Cloud standards, various protocols used, and best practices intended for delivering Cloud-based services. Identification of the cloud threats, vulnerabilities, and privacy issues of cloud-based IT services. Common attack vectors and threats, encryption, data redaction, tokenization, obfuscation, PKI and Key management, assuring data deletion, data retention, and archiving procedures for tenant data, data protection strategies.	10
Unit-II	**Cloud Design principles with the perspective of security**: Identification and understanding of the core principles for designing and implementing appropriate safeguards and methods for cloud services. Secure isolation strategies multitenancy, virtualization strategies inter-tenant network segmentation strategies, storage isolation strategies. OS Hardening and minimization, securing remote access, verified and measured boot, firewalls, IDS, IPS, and honeypots. end-to-end identity and access management, monitoring and auditing processes, and compliance with industry and regulatory mandates.	09

Unit-III	**Trusted Platform for Cloud**: Trust and Reputation Model in Cloud, trusted cloud resource pools, secure cloud interfaces, cloud data breach protection, permanent data loss protection, cloud traffic hijacking protection, cloud authentication gateway, federated cloud authentication cloud key management, trust attestation service, collaborative monitoring and logging independent cloud auditing. Privacy requirements for Cloud computing, metrics for service level agreements (SLA), metrics for risk management. Study of Docker and cloud agnostic architecture and its security issues.	09
Unit-IV	**Cloud Computing Security Design Patterns-I**: Security Patterns for Cloud Computing, Geo-tagging, Cloud VM Platform Encryption, Cloud Resource Access Control, Cloud Data Breach Protection, Permanent Data Loss Protection, In-Transit Cloud Data Encryption.	08
Unit-V	**Cloud Computing Security Design Patterns –II**: Security Patterns for Cloud Computing, network security, identity & access management & trust secure on-premise internet access, secure external cloud connection, cloud denial-of-service protection, cloud traffic hijacking protection, automatically defined perimeter, cloud authentication gateway federated cloud authentication, cloud key management, Case Study: HIPAA compliance.	09

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

Suggested Readings/ References:

1. Vic (J.R.) Winkler, Securing the Cloud: Cloud Computing Security Techniques and Tactics, (Syngress/Elsevier).
2. Thomas Erl, Cloud Computing Design Patterns, Prentice Hall.
3. Raj Samani, Brain Hoanan, Jem Reavis, Vladimir Jirasek, CSA guide to Cloud Computing: Implementing Cloud Privacy and Security, Elsevier.
4. Chris Doston, Practical Cloud Security: A guide for secure design and deployment, OREILLY.

Suggested List of Experiments:

Sr. No.	Practical Title	Hours
1	To work with AWS IAM (Identity Access Management) to assign the various rights to the cloud user for dedicated services	02
2	To configure the private cloud for performing the security approaches and creating a Test bed to perform various attacks and identifying its effect	04

	3	To introduce the Command line configuration for open stack open-source cloud.	02
	4	To get familiar with End-User/ Cloud Operator operations to be conducted in the openstack environment.	02
	5	To understand the network topology and its configuration for open stack open-source cloud.	04
	6	To explore and implement the open-source cloud security tools. To understand and analyse its impact to the cloud resources components	02
	7	To perform a DDoS simulation attack and identifying its pattern using Wireshark tool/ or any other networking tool (Goldeneye simulator)	02
	8	To implement the cloud monitoring strategy on any public/ private cloud and identify the traces of the attack	04
	9	To identify the SLA violation using Rally and analysing its results in terms of a graph representation and to trace the anomaly detection.	04
	10	To perform the malware analysis using a suspicious hash repository from virus total API.	04
	11	Introduction to libVMI for virtual machine monitoring using VM inspection tool.	04
Suggested Case List:		-NA-	