Faculty of Engineering & Technology
Masters of Technology (M. Tech (CS))
(W. E. F.: 2023-24)

Document ID: SUTEEB-01

Name of Faculty	:	Faculty of Engineering & Technology
Name of Program	:	Industry Collaboration Masters of Technology in Cyber Security (M.Tech (CS).)
Course Code	:	2MCS04
Course Title	:	Cloud computing and Security
Type of Course	:	Cyber Security
Year of Introduction	:	2023-24

Prerequisite	:	Fundamental of computer networks, OS fundamentals, Concepts of virtualization, Programming language basics, Concepts of system architecture used
Course Objective	:	
Course Outcomes	:	At the end of this course, students will be able to:
	CO1	Classify the various layers of cloud infrastructure
	CO2	Make use of modern security concepts in cloud computing.
	CO3	Analyze the security of virtual systems
	CO4	Examine the cloud forensics challenges.
	CO5	Assess compliance issues that arise from cloud computing.

Teaching and Examination Scheme

Teaching Scheme (Contact Hours)			Credits	Examination Marks				
				Theory Marks		Practical Marks		Total Marks
L	T	P	C	SEE	CIA	SEE	CIA	
3	0	2	4	70	30	30	20	150

Legends: ***L****-Lecture;* ***T****–Tutorial/Teacher Guided Theory Practice;* ***P*** *– Practical,* ***C*** *– Credit,* ***SEE*** *– Semester End Examination,* ***CIA*** *- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.))*

Course Content

Unit No.	Topics	Teaching Hours	Weightage	Mapping with CO
1	**Cloud Computing Fundamentals**: Definition of Cloud Computing, Cloud Deployment Models: Public, Private, Hybrid and Community Cloud, Service Models: SaaS, PaaS and IaaS, Business Agility: Benefits, Risks and challenges to Cloud architecture. Application availability, performance, security and disaster recovery in cloud, next	05	10%	CO1

	generation Cloud Applications.			
2	**Concepts of Security:** CIA Triad (Confidentiality, integrity, availability), privacy, authentication, non-repudiation, access control, defense in depth, least privilege, how these concepts applicable in the cloud, their importance in PaaS, IaaS and SaaS. e.g., User authentication in the cloud; Cryptographic Systems Symmetric cryptography, stream ciphers, block ciphers, modes of operation, public-key cryptography, hashing, digital signatures, public key infrastructures, key management, X.509 certificates, OpenSSL.	05	05%	CO2
3	**Multi-Tenancy Issues:** Isolation of users/VMs from each other, How the cloud provider can provide this; Virtualization System Security Issues- e.g., ESX and ESXi Security, ESX file system security, storage considerations, backup and recovery; Virtualization System Vulnerabilities- Management console vulnerabilities, management server vulnerabilities, administrative VM vulnerabilities, guest VM vulnerabilities, hypervisor vulnerabilities, hypervisor escape vulnerabilities, configuration issues, malware (botnets etc.)	09	20%	CO3
4	**Virtualization System Specific Attacks**: Guest hopping, attacks on the VM (delete the VM, attack on the control of the VM, code or file injection into the virtualized file structure), VM migration attack, hyper jacking, Kubernetes.	08	20%	CO3
5	**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, assuring data deletion, Data retention, deletion and archiving procedures for tenant Data Protection Strategies	06	15%	CO4
6	**Cloud Forensics:** Cloud Computing Forensic Science Challenges, Confiscation of Cloud resources, Legal challenges and	06	15%	CO5

	standards, Challenges with location, data and logs, Live Forensics, Artifacts gathering from cloud computing, log management, Cloud forensics research & development work			
7	**Legal and Compliance Issues:** Responsibility, ownership of data, right to penetration test, local law where data is held, examination of modern Security Standards (e.g., PCIDSS, FISMA, NIST 800), how standards deal with cloud services and virtualization, compliance for the cloud provider vs. compliance for the customer.	06	15%	CO5

Suggested Distribution of Theory Marks Using Bloom's Taxonomy						
Level	Remembrance	Understanding	Application	Analyse	Evaluate	Create
Weightage	**20**	**30**	**30**	**20**	**0**	**0**

NOTE: This specification table shall be treated as a general guideline for the students and the teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Suggested List of Experiments/Tutorials

Sr. No.	Name of Experiment/Tutorial	Teaching Hours
1	Working with AWS IAM to assign the various rights to the cloud user 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 the same for network security	02
5	Understanding the cloud network topology and analysing its network behaviour with different cloud based tasks.	04
6	Performing a DDoS simulation attack and identifying its pattern using Wireshark tool/ or any other networking tool	04
7	Identifying the SLA violation using Rally and representation and tracing the anomaly detection	04
8	Introduction to libVMI for virtual machine monitoring using inspection tool	04
9	Performing the malware analysis using a suspicious hash repository form virus total API. And identify the suspicious executable files	06

Major Equipment/ Instruments and Software Required

Sr. No.	Name of Major Equipment/ Instruments and Software
1	Wireshark
2	Kali Linux OS
3	VMWare

Suggested Learning Websites

Sr. No.	Name of Website
1	Course-related online MOOCs on NPTEL/SWAYAM/Coursera platform
2	https://www.javatpoint.com/ Cloud computing and Security
3	https://www.coursera.org/specializations/ Cloud computing and Security

Reference Books

Sr. No.	Name of Reference Books
1	"Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, SubraKumaraswamy, ShahedLatif, - O'Reilly Media
2	"Cloud Security" by Ronald L. Krutz, Russell Dean Vines, [ISBN: 0470589876], 2010
3	Handbook of Cloud Computing, BorkoFurht, Armando Escalante, Springer, 2010