GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering

WEF Academic Year	: 2021-22
Semester	: 2
Category of the Course	: Program Elective Course - III
Course Name & Code	: Cloud Computing and Security (4725905)

Prerequisite:

- Fundamental of computer networks, OS fundamentals, Concepts of virtualization, Programming language basics, Concepts of system architecture.

Rationale:

- The course on cloud computing and security introduces the basic concepts of Cloud Computing as well as security systems and cryptographic protocols, which are widely used in the design of cloud security.
- The course is also focused upon the security issues related to multi-tenancy operation, virtualized infrastructure and environment of security and methods to improve virtualization security are also dealt with in this course.

Course Scheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	02	04	70	30	30	20	150

Course Content:

Sr No	Course Content	No of Hours	%
1	UNIT - I: 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 generation Cloud Applications.	05	10%
2	UNIT - II: 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	04	05%

	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.		
3	UNIT - III: 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.)	08	20%
4	UNIT - IV: 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%
5	UNIT - V: 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%
6	UNIT – VI: Cloud Forensics: Cloud Computing Forensic Science Challenges, Confiscation of Cloud resources, Legal challenges and standards, Challenges with location, data and logs, Live Forensics, Artifacts gathering from cloud computing, log management, Cloud forensics research & development work.	06	15%
7	UNIT – VII: 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.	05	15%

Text Books/Reference Books:

1. Tim Mather, SubraKumaraswamy, ShahedLatif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" O'Reilly Media; 1 edition [ISBN: 0596802765], 2009.
2. Ronald L. Krutz, Russell Dean Vines, "Cloud Security" [ISBN: 0470589876], 2010.
3. Handbook of Cloud Computing, BorkoFurht, Armando Escalante, Springer, 2010.

Course Outcome:

After completion of the Course, Students will be able to:

No	Course Outcomes	RBT Level*
01	Classify the various layers of cloud infrastructure.	UN
02	Make use of modern security concepts in cloud computing.	AP
03	Analyze the security of virtual systems.	AN
04	Examine the cloud forensics challenges.	AN
05	Assess compliance issues that arise from cloud computing.	EL

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

Suggested Course Practical List:

- The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required:

- Course-related online MOOCs on NPTEL/SWAYAM/Coursera platform
- Recently Published papers/articles in reputed journals