GUJARAT TECHNOLOGICAL UNIVERSITY

BRANCH NAME:Cyber Security
SUBJECT NAME: Cloud security
SUBJECT CODE:2745903
M.E. 4st Semester

Type of course: Core

Prerequisite: Operating system with memory and input output management

Rationale: Organizations look for cloud solutions rather than investing and maintaining infrastructure on their part. Since the Cloud structure is complex, investigations are necessary from security perspective. Organizations are looking for Cloud service providers which are stable, secure and offer more than one layer of security for their client's data. This course will help in analyzing the security issues, writing incidence report and deploying the security architecture for cloud platform.

Teaching and Examination Scheme

Teaching Scheme			Credits	Examination Marks						Total Marks
				Theory Marks		Practical Marks				
L	T	P	C	ESE (E)	PA (M)	ESE (V)		PA (I)		
						ESE	OEP	PA	RP	
4	0	2	5	70	30	20	10	10	10	150

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	Cloud Computing Fundamentals Essential Characteristics, Architectural Influences, Technological Influences, Operational Influences, Outsourcing, IT Service Management	**5**	10
2	Cloud Computing Architecture Cloud Delivery Models, Cloud Deployment Models, Expected Benefits	**5**	10
3	Cloud Computing Software Security Fundamentals Cloud Information Security Objectives, Cloud Security Services, Relevant Cloud Security Design Principles, Secure Cloud Software Requirements, Secure Cloud Software Testing, Cloud Computing and Business Continuity Planning/Disaster Recovery	**12**	30
4	Cloud Computing Risk Issues The CIA Triad, Privacy and Compliance Risks, Threats to Infrastructure, Data, and Access Control, Cloud Service Provider Risks,	**6**	10
5	Cloud Computing Security Challenges	**8**	20

	Security Policy Implementation, Computer Security Incident Response Team (CSIRT),		
6	Cloud Computing Security Architecture Architectural Considerations, Identity Management and Access Control, Autonomic Security	**6**	10
7	Cloud Computing Life Cycle Issues Standards, The Distributed Management Task Force (DMTF),The International Organization for Standardization (ISO),Incident Response	**6**	10

Suggested Specification table with Marks (Theory):

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
10	**30**	**30**			

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

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

Reference Books:

(i) cloud security - A comprehensive guide to secure cloud computing
By Ronald Krut, Russell Dean Vines , WILEY publication

(ii) cloud security and privacy
by Mather Tim, **Subra Kumaraswamy, Shahed Latif**, SPD ORELLY publication,

(iii) securing the cloud
By Winkler Vic, Syngress publication

Course Outcome:

After learning the course the students should be able to:

- Analyze the cloud computing software security
- Design security models for cloud that minimize risk
- Apply alternate approaches for securing a piece of the cloud.

List of Experiments:

1) Install public cloud. Analyze how handling in public cloud differs from private cloud?

2) Implement phishing attack on cloud.

3) Write a case study of incidence reporting in case of breach of cloud security.

4) Use the services offered by Azure, AWS and GOOGLE. Compare them.

5) Use open source tool to evaluate performance of cloud platform.

6) Prepare a case study of security policy or service level agreement is signed by cloud service provider.

7) Prepare a case study of facebook, twitter data which is stored on cloud. Write a program to inject malware in this data.

8) Implement attribute based encryption algorithm for cloud.

9) Implement compartmentalization techniques, the provider can use to prevent access into virtual container of one customer by other customers.

10) Implement identity management mechanism in cloud.

Design based Problems (DP)/Open Ended Problem:

1) Design an intrusion prevention system for cloud. If the system can not prevent the attack, it should at least reduce the attack.

Major Equipment:

Computer systems having following minimum technical configurations

Processor:i3 or i5 or higher

RAM : minimum 4 GB

HDD : 1 TB

Internet and wifi connectivity

Licence Window/Linux operating system

List of Open Source Software/learning website:

1) **https://cyberforensics.tech.purdue.edu**