

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Security in Cloud Practical
Course Code:	2ET2070301P
Pre-requisite Course:	Computer Network, Network Security and Some web application development and/or systems administration experience is helpful

Course Objectives:

After successful completion of the course, student will be able to

1. Understand core cloud computing concepts and fundamental principles, including standard delivery models and service designs.
2. Understand the foundational security practices that are required to secure modern cloud computing infrastructures.
3. Understand standard cloud security network designs and architecture models.
4. Understand the complexity of cloud threat actors and techniques used to attack a cloud computing infrastructure
5. Understand the regulatory requirements needed to secure data in the cloud and the difficulties in meeting those requirements.

Teaching and Examination Scheme:

Teaching and Examination Scheme:													
Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								
					Theory (Marks)				Practical (Marks)				Total (Marks)
	SEE		CCA		SEE		CCA						
	L	T	P	Total	Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
1	-	-	2	2	-	-	-	-	10	25	10	25	50

Course Contents:

Sr.No	List of Practical	Total Hour
1	Build a threat model for migrating to cloud.	2
2	Create a basic cloud instance on public cloud infrastructure and a security baseline	2
3	Encrypt public cloud data: learn about cloud storage options and encrypt the data for the public cloud deployment.	2
4	Identity Management for the cloud: Create a basic federated identity infrastructure to support their cloud application and learn additional details on standards like SAML and Oauth.	2
5	Private Cloud Analysis Risk	2
6	Create and Secure Private Cloud.	2
7	Implementation of Virtualization in Cloud Computing to Learn Virtualization Basics, Benefits of Virtualization in Cloud using Open Source Operating System.	2
8	Configure Hyper-V • Create and configure virtual machine settings. • Create and configure virtual machine storage. • Create and configure virtual networks	2
9	Implement a Server Virtualization Infrastructure • Implement virtualization hosts. • Implement virtual machines. • Implement virtualization networking. • Implement virtualization storage. • Manage and maintain a server virtualization infrastructure.	2
10	Case Study: Security in Cloud	2
11	Case study on Amazon EC2/Microsoft Azure/ Google Cloud Platform	2

Reference Books:

1. Cloud Computing: Principles and Paradigms, Editors: Rajkumar Buyya, James Broberg, Andrzej M. Goscinski, Wile, 2011
2. Ronald L. Krutz, Russell Dean Vines, Cloud Security
3. Tim Mather, Subra Kumara swamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009.
4. Ronald L. Krutz, Russell Dean Vines: "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley-India, 2010

Course Outcomes:

Course Outcomes	Description	Bloom's Taxonomy Level
CO1	Identify the security issues in the network and resolve it.	Understanding (2)
CO2	Analyse the vulnerabilities in any computing system and hence be able to design a security solution	Understanding (2)
CO3	evaluate security mechanisms using rigorous approaches by key ciphers and Hash functions.	Applying (3)
CO4	Demonstrate various network security applications, IPSec, Firewall, IDS, Web Security, Email Security and Malicious software etc.,	Applying (3)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	M	M		M											
CLO2	H	M			M							L				
CLO3	H	M	M		M											
CLO4	M	M	M		M							L				

H: High, M: Medium, L: Low