

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Security in Cloud
Course Code:	2ET2070301T
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

- Understand core cloud computing concepts and fundamental principles, including standard delivery models and service designs.
- Understand the foundational security practices that are required to secure modern cloud computing infrastructures.
- Understand the differences between traditional data security practices and cloud-based data security methodologies.
- Understand the identity and access management practices of both cloud providers and consumers.
- Understand how to protect data-at-rest, data-in-transit, and data-in-use within a cloud environment.
- Understand standard cloud security network designs and architecture models.
- Understand the complexity of cloud threat actors and techniques used to attack a cloud computing infrastructure
- Understand the regulatory requirements needed to secure data in the cloud and the difficulties in meeting those requirements.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								Total (Marks)
					Theory (Marks)				Practical (Marks)				
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Course Contents:

Unit No	Topics	Total Hours	Weightage (%)
1	Cloud Computing Fundamental: Cloud computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud, Security Concepts: Confidentiality, privacy, integrity, authentication, non-repudiation Threats and Vulnerabilities to Infrastructure, Data, and Access Control; Risk Management and Risk Assessment in Cloud, Cloud Service Provider Risks, Virtualization Security Management in the Cloud, Trusted Cloud Computing, Identity Management and Access Control.	08	25
2	Security Design and Architecture for Cloud Computing: Guiding Security design principles for Cloud Computing Secure Isolation Comprehensive data protection End-to-end access control Monitoring and auditing Quick look at CSA, NIST and ENISA guidelines for Cloud Security, Common attack vectors and threats	07	20
3	Virtualization Compute and, Compute Management: Virtualization in Cloud Computing, Compute Virtualization, Cloud Network Virtualization, Virtual Appliance, Containers and Compute and Configuration Management: Introduction to Docker, Secure Instance Deployment and Lifecycle Management, Image Creation and Hardening, Host Configuration Management. Cloud Infrastructure Automation, Secure Deployment in the Cloud, Vulnerability Scanning	07	20
4	Monitoring, Auditing and Management: Proactive activity monitoring, Incident Response · Monitoring for unauthorized access, malicious traffic, abuse of system privileges, intrusion detection, events and alerts · Auditing – Record generation, Reporting and Management · Tamper-proofing audit logs · Quality of Services · Secure Management · User management · Identity management · Security Information and Event Management	07	20

5	Policy, Compliance & Risk Management in Cloud Computing: security, forensics, personal & data privacy issues within Cloud environment · Cloud security assessment & audit reports, Laws & regulatory mandates · Personal Identifiable Information & Data Privacy · Privacy requirements for Cloud computing (ISO 27018) · Metrics for Service Level Agreements (SLA) · Metrics for Risk Management	07	15
---	---	----	----

Reference Books:

1. Cloud Computing: Principles and Paradigms, Rajkumar Buyya, James Broberg, Andrzej Goscinski
Publisher: Wiley, Publication Year: 2011
2. Cloud Computing: Implementation, Management, and Security, John W. Rittinghouse and James F. Ransome
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 Publishing, 2010.
5. Tim Mather, SubraKumaraswamy, and ShahedLatif, " Cloud Security and Privacy", Published by O'Reilly Media, Inc., 2009

Course Learning Outcomes (CLO):

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	Understand basic of cloud computing and Identify the security issues in the network and resolve it	Understanding (2) / Applying (3)
COL2	Analyse the vulnerabilities in any computing system and hence be able to design a security solution	Understanding (2) / Applying (3)
COL3	Understanding the concept of Virtualization Compute and, Compute Management:	Applying (3)
COL4	Demonstrate various network security applications, IPSec, Firewall, IDS, Web Security, Email Security and Malicious software etc.,	Applying (3)
COL5	Illustrate the Infrastructure and Policy, Compliance & Risk Management in Cloud Computing Infrastructure :	Understanding (2) / 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	H	H	H			L							H	M
CLO2	H	M	H	H	H			L				L			H	M
CLO3	H	M	M	M	H			L							M	M
CLO4	M	M	M	H	H			L				L			M	M
CLO5	M	M	M	H				L				L			M	M

H: High, M: Medium, L: Low