



Programme		B.Sc. IT Honours (Cyber Security)				Branch	Computer Applications		
Semester		VI				Version	1.0.0.0		
Effective from Academic Year			2026-27			Effective for the batch Admitted in		June 2024	
Subject code		U66A2CSE		Subject Name		Cloud Security Essentials			
Teaching scheme						Examination scheme(Marks)			
(Per week)	Lecture (DT)		Practical (Lab.)		Total		CCE	SEE	Total
	L	TU	P	TW					
Credit	2	-	2	-	4	Theory	50	50	100
Hours	2	-	4	-	6				

Objective:

To provide students with a fundamental understanding of cloud security concepts and Google Cloud security practices, enabling them to identify security risks, implement access control mechanisms, apply security monitoring and incident response techniques, and understand basic security operations and automation in cloud environments.

Pre-requisites:

- Basic understanding of computer networks and operating systems
- Fundamental knowledge of cloud computing concepts
- Basic understanding of cybersecurity principles
- Familiarity with programming concepts is desirable but not mandatory

Learning Outcome:

Name of CO	Description
CO1	Understand cloud security fundamentals, shared responsibility principles, and governance concepts in cloud environments.
CO2	Explain identity and access management concepts, authentication mechanisms, and access control strategies in Google Cloud.
CO3	Identify cloud security threats, vulnerabilities, and suitable security control mechanisms for risk mitigation.
CO4	Apply security monitoring and incident response concepts for detecting and managing cloud security events.
CO5	Demonstrate understanding of security automation techniques and cloud security operations practices using Google Cloud tools.

Mapping of CO and PO:

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	2	1	2	1	2	2	1	1
CO2	3	2	2	2	3	1	2	2	2	1	1	1
CO3	3	2	2	2	3	1	2	2	2	1	1	1
CO4	3	2	3	2	3	3	2	2	3	2	2	1
CO5	3	2	3	2	3	2	2	3	3	2	2	2

Content:

Unit	Content	Hrs.
------	---------	------

1	Cloud Security Foundations & Shared Responsibility Introduction to Cloud Computing Models (IaaS, PaaS, SaaS), Shared Responsibility Model, Core Security Concepts (CIA Triad), Risk Types in Cloud, Governance & Compliance in Cloud	06
2	Identity & Access Management (IAM) in Google Cloud Identity, Authentication & Authorization (AAA), IAM roles & policies, MFA, Least privilege principle, Resource hierarchy, Zero Trust model	06
3	Threats, Vulnerabilities & Security Controls Cloud Threat Landscape, Vulnerability Management Basics, Threat Modeling Basics, Administrative, Technical & Physical Controls, Encryption (At Rest & In Transit), Key Management Concepts	06
4	Security Monitoring & Incident Response Logging & Monitoring Concepts, Security Command Center Overview, SIEM Fundamentals, Incident Response Lifecycle, Disaster Recovery & Business Continuity Concepts	06
5	Automation & Security Operations in Google Cloud Basics of Security Automation, Using Python for Security Tasks (Introductory), Automating Log Analysis, Introduction to Cloud Security Analyst Role, Professional Ethics in Cybersecurity	06
Practical Content:		
List of practical specified by subject teacher based on above mentioned topics		
Reference Books:		
1	Surianarayanan, C., & Chelliah, P. R. (2023). Essentials of Cloud Computing: A Holistic, Cloud-Native Perspective. Springer.	
2	Kaiser, A. K. (2024). Become GCP Cloud Digital Leader Certified in 7 Days: Getting to Know Google Cloud. Apress.	
Web Reference:		
1	https://cloud.google.com/docs	
2	https://skills.google.com/learn/certificates/cloud-computing-foundations	
MOOC/Certificate Course:		
1	https://www.coursera.org/professional-certificates/google-cybersecurity	
Question Paper Scheme:		
End Semester Examination Duration: (2 Hours Theory Examination) Note for Examiner: - Q-1 Any Five out of Seven (25 Marks) Q-2 Any Two out of Three (06 Marks) Q-3 Mandatory question (05 Marks) Q-4 Any Two out of Three (08 Marks) Q-5 Any Two out of Three (06 Marks) *The question paper must comprehensively address all Course Outcomes (COs), align with Bloom's Taxonomy levels, and ensure complete syllabus coverage.		

