

CCY4307 Cloud Computing Security**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001 & CCS3203	4	7/8	2	--	2	3

COURSE AIM

To get the students to:

- To provide students with a comprehensive understanding of cloud computing security, covering essential concepts and principles.
- To equip students with the knowledge and skills to design secure cloud architectures and implement security measures in compliance with industry standards and regulatory requirements.
- To enable students to identify and mitigate security risks in cloud environments, including isolation and protection of physical and logical infrastructures.
- To familiarize students with security guidelines and best practices from prominent organizations such as ISO, NIST, ENISA, and CSA in the context of cloud computing

COURSE WEEKLY CONTENTS

- 1 Introduction to Cloud Computing Security
- 2 Cloud Landscape and Architecture Principles
- 3 Cloud Design Patterns for Security
- 4 Case Studies in Cloud Security and Security Approaches
- 5 Security Approaches for Cloud Architecture
- 6 Design Patterns for Cloud Security
- 7 7th Week Assessment
- 8 Industry Standards and Regulatory Compliance Requirements for Cloud Security
- 9 Risk Identification and Mitigation in the Cloud
- 10 Isolation and Protection in Cloud Environments
- 11 Data Protection for OSI Layers in Cloud
- 12 12th Week Assessment
- 13 End-to-End Identity and Access Control
- 14 Cloud Security Monitoring and Auditing
- 15 Security Guidelines from ISO, NIST, ENISA, and CSA for Cloud Computing

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		30	MARKS		→	30
8 to 12	←		20	MARKS		→	20
1 to 15	←		10	MARKS		→	10
16 or 17			Final Exam				40

REFERENCES

Textbook John R. Vacca, Cloud Computing Security, CRC Press