

CCY4203 Internet of Things Security**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY3201	4	7/8	2	--	2	3

COURSE AIM

To get the students to:

- Understand fundamentals of Internet of Things (IoT), its use cases and the implications of security and privacy attacks.
- Learn about attacks against IoT implementations and deployments at the various layers of IoT architecture.
- Gain a deeper understanding of how to systematically identify security threats in IoT and discuss system security lifecycle
- Deploy a simulation tool to develop security and privacy threats mitigation techniques

COURSE WEEKLY CONTENTS

- 1 Course outline, understanding IoT and implications of IoT security attacks
- 2 IoT Architecture and Core Modules - IoT Application Areas and Use Cases
- 3 IoT design, standards and Protocols
- 4 Security threats and vulnerabilities of IoT
- 5 Security Requirements in IoT Architecture
- 6 Security Engineering for IoT
- 7 IoT System Security Lifecycle
- 8 7th week Assessment
- 9 Cryptographic fundamentals for IoT Security Engineering
- 10 Cryptographic fundamentals for IoT Security Engineering (cont.)
- 11 Identity and Access Management Solutions for IoT
- 12 12th week Assessment
- 13 Identity and Access Management Solutions for IoT (cont.)
- 14 Trust and Privacy in IoT
- 15 Mitigating IoT privacy concerns

STUDENT GRADING & ASSESSMENT

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

REFERENCES

Textbook	Russell, Brian, and Drew Van Duren, "Practical Internet of Things Security: A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world". Packt Publishing Ltd.
-----------------	--