EUROPEAN UNIVERSITY

Co-funded by the European Union

EUROPEAN UNIVERSITY FOR CUSTOMISED EDUCATION

STUDY GUIDE

IoT appliacations – Opportunities and Security Challenges

Organised by

Poznan University of Technology

1. IDENTIFYING DATA	
· Course Name.	IoT applications - Opportunities and Security Challenges
· Coordinating University.	Poznan University of Technology
· Partner Universities Involved.	n/a
· Course Field(s).	Computer Science – Internet of Thing
· Related Study Programme.	Undergraduate
· ISCED Code.	645, 655 or 665; 640, 650
· SDG.	2. Good Health and Well-Being 9. Industry, Innovation and Infrastructure
· Study Level.	Bachelor (B)
· EUNICE Key Competencies	[Indicate the Key Competencies offered by the course.] • Green – strongly • Orange - moderately • Red – partially • Blank cell - not at all

Problem solving	Strongly
Teamworking	Strongly
Communication	Strongly
Self-management	Strongly
Cognitive flexibility	
Digital competence	Strongly
Technical competence	Strongly

	Global intercultural competence	• Red – partially

· Number of ECTS credits allocated.	3
· Mode of Delivery.	Hybrid format: self-study + labs + synchronous (consultations)
· Language of Instruction.	English
· Course Dates.	01 march – 31 may 2027
· Precise Schedule of the Lectures.	1.5h every second week – Thursdays 11:45 – 13:15 CEST
· Key Words.	Internet of Things, Sensors, Microcontrollers
· Catchy Phrase.	The IoT is all around us and helps us live better

· Prerequisites and co-requisites.	A student starting this course should have a basic knowledge of digital electronics, microcontrollers, and microprocessors. He should have knowledge to be able to design and implement computer programs in chosen programming languages (e.g., C, Python). He should also have the ability to obtain information from the indicated sources and be ready to cooperate as part of a team. In the area of social competence, he must present attitudes such as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, and respect for other people.; This course is available for bachelor level. Required linguistic skills: English
· Number of EUNICE students that can attend the Course.	30
· Number of EUNICE students that can attend the course per institution	3
· Course inscription procedure(s).	Standard procedure

2. CONTACT DETAILS.	
· Department.	Computing Science
· Name of Lecturer.	Paweł Śniatała | Maciej Sobieraj
· E-mail.	pawel.sniatala@put.poznan.pl | maciej.sobieraj@put.poznan.pl
· Other Lecturers.	n/a

3. COURSE CONTENT.

Lecture topics:
- Internet of Things (IoT) - applications, systems, devices, sensors.
- Principles of operation of selected sensors used in IoT.
- Overview of selected IoT hardware platforms.
- Connectivity / communication of IoT devices (network technologies).
- Data processing in IoT systems (Big data / Cloud Computing / Fog processing).
- Internet of Things security.

Laboratory topics:
- Using Arduino to retrieve information about environmental parameters (temperature sensors, fororesistors, etc.)
- Emergency stop of the production process in response to environmental alarms (Raspberry PI, JSON, MongoDB).
- Using Packet Tracer to test solutions in the field of smart cities and networks (smart grids).
- Prototyping and testing of smart home installations using Packet Tracer (Python, Single Board Computer, smartphone / tablet, router, door opening sensor, etc.)
- Smile-sensitive smart camera (Raspberry PI, Raspberry PI camera, Python, machine learning)
- Intrusion Prevention System (IPS) configuration.
- Testing the vulnerability of simple IoT solutions (Sensor-Actuator System, IFTTT) in the field of ICT security

4. LEARNING OUTCOMES.

A student has structured and theoretically founded general knowledge related to key issues in the field of IoT including sensors and hardware platforms.
A student has advanced detailed knowledge of integrating selected sensors with hardware platforms (Raspberry Pi, Arduino, Intel Edison).
A student has knowledge of development trends and the most important new achievements of IT and telecommunications in the field of IoT systems, Wireless Sensor Networks and hardware platforms used in these systems.

5. OBJECTIVES.
To provide students with knowledge in the field of broadly understood ICT security as well as methods and tools used to estimate and control the risk of compromising confidentiality, integrity and data availability. To acquaint students with advanced methods, techniques and tools used in solving complex engineering tasks in the area of designing and maintaining network systems responsible for the security of transmitting data.

6. COURSE ORGANISATION.	
UNITS	
1.	Internet of Things (IoT) - applications, systems, devices, sensors. Lab: Using Arduino to retrieve information about environmental parameters (temperature sensors, fororesistors,
2.	Principles of operation of selected sensors used in IoT. Lab: Emergency stop of the production process in response to environmental alarms (Raspberry PI, JSON, MongoDB).
3.	Overview of selected IoT hardware platforms. Lab: Using Packet Tracer to test solutions in the field of smart cities and networks (smart grids).
4.	Connectivity / communication of IoT devices (network technologies). Lab: Prototyping and testing of smart home installations using Packet Tracer (Python, Single Board Computer, smartphone / tablet, router, door opening sensor, etc.)
	Data processing in IoT systems (Big data / Cloud Computing / Fog processing). Lab: Smile-sensitive smart camera (Raspberry PI, Raspberry PI camera, Python, machine learning)
	Internet of Things security. Lab: Testing the vulnerability of simple IoT solutions (Sensor-Actuator System, IFTTT) in the field of ICT security
LEARNING RESOURCES AND TOOLS.	
Lab Manuals available on e-kursy. Lectures.	
PLANNED LEARNING ACTIVITIES AND TEACHING METHODS.	
Lectures & Labs	

7. ASSESSMENT METHODS, CRITERIA AND PERIOD.

70% - labs assignemts + 30% - short test from a lecture

OBSERVATIONS.

-

8. BIBLIOGRAPHY AND TEACHING MATERIALS.

[1] Dominique Guinard, Vlad Trifa: Building the Web of Things, Manning Publications, June 2016. ISBN 9781617292682.
[2] Amita Kapoor: Hands-On Artificial Intelligence for IoT: Expert machine learning and deep learning techniques for developing smarter IoT systems, Packt Publishing, 2019.
[3] Colin Dow: Mastering IoT, Packt Publishing, 2019. EAN: 9781838645434
[4] P. Śniatała, S. S. Iyengar, and S. K. Ramani, Evolution of smart sensing ecosystems with tamper evident security. Springer International Publishing, 2021.
[5] P. Śniatała, M. H. Amini, and K. G. Boroojeni, Fundamentals of brooks-iyengar distributed sensing algorithm – trends, advances, and future prospects. Springer International Publishing, 2020.