MODULE HANDBOOK DESCRIPTION

Module designation	*IoT (Internet of Things) Technology*	
Code	*FBD4117*	
Semester(s) in which the module is taught	*6 / third year*	
Person responsible for the module	*A.S.Rachman, ST., MT.*	
Language	*Indonesian*	
Relation to curriculum	*Elective for Computer Engineering*	
Teaching methods	*lectures, small group discussion, project & case base method.*	
Workload (incl. contact hours, self-study hours)	Contact minutes every week, each week of the 16 weeks/semester: • Lectures: 2 x 50 minutes • Exercises and Assignments: 2 x 60 minutes • Self-study: 2 x 60 minutes. Total study hours = 8 hours 30 minutes/week.	
Credit points	*2 SKS (~3.2 ECTS)*	
Required and recommended prerequisites for joining the module	-	
Module objectives/intended learning outcomes	1. *Students are able to understand the basics of IoT and learn about the key concepts and principles of IoT, such as the Internet, connected devices, data, and analytics.* 2. *Students are able to understand the knowledge of hardware and software components that make up an IoT system, including sensors, actuators, microcontrollers, communication protocols, and IoT platforms.*	*PLO3 (M)*

	3. *Students are able to design and implement IoT systems and gain the skills to design, develop, and implement IoT systems by combining hardware and software components, using various communication protocols, and leveraging IoT platforms.* 4. *Students are able to learn and design about the security and privacy challenges associated with IoT technology, such as data breaches, cyber-attacks, and unauthorized access, and explore ways to mitigate these risks.*	*PLO4 (H)*
	5. Students are able to produce real-world applications of IoT technology, such as smart homes, healthcare, transportation, agriculture, and industrial automation, and how IoT is transforming various industries.	*PLO8 (L)*

Content	*IoT technology encompasses a range of hardware and software components and processes, including:* 1. *Sensors and Actuators: Sensors are devices that detect physical and environmental changes, such as temperature, humidity, and light, while actuators are devices that perform physical actions, such as opening doors, turning on lights, and controlling motors.* 2. *Communication Protocols: Communication protocols enable devices to communicate with each other and with the internet, using wireless technologies such as Wi-Fi, Bluetooth, Zigbee, NB-IoT, and LoRaWAN.* 3. *IoT Platforms: IoT platforms provide a framework for managing and processing data from connected devices, enabling data storage, processing, and analytics.* 4. *Cloud Computing: Cloud computing is used to store and process large amounts of data generated by IoT devices, providing a scalable and cost-effective solution for managing IoT data.* 5. *Machine Learning and Artificial Intelligence: Machine learning and artificial intelligence (AI) algorithms are used to analyze and derive insights from the vast amounts of data generated by IoT devices, enabling predictive maintenance, anomaly detection, and other intelligent applications.* 6. *Cybersecurity: IoT security encompasses a range of technologies and practices to ensure the confidentiality, integrity, and availability of IoT devices and data, including encryption, authentication, access control, and intrusion detection.* 7. *Real-World Applications: IoT technology is used in a wide range of real-world applications, such as smart homes, wearables, transportation, healthcare, agriculture, industrial automation, and smart cities.*
Examination forms	- *Case based* - *Project based*
Study and examination requirements	*The final grade in the module is composed of:* *a. Case I assessment: 20%* *b. Case II assessment: 20%* *c. Project based: 60%* *Students must have a final grade of 65% or higher to pass*

Reading list	1. *Maciej Kranz, 2016, "Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry".* 2. *Perry Lea, 2018, "Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security".* 3. *David Hanes, Gonzalo Salgueiro, Patrick Grossetete, 2017, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things".* 4. *Peter Waher, 2015, "Learning Internet of Things".* 5. *Fotis Chantzis, Ioannis Stais, 2019, "Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things".* 6. *Scott Klein, Manuel Meyer, 2017, "IoT Solutions in Microsoft's Azure IoT Suite: Data Acquisition and Analysis in the Real World".* 7. *Amit Kumar Salecha, 2019, "Hands-On IoT Solutions with Blockchain: Build end-to-end IoT applications using Ethereum and Hyperledger".* 8. *by Arshdeep Bahga, Vijay Madisetti (2014), "Internet of Things: A Hands-On Approach".* 9. *by Michael Karnerfors, Christian Berger, Martin Sjödin, Henrik Lönn, 2020, "IoT Automation: Arrowhead Framework".*