Module Specification

Internet of Things (IoT)

Version: 2027-28, v2.0, 20 Jan 2025

Contents

Part 1: Information

Module title: Internet of Things (IoT)

Module code: UFCFBR-30-3

Level: Level 6

For implementation from: 2027-28

UWE credit rating: 30

ECTS credit rating: 15

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: The Internet of Things (IoT), is the connecting and internetworking of multiple devices over the internet, allowing them to communicate with us, applications, and each other.

Features: Not applicable

Educational aims: This module aims to provide learners with an in-depth appreciation of the Internet of Things (IoT) and the tools to design and develop their own multi-device IoT Solution to meet a project requirement.

In completion of this module learners should be able to plan, develop and test a secure multi-client IoT solution to meet a defined scenario using suitable IoT enabled hardware and IoT software.

Evaluate different Machine to Machine (M2M) protocols.

Use a variety of sensors to monitor, record data and trigger actions accordingly

Provide clear and meaningful user access to sensors/data via a web accessible interface or dashboard hosted on a suitable web/cloud/IoT platform.

Identify key legislation impacting the publication of IoT Solutions, data governance, privacy policies, use of data etc.

Outline syllabus: Delivery will cover modern system architecture, key technologies, and legal, social and ethical/moral implications to implementing these technologies.

System architecture (e.g. centralised and decentralised)
Machine-to-Machine (M2M) Communication (e.g. Wireless technologies, Messaging/communication protocols)

Hardware and software platforms for IoT
Legal, social, ethical, and moral implications of IoT
Effective cyber security in relation to IoT

Students will be able to cultivate independent technical judgement in the use of techniques and tools associated with IoT devices and M2M communication protocols. As well as being able to develop the ability to think conceptually and translate concepts into reality, learners will go beyond programming web applications, and develop skills in security, penetration testing and user experience.

Additionally, theoretical content may include

Fundamentals of IoT technology (e.g. Hardware, software, sensors, frameworks)
Comparing key M2M protocols used in IoT
Key legislation impacting the publication of IoT Solutions, e.g. Data Governance (IPO, GDPR, Data Protection), privacy policies, use of data etc.

Part 3: Teaching and learning methods

Teaching and learning methods: Introductory lectures are supported by case studies and practical workshops. Students must have access to a suitable IoT electronics/lab and a hosting platform/database server to be able to complete this module.

Scheduled learning includes lectures, seminars, tutorials, demonstration, practical classes and workshops.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Explain common security risks present when building and publishing web driven IoT solutions.

MO2 Evaluate key IoT hardware, software and Machine to Machine (M2M) protocols.

MO3 Understand key legislation impacting the publication of IoT solutions.

MO4 Plan, develop and test a secure multi-client IoT solution to meet a defined scenario using suitable IoT enabled hardware and software.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 192 hours

Face-to-face learning = 108 hours

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/index.html

Part 4: Assessment

Assessment strategy: This module is assessed by a combination of an online exam (1.5 hour) and a practical portfolio.

The Practical Portfolio will require students to document:
Evidence the planning and design of a IoT solution to support an agreed scenario and the implementation and deployment an IoT solution.

Opportunities for formative assessment exist for the assessment strategy used. Where appropriate, a re-work of the practical portfolio may be considered for the resubmission.

The resit follows the same format as the first sit.

Assessment tasks:

Practical Skills Assessment (First Sit)
Description: The Practical Portfolio will require students to document:
Evidence the planning and design of a IoT solution to support an agreed scenario and the implementation and deployment an IoT solution.
Weighting: 70 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO4

Examination (Online) (First Sit)
Description: Online exam (1.5 hours)
Weighting: 30 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Practical Skills Assessment (Resit)

Description: The Practical Portfolio will require students to document:

Evidence the planning and design of a IoT solution to support an agreed scenario and the implementation and deployment an IoT solution.

Opportunities for formative assessment exist for the assessment strategy used.

Where appropriate, a re-work of the practical portfolio may be considered for the resubmission.

Weighting: 70 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO4

Examination (Online) (Resit)

Description: Online exam (1.5 hours)

Weighting: 30 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1, MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Networking {Top-up} [UCW] BSc (Hons) 2027-28

Software Development {Top-up} [UCW] BSc (Hons) 2027-28

Applied Computing [UCW] BSc (Hons) 2025-26