Bournemouth University

KEY PROGRAMME INFORMATION

Originating institution(s) Bournemouth University	**Faculty responsible for the programme** Faculty of Science and Technology
Final award(s), title(s) and credits MSc Internet of Things with Cyber Security – 180 credits (90 ECTS)	
Intermediate award(s), title(s) and credits PGDip Internet of Things with Cyber Security – 120 Credits (60 ECTS) PGCert Computing– 60 Credits (30 ECTS)	
UCAS Programme Code(s) (where applicable and if known) N/A	**HECoS (Higher Education Classification of Subjects) Code and balanced or major/minor load.** 100365 - Computer Networks (major), 100373 - Internet Technologies (minor) 100376 - Computer and Information Security (minor)

External reference points
The UK Quality Code for Higher Education;
Chapter A1: The National Level (incorporating the Framework for Higher Qualifications (FHEQ) in England, Wales and Northern Ireland);
Chapter A2: The Subject and Qualification Level (incorporating the Subject benchmark statements for Computing (2015));	

Professional, Statutory and Regulatory Body (PSRB) links N/A	
Places of delivery Bournemouth University, Talbot Campus	
Mode(s) of delivery Full-time/Part-time	**Language of delivery** English
Typical duration Sept FT = 12 months, with placement 24 months Sept PT = 24 months, with placement 36 months Jan FT = 16 months, with placement 24 months Jan PT = 32 months, with placement 44 months	
Date of first intake September 2019	**Expected start dates** September and January
Maximum student numbers N/A	**Placements** 30 weeks, optional
Partner(s) Not applicable	**Partnership model** Not applicable
Date of this Programme Specification February 2022	
Version number 2.2-0923	
Approval, review or modification reference numbers E20181916 EC 1819 33 EC 1920 03 FST 2122 01 Approved 25/09/2021, previously version 2.0-0921 FST 2122 14 Approved 02/02/2022, previously version v2.1-092	

EC 2122 72 Approved 25/07/2022
Author Dr. Marios Angelopoulos

PROGRAMME STRUCTURE

Programme Award and Title: MSc Internet of Things with Cyber Security

Stage 1/Level 7
Students are required to complete 4 core units and choose 2 optional units

Unit Name	Core/ Option	No of credits	Assessment Element Weightings			Expected contact hours per unit	Unit version no.	HECoS Code
			Exam 1	Cwk 1	Cwk 2			
Wireless Sensor and Actuator Networks	Core	20	-	100 %		30	2.0	100365; 100367 (balanced)
Mobile and Wireless Networks	Core	20	-	100 %	-	30	1.0	100373; 100367 (balanced)
Research Methods & Professional Issues	Core	20	-	100 %	-	30	2.0	100962 (major); 101090 (minor)
Security and Privacy in Internet of Things	Core	20	-	100%	-	30	2.0	100365; 100376 (balanced)
Human Factors	Option	20	-	100 %	-	30	1.0	100736 (major); 100753 (minor)
Security by Design	Option	20	-	100 %	-	30	1.0	100736 (major); 100753 (minor)
Security Information and Event Management	Option	20	-	100 %	-	30	2.0	100376 (major); 100755 (minor)
Cyber Security	Option	20	-	100 %	-	30	2.0	100376

Progression requirements: There are no progression requirements.

Exit qualification:
PG Cert Computing requires 60 credits at Level 7 (any 60 credits out of these units).

PG Dip MSc Internet of Things with Cyber Security requires 120 credits at Level 7 (completion of all core units and 2 optional units).

Stage 2/Level 7
Students are required to complete the Masters Project.

Unit Name	Core/ Option	No of credits	Assessment Element Weightings			Expected contact hours per unit	Unit version no.	HECoS Code
			Exam 1	Cwk 1	Cwk 2			
Individual Masters Project	Core	60	-	100%	-	10	1.0	100367 (major) 100962 (minor)

Exit qualification
MSc Internet of Things with Cyber Security requires 180 credits at level.

Placement: Optional non-credit bearing placement in industry normally after completion of the taught units and individual masters project (30 weeks minimum). Students are expected to search for suitable placement opportunities, with the support of the Faculty placements team

AIMS OF THE DOCUMENT

The aims of this document are to:

- define the structure of the programme;
- specify the programme award titles;
- identify programme and level learning outcomes;
- articulate the regulations governing the awards defined within the document.

AIMS OF THE PROGRAMME

Internet of Things is an emerging computing and networking paradigm that provisions the massive and seamless integration of everyday devices and automations into the Internet. This seamless integration allows to automatically capture data from and communicate with embedded devices and objects, thus enabling the design and development of more efficient and safe cyber-physical systems. IoT is a key enabling technology for broader and more high level paradigm shifts such as Smart Cities, Smart Health, Industry 4.0 and Circular Economies. The particular characteristics of IoT systems and networks (massive numbers of connections, highly constrained low-end devices, interactions and feedback loops between the digital and physical space, Machine-to-Machine communication, etc) ask for highly-skilled professionals with a focused expertise on IoT that are currently (as of 2018) scarcely available in the market.

In 2012, the number of connected devices overcame the human population. The IoT paradigm provisions billions (and perhaps trillions) of devices to communicate over the Internet. As such, the potential attack surface in IT systems has significantly grown. Furthermore, IoT is a key enabling technology for cyber-physical systems largely affecting critical infrastructure as well as the physical security of people (consider self-driving cars, IoT-enabled pacemakers, etc). The programme aims at educating professional experts capable of efficiently addressing such new challenges.

MSc Internet of Things with Cyber Security is intended for candidates that already have a solid background in Computer Science, Computer Engineering or a relevant field, who wish to become IoT expert professionals with strong background on cyber security. The programme assumes a multi-faceted approach combining theoretical foundations of IoT and ad-hoc networks, hands-on experience with real-life IoT systems and technologies, and an all-around understanding of how IoT is positioned in the context of broader paradigms by integrating managerial and business aspects. The latter is achieved by incorporating corresponding material in the curriculum, by informing (and if possible engaging) students in relevant standardisation activities in which BU is involved (such as in International Telecommunications Union) and by hosting guest lecturers from local and national industry. Finally, the programme equips students with methodological thinking, research disposition and communication skills.

This programme aims to develop critically informed, agile and resourceful graduates, who:

- have a clear and multi-faceted understanding of the IoT paradigm;
- have a deep understanding of the technical aspects of IoT systems and networks;
- have a critical understanding of the latest advances in the field of IoT in terms of research and industry;
- have a strong background on cyber security;
- can demonstrate research skills in areas such as literature reviews, critical analysis of research findings, project proposals, planning, experiment design and analysis, and dissemination.

ALIGNMENT WITH THE UNIVERSITY’S STRATEGIC PLAN

The MSc Internet of Things with Cyber Security programme is informed by, well aligned with, and contributes to BU 2025 strategic plan and the University’s fusion agenda. It also serves the core BU 2025 values of Excellence, Inclusivity, Creativity and Responsibility. In particular, students are supported by academics that are active and esteemed by the international research community.

Involved academics are also very active in international standardisation activities (such as in ITU and ETSI) and have strong synergy liaisons with local, national and international industry. The programme's innovative pedagogic approach offers students the opportunity to learn via hands-on experience with real IoT hardware and commercially available technologies; via collaborative learning; and by engaging with the industry via guest lectures. As a result, students are equipped with the full range of skills (both "hard"-technical and "soft"-transferable ones) needed in order to successfully pioneer in the IoT domain. It is worth noting that Internet of Things is a key enabling technology for future and emerging network and system paradigms (such as 5G networks, Machine Intelligence, the Future Internet, etc) and therefore is directly related to the Strategic Investment Areas of BU in a horizontal and overarching manner and in particular to "*Sustainability & Low Carbon Technology*" and to "*Assistive Technology*".

LEARNING HOURS AND ASSESSMENT

Bournemouth University taught programmes are composed of units of study, which are assigned a credit value indicating the amount of learning undertaken. The minimum credit value of a unit is normally 20 credits, above which credit values normally increase at 20-point intervals. 20 credits is the equivalent of 200 study hours required of the student, including lectures, seminars, assessment and independent study. 20 University credits are equivalent to 10 European Credit Transfer System (ECTS) credits.

The assessment workload for a unit should consider the total time devoted to study, including the assessment workload (i.e. formative and summative assessment) and the taught elements and independent study workload (i.e. lectures, seminars, preparatory work, practical activities, reading, critical reflection).

Assessment per 20 credit unit should normally consist of 3,000 words or equivalent. Dissertations and Level 6 and 7 Final Projects are distinct from other assessment types. The word count for these assignments is 5,000 words per 20 credits, recognising that undertaking an in-depth piece of original research as the capstone to a degree is pedagogically sound.

STAFF DELIVERING THE PROGRAMME

Students will usually be taught by a combination of senior academic staff with others who have relevant expertise including – where appropriate according to the content of the unit – academic staff, qualified professional practitioners, demonstrators/technicians and research students.

PROGRAMME AND LEVEL 7 INTENDED PROGRAMME OUTCOMES

A: Subject knowledge and understanding This programme provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
A1 The IoT paradigm; what is IoT, what are its specific characteristics and the challenges they pose. **A2** The core and enabling technologies for IoT; wireless access technologies, hardware platforms, how IoT systems interact/communicate with other systems. **A3** State of the art research and latest advances in the field of IoT (both academic and industrial). **A4** IoT-related protocols, algorithms and architectures (existing but also how to develop new ones) **A5** How to design and develop an IoT solution for a specific need / application / problem.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (A1 – A6); • seminars (A1 – A6); • lab sessions (A1 – A6); • directed reading (A1 – A6); • independent research (for dissertation) (A1 – A6).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes):

A6 How can the IoT systems and networks be improved and defended in terms of cyber security	- coursework essays (A1 – A6); - dissertation (A1 – A6).
B: Intellectual skills This programme provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme outcomes:
B1 Think critically, analytically and make decisions to solve real-world problems in the context of IoT with a focus on cyber security. **B2** Formulate, plan, execute and report on an IoT-related project involving original contributions in a structured and disciplined manner. **B3** Critically evaluate and justify alternative approaches to solutions development **B4** Analyse and synthesise information relevant to the development **B5** Select and apply different techniques to synthesise solutions **B6** Effectively conduct research and critical evaluation of different methodologies **B7** Communicate findings to professional and academic standards	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): - lectures (B1- B7); - seminars (B1 – B7); - workshops (B1 – B7); - directed reading (B4 – B6); - use of the VLE (B4 – B6); - independent research (for project) (B1 – B8). Assessment strategies and methods (referring to numbered Intended Learning Outcomes): - coursework essays (B1 – B7); - dissertation (B1 – B7).
C: Practical skills This programme provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
C1 define functional and technical requirements for IoT systems/networks; **C2** feel confident programming, configuring and working with IoT equipment and development frameworks; **C3** select appropriate methodologies, technologies and tools for solving IoT related problems with a focus on cyber security; **C4** conduct strategic analysis with respect to the operation of IoT systems (e.g. risk assessment, develop business cases, etc);	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): - lectures (C1 – C4); - coursework essays (C1 – C4); - independent research for empirical dissertation (C1 – C4); - group exercises (C1 – C4). Assessment strategies and methods (referring to numbered Intended Learning Outcomes): - coursework essays (C1 – C4); - dissertation (C1 – C4).
D: Transferable skills This programme provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to

	demonstrate the programme learning outcomes:
D1 Demonstrate problem solving skills and the application of knowledge across the IoT area; **D2** Gather, select, and analyse a range of data and present professionally using appropriate media; **D3** Distil, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere; **D4** Demonstrate initiative, self-direction and exercise personal responsibility for management of own learning; **D5** Work autonomously and become reflective learners; **D6** Communicate effectively and confidentially to appropriate professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (D1 – D6); • seminars (D1 – D6); • workshops (D1 – D6); • directed reading (D2 – D5); • use of the VLE (D2 – D5); • independent research (for project) (D1 – D6).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (D1 – D6); • dissertation (D1- D6).

7

LEVEL 7/PG Dip INTENDED LEVEL OUTCOMES

A: Subject knowledge and understanding This programme provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
A1 The IoT paradigm; what is IoT, what are its specific characteristics and the challenges they pose. **A2** The core and enabling technologies for IoT; wireless access technologies, hardware platforms, how IoT systems interact/communicate with other systems. **A3** State of the art research and latest advances in the field of IoT (both academic and industrial). **A4** IoT-related protocols, algorithms and architectures (existing but also how to develop new ones) **A5** How to design and develop an IoT solution for a specific need / application / problem. **A6** How can the IoT systems and networks be improved and defended in terms of cyber security.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (A1 – A6); • seminars (A1 – A6); • lab sessions (A1 – A6); • directed reading (A1 – A6);
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (A1 – A6);
B: Intellectual skills This programme provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme outcomes:
B1 Think critically, analytically and make decisions to solve real-world problems in the context of IoT with a focus on cyber security.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):

B2 Formulate, plan, execute and report on an IoT-related project involving original contributions in a structured and disciplined manner. **B3** Critically evaluate and justify alternative approaches to solutions development **B4** Analyse and synthesise information relevant to the development **B5** Select and apply different techniques to synthesise solutions **B6** Communicate findings to professional and academic standards	• lectures (B1- B6); • seminars (B1 – B6); • workshops (B1 – B6); • directed reading (B4 – B6); • use of the VLE (B4 – B6);
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (B1 – B6);
C: Practical skills This programme provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
C1 define functional and technical requirements for IoT systems/networks; **C2** feel confident programming, configuring and working with IoT equipment and development frameworks; **C3** select appropriate methodologies, technologies and tools for solving IoT related problems with a focus on cyber security; **C4** conduct strategic analysis with respect to the operation of IoT systems (e.g. risk assessment, develop business cases, etc);	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (C1 – C4); • coursework essays (C1 – C4); • group exercises (C1 – C4).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (C1 – C4).
D: Transferable skills This programme provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme learning outcomes:
D1 Demonstrate problem solving skills and the application of knowledge across the IoT area; **D2** Gather, select, and analyse a range of data and present professionally using appropriate media; **D3** Distil, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere; **D4** Demonstrate initiative, self-direction and exercise personal responsibility for management of own learning; **D5** Work autonomously and become reflective learners;	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (D1 – D6); • seminars (D1 – D6); • workshops (D1 – D6); • directed reading (D2 – D5); • use of the VLE (D2 – D5);
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (D1 – D6).

D6 Communicate effectively and confidentially to appropriate professional and academic standards.	

LEVEL 7/PG Cert INTENDED LEVEL OUTCOMES

A: Subject knowledge and understanding This programme provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
A1 The IoT paradigm; what is IoT, what are its specific characteristics and the challenges they pose. **A2** IoT-related protocols, algorithms and architectures (existing but also how to develop new ones) **A3** How can the IoT systems and networks be improved and defended in terms of cyber security.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (A1 – A3); • directed reading (A1 – A3);
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (A1 – A3);
B: Intellectual skills This programme provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme outcomes:
B1 Think critically, analytically and make decisions to solve real-world problems in the context of IoT with a focus on cyber security. **B2** Formulate, plan, execute and report on an IoT-related project involving original contributions in a structured and disciplined manner. **B3** Select and apply different techniques to synthesise solutions **B4** Communicate findings to professional and academic standards	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (B1- B4); • directed reading (B2 – B4); • use of the VLE (B4);
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (B1 – B4)
C: Practical skills This programme provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
C1 select appropriate methodologies, technologies and tools for solving IoT related problems;	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (C1 – C2);

C2 conduct strategic analysis with respect to the operation of IoT systems (e.g. risk assessment, develop business cases, etc) with a focus on cyber security;	• coursework essays (C1 – C2). Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (C1 – C4);
D: Transferable skills This programme provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme learning outcomes:
D1 Gather, select, and analyse a range of data and present professionally using appropriate media; **D2** Demonstrate initiative, self-direction and exercise personal responsibility for management of own learning; **D3** Work autonomously and become reflective learners; **D4** Communicate effectively and confidentially to appropriate professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (D1 – D4); • directed reading (D1 – D4); • use of the VLE (D1 – D4); Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (D1 – D6);

ADMISSION REGULATIONS

The regulations for this programme are the University's Standard Postgraduate/ Graduate Diploma/ Graduate Certificate Admission Regulations with the following exceptions: Applicants whose mother tongue is not English must offer evidence of qualifications in written and spoken English. Acceptable qualifications are:
IELTS (academic) 6.0 (with a minimum of 5.5 in each of four categories) or direct equivalent.

https://intranetsp.bournemouth.ac.uk/pandptest/3a-postgraduate-admissions-regulations.pdf

The programme is specifically targeting to recruit students who have either recently graduated, wish to extend their knowledge to Masters level, or would like to prepare themselves to undertake PhD research. When considering applicants, their academic profile and relevant experience, as well as their commitment to study are normally considered.

MSc Internet of Things with Cyber Security is for students who have graduated from a computing-related or STEM degree and want to increase their knowledge and skills before starting work, or have significant experience working in the industry in a closely related field. It addresses the work force skills-gap that is currently present (as of 2018) in the market in the areas of IoT, cyber-physical systems, smart cities/buildings/homes, etc

PROGRESSION ROUTES

Recognition arrangements provide formally approved entry or progression routes through which students are eligible to apply for a place on a programme leading to a BU award. Recognition does not guarantee entry onto the BU receiving programme only eligibility to apply. In some cases, additional entry criteria such as a Merit classification from the feeder programme may also apply. Please see the Recognition Register
(https://intranetsp.bournemouth.ac.uk/pandptest/7J_Recognition_Register_Public.xlsx) for a full list of approved Recognition arrangements and agreed entry criteria.

In order to take advantage of exciting new approaches to learning and teaching, as well as developments in industry, the current, approved Articulation/Recognition/Progression route(s) for this programme may be subject to change. Where this happens students will be informed and supported by the Faculty as early as possible.

ASSESSMENT REGULATIONS

The regulations for this programme are the University's Standard Postgraduate / Graduate Diploma / Graduate Certificate Assessment Regulations. In particular,
For MSc Internet of Things with Cyber Security:
https://intranetsp.bournemouth.ac.uk/pandptest/6a-standard-assessment-regulations-postgraduate.pdf

For PGDip Internet of Things with Cyber Security and PGCert Computing:
https://intranetsp.bournemouth.ac.uk/pandptest/6a-standard-assessment-regulations-gradcert-graddip.pdf

WORK BASED LEARNING (WBL) AND PLACEMENT ELEMENTS

A 30 week placement is optional for students, which normally starts after they have completed all the taught units and the project.

The placement is non-credit bearing and is assessed on a pass/fail basis (i.e. satisfactory completion of 30 weeks). The placement will appear on students' degree transcripts. Students are required to find their own placements. Students must comply with visa requirements. Students will normally have completed all 180 credits before proceeding to the placement but this requirement may be relaxed in the case of students who need to resit an assessment. In such cases, decisions will be made on an individual basis and in the best interests of the student.
Refer to *4K – Placements: Policy and Procedure* for more details.

Programme Skills Matrix

Units		Programme Intended Learning Outcomes																						
		A 1	A 2	A 3	A 4	A 5	A 6	B 1	B 2	B 3	B 4	B 5	B 6	B 7	C 1	C 2	C 3	C 4	D 1	D 2	D 3	D 4	D 5	D 6
STAGE 1 /L7	**Wireless Sensor & Actuator Networks**	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Mobile and Wireless Networks	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Research Methods & Professional Issues					X	X		X	X	X	X	X	X			X	X	X	X	X	X	X	X
	Security and Privacy in IoT	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Human Factors					X	X			X	X	X	X	X			X	X	X	X	X	X	X	X
	Security by Design					X	X			X	X	X	X	X	X		X	X	X	X	X	X	X	X
	Security Information and Event Management					X	X	X		X		X	X	X										
	Cyber Security			X		X	X			X	X	X	X	X			X	X	X	X	X	X	X	X
STG 2 / L7	**Individual Masters Project**	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

A – Subject Knowledge and Understanding
This programme provides opportunities for students to develop and demonstrate knowledge and understanding of:

1. The IoT paradigm; what is IoT, what are its specific characteristics and the challenges they pose.
2. The core and enabling technologies for IoT; wireless access technologies, hardware platforms, how IoT systems interact/communicate with other systems.
3. State of the art research and latest advances in the field of IoT (both academic and industrial).
4. IoT-related protocols, algorithms and architectures (existing but also how to develop new ones)
5. How to design and develop an IoT solution for a specific need / application / problem.
6. How can the IoT systems and networks be improved and defended in terms of cyber security

B – Intellectual Skills
This programme provides opportunities for students to:

1. Think critically, analytically and make decisions to solve real-world problems in the context of IoT with a focus on cyber security.
2. Formulate, plan, execute and report on an IoT-related project involving original contributions in a structured and disciplined manner.
3. Critically evaluate and justify alternative approaches to solutions development
4. Analyse and synthesise information relevant to the development
5. Select and apply different techniques to synthesise solutions
6. Effectively conduct research and critical evaluation of different methodologies
7. Communicate findings to professional and academic standards

C – Subject-specific/Practical Skills
This programme provides opportunities for students to:

1. Define functional and technical requirements for IoT systems/networks;
2. Feel confident programming, configuring and working with IoT equipment and development frameworks;
3. Select appropriate methodologies, technologies and tools for solving IoT related problems with a focus on cyber security;
4. Conduct strategic analysis with respect to the operation of IoT systems (e.g. risk assessment, develop business cases, etc);

D – Transferable Skills
This programme provides opportunities for students to:
1. Demonstrate problem solving skills and the application of knowledge across the IoT area;
2. Gather, select, and analyse a range of data and present professionally using appropriate media;
3. Distil, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere;
4. Demonstrate initiative, self-direction and exercise personal responsibility for management of own learning;
5. Work autonomously and become reflective learners;
6. Communicate effectively and confidentially to appropriate professional and academic standards.